

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

การอนุมัติเอกสาร

| ลงนาม      | ผู้เรียบเรียง/จัดทำโดย                                                            | ผู้ตรวจทาน/ผู้ทบทวน                                                               | ผู้อนุมัติ                                                                          |
|------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| ลายเซ็น    |  |  |  |
| ชื่อ-สกุล  | นางสาวประภัสสร สุรวิตย์                                                           | นายธีระวัฒน์ ศรีละพันธ์                                                           | นายแพทย์ต่อตระกูล ศรีทา                                                             |
| ตำแหน่ง    | นักวิชาการสาธารณสุข                                                               | หัวหน้างานเทคโนโลยีสารสนเทศ<br>(Lead Implementer)                                 | ผู้อำนวยการ โรงพยาบาลน้ำเกลี้ยง<br>(CISO)                                           |
| วันเดือนปี | 16 มีนาคม 2569                                                                    | 20 มีนาคม 2569                                                                    | 23 มีนาคม 2569                                                                      |

ประวัติการแก้ไข

| ครั้งที่ | วันที่ประกาศใช้ | รายละเอียดการแก้ไข                             |
|----------|-----------------|------------------------------------------------|
| 00       | 23 มี.ค. 2569   | จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ. ไซเบอร์ |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

## สารบัญ

|                                                                                                                                                                                                 |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. หลักการและเหตุผล .....                                                                                                                                                                       | 3  |
| 2. วัตถุประสงค์.....                                                                                                                                                                            | 4  |
| 3. ขอบเขต .....                                                                                                                                                                                 | 4  |
| 4. คำจำกัดความ/นิยามศัพท์เฉพาะ .....                                                                                                                                                            | 4  |
| 5. ขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์.....                                                                                                                                                 | 5  |
| 6. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)                                                                                         | 22 |
| 6.1 โครงสร้างทีมบริหารจัดการการรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ผิดพลาด! ไม่ได้กำหนดบัญชีมาร์ก                                                                                |    |
| 6.2 โครงสร้างทีมสนับสนุนการดำเนินการการรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ .....                                                                                                | 25 |
| 6.3 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) .....                                                                                                                            | 33 |
| 7. แผนรับมือเหตุการณ์ทางไซเบอร์ .....                                                                                                                                                           | 34 |
| 7.1 การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Web Defacement) .....                                                                                                                | 34 |
| 7.2 การถูกโจมตีจากโปรแกรมประสงค์ร้ายเข้ารหัสข้อมูลเรียกค่าไถ่ (Ransomware) / การโจมตียึดครองเครื่องแม่ข่าย (Server compromise injection attack) / การบุกรุกโดยใช้มัลแวร์ (Malicious Logic) .... | 36 |
| 7.3 การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) .....                                                                                                                      | 38 |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

|                                   |    |
|-----------------------------------|----|
| 8. การติดตาม ควบคุม และทบทวน..... | 40 |
| ภาคผนวก .....                     | 41 |
| ภาคผนวก ก.....                    | 41 |
| ภาคผนวก ข.....                    | 42 |
| ภาคผนวก ค.....                    | 45 |

#### แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure : CIRP)

อ้างอิง : พรบ ไซเบอร์ (ม. 43, ม. 44, ม. 45, ม. 56, ม. 57, ม. 58) , ประมวลและกรอบ [ข้อ 24.1.1]

### 1. หลักการและเหตุผล

แผนรับมือภัยคุกคามทางไซเบอร์ของโรงพยาบาลน้ำเกลี้ยงฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงาน ควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผน ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติด้านการรักษาความ มั่นคงปลอดภัยระบบสารสนเทศ กระทรวงสาธารณสุข โดยที่แผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้จะใช้เป็น แนวทางในการเตรียมความพร้อมเพื่อป้องกัน รับมือ ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ โดย จะระบุขั้นตอนที่จำเป็นในการตอบสนองต่อภัยคุกคามทางไซเบอร์เพื่อให้หน่วยงานสามารถนำไปประยุกต์ใช้ได้ อย่างมีประสิทธิภาพ โดยจะมีการทบทวนแผนฉบับนี้อย่างน้อยปีละหนึ่งครั้ง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยัง บุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

## 2. วัตถุประสงค์

2.1 เพื่อใช้เป็นแผนรับมือภัยคุกคามทางไซเบอร์ของโรงพยาบาลน้ำเกลี้ยงให้เกิดการดำเนินการอย่างเป็นระบบ มีเอกภาพ มีประสิทธิภาพ และทันต่อเหตุการณ์

2.2 เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้มีการดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องของข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติกรรมแวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์

2.3 เพื่อให้เกิดความร่วมมือระหว่าง หน่วยงานอื่น ๆ ในการรับมือกับภัยคุกคามทางไซเบอร์ รวมทั้งบริหารสถานการณ์ต่าง ๆ ที่เกิดขึ้น เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของโรงพยาบาลน้ำเกลี้ยง

## 3. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของโรงพยาบาลน้ำเกลี้ยงรวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

## 4. คำจำกัดความ/นิยามศัพท์เฉพาะ

| ลำดับ | คำศัพท์                        | คำจำกัดความ                                                                                                                                                                                                                                                    |
|-------|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | การระงับภัยคุกคามทางไซเบอร์    | การดำเนินการเพื่อจำกัดความเสียหายจากภัยคุกคามทางไซเบอร์ที่กำลังเกิดขึ้น กักกันภัยคุกคามไม่ให้แพร่กระจาย และป้องกันไม่ให้ความเสียหายเพิ่มมากขึ้น โดยผู้เผชิญเหตุภัยคุกคามทางไซเบอร์ต้องระมัดระวังไม่ให้หลักฐานทางนิติวิทยาศาสตร์ ถูกทำลายในการดำเนินการดังกล่าว |
| 2     | การปราบปรามภัยคุกคามทางไซเบอร์ | การดำเนินการกำจัดภัยคุกคาม ผู้เผชิญเหตุภัยคุกคามทางไซเบอร์จะต้องลบโปรแกรมหรือสิ่งที่ไม่พึงประสงค์ (Malicious Object) ออกให้หมด และ                                                                                                                             |

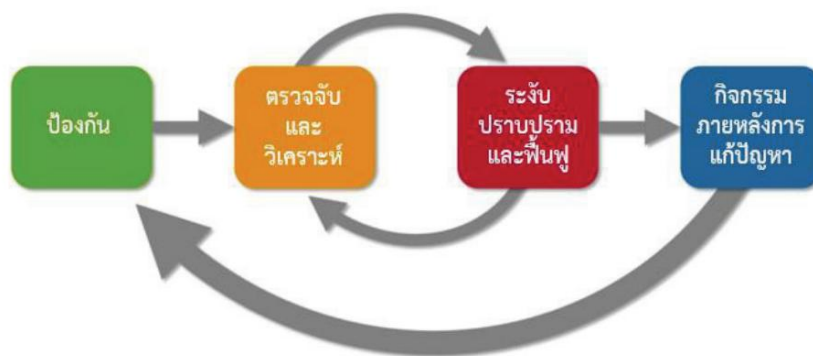
เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับ | คำศัพท์                          | คำจำกัดความ                                                                                                                                                                                                |
|-------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                  | ตรวจสอบระบบที่ได้รับผลกระทบทั้งระบบเพื่อให้มั่นใจถึงความปลอดภัยด้านไซเบอร์ โดยพยายาม ให้ความเสียหายต่อข้อมูลน้อยที่สุด                                                                                     |
| 3     | การฟื้นฟูระบบงานที่ได้รับผลกระทบ | การดำเนินการเพื่อนำระบบให้กลับมาอยู่ในสถานะปกติที่มั่นใจว่าปราศจากการโจมตีที่เป็นภัยคุกคาม ทางไซเบอร์ โดยรวมถึงการเฝ้าระวังและตรวจสอบระบบที่ถูกกู้คืนในระยะแรกของการนำกลับมาใช้งาน เพื่อป้องกันการโจมตีซ้ำ |

## 5. ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์

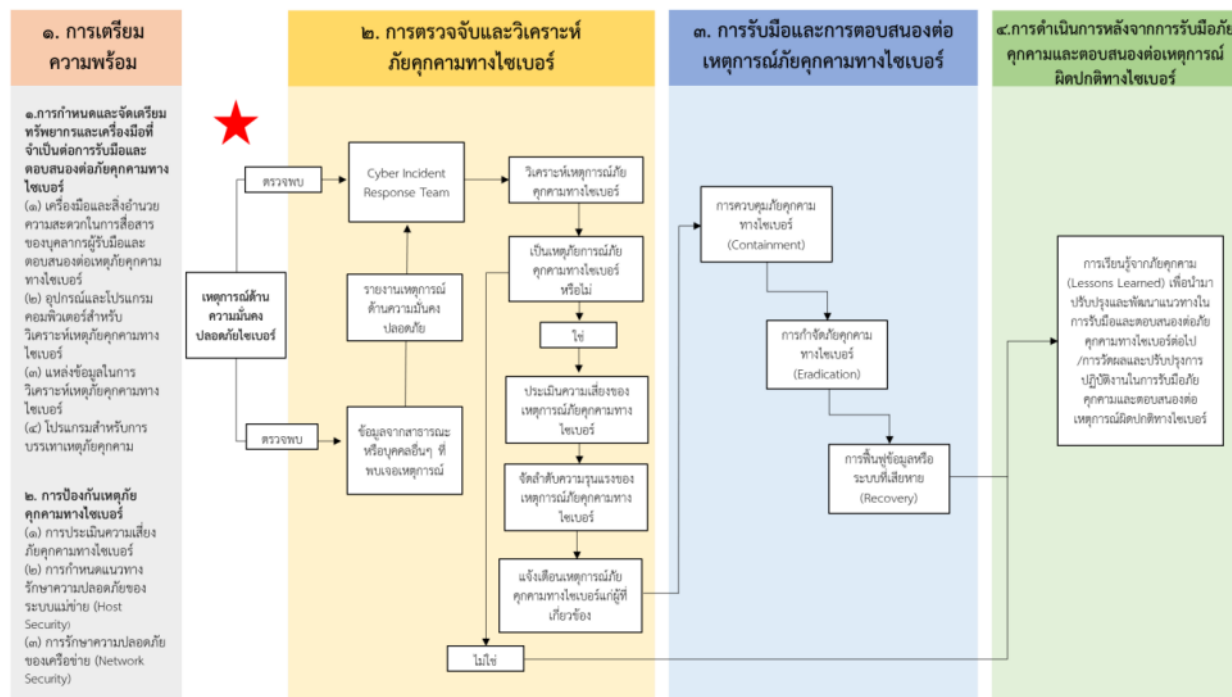
มาตรการป้องกัน รับมือ ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับนั้น มีการดำเนินการมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (incident handling) โดยสามารถแบ่งขั้นตอนการดำเนินการออกได้เป็น 4 ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ตามภาพที่ 1 และภาพที่ 2 ดังนี้



**ภาพที่ 1** แสดงขั้นตอนการดำเนินการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์  
(Incident Handling Cycle)

เอกสารนี้ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |



ภาพที่ 2 แสดงรายละเอียดขั้นตอนการดำเนินการรับมือภัยคุกคามทางไซเบอร์

### ขั้นตอนที่ 1 : การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

การดำเนินการมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยพิจารณาดำเนินการตามรายการรายละเอียดที่ระบุในตารางที่ 2.1

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

## ขั้นตอนที่ 2 : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมไม่ให้เกิดภัยคุกคามทางไซเบอร์ ขึ้นแล้วก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยพิจารณาดำเนินมาตรการ ตามรายละเอียดที่ระบุในตารางที่ 2.2

## ขั้นตอนที่ 3 : การระงับภัยคุกคามทางไซเบอร์ ปรามปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์การปรามปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ 2.3 ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปรามปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

#### องค์ประกอบด้วยการดำเนินการ

- 1) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 2) เรียกใช้งานกระบวนการกู้คืน (Recovery Process) โดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 3) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์ โดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 4) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน ตามโดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 5) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี โดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 6) ดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.3 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

#### ขั้นตอนที่ 4 : การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity) นั้น หน่วยงานควรกำหนดขั้นตอนวิธีปฏิบัติหรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ 2.4 ซึ่งการปฏิบัติตามมาตรการดังกล่าวจะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่อง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

และพัฒนาแนวทางรับมือภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณี ที่ต้องการร้องทุกข์หรือดำเนินคดีเนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตาม ประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง (โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็น ต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไป ในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี)

เมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นตามวรรคหนึ่งแล้ว นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็น รายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอน ที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

## ตารางที่ 2.1 การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation)

| ระดับ                                                                                                                                                                                                                                             | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- กรณีบริการระบบหรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง</li> <li>- กรณีบริการระบบหรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง</li> </ul> | <ol style="list-style-type: none"> <li>1. จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคลหรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใดที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น</li> <li>2. จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์</li> </ol> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ                                                                                    | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| - กรณีบริการระบบหรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ | <p>3. ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับ แนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศดังกล่าว</p> <p>4. จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network diagrams) เป็นต้น</p> <p>5. พิจารณาช่องบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น</p> <p>6. ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่า หรือ การเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan)</p> <p>7. กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการ ที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง</p> <p>8. จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทางการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์ สำหรับ การเข้าถึงระบบต่าง ๆ (cryptography / key managements) เป็นต้น</p> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>9. ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่ายแอปพลิเคชัน หรือระบบงาน ต่าง ๆ</p> <p>10. ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Respond Capability Testing)</p> <p>11. รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence)</p> <p>12. กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์</p> <p>13. ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่า หรือ การเปลี่ยนแปลง ค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไกที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร การแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มีกลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม)</p> <p>14. จัดให้มีการฝึกรอบมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัย คุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว</p> <p>15. สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์</p> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

**ตารางที่ 2.2** การดำเนินการมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

| ระดับ                                                                                                                                                                                                | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| - กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะ เกิดผลกระทบเป็น ภัยคุกคามทางไซเบอร์ ในระดับไม่ ร้ายแรง กรณีบริการ ระบบ หรือ อุปกรณ์ มี แนวโน้มที่ จะเกิด ผลกระทบเป็นภัยคุกคาม ทางไซเบอร์ในระดับร้ายแรง | <ol style="list-style-type: none"> <li>1. จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัย ข้อมูลจากแหล่งข้อมูล ต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคง ปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ เป็นต้น</li> <li>2. จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทาง ไซเบอร์</li> <li>3. จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทาง คอมพิวเตอร์ (Logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัย จากเครื่องมือรักษา ความปลอดภัยด้านไซเบอร์ และการตรวจสอบ ระบบงานที่มีความสำคัญ (Critical Systems) โดยจะต้องจัดให้มีข้อพึง ปฏิบัติที่สูงขึ้นสำหรับทุกระบบงาน ที่มีความสำคัญมากขึ้น</li> <li>4. วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้ งานเครือข่าย และระบบงาน (Profile Networks and Systems) เป็น ต้น เพื่อทำความเข้าใจ พฤติกรรมการใช้งานในช่วงเวลาปกติ (Normal Behaviours) ทางการศึกษา วิจัยและค้นหาความสัมพันธ์ของข้อมูล ในระบบกับสถานการณ์ต่าง ๆ (Event Correlation)</li> </ol> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยัง บุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>5. ทันทีที่พบว่า มี หรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและ รวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ ในการโจมตี, สถานการณ์ของการโจมตี (อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้ สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการ ที่ได้รับผลกระทบ, โฮสต์ เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับ ผลกระทบ ข้อมูล ผู้ใช้ เวลาประทับ ข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และ ข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้อง เก็บ รักษาข้อมูลดังกล่าว (safeguard incident data) ให้มีความปลอดภัย เพื่อใช้ ในกระบวนการทางนิติวิทยาศาสตร์และใช้ เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์</p> <p>6. ระบุมวดยของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตาม เพื่อระบุมวดยของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลง ไปจนกว่าสถานการณ์ ดังกล่าวจะสิ้นสุด โดยอาจพิจารณาจากข้อมูล ตามที่ระบุในข้อ 2 ของภาคผนวก ข แนบท้ายนี้</p> <p>7. จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงาน ของระบบ (functional impact) ผลกระทบต่อ ข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น</p> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ                                                                                           | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                 | <p>8. ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทาง ไซเบอร์รวมถึงจุดอ่อนของระบบที่ถูกโจมตี</p> <p>9. ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทาง ที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูล เพื่อให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ ที่เกิดขึ้น</p> <p>10. รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบภายในระยะเวลาที่ หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแล อาจจะนำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการ พิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ 3 ของ ภาคผนวก ข แนบท้ายนี้ แล้วแต่กรณี</p> |
| - กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบเป็น ภัยคุกคาม ทางไซเบอร์ในระดับวิกฤติ | <p>ให้ดำเนินการตามข้อ 1 ถึงข้อ 2 และดำเนินการมาตรการเพิ่มเติม ดังนี้</p> <ol style="list-style-type: none"> <li>1. จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่า มีภัยคุกคามทางไซเบอร์เกิดขึ้น</li> <li>2. จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจับเก็บและ วิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม)</li> <li>3. จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจลจล</li> </ol>                                                                                                                                                                                           |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>ทางคอมพิวเตอร์ เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบ งานหลักที่สูงผิดปกติ หรือเมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น</p> <p>4. วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูล ในระบบ เพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ</p> |

**ตารางที่ 2.3** การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทาง ไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication and Recovery)

| ระดับ                                                                                             | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| - กรณีบริการระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิดผลกระทบ เป็นภัยคุกคามทางไซเบอร์ในระดับ ไม่ร้ายแรง | <p>1. ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับ ภัยคุกคาม ทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมี หลักเกณฑ์ที่ชัดเจนเพื่อใช้ ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้ แนวทางดังกล่าวรวมถึง</p> <p>1.1 การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชี ของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบ จากเครือข่ายภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้</p> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>ใน กระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนิน คดีแล้ว เป็นต้น</p> <p>1.2 การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือ การตัดสินใจของฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและ ภายนอกหน่วยงาน เป็นต้น</p> <p>1.3 การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด</p> <p>2. ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการ หลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันที หลังจากที่เกิดตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำ ประเภทที่สามารถสูญหายได้ เมื่อปิดอุปกรณ์ (volatile data) การเก็บ ข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะ ของระบบ (system snapshot) หรือ ข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอ สำหรับใช้วิเคราะห์ในเชิงเทคนิค และ เพื่อทางนิติวิทยาศาสตร์และใช้ เป็นพยานหลักฐานในการดำเนินคดี</p> <p>3. ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุ ช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูล ต่าง ๆ เช่น ฐานข้อมูล ภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลาย แหล่ง เป็นต้น</p> <p>4. ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคาม ทางไซเบอร์ และความคืบหน้าในการตอบสนองไปยังบุคคลหรือ</p> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยัง บุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>หน่วยงานที่เกี่ยวข้อง ตลอดจนผู้ที่อาจได้รับผลกระทบ อย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยัง บุคคลหรือหน่วยงานต่าง ๆ โดยเฉพาะ การเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ใน หมวดหมู่ที่ 1, 2, 4, 5 และ 7 ตามที่ระบุในข้อ 1 ของภาคผนวก ข แนบท้ายนี้ ทั้งนี้ ในการแจ้งหรือ รายงานสถานการณ์นั้น หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสม และปลอดภัยและดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่ หน่วยงานควบคุมหรือกำกับดูแลกำหนด หรืออาจเทียบเคียงจากตัวอย่าง ตามที่ระบุในข้อ 3 ของภาคผนวก ข แนบท้ายนี้ แล้วแต่กรณี</p> <p>5. ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัย คุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความ เสี่ยงภัยที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึง เครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้ง ลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพ ในโครงสร้างพื้นฐาน และ ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดย ทันทีหลังจากที่ตรวจ พบ เป็นต้น</p> <p>6. ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถ ใช้งานได้ ตามปกติภายในกรอบระยะเวลาที่กำหนด (Restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (Integrity restoration) การสร้างระบบงานขึ้นใหม่ (Rebuild) การ แทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์</p> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยัง บุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ                                                                                                  | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                        | <p>(install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น</p> <p>7. สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทาง ไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการ ฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคาม ทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น</p> <p>8. สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการ ฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น</p>                     |
| <p>- กรณีบริการระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็นภัยคุกคามทางไซเบอร์ในระดับ ร้ายแรง</p> | <p>ให้หน่วยงานดำเนินการตามข้อ 1 และดำเนินการมาตรการเพิ่มเติม ดังนี้</p> <p>1. หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรอง สำหรับการประมวลผล (Alternate Processing) การจัดเก็บข้อมูล (Storage Site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (Transaction Recovery)</p> <p>2. ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (Supply Chain Coordination) รวมถึงแจ้งไปยังศูนย์ ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ</p> <p>3. ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และ</p> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ                                                                                         | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                               | <p>เนื้อหาที่ต้องรายงาน ลำดับชั้นการรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ (ถ้าหน่วยงาน มีความพร้อม)</p> <p>4. ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติ หน้าที่ตามกฎหมาย</p> <p>5. พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ ในการรับมือหรือสนับสนุนการรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (Automated Incident Handling Processes) (ถ้าหน่วยงานมีความพร้อม)</p> |
| - กรณีบริการระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ | <p>ให้หน่วยงานดำเนินการตามข้อ 1 ถึงข้อ 2 และดำเนินการมาตรการเพิ่มเติม ดังนี้</p> <p>1. ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถ ให้บริการได้ภายในกรอบระยะเวลาที่กำหนด Restore within Time Period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและ เครือข่ายของหน่วยงานทำได้อย่างรวดเร็ว</p>                                                                                                                                                                                                                                                                             |

**หมายเหตุ:** ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นแล้ว แต่หน่วยงานยังไม่สามารถระบุระดับของภัยคุกคามทางไซเบอร์ได้ ซึ่งอาจเกิดจากการที่หน่วยงานยังไม่สามารถรวบรวมรายละเอียดหรือข้อมูลที่จำเป็นเพื่อใช้ในการวิเคราะห์ได้ในช่วงแรก หรือไม่ว่าด้วยเหตุอื่นใดก็ตาม ให้หน่วยงานดำเนินการประเมินผลกระทบเบื้องต้น

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกกระบวนบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

โดยพิจารณาจากตัวอย่างตาม ที่ระบุในข้อ 1 ของภาคผนวก ข แนบท้ายนี้ จนกว่าจะมีข้อมูลหรือปรากฏหลักฐานที่เพียงพอต่อการวิเคราะห์ เพื่อระบุระดับของภัยคุกคามทางไซเบอร์

**ตารางที่ 2.4** การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident Activity)

| ระดับ                                                                                                                                                                                                                                                                                                                                                                         | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็น ภัยคุกคามทาง ไซเบอร์ใน ระดับไม่ร้ายแรง</li> <li>- กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็น ภัยคุกคามทาง ไซเบอร์ใน ระดับร้ายแรง</li> <li>- กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็น ภัยคุกคามทาง ไซเบอร์ใน ระดับวิกฤต</li> </ul> | <p>ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณา ดำเนินการดังนี้</p> <ol style="list-style-type: none"> <li>1. นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็น ภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึง จุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและ กระบวนการ การฝึก บุคลากร การระบุผู้มีอำนาจดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหา แนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัย คุกคามทางไซเบอร์ที่มี ลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงาน ที่เกี่ยวข้อง</li> <li>2. รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทาง ไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของ ภัยคุกคาม ทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคาม</li> </ol> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยัง บุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ระดับ | แนวปฏิบัติพื้นฐาน (Security Control Baselines)                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>ทางไซเบอร์ประเภท ต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแล และรับผิดชอบภายในหน่วยงาน</p> <p>3. ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปรามปราม และระงับภัย คุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน</p> <p>4. เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ตามแนวทางและระยะเวลาการ เก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด</p> |

อนึ่งแนวปฏิบัติพื้นฐาน (Security Control Baselines) ตามรายละเอียดที่กำหนด ไว้ในตารางที่ 2.1 – ตารางที่ 2.4 นี้ เป็นเพียงแนวทางมาตรการเตรียมการและป้องกัน รับมือปรามปราม และ ระงับภัยคุกคามทางไซเบอร์แต่ละระดับได้อย่างมีประสิทธิภาพ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

6. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: Namkiang - CSIRT)

6.1 โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                               | หน้าที่/ตำแหน่ง            | ความรับผิดชอบ                                                                                                                                                                                                        |
|----------|--------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | นายแพทย์ต่อตระกูล ศรีทา<br>ผู้อำนวยการโรงพยาบาลน้ำเกลี้ยง<br>โทร. 090 602 3950 | Executive<br>Sponsor/ CISO | ให้การสนับสนุนเชิงนโยบายและทรัพยากร                                                                                                                                                                                  |
| 2        | นางสาวศิริลักษณ์ สมศิริ<br>นักวิชาการสาธารณสุขปฏิบัติการ<br>โทร 097 018 3720   | CSIRT Manager              | กำกับดูแลการดำเนินงาน, ประสานงานกับผู้บริหาร และหน่วยงานภายนอก                                                                                                                                                       |
| 3        | นายธีระวัฒน์ ศรีละพันธ์<br>นักวิชาการคอมพิวเตอร์ปฏิบัติการ<br>โทร 094 290 2511 | Incident lead              | เฝ้าระวังระบบไซเบอร์และสารสนเทศ เครือข่ายและระบบบริหารจัดการโรงพยาบาล (HIS-Hospital Information System), ประเมินระดับความร้ายแรงและผลกระทบของเหตุการณ์, รายงานความคืบหน้าให้ CSIRT Manager และประสานงานกับ ทีมงานที่ |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                          | หน้าที่/ตำแหน่ง  | ความรับผิดชอบ                                                                                                                                                                                                                                             |
|----------|---------------------------------------------------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          |                                                                           |                  | เกี่ยวข้อง เพื่อแก้ไขปัญหาที่เกิดขึ้น                                                                                                                                                                                                                     |
| 4        | นายธนวัฒน์ หล้าแหล่ง<br>เจ้าพนักงานเครื่องคอมพิวเตอร์<br>โทร 090 040 5833 | Incident Handler | เฝ้าระวังระบบไซเบอร์และสารสนเทศ เครือข่ายและระบบบริหารจัดการโรงพยาบาล (HIS-Hospital Information System), ประเมินระดับความร้ายแรงและผลกระทบของเหตุการณ์, รายงานความคืบหน้าให้ CSIRT Manager และประสานงานกับ ทีมงานที่เกี่ยวข้อง เพื่อแก้ไขปัญหาที่เกิดขึ้น |
| 5        | นางสาว ประภัสสร สุรวีทย์<br>นักวิชาการสาธารณสุข<br>โทร 085 768 1867       | Incident Handler | เฝ้าระวังระบบไซเบอร์และสารสนเทศ เครือข่ายและระบบบริหารจัดการโรงพยาบาล (HIS-Hospital Information System), ประเมินระดับ                                                                                                                                     |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                        | หน้าที่/ตำแหน่ง  | ความรับผิดชอบ                                                                                                                                                                                                                                             |
|----------|-------------------------------------------------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          |                                                                         |                  | ความร้ายแรงและผลกระทบของเหตุการณ์, รายงานความคืบหน้าให้ CSIRT Manager และประสานงานกับ ทีมงานที่เกี่ยวข้อง เพื่อแก้ไขปัญหาที่เกิดขึ้น                                                                                                                      |
| 6        | นางสาวสวัสดิ์ แสงสันต์<br>พยาบาลวิชาชีพชำนาญการพิเศษ<br>โทร 045 605 055 | Incident Handler | เฝ้าระวังระบบไซเบอร์และสารสนเทศ เครือข่ายและระบบบริหารจัดการโรงพยาบาล (HIS-Hospital Information System), ประเมินระดับความร้ายแรงและผลกระทบของเหตุการณ์, รายงานความคืบหน้าให้ CSIRT Manager และประสานงานกับ ทีมงานที่เกี่ยวข้อง เพื่อแก้ไขปัญหาที่เกิดขึ้น |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

## 6.2 โครงสร้างทีมสนับสนุนการดำเนินการรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (ทีมสนับสนุน)

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                                                                                                                                                                                                                                                   | หน้าที่          | ความรับผิดชอบ                                                                                                                                                                                                                                                                          |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | นางสาวศิริลักษณ์ สมศิริ<br>นักวิชาการสาธารณสุขปฏิบัติการ<br>โทร 097 018 3702                                                                                                                                                                                                                       | HIS              | 1. กำกับดูแลและประสานงานด้านการใช้งานระบบแอปพลิเคชันหลัก<br>2. ตรวจสอบความถูกต้องครบถ้วน และปลอดภัยของข้อมูลทางคลินิก                                                                                                                                                                  |
| 2.       | 1. นายธีระวัฒน์ ศรีละพันธ์<br>นักวิชาการคอมพิวเตอร์ปฏิบัติการ<br>โทร 094 290 2511<br>(Lead Implementer)<br>2. นายธนวัฒน์ หล้าแหล่ง<br>เจ้าพนักงานเครื่องคอมพิวเตอร์<br>โทร 090 040 5833<br>(Implementer)<br>3. นางสาวประภัสสร สุรวีทย์<br>นักวิชาการสาธารณสุข<br>โทร 085 768 1867<br>(Implementer) | Implementer Team | 1. วางแผนและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามกฎหมาย พรบไซเบอร์<br>2. จัดทำและดูแลให้มีการปฏิบัติ นโยบาย ระเบียบปฏิบัติ ขั้นตอนการทำงาน และบันทึกต่าง ๆ พร้อมประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อให้มาตรการความมั่นคงปลอดภัยไซเบอร์ถูกนำไปปฏิบัติได้จริง |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                                                                                                                                | หน้าที่      | ความรับผิดชอบ                                                                                                                                                                                                                          |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          |                                                                                                                                                                                 |              | 3.บริหารจัดการความเสี่ยงสารสนเทศทางด้านไซเบอร์และข้อมูลสารสนเทศ<br>4.จัดทำรายงานผลการดำเนินงานและข้อเสนอแนะในการปรับปรุงระบบความมั่นคงปลอดภัยไซเบอร์<br>5.ติดตามและสนับสนุนการปรับปรุงกระบวนการอย่างต่อเนื่อง (Continuous Improvement) |
| 3.       | 1.นางสาวสวัสดี แสงสันต์<br>พยาบาลวิชาชีพชำนาญการพิเศษ<br>(Lead Auditor)<br>โทร 045 605 055<br>2.นางวิรดา พิมพ์ทอง<br>พยาบาลวิชาชีพชำนาญการพิเศษ<br>(Auditor)<br>โทร 045 605 055 | Auditor Team | 1.วางแผนและดำเนินการตรวจสอบภายในด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศขององค์กร<br>2.ประเมินความสอดคล้องของระบบบริหารจัดการกับมาตรฐาน พรบ ไซเบอร์,                                                                              |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                                                                                                                              | หน้าที่   | ความรับผิดชอบ                                                                                                                                                                                                                                                                                                           |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | 3.นางสาวศิริลักษณ์ สมศิริ<br>นักวิชาการสาธารณสุขปฏิบัติการ<br>(Auditor)<br>โทร 097 018 3702<br>4.นางสาวเอี่ยมพร สังฆะพงษ์<br>เจ้าพนักงานเวชสถิติ (Auditor)<br>โทร 045 605 055 |           | ISO/IEC 27001, PDPA<br>และกฎหมาย/ข้อบังคับที่เกี่ยวข้อง<br>3.ตรวจสอบการปฏิบัติตามนโยบายและมาตรการความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศของทุกหน่วยงาน<br>4.จัดทำรายงานผลการตรวจสอบ พร้อมข้อเสนอแนะเพื่อการแก้ไขปรับปรุง<br>5.ติดตามผลการแก้ไขข้อบกพร่อง (Follow-up Audit) เพื่อให้มั่นใจว่ามีการปรับปรุงอย่างแท้จริง |
| 4.       | 1.นางสาวกรรณิกา ทองเกลียว<br>นายแพทย์ชำนาญการ<br>โทร 045 605 055<br>2.นางสาวสวัสดิ์ แสงสันต์<br>พยาบาลวิชาชีพชำนาญการพิเศษ                                                    | Risk Team | 1.วางแผนและดำเนินการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์                                                                                                                                                                                                                                                        |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                                                                                                                                                                                                                                                                                     | หน้าที่ | ความรับผิดชอบ                                                                                                                                                                                                                                                                                                                                                                |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | โทร 045 605 055<br>3.นางวิรดา พิมพ์ทอง<br>พยาบาลวิชาชีพชำนาญการพิเศษ<br>โทร 045 605 055<br>4.นางสาววรรณวรรณ วิเศษหมื่น<br>พยาบาลวิชาชีพชำนาญการพิเศษ<br>โทร 045 605 055<br>5.นางสาววลัยพร ทิพย์รักษา<br>พยาบาลวิชาชีพชำนาญการ<br>โทร 045 605 055<br>6.นายธีระวัฒน์ ศรีละพันธ์<br>นักวิชาการคอมพิวเตอร์ปฏิบัติการ<br>โทร 094 290 2511 |         | เบอร์และข้อมูลสารสนเทศ<br>ขององค์กร<br>2.ติดตามและประเมิน<br>ความเสี่ยงใหม่ ๆ ที่อาจ<br>เกิดขึ้นจากกระบวนการ<br>ทำงานและการใช้<br>เทคโนโลยี<br>3.เสนอแนะแนวทางการ<br>ป้องกัน แก้ไข และลด<br>ผลกระทบจากความเสี่ยงที่<br>พบ<br>4.จัดทำรายงานความเสี่ยง<br>และเสนอผู้บริหารเพื่อการ<br>ตัดสินใจ<br>5.สนับสนุนการสร้าง<br>วัฒนธรรมองค์กรที่<br>ตระหนักถึงการบริหาร<br>ความเสี่ยง |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารในส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                                                                                                                                                                                                                                                                                                                                     | หน้าที่              | ความรับผิดชอบ                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.       | 1.นายแพทย์ต่อตระกูล ศรีทา<br>ผู้อำนวยการโรงพยาบาลน้ำเกลี้ยง<br>โทร 090 602 3950<br>2.นางสาวสวัสดิ์ แสงสันต์<br>พยาบาลวิชาชีพชำนาญการพิเศษ<br>3.นายธีระวัฒน์ ศรีละพันธ์<br>นักวิชาการคอมพิวเตอร์ปฏิบัติการ<br>โทร 094 290 2511<br>4.นายธนวัฒน์ หล้าแหล่ง<br>โทร 090 040 5833<br>เจ้าพนักงานเครื่องคอมพิวเตอร์<br>5.นางสาวประภัสสร สุรวิทย์<br>นักวิชาการสาธารณสุข<br>โทร 085 768 1867 | Crisis Communication | 1.จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์<br>2.ตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต<br>3.ดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันทั่วถึงและมีประสิทธิภาพในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่ |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารในส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                                                                                                                                                                                                                                                                      | หน้าที่                             | ความรับผิดชอบ                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          |                                                                                                                                                                                                                                                                                                                       |                                     | เกี่ยวกับความมั่นคง<br>ปลอดภัยไซเบอร์<br>4.ประสานงานกับบุคลากร<br>ในองค์กรและภายนอก<br>รวมถึงตรวจสอบประเด็น<br>ทางกฎหมายและ PDPA                                                                                                                                                                                                                                                               |
| 6.       | 1.นายธีระวัฒน์ ศรีละพันธ์<br>นักวิชาการคอมพิวเตอร์ปฏิบัติการ<br>โทร 094 290 2511<br>2.นายธนวัฒน์ หล้าแหล่ง<br>เจ้าพนักงานเครื่องคอมพิวเตอร์<br>โทร 090 040 5833<br>3.นางสาวอิศราภรณ์ ชูเลิศ<br>นักวิชาการพัสดุ<br>โทร 045 605 055<br>นางสาวสุภาพร พรหมธร<br>เจ้าพนักงานการเงินและบัญชีชำนาญ<br>งาน<br>โทร 045 605 055 | BCP – Business Continuity Plan Team | 1.จัดทำแผนความต่อเนื่อง<br>ทางธุรกิจ (Business Continuity Plan : BCP)<br>เพื่อให้แน่ใจว่าบริการที่<br>สำคัญขององค์กรสามารถ<br>ให้บริการที่จำเป็นต่อไปได้<br>ในกรณีที่เกิดการหยุดชะงัก<br>2.ต้องมีการสอบทานแผน<br>ของผู้ให้บริการภายนอกเพื่อ<br>พิจารณาความสอดคล้องกับ<br>แผนของหน่วยงานของ<br>องค์กร เช่น ความสอดคล้อง<br>กันของขอบเขตค่านิยามและ<br>การกำหนดระยะเวลาที่<br>สำคัญ เช่น Maximum |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                        | หน้าที่ | ความรับผิดชอบ                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------|-------------------------------------------------------------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | นางสาวสวัสดิ์ แสงสันต์<br>พยาบาลวิชาชีพชำนาญการพิเศษ<br>โทร 045 605 055 |         | <p>Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น</p> <p>3.จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด</p> <p>4.มีการตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ (หนึ่ง) ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์</p> |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ                                | หน้าที่                       | ความรับผิดชอบ                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|-----------------------------------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.       | นายพนมมิตร ย้อยสร้อยสุด<br>ทันตแพทย์ชำนาญการ<br>โทร 045 605 055 | DPO - Data Protection Officer | 1.ให้คำแนะนำทั้งกับผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล รวมถึงลูกจ้างหรือผู้รับจ้างที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล<br>2.ตรวจสอบการดำเนินการขององค์กร เพื่อให้แน่ใจว่าการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามข้อกำหนดของกฎหมาย PDPA<br>3.เมื่อเกิดปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ข้อมูลรั่วไหล , DPO จะต้องทำหน้าที่ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส) |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                             |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                                  | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                               | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของ<br>เอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ลำดับที่ | ชื่อ นามสกุล รายละเอียดการติดต่อ | หน้าที่ | ความรับผิดชอบ                                                                                                                                                                                                                             |
|----------|----------------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          |                                  |         | 4.ต้องรักษาข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มา<br>ในระหว่างการปฏิบัติหน้าที่ให้เป็นไปความลับ<br>5.ต้องมีบทบาทในการสร้างความเข้าใจและการตระหนักรู้เรื่อง PDPA<br>ให้แก่พนักงานในองค์กร เพื่อให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง |

### 6.3 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ตามแผนฉบับนี้ เป็นการกำหนดตามประมวลและแนวทางปฏิบัติฯ ว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีโครงสร้างการรายงานและ Flow การรายงาน ตามภาคผนวก ก

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้เป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

## 7. แผนรับมือเหตุการณ์ทางไซเบอร์

### 7.1 การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Web Defacement)

| ข้อ | รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ                                                                                                                                                                                                                                                                                                                                                                                                                                                             | ผู้รับผิดชอบ |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 1   | ติดต่อประสานงานผู้ที่เกี่ยวข้อง<br>ทีมสนับสนุนดำเนินการแจ้งเหตุการณ์ถูกโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Web Defacement) ไปยังทีมบริหาร เพื่อแนะนำและพิจารณาอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ และติดต่อประสานไปผู้ที่เกี่ยวข้อง                                                                                                                                                                                                                                        | ทีม CSIRT    |
| 2   | ทีมบริหารให้คำแนะนำและอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์                                                                                                                                                                                                                                                                                                                                                                                                                                  | ทีมบริหาร    |
| 3   | ดำเนินการจัดการเชื่อมต่อของระบบ                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ทีม CSIRT    |
| 4   | ทีมสนับสนุนเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์ เช่น<br><ul style="list-style-type: none"> <li>- การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อทำการปิดอุปกรณ์ (Volatile data)</li> <li>- การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs)</li> <li>- ข้อมูลสถานะของระบบ (system snapshot)</li> <li>- ข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และ เพื่อทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี</li> </ul> | ทีม CSIRT    |
| 5   | ทีมสนับสนุนดำเนินการวิเคราะห์ ดังนี้<br><ul style="list-style-type: none"> <li>- เพื่อระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น</li> </ul> ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง                                                                                                                                                                 | ทีมสนับสนุน  |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ข้อ | รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ                                                                                                                                                                                                                                                                                                                                                                                                                           | ผู้รับผิดชอบ |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
|     | - ตรวจสอบช่องโหว่ที่ทำให้เกิดเหตุการณ์ถูกโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Web Defacement)                                                                                                                                                                                                                                                                                                                                                         |              |
| 6   | <b>ทีมสนับสนุนดำเนินการตั้งค่าระบบให้มีความมั่นคงปลอดภัย ดังนี้</b> <ul style="list-style-type: none"> <li>- การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่ายจากเซ่น อุปกรณ์ Firewall อุปกรณ์เครือข่าย เป็นต้น</li> <li>- การติดตั้งหรือ Update Anti-Virus หรือ IDS/IPS</li> <li>- การเปลี่ยนแปลงทางกายภาพโครงสร้างพื้นฐาน</li> <li>- ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ</li> </ul>                                                      | ทีมสนับสนุน  |
| 7   | <b>ทีมสนับสนุนดำเนินการกู้คืนระบบโดยพิจารณา วิธีการตามความเหมาะสมได้ ดังนี้</b> <ul style="list-style-type: none"> <li>- การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration)</li> <li>- การสร้างระบบงานขึ้นใหม่ (rebuild)</li> <li>- การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace)</li> <li>- การติดตั้งโปรแกรมคอมพิวเตอร์ (install)</li> <li>- การเปลี่ยนแปลงรหัสผ่านของเครื่อง Web Server</li> <li>- การปรับปรุงหรือ Update ระบบปฏิบัติการ (OS)</li> </ul> | ทีมสนับสนุน  |
| 8   | <b>ทีมสนับสนุนกำหนดการเฝ้าระวังในการถูกโจมตีซ้ำ</b>                                                                                                                                                                                                                                                                                                                                                                                                                  | ทีมสนับสนุน  |
| 9   | <b>ทีมสนับสนุนตรวจสอบข้อมูลและการทำงานของระบบ เพื่อกลับมาใช้งานได้อย่างปกติ</b>                                                                                                                                                                                                                                                                                                                                                                                      | ทีมสนับสนุน  |
| 10  | <b>ติดต่อประสานงานผู้ที่เกี่ยวข้อง</b><br>ทีมสนับสนุนแจ้งผลการดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ไปยังทีมบริหารและผู้ที่ส่วนเกี่ยวข้องรับทราบว่า Web Site กลับมาใช้งานได้ปกติ                                                                                                                                                                                                                                                                                   | ทีมสนับสนุน  |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

**7.2 การถูกโจมตีจากโปรแกรมประสงค์ร้ายเข้ารหัสข้อมูลเรียกค่าไถ่ (Ransomware) / การโจมตียึดเครื่องแม่ข่าย (Server compromise injection attack) / การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)**

| ข้อ | รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ผู้รับผิดชอบ |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 1   | ติดต่อประสานงานผู้ที่เกี่ยวข้อง<br>ทีมสนับสนุนดำเนินการแจ้งเหตุการณ์ถูกโจมตีจากโปรแกรมประสงค์ร้ายเข้ารหัสข้อมูลเรียกค่าไถ่ (Ransomware) ไปยังทีมบริหาร เพื่อแนะนำและพิจารณาอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ และติดต่อประสานไปผู้ที่เกี่ยวข้อง                                                                                                                                                                                                                                                 | ทีม CSIRT    |
| 2   | ทีมบริหารให้คำแนะนำและอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์                                                                                                                                                                                                                                                                                                                                                                                                                                        | ทีมบริหาร    |
| 3   | ดำเนินการตัดการเชื่อมต่อของระบบ                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | ทีมสนับสนุน  |
| 4   | ทีมสนับสนุนเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อกำเนิดภัยคุกคามทางไซเบอร์ เช่น<br><ul style="list-style-type: none"> <li>- การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อทำการปิดอุปกรณ์ (Volatile data)</li> <li>- การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs)</li> <li>- ข้อมูลสถานะของระบบ (system snapshot)</li> <li>- ข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และ เพื่อทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี</li> </ul> | ทีมสนับสนุน  |
| 5   | ทีมสนับสนุนดำเนินการวิเคราะห์ ดังนี้                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | ทีมสนับสนุน  |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ข้อ | รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ                                                                                                                                                                                                                                                                                                                                                                                                                       | ผู้รับผิดชอบ |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
|     | <ul style="list-style-type: none"> <li>- เพื่อระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น</li> <li>ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง</li> <li>- ตรวจสอบช่องโหว่ที่ทำให้เกิดเหตุการณ์ถูกโจมตี</li> </ul>                                                                                                  |              |
| 6   | <b>ทีมสนับสนุนดำเนินการตั้งค่าระบบให้มีความมั่นคงปลอดภัย ดังนี้</b> <ul style="list-style-type: none"> <li>- การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่ายจากเซ่น อุปกรณ์ Firewall อุปกรณ์เครือข่าย เป็นต้น</li> <li>- การติดตั้งหรือ Update Anti-Virus หรือ IDS/IPS</li> <li>- การเปลี่ยนแปลงทางกายภาพโครงสร้างพื้นฐาน</li> <li>- ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ</li> </ul>                                                  | ทีมสนับสนุน  |
| 7   | <b>ทีมสนับสนุนดำเนินการกู้คืนระบบโดยพิจารณา วิธีการตามความเหมาะสมได้ ดังนี้</b> <ul style="list-style-type: none"> <li>- การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration)</li> <li>- การสร้างระบบงานขึ้นใหม่ (rebuild)</li> <li>- การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace)</li> <li>- การติดตั้งโปรแกรมคอมพิวเตอร์ (install)</li> <li>- การเปลี่ยนแปลงรหัสผ่านของเครื่องแม่ข่าย</li> <li>- การปรับปรุงหรือ Update ระบบปฏิบัติการ (OS)</li> </ul> | ทีมสนับสนุน  |
| 8   | <b>ทีมสนับสนุนกำหนดการเฝ้าระวังในการถูกโจมตีซ้ำ</b>                                                                                                                                                                                                                                                                                                                                                                                                              | ทีมสนับสนุน  |
| 9   | <b>ทีมสนับสนุนตรวจสอบข้อมูลและการใช้งานของระบบ เพื่อกลับมาใช้งานได้อย่างปกติ</b>                                                                                                                                                                                                                                                                                                                                                                                 | ทีมสนับสนุน  |
| 10  | <b>ติดต่อประสานงานผู้ที่เกี่ยวข้อง</b>                                                                                                                                                                                                                                                                                                                                                                                                                           | ทีมสนับสนุน  |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ข้อ | รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ                                                                                                | ผู้รับผิดชอบ |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------|--------------|
|     | ทีมสนับสนุนแจ้งผลการดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ไปยังทีมบริหารและผู้ที่ส่วนเกี่ยวข้องรับทราบว่าจะระบบกลับมาใช้งานได้อย่างปกติ |              |

### 7.3 การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)

| ข้อ | รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ                                                                                                                                                                                                                                                                                                                                                                                                                                                             | ผู้รับผิดชอบ |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 1   | ติดต่อประสานงานผู้ที่เกี่ยวข้อง<br>ทีมสนับสนุนดำเนินการแจ้งเหตุการณ์การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) ไปยังทีมบริหาร เพื่อแนะนำและพิจารณาอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ และติดต่อประสานไปผู้ที่เกี่ยวข้อง                                                                                                                                                                                                                                              | ทีมสนับสนุน  |
| 2   | ทีมบริหารให้คำแนะนำและอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์                                                                                                                                                                                                                                                                                                                                                                                                                                  | ทีมบริหาร    |
| 3   | ทีมสนับสนุนประสานผู้ให้บริการภายนอกเพื่อปิดกั้นการบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)                                                                                                                                                                                                                                                                                                                                                                                        | ทีมสนับสนุน  |
| 4   | ทีมสนับสนุนเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์ เช่น<br><ul style="list-style-type: none"> <li>- การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อทำการปิดอุปกรณ์ (Volatile data)</li> <li>- การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs)</li> <li>- ข้อมูลสถานะของระบบ (system snapshot)</li> <li>- ข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และ เพื่อทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี</li> </ul> | ทีมสนับสนุน  |
| 5   | ทีมสนับสนุนดำเนินการวิเคราะห์ ดังนี้                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ทีมสนับสนุน  |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| ข้อ | รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ                                                                                                                                                                                                                                                                                                                                                                      | ผู้รับผิดชอบ |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
|     | <ul style="list-style-type: none"> <li>- เพื่อระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง</li> <li>- ตรวจสอบช่องโหว่ที่ทำให้เกิดเหตุการณ์การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</li> </ul>  |              |
| 6   | <b>ทีมสนับสนุนดำเนินการตั้งค่าระบบให้มีความมั่นคงปลอดภัย ดังนี้</b> <ul style="list-style-type: none"> <li>- การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่ายจากเซ่น อุปกรณ์ Firewall อุปกรณ์เครือข่าย เป็นต้น</li> <li>- การติดตั้งหรือ Update Anti-Virus หรือ IDS/IPS</li> <li>- การเปลี่ยนแปลงทางกายภาพโครงสร้างพื้นฐาน</li> <li>- ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ</li> </ul> | ทีมสนับสนุน  |
| 7   | <b>ทีมสนับสนุนกำหนดการเฝ้าระวังในการถูกโจมตีซ้ำ</b>                                                                                                                                                                                                                                                                                                                                                             | ทีมสนับสนุน  |
| 8   | <b>ทีมสนับสนุนตรวจสอบข้อมูลและการใช้งานของระบบ เพื่อกลับมาใช้งานได้ปกติ</b>                                                                                                                                                                                                                                                                                                                                     | ทีมสนับสนุน  |
| 9   | <b>ติดต่อประสานงานผู้ที่เกี่ยวข้อง</b><br>ทีมสนับสนุนแจ้งผลการดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ไปยังทีมบริหารและผู้ที่ส่วนเกี่ยวข้องรับทราบว่ารระบบในการให้บริการกลับมาใช้งานได้ปกติ                                                                                                                                                                                                                     | ทีมสนับสนุน  |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

## 8. การติดตาม ควบคุม และทบทวน

แผนการรับมือภัยคุกคามฉบับนี้ จะต้องมีการติดตาม ควบคุม และทบทวน ดังนี้

- 1) ต้องติดตามและควบคุมให้แผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ได้มีการสื่อสารไปยังบุคลากรที่เกี่ยวข้องทั้งหมดอย่างมีประสิทธิภาพ เพื่อสนับสนุนบริการสำคัญของสำนักงานปลัดกระทรวงสาธารณสุข
- 2) ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ อย่างน้อยปีละ 1 ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ
- 3) ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของสำนักงานปลัดกระทรวงสาธารณสุข หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

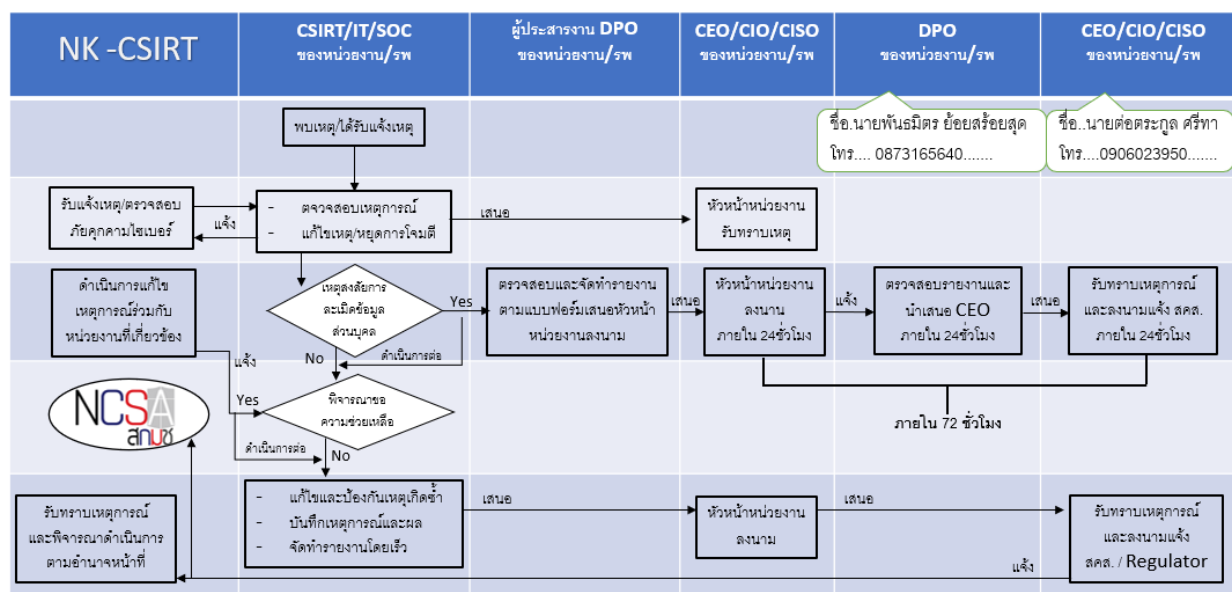
เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

ภาคผนวก

ภาคผนวก ก

### โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) และ Flow การรายงาน



เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

## ภาคผนวก ข

### ข้อ 1 การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

| หมวดหมู่ | คำอธิบาย                                                                                        |
|----------|-------------------------------------------------------------------------------------------------|
| 1        | เหตุการณ์จำลองและการฝึกซ้อมของหน่วยงานเอง (Training and Exercises)                              |
| 2        | การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)                                |
| 3        | การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)                                |
| 4        | การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)         |
| 5        | การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)                                                     |
| 6        | การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)                                                |
| 7        | การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)                                            |
| 8        | การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)                                |
| 9        | เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)                                       |
| 10       | เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly) |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

## ข้อ 2 ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

| ประเภทอุปกรณ์เครือข่าย                                      | หมวดหมู่ภัยคุกคาม |                |                |                |                |                |         |
|-------------------------------------------------------------|-------------------|----------------|----------------|----------------|----------------|----------------|---------|
|                                                             | 1                 | 2              | 3              | 4              | 5              | 6              | 7       |
| Backbone                                                    | ไม่<br>ร้ายแรง    | ไม่<br>ร้ายแรง | ไม่<br>ร้ายแรง | ไม่<br>ร้ายแรง | วิกฤต          | วิกฤต          | วิกฤต   |
| เราเตอร์                                                    | ไม่<br>ร้ายแรง    | ไม่<br>ร้ายแรง | ร้ายแรง        | ไม่<br>ร้ายแรง | วิกฤต          | วิกฤต          | วิกฤต   |
| เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือ ดูแลความปลอดภัย | ไม่<br>ร้ายแรง    | ไม่<br>ร้ายแรง | ร้ายแรง        | ร้ายแรง        | วิกฤต          | วิกฤต          | วิกฤต   |
| เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ                  | ไม่<br>ร้ายแรง    | ไม่<br>ร้ายแรง | ร้ายแรง        | ร้ายแรง        | วิกฤต          | ร้ายแรง        | ร้ายแรง |
| เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ                    | ไม่<br>ร้ายแรง    | ไม่<br>ร้ายแรง | ไม่<br>ร้ายแรง | ร้ายแรง        | ไม่<br>ร้ายแรง | ไม่<br>ร้ายแรง | ร้ายแรง |
| เครื่องเวิร์กสเตชัน                                         | ไม่<br>ร้ายแรง    | ไม่<br>ร้ายแรง | ไม่<br>ร้ายแรง | ร้ายแรง        | ไม่<br>ร้ายแรง | ไม่<br>ร้ายแรง | ร้ายแรง |

## ข้อ 3 ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

การแจ้งหรือรายงานภัยคุกคามตามหมวดนี้เกิดขึ้นเมื่อผู้เผชิญเหตุยังไม่ทราบรายละเอียดภัยคุกคาม และกำลังดำเนินการวิเคราะห์เหตุการณ์ (เช่น อาจอยู่ในช่วงแรก ๆ ที่พบการกระทำผิด) โดยหากทราบผลของการ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

สอบสวนแล้ว ผู้รายงานควรเปลี่ยนเป็นหมวดอื่นให้ถูกต้อง และ ในรายงานสรุปปิดเหตุการณ์ ไม่ควรมีภัยคุกคามที่อยู่ในหมวดนี้ เนื่องจากการวิเคราะห์สอบสวนเสร็จสิ้นแล้ว)

| หมวดหมู่ภัยคุกคามทางไซเบอร์ | ระดับภัยคุกคามทางไซเบอร์ | การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา) | การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา) | การส่งรายงานให้สำนักงาน (ภายในเวลา) |
|-----------------------------|--------------------------|------------------------------------------------|--------------------------------------------------------|-------------------------------------|
| 1                           | ทุกเหตุการณ์             | 30 นาที                                        | 2 ชั่วโมง                                              | 4 ชั่วโมง                           |
| 2                           | ทุกเหตุการณ์             | ตามหน่วยงานกำหนด                               | ตามหน่วยงานกำหนด                                       | ตามหน่วยงานกำหนด                    |
| 3                           | ทุกเหตุการณ์             | 30 นาที                                        | 2 ชั่วโมง                                              | 8 ชั่วโมง                           |
| 4                           | วิกฤต                    | 10 นาที                                        | 30 นาที                                                | 1 ชั่วโมง                           |
|                             | ร้ายแรง                  | 20 นาที                                        | 1 ชั่วโมง                                              | 2 ชั่วโมง                           |
|                             | ไม่ร้ายแรง               | ตามหน่วยงานกำหนด                               | ตามหน่วยงานกำหนด                                       | ตามหน่วยงานกำหนด                    |
| 5                           | วิกฤต                    | 10 นาที                                        | 30 นาที                                                | 1 ชั่วโมง                           |
|                             | ร้ายแรง                  | 20 นาที                                        | 1 ชั่วโมง                                              | 2 ชั่วโมง                           |
|                             | ไม่ร้ายแรง               | 30 นาที                                        | 2 ชั่วโมง                                              | 4 ชั่วโมง                           |
| 6                           | วิกฤต                    | 10 นาที                                        | 30 นาที                                                | 1 ชั่วโมง                           |
|                             | ร้ายแรง                  | 20 นาที                                        | 1 ชั่วโมง                                              | 2 ชั่วโมง                           |
|                             | ไม่ร้ายแรง               | 30 นาที                                        | 2 ชั่วโมง                                              | 4 ชั่วโมง                           |
| 7                           | วิกฤต                    | 10 นาที                                        | 30 นาที                                                | 1 ชั่วโมง                           |
|                             | ร้ายแรง                  | 30 นาที                                        | 1 ชั่วโมง                                              | 1 ชั่วโมง                           |
|                             | ไม่ร้ายแรง               | ตามหน่วยงานกำหนด                               | ตามหน่วยงานกำหนด                                       | ตามหน่วยงานกำหนด                    |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้เป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

| หมวดหมู่ภัยคุกคามทางไซเบอร์ | ระดับภัยคุกคามทางไซเบอร์ | การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา) | การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา) | การส่งรายงานให้สำนักงาน (ภายในเวลา) |
|-----------------------------|--------------------------|------------------------------------------------|--------------------------------------------------------|-------------------------------------|
| 8                           | -                        | 20 นาที                                        | ตามเวลาที่ต้องใช้ในการสืบสวน                           | 4 ชั่วโมง                           |
| 9                           | -                        | -                                              | 4 ชั่วโมง                                              | 12 ชั่วโมง                          |

#### ภาคผนวก ค

**ข้อ 1 วิธีการ/ขั้นตอนจำกัดขอบเขตหรือควบคุมความเสียหาย (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาเลือกใช้ที่เหมาะสม ดังนี้**

- 1) ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- 2) แยกระบบที่ได้รับผลกระทบออกจากเครือข่ายหลักเพื่อป้องกันการแพร่กระจายไปยังระบบอื่น
- 3) หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- 4) Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Black hole/ Sandbox/ Honeypot
- 5) ประเมินความเสียหายและระบุว่ามียังมีระบบใดที่เกี่ยวข้อง
- 6) ดำเนินการแก้ไขเบื้องต้น เช่น การปิดพอร์ตที่ถูกโจมตีหรือการบล็อก IP ที่มีพฤติกรรมไม่พึงประสงค์
- 7) เก็บข้อมูลสำคัญจากระบบที่ได้รับผลกระทบเพื่อใช้ในการกระบวนการสอบสวน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการ/ขั้นตอนใดที่จะจำกัดขอบเขตหรือควบคุมความเสียหาย ขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

**ข้อ 2 การจัดเก็บและดูแลรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน**

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทางกฎหมาย ดังนั้น การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณาตามหลักการ/ขั้นตอน ที่เหมาะสม ดังนี้

- 1) ดำเนินการให้เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวข้องกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ได้ในพื้นที่
- 2) บันทึกการเข้าถึงและการกระทำใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม
- 3) บันทึกรายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
  - 3.1) ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น
  - 3.2) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident
  - 3.3) สถานที่จัดเก็บหลักฐาน
- 4) บันทึกข้อมูลจากระบบที่ได้รับผลกระทบ เช่น ล็อกไฟล์ การจับภาพหน้าจอ และอุปกรณ์เครือข่ายที่เกี่ยวข้อง
- 5) จัดเก็บอุปกรณ์ที่มีหลักฐานไว้ในที่ปลอดภัยเพื่อป้องกันการดัดแปลง เช่น จัดเก็บในตู้ที่มีการล็อก และการควบคุมการเข้าถึง
- 6) ทำรายการหลักฐานทั้งหมดที่ถูกเก็บรวบรวม พร้อมระบุวันที่และเวลาที่รับหลักฐาน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

ทั้งนี้ให้พิจารณาดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญตามขั้นตอน ดังนี้

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Assessment        | การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลังรับมือ และตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น                                                                                                                                                                                                                                                                                                                                                                                         |
| 2. Acquisition       | ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้<br>1. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker<br>2. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น<br>3. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด<br>4. ต้องทำการบันทึกหลักฐาน (Chain of Custody) |
| 3. Authentication    | ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับ ด้วยวิธี Cryptographic Hash เช่น MD5, SHA1, SHA256                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 4. Analysis & Report | วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิด Incident                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 5. Archive           | จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย                                                                                                                                                                                                                                                                                                                                                                                                   |

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

### ข้อ 3 การจัดการสาเหตุ

เมื่อมีการจำกัดขอบเขต/การควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเรียบร้อยแล้วข้อมูลทั้งหมดจะต้องนำกลับมาวิเคราะห์ตามหลักการในขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ จนกว่าจะสามารถจัดการสาเหตุที่ทำให้เกิด Incident และจัดการช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามาในโจมตีระบบทั้งหมดได้เรียบร้อยแล้ว ซึ่งการจัดการสาเหตุที่ทำให้เกิด Incident และผลกระทบ พิจารณาดำเนินการ ดังนี้

- 1) ปิดช่องโหว่ของระบบ
- 2) ยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- 3) แจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- 4) ลบโปรแกรมประเภท Backdoor ออกจากระบบ
- 5) ใช้ข้อมูล Indicator of Compromise (IoC) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการจัดการให้ออกจากระบบทั้งหมด

### ข้อ 4 การสอบสวน (Investigation)

- 1) เก็บหลักฐานทางดิจิทัลจากระบบที่ได้รับผลกระทบ เช่น ไฟล์ล็อก การจับภาพหน้าจอ การตรวจสอบ ข้อมูลเครือข่าย
- 2) วิเคราะห์สาเหตุของเหตุการณ์ เช่น ตรวจสอบวิธีการที่ผู้โจมตีใช้ในการเข้าถึงระบบ
- 3) ระบุผู้ที่อาจรับผิดชอบต่อเหตุการณ์ เช่น การระบุที่อยู่ IP หรือการตรวจสอบพฤติกรรมที่ผิดปกติ
- 4) จัดทำรายงานการสอบสวนและเสนอแนวทางการป้องกันเพื่อไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

#### ข้อ 5 การกู้คืนระบบให้กลับมาทำงานปกติ

หลังจากจำกัดขอบเขต/การควบคุมความเสียหาย จัดการสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการกู้คืนระบบ/การฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ ซึ่งจะต้องจัดเตรียมข้อมูลสำหรับกู้คืนระบบไว้ก่อน โดยพิจารณาดำเนินการ ดังนี้

- 1) ตรวจสอบและซ่อมแซมระบบที่ได้รับผลกระทบเพื่อให้แน่ใจว่าไม่มีช่องโหว่ที่ยังไม่ได้รับการแก้ไข
- 2) ฟื้นฟูระบบโดยการกู้คืนข้อมูลจากระบบสำรองล่าสุด (Backup)
- 3) Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- 4) Restore ข้อมูลกลับเข้าสู่ระบบจาก Back Up Storage
- 5) ทดสอบระบบทั้งหมดเพื่อยืนยันว่าระบบปลอดภัยและสามารถทำงานได้ปกติ
- 6) ตรวจสอบการทำงานของระบบสำรองเพื่อให้แน่ใจว่าข้อมูลที่กู้คืนครบถ้วน

#### ข้อ 6 การมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก

การมีส่วนร่วมกับหน่วยงานภายนอกองค์กร (Information Sharing) ควรกำหนดขั้นตอนการสื่อสารและประเภทข้อมูล ที่สามารถนำไปแบ่งปันได้กับบุคคลภายนอก ทั้งหน่วยงานบังคับใช้กฎหมาย หน่วยงานกำกับดูแลองค์กรอื่น หรือการติดต่อเพื่อขอความช่วยเหลือจากผู้เชี่ยวชาญจากภายนอกองค์กรที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ อาทิ Thai CERT หรือ CERT ของ Sector อื่น ๆ เป็นต้น เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทาง ไซเบอร์เพื่อช่วยให้การป้องกันและตอบสนองต่อภัยคุกคามได้เร็วยิ่งขึ้น โดยพิจารณาดำเนินการ ดังนี้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

|                                                                                   |                                                                                                   |                                         |                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                   | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                   | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

- 1) ติดต่อบุคคลภายนอกตามความจำเป็น
- 2) ประสานงานกับหน่วยงานบังคับใช้กฎหมาย หากมีความจำเป็นในการดำเนินคดี
- 3) ส่งมอบหลักฐานที่เกี่ยวข้องให้กับผู้เชี่ยวชาญภายนอก พร้อมรายการหลักฐานทั้งหมดเพื่อใช้ในการตรวจสอบ

#### ข้อ 7 กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process)

- 1) ประเมินผลการดำเนินการ เช่น ความเร็วในการตอบสนอง การกู้คืนระบบ และการจำกัดขอบเขตเหตุการณ์
- 2) ระบุข้อบกพร่องและข้อเสนอแนะสำหรับการปรับปรุงกระบวนการตอบสนอง
- 3) เสนอมาตรการปรับปรุงแผนรับมือภัยคุกคาม เพื่อให้มีประสิทธิภาพมากขึ้นในการป้องกันเหตุการณ์ในอนาคต

#### ข้อ 8 การสื่อสารและการทบทวนแผน (Communication and Plan Review)

- 1) สื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ให้กับบุคลากรที่เกี่ยวข้องทั้งหมดผ่านการอบรมและเอกสารที่เกี่ยวข้อง
- 2) จัดอบรมพนักงานอย่างสม่ำเสมอเกี่ยวกับการตอบสนองต่อเหตุการณ์ฉุกเฉิน
- 3) ทบทวนแผนการรับมือภัยคุกคามทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในสภาพแวดล้อมทางไซเบอร์
- 4) ปรับปรุงแผนตามผลการทบทวนและการฝึกซ้อมแผนรับมือภัยคุกคาม

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



|                                                                                   |                                                                                                       |                                         |                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------|
|  | <b>แผนการรับมือภัยคุกคามทางไซเบอร์</b><br><br><b>(Cybersecurity Incident Response Plan Procedure)</b> | รหัสเอกสาร                              | NK MOPH<br>IR Plan -01            |
|                                                                                   |                                                                                                       | แก้ไขครั้งที่                           | 00                                |
|                                                                                   |                                                                                                       | วันที่บังคับใช้<br>ชั้นความลับของเอกสาร | 23 มี.ค. 2569<br>ใช้ภายในเท่านั้น |

### การทบทวนแผนการรับมือภัยคุกคาม

แผนการรับมือภัยคุกคาม นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพ และถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

### เอกสารอ้างอิง

1. โครงสร้างทีมรับมือภัยคุกคามทางไซเบอร์
2. รายงานสรุปเหตุการณ์
3. แผนการรับมือภัยคุกคามทางไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลน้ำเกลี้ยง ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลน้ำเกลี้ยง เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

# เอกสารแนบท้ายประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

## เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

### ว่าด้วยข้อมูลที่ต้องแจ้งและแบบการรายงานภัยคุกคามทางไซเบอร์

#### บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ และให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นั้น

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานการดำเนินการตามที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ จึงกำหนดให้หน่วยงานดังกล่าวจัดทำรายงานเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานตามรายการที่กำหนดไว้ในแนบท้ายนี้ ผ่านการส่งทางอีเมล โทรสาร หรือด้วยวิธีการทางอิเล็กทรอนิกส์อื่นใดที่มีความปลอดภัย เช่น การส่งรายงานที่เข้ารหัสด้วย PGP มาทางอีเมล (เป็นอย่างน้อย)

เนื่องด้วยการส่งรายงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ทันการณ์ เป็นเรื่องที่สำคัญ ในกรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศยังไม่สามารถแจ้งข้อมูลตามแบบรายงานได้อย่างครบถ้วนภายในระยะเวลา ๒๔ ชั่วโมง ให้หน่วยงานดังกล่าวจัดส่งรายงานด้วยข้อมูลเท่าที่มี และเมื่อมีความคืบหน้าหรือมีข้อมูลเพิ่มเติมในการดำเนินการรับมือ ให้แจ้งต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นระยะ และรีบจัดทำและส่งรายงานที่สมบูรณ์ให้แก่สำนักงาน โดยเร็ว ทั้งนี้ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศพิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายการรักษาความลับของหน่วยงาน

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่สามารถดำเนินการจัดเตรียมข้อมูลในรายงานได้ด้วยเหตุผลบางประการ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งหน่วยงานควบคุมหรือกำกับดูแลของตนและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ทราบ โดยเร็ว

<sup>๑</sup> การรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต้องรายงานภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

<sup>๒</sup> มาตรา ๗๓ กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกิน ๒๐๐,๐๐๐ บาท

ทั้งนี้ เพื่อให้หน่วยงานของรัฐ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานเหตุภัยคุกคามทางไซเบอร์ กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของหน่วยงานของรัฐ จึงให้นำหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวข้างต้น มาบังคับใช้แก่หน่วยงานของรัฐโดยอนุโลม

## เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

| ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                    |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-----------|----------|---------------|------------------------------------------------------------------|---------------|------------------------------------------------------------------------------------|---------------|------------------------------------------|---------------|--------------------------------------------------|---------------|------------------------------------------------------|---------------|------------------------------------------------------------------|---------------|-----------------------------------------------------------|
| <b>๑. ข้อมูลการประสานงาน</b><br>ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม<br>วันที่และเวลาที่แจ้ง                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                    |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| <b>๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม</b><br>ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม<br>ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                    |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| <b>๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม</b><br><div style="display: flex; justify-content: space-between;"> <span>ชื่อ-นามสกุล</span> <span>ตำแหน่งงาน</span> </div> <div style="display: flex; justify-content: space-between;"> <span>ชื่อหน่วยงาน</span> <span>อีเมล</span> </div> <span>โทรศัพท์ (ที่ทำงาน / มือถือ)</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                    |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| <b>๔. ความต่อเนื่องของเหตุภัยคุกคาม</b><br><div style="display: flex; justify-content: space-around;"> <input type="checkbox"/> เหตุภัยคุกคามใหม่                         <input type="checkbox"/> การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม                     </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                    |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| <b>๕. ลักษณะภัยคุกคามทางไซเบอร์</b><br>ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่<br>เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ <sup>๑</sup> ในระดับใด (มาตรา ๖๐)<br><div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="checkbox"/> ไม่ร้ายแรง                         <input type="checkbox"/> ร้ายแรง                         <input type="checkbox"/> วิฤต (ก)                         <input type="checkbox"/> วิฤต (ข)                     </div> <input type="checkbox"/> ยังไม่สามารถระบุได้                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                    |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| <b>๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)</b> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 15%;">หมวดหมู่*</th> <th>คำอธิบาย</th> </tr> </thead> <tbody> <tr> <td>หมวดหมู่ที่ ๒</td> <td>การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)</td> </tr> <tr> <td>หมวดหมู่ที่ ๓</td> <td>การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)</td> </tr> <tr> <td>หมวดหมู่ที่ ๔</td> <td>การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)</td> </tr> <tr> <td>หมวดหมู่ที่ ๕</td> <td>การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)</td> </tr> <tr> <td>หมวดหมู่ที่ ๖</td> <td>การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)</td> </tr> <tr> <td>หมวดหมู่ที่ ๗</td> <td>การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</td> </tr> <tr> <td>หมวดหมู่ที่ ๘</td> <td>เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)</td> </tr> </tbody> </table> |                                                                                    | หมวดหมู่* | คำอธิบาย | หมวดหมู่ที่ ๒ | การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) | หมวดหมู่ที่ ๓ | การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity) | หมวดหมู่ที่ ๔ | การบุกรุกโดยใช้มัลแวร์ (Malicious Logic) | หมวดหมู่ที่ ๕ | การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) | หมวดหมู่ที่ ๖ | การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) | หมวดหมู่ที่ ๗ | การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) | หมวดหมู่ที่ ๘ | เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating) |
| หมวดหมู่*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | คำอธิบาย                                                                           |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| หมวดหมู่ที่ ๒                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)                   |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| หมวดหมู่ที่ ๓                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity) |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| หมวดหมู่ที่ ๔                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)                                           |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| หมวดหมู่ที่ ๕                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)                                   |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| หมวดหมู่ที่ ๖                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)                               |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| หมวดหมู่ที่ ๗                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)                   |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |
| หมวดหมู่ที่ ๘                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)                          |           |          |               |                                                                  |               |                                                                                    |               |                                          |               |                                                  |               |                                                      |               |                                                                  |               |                                                           |

<sup>๑</sup> พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

\* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ส่วนที่ ๑</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น</b>                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ</p> <p>หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ</p> <p>วันที่: เลือกวันที่ เวลา: โปรดระบุ</p>                                                                                                                                                                                                                                                                                                       |
| <p><b>ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม</b></p> <p>ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ</p> <p>ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ</p>                                                                                                                                                                                                                                                           |
| <p><b>ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม</b></p> <p>ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ</p> <p>ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ</p> <p>โทรศัพท์ (ที่ทำงาน / มือถือ): โปรดระบุ</p>                                                                                                                                                                                                                                                            |
| <p><b>ก๓. ความต่อเนื่องของเหตุภัยคุกคาม</b></p> <p><input type="checkbox"/> เหตุภัยคุกคามใหม่ <input type="checkbox"/> การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม</p>                                                                                                                                                                                                                                                                                                    |
| <p><b>ก๔. ลักษณะภัยคุกคามทางไซเบอร์</b></p> <p>ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน</p> <p><input type="checkbox"/> ใช่ <input type="checkbox"/> ไม่ใช่</p> <p>เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์<sup>๒</sup> ในระดับใด (มาตรา ๖๐)</p> <p><input type="checkbox"/> ไม่ร้ายแรง <input type="checkbox"/> ร้ายแรง <input type="checkbox"/> วิฤต (ก) <input type="checkbox"/> วิฤต (ข)</p> <p><input type="checkbox"/> ยังไม่สามารถระบุได้</p> |

<sup>๒</sup> พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง





| หมวด ค: ข้อมูลการรับมือภัยคุกคาม                                                      |                                                                    |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| <b>ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)</b>              |                                                                    |
| <input type="checkbox"/> เพิ่งพบเหตุการณ์                                             | <input type="checkbox"/> อยู่ในขั้นตอนการขอความช่วยเหลือ           |
| <input type="checkbox"/> อยู่ในขั้นตอนการสอบสวน                                       | <input type="checkbox"/> กำลังลุกลาม                               |
| <input type="checkbox"/> อยู่ในขั้นตอนการระงับภัย                                     | <input type="checkbox"/> สามารถระงับภัยได้แล้ว                     |
| <input type="checkbox"/> รายงานปิดเหตุการณ์ภัยคุกคามแล้ว                              | <input type="checkbox"/> อื่น ๆ: โปรดระบุ                          |
| <b>ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว</b>                                      |                                                                    |
| <input type="checkbox"/> ยังไม่ได้ดำเนินการแก้ไขใด ๆ                                  | <input type="checkbox"/> ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว |
| <input type="checkbox"/> ตรวจสอบข้อมูลจราจร (Log) แล้ว                                | <input type="checkbox"/> ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว  |
| <input type="checkbox"/> กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว |                                                                    |
| <input type="checkbox"/> รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ    |                                                                    |
| <b>ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)</b>                                 |                                                                    |
| โปรดระบุ                                                                              |                                                                    |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| ส่วนที่ ๒                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |
| หมวด ง : รายละเอียดภัยคุกคาม                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |
| <b>ง๑. ข้อมูลการตรวจจับและการวิเคราะห์</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |
| <b>ง๑.๑ วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access)</b><br><div style="display: flex; justify-content: space-between; margin-top: 5px;"> <span>วันที่: <input type="text"/></span> <span>เวลา: <input type="text"/></span> <span>ไม่ทราบ: <input type="checkbox"/></span> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
| <b>ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์</b><br><div style="margin-top: 5px;"> <p>รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การฉ้อโกง, ความผิดพลาดจากคนนอกองค์กร):</p> <p><input type="text"/></p> <p>บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):</p> <p><input type="text"/></p> <p>รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):</p> <p><input type="text"/></p> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  |
| <b>ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)</b><br><div style="margin-top: 5px;"> <p>จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): <input type="text"/></p> <p>ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: <input type="text"/></p> <p>จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): <input type="text"/></p> <p>มูลค่าความเสียหาย (โดยประมาณ): <input type="text"/></p> <p>ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):</p> <p>จำนวนบุคคลที่เป็นเจ้าของข้อมูล : <input type="text"/></p> <p>ชนิดของข้อมูล (เลือกทุกข้อที่ใช้):</p> <div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;"><input type="checkbox"/> ข้อมูลไปโอเมตริกซ์</div> <div style="width: 50%;"><input type="checkbox"/> ข้อมูลการติดต่อ</div> <div style="width: 50%;"><input type="checkbox"/> ข้อมูลการเงิน</div> <div style="width: 50%;"><input type="checkbox"/> ข้อมูลบุคลากรของรัฐ</div> <div style="width: 50%;"><input type="checkbox"/> หมายเลขบัตรประชาชน</div> <div style="width: 50%;"><input type="checkbox"/> ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ</div> <div style="width: 50%;"><input type="checkbox"/> ข้อมูลทางการแพทย์</div> <div style="width: 50%;"><input type="checkbox"/> อื่น ๆ : <input type="text"/></div> </div> <p>จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: <input type="text"/></p> <p>ผลกระทบอื่น ๆ ที่เกิดขึ้น: <input type="text"/></p> </div> |  |

**ง๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)**

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้โจมตี: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อโจมตีขยายผลไปยังระบบหรือเครื่องอื่น:

โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

- |                                                                                                                  |                                                                                       |
|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <input type="checkbox"/> ระบบล่ม                                                                                 | <input type="checkbox"/> รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ                    |
| <input type="checkbox"/> บัญชีผู้ใช้ถูกสร้างขึ้นใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ               |                                                                                       |
| <input type="checkbox"/> การโจมตีด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ                |                                                                                       |
| <input type="checkbox"/> ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)        |                                                                                       |
| <input type="checkbox"/> การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ                 |                                                                                       |
| <input type="checkbox"/> การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ                                          |                                                                                       |
| <input type="checkbox"/> การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย    |                                                                                       |
| <input type="checkbox"/> การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง |                                                                                       |
| <input type="checkbox"/> การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก                                               |                                                                                       |
| <input type="checkbox"/> การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย                      |                                                                                       |
| <input type="checkbox"/> รูปแบบการใช้งานที่ผิดปกติ                                                               | <input type="checkbox"/> การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ                    |
| <input type="checkbox"/> ความพยายามที่จะเขียนไฟล์ของระบบ                                                         | <input type="checkbox"/> การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ               |
| <input type="checkbox"/> การแก้ไขหรือลบข้อมูลที่ผิดปกติ                                                          | <input type="checkbox"/> การโจมตีให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)             |
| <input type="checkbox"/> ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ                                                    | <input type="checkbox"/> การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ไม่ปกติ                |
| <input type="checkbox"/> การแก้ไขหน้าเว็บ                                                                        | <input type="checkbox"/> การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น |
| <input type="checkbox"/> การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ                       |                                                                                       |
| <input type="checkbox"/> การตรวจพบโปรแกรมเจาะระบบ (Crack utility)                                                |                                                                                       |
| <input type="checkbox"/> สิ่งผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ                                                    |                                                                                       |

**ง๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การโจมตีครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการโจมตี, Attack vector, เทคนิคหรือเครื่องมือที่ผู้โจมตีใช้ ฯลฯ)**

โปรดระบุ

**ง๑.๖ รายละเอียดอื่น ๆ ที่เกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ**

**ง๒. ข้อมูลการระงับ ปรามปราม และฟื้นฟู**

**ง๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ**

**ง๒.๒ การคาดการณ์ความสามารถฟื้นฟู**

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

**ง๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)**

**ง๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ**

**ง๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ**

ง๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรรระบุ

|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใช้นอก</b>                                                                                              | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่ 1 ของ 10</b>        |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |                                              |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------------------------------|--|
| <b>เลขที่.....(ส่วนหน่วยงานผู้แจ้ง/รับแจ้ง)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  | <b>วันที่แจ้ง/รับแจ้ง.....</b>               |  |
| <p>แบบฟอร์มฉบับนี้ใช้สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขอความกรุณาอย่ากรอกข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลในแบบฟอร์มฉบับนี้ เช่น ห้ามใส่ชื่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หาก สสจ/สป.สธ. และ สคส. ต้องการข้อมูลดังกล่าว จะทำการติดต่อท่านไปในภายหลัง</p> <p>หน่วยงานควรตรวจสอบให้แน่ใจว่าข้อมูลที่ให้นั้นถูกต้องที่สุดและมีรายละเอียดครบถ้วนมากที่สุดเกี่ยวกับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</p> <p>กรุณาตอบคำถามต่อไปนี้เพื่อช่วยให้ สสจ/สป.สธ. และ สคส. ดำเนินการเกี่ยวกับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของท่านอย่างมีประสิทธิภาพและเพื่อทำความเข้าใจหน่วยงานของท่านได้ดียิ่งขึ้น</p> |  |                                              |  |
| <b>ส่วนที่ 1 ผู้แจ้ง/ผู้รับแจ้งเหตุการณ์</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |                                              |  |
| ชื่อ-นามสกุล: .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  | ตำแหน่ง: .....                               |  |
| หน่วยงาน: .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |                                              |  |
| เบอร์โทร: .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  | เบอร์โทรสาร: .....                           |  |
| อีเมล : ..... หน่วยงาน/ผู้ประสานงานสำหรับติดต่อ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |                                              |  |
| ที่อยู่เพื่อการติดต่อ .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |                                              |  |
| <b>ส่วนที่ 2 รายละเอียดเหตุการณ์</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |                                              |  |
| วันที่พบเหตุการณ์ละเมิด : .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  | เวลาที่พบเหตุการณ์ละเมิด : ..... นาฬิกา      |  |
| วันที่เกิดเหตุการณ์ละเมิดขึ้น : .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  | เวลาที่เกิดเหตุการณ์ละเมิดขึ้น: ..... นาฬิกา |  |
| กิจกรรม/ระบบที่เกิดเหตุ : .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |                                              |  |
| รายละเอียดเหตุการณ์ :                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |                                              |  |
| (1) กรุณาอธิบายเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น<br>.....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |                                              |  |
| (2) กรุณาอธิบายว่าเหตุการณ์ละเมิดข้อมูลส่วนบุคคลเกิดขึ้นได้อย่างไร<br>.....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |                                              |  |
| (3) หน่วยงานพบเหตุการณ์ละเมิดข้อมูลส่วนบุคคลได้อย่างไร เช่น พบเหตุจากกระบวนการตรวจสอบภายใน<br>.....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |                                              |  |
| (4) หน่วยงานมีมาตรการป้องกันอะไรบ้าง                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |                                              |  |

หมายเหตุ : เอกสารนี้ถูกควบคุมในระดับ [ลับมาก] เมื่อข้อมูลถูกกรอกลงในแบบฟอร์ม

|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใ้ภายนอก</b>                                                                                            | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่2ของ10</b>           |

(5) ประเภทของการละเมิด

☐ รูปแบบเอกสาร      ☐ รูปแบบอิเล็กทรอนิกส์      ☐ ระบบงาน

(6) เหตุการณ์ละเมิดข้อมูลส่วนบุคคลเกิดจากสาเหตุทางไซเบอร์หรือไม่

☐ ใช่                      ☐ ไม่ใช่                      ☐ ไม่ทราบ

**ส่วนที่ 3 ผลกระทบ** (ทำเครื่องหมายทุกข้อที่เกี่ยวข้อง ได้มากกว่า 1 ข้อ)

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ประเภทของ<br>ข้อมูลที่ถูกละเมิด: | <input type="checkbox"/> ข้อมูลเจ้าหน้าที่และผู้บริหาร<br><input type="checkbox"/> ข้อมูลผู้มารับบริการ เช่น ผู้ป่วย ผู้มาติดต่อ<br><input type="checkbox"/> ข้อมูลผู้สมัครงาน<br><input type="checkbox"/> ข้อมูลผู้เข้าร่วมฝึกอบรมภายในหน่วยงาน<br><input type="checkbox"/> ที่ปรึกษา และบุคคลที่เกี่ยวข้อง<br><input type="checkbox"/> ลูกจ้างตามสัญญาจ้าง หรือผู้ทำงาน หรือปฏิบัติงาน<br><input type="checkbox"/> กรรมการ และผู้บริหาร<br><input type="checkbox"/> ข้อมูลอื่นๆ (ระบุ).....<br><input type="checkbox"/> ข้อมูลอื่นๆ (ระบุ).....<br><input type="checkbox"/> ไม่สามารถระบุได้ในขณะนี้ |
| ข้อมูลที่ถูกละเมิด:              | <b>ข้อมูลส่วนบุคคลทั่วไป</b><br><input type="checkbox"/> ข้อมูลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อีเมล วันเดือนปีเกิด การศึกษา ข้อมูลติดต่อ Username Password เป็นต้น<br><input type="checkbox"/> ประวัติการทำงาน เช่น สถานะวิชาชีพ ตำแหน่งงาน ผลการประเมินผลการปฏิบัติงาน<br><input type="checkbox"/> ข้อมูลเอกสารราชการ บัตรประจำตัวประชาชน หนังสือเดินทาง ใบขับขี่ บัตรข้าราชการ<br><input type="checkbox"/> ข้อมูลด้านการเงิน เช่น ธุรกรรมทางการเงิน ข้อมูลภาษี เลขที่บัญชี หมายเลขบัตรเครดิต<br><input type="checkbox"/> ข้อมูลภาพวิถีทัศน์กล้องวงจรปิด                            |

หมายเหตุ : เอกสารนี้ถูกควบคุมในระดับ [ลับมาก] เมื่อข้อมูลถูกกรอกลงในแบบฟอร์ม

|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใช้นายนอก</b>                                                                                           | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่3ของ10</b>           |

|                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                           | <input type="checkbox"/> ข้อมูลที่เกี่ยวข้องกับบุคคล เช่น IP address บทสนทนา และการสื่อสารทางโทรศัพท์ หรืออุปกรณ์อิเล็กทรอนิกส์<br><input type="checkbox"/> ข้อมูลอื่นๆ (โปรดระบุ) .....<br><input type="checkbox"/> ไม่สามารถระบุได้ในขณะนี้<br><b>ข้อมูลส่วนบุคคลที่มีความอ่อนไหว</b><br><input type="checkbox"/> ข้อมูลเกี่ยวกับเชื้อชาติ<br><input type="checkbox"/> ข้อมูลเกี่ยวกับศาสนา<br><input type="checkbox"/> ข้อมูลด้านความคิดเห็นทางการเมือง<br><input type="checkbox"/> ประวัติอาชญากรรม<br><input type="checkbox"/> ข้อมูลสุขภาพ/สุขภาพจิต<br><input type="checkbox"/> ข้อมูลสภาพแรงงาน<br><input type="checkbox"/> ข้อมูลพันธุกรรม<br><input type="checkbox"/> ข้อมูลเกี่ยวกับชีวิตทางด้านเพศ<br><input type="checkbox"/> ข้อมูลเกี่ยวกับบรรณนิยมทางเพศ<br><input type="checkbox"/> ข้อมูลการแปลงเพศ<br><input type="checkbox"/> ข้อมูลตำแหน่ง เช่น พิกัด<br><input type="checkbox"/> ข้อมูลชีวมิติ (อาทิ ภาพสแกนใบหน้า/ม่านตา ลายนิ้วมือ फिल्मเอกซเรย์ เสียง)<br><input type="checkbox"/> ข้อมูลอื่นๆ (โปรดระบุ).....<br><input type="checkbox"/> ไม่สามารถระบุได้ในขณะนี้ |
| ปริมาณของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ                                           | <input type="checkbox"/> โดยประมาณจำนวน.....คน/record<br><input type="checkbox"/> ไม่สามารถระบุจำนวนได้ในขณะนี้                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ลักษณะเหตุการณ์ละเมิด<br>อาจส่งผลกระทบต่อสิทธิ<br>และเสรีภาพของเจ้าของ<br>ข้อมูลส่วนบุคคล | <input type="checkbox"/> กลุ่มของข้อมูลที่มีความเฉพาะข้อมูลที่เป็นความลับหรือข้อมูลที่มีความเสี่ยงสูง เมื่อเกิดเหตุละเมิด เช่น ข้อมูลทางการเงิน ประวัติสุขภาพ เป็นต้น<br><input type="checkbox"/> จำนวนความหลากหลายของข้อมูลส่วนบุคคล เช่นกลุ่มของข้อมูลที่รั่วไหล ประกอบด้วย ชื่อ ที่อยู่ อาชีพ ประวัติการศึกษา อายุ<br><input type="checkbox"/> ความยากง่ายในการระบุถึงตัวบุคคล เช่น ข้อมูลที่ถูกละเมิดไม่ได้เป็น ข้อมูลแฝง หรือเป็นข้อมูลที่เข้ารหัส                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

หมายเหตุ : เอกสารนี้ถูกควบคุมในระดับ [ลับมาก] เมื่อข้อมูลถูกกรอกลงในแบบฟอร์ม

|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใช้นายนอก</b>                                                                                           | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่4ของ10</b>           |

|                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                   | <input type="checkbox"/> ข้อมูลส่วนบุคคลของผู้ที่มีความเสี่ยงต่อการล่วงละเมิดหรืออาชญากรรม เช่น ข้อมูลของพยานในคดี ข้อมูลของเหยื่อผู้ถูกล่วงละเมิด<br><input type="checkbox"/> การรั่วไหลที่มีสาเหตุมาจากการโจมตีโดยผู้ไม่ประสงค์ดีที่มุ่งเน้นในการ เข้าถึงข้อมูลที่เป็นความลับ<br><input type="checkbox"/> ข้อมูลอื่นๆ (โปรดระบุ).....                                                                                   |
| รายละเอียดของผลกระทบที่<br>อาจเกิด หรือ<br>เกิดไปแล้วต่อเจ้าของ<br>ข้อมูลส่วนบุคคล :                                                                                                              | .....<br>.....<br>.....<br>.....                                                                                                                                                                                                                                                                                                                                                                                          |
| รายละเอียดของผลกระทบที่<br>น่าจะเกิดจากการละเมิด:                                                                                                                                                 | .....<br>.....<br>.....                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>การประเมินความเสี่ยง</b> ที่จะมี<br>ผลกระทบต่อสิทธิและเสรีภาพของ<br>เจ้าของข้อมูลส่วนบุคคล (ตามเกณฑ์<br>ภาคผนวก)                                                                               | <input type="checkbox"/> สูง - ส่งผลกระทบต่อสุขภาพ เสรีภาพ และชีวิตของเจ้าของข้อมูล<br><input type="checkbox"/> ปานกลาง - ส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงของเจ้าของข้อมูล<br><input type="checkbox"/> ต่ำ - ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลต่ำ<br><input type="checkbox"/> ไม่มีความเสี่ยง - ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เช่น ข้อมูลนิรนามและข้อมูลภาพรวมเชิงสถิติ เป็นต้น และข้อมูลทั่วไปที่สามารถระบุตัวบุคคลได้ |
| <b>ส่วนที่ 4 การตอบสนองเพื่อระงับเหตุการณ์</b>                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>การตอบสนอง เพื่อระงับ<br/>         เหตุการณ์</b> (ตามประกาศ<br>คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการ<br>ในการแจ้งเหตุการณ์ละเมิดข้อมูล<br>ส่วนบุคคล พ.ศ. 2565 ข้อ 5(5)) | .....<br>.....<br>.....<br>.....<br>.....                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>แนวทางเยียวยาเจ้าของข้อมูล</b><br>(กรณีผลกระทบสูง)<br>ประกาศคณะกรรมการคุ้มครอง<br>ข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์                                                                             | (โปรดระบุมาตรการการแก้ไขปัญหา เช่น ดำเนินการเปลี่ยนรหัสความปลอดภัย ดำเนินการ<br>ค้นหาตามสถานที่ที่คาดว่าอุปกรณ์จะสูญหาย เป็นต้น)<br>สาเหตุของปัญหา.....<br>.....                                                                                                                                                                                                                                                          |

หมายเหตุ : เอกสารนี้ถูกควบคุมในระดับ [ลับมาก] เมื่อข้อมูลถูกกรอกลงในแบบฟอร์ม



|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใช้นายนอก</b>                                                                                           | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่5ของ10</b>           |

|                                                                                         |                                                                 |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| และวิธีการในการแจ้งเหตุการณ์<br>ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565<br>ประกาศ สคส. ข้อ 6(4) | การแก้ไขระยะสั้น.....<br>.....<br>การแก้ไขระยะยาว.....<br>..... |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------|

#### ส่วนที่ 5 การวิเคราะห์สาเหตุ และป้องกันการเกิดซ้ำ

|                                      |                                                                                                                                                                                                          |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>สาเหตุ</b>                        | (โปรดอธิบาย เพื่อขยายความลักษณะเหตุละเมิด เพื่อให้เข้าใจเนื้อหาของการละเมิดข้อมูลส่วนบุคคล โดยอธิบายเนื้อหาเท่าที่สามารถระบุได้ รวมไปถึงคำขยายความประเภทข้อมูลที่ทราบโดยละเอียด)<br>.....<br>.....       |
| <b>การป้องกัน/<br/>การขจัดสาเหตุ</b> | (โปรดระบุ แผนงาน และการป้องกัน การเกิดเหตุการณ์ซ้ำ)<br>.....<br>.....<br>.....                                                                                                                           |
| <b>หน่วยงานที่<br/>รับผิดชอบ</b>     | (โปรดระบุ หน่วยงาน/กลุ่ม/ฝ่าย/งาน ที่รับผิดชอบในการดำเนินการตามแผนข้างต้น)<br>1.....<br>เบอร์โทร:..... e-Mail :.....<br>2.....<br>เบอร์โทร:..... e-Mail :.....<br>3.....<br>เบอร์โทร:..... e-Mail :..... |

|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใช้นายนอก</b>                                                                                           | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่ 6 ของ 10</b>        |

### ส่วนที่ 6 การแจ้งต่อหน่วยงานที่เกี่ยวข้อง

|                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. แจ้งต่อผู้คุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวง <input type="checkbox"/> ยังไม่แจ้ง<br><input type="checkbox"/> แจ้งแล้ว เลขที่หนังสือ..... วันที่..... เวลา..... |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2. แจ้งต่อผู้บริหารของหน่วยงาน <input type="checkbox"/> แจ้งแล้ว วันที่..... เวลา..... <input type="checkbox"/> ยังไม่แจ้ง                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 3. แจ้งความ / ลงบันทึกประจำวันต่อเจ้าหน้าที่ตำรวจ <input type="checkbox"/> ยังไม่แจ้ง<br><input type="checkbox"/> แจ้งแล้ว เลขที่หนังสือ..... วันที่..... เวลา.....        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 4. แจ้งต่อเจ้าของข้อมูลส่วนบุคคล*                                                                                                                                          | <input type="checkbox"/> ดำเนินการแจ้งเจ้าของข้อมูลเรียบร้อยแล้ว<br>วันที่.....<br>ช่องที่ใช้ในการแจ้ง.....<br><input type="checkbox"/> อยู่ระหว่างการดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล<br><input type="checkbox"/> สสจ/สำนักงานปลัดกระทรวงสาธารณสุข และ/หรือ หน่วยงาน<br>ตัดสินใจที่จะไม่แจ้งเจ้าของข้อมูลส่วนบุคคล<br><input type="checkbox"/> อยู่ระหว่างการพิจารณาของสสจ/สำนักงานปลัดกระทรวงสาธารณสุข<br>สำนักงานปลัดกระทรวงสาธารณสุข และ/หรือ หน่วยงาน<br><input type="checkbox"/> อื่นๆ (โปรดระบุ)..... |

\* หมายเหตุ หากเป็นกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล ต้องมีการแจ้งเจ้าของข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง

|                                                |           |
|------------------------------------------------|-----------|
| <b>ผู้รายงาน (หัวหน้าหน่วยงานที่ถูกละเมิด)</b> |           |
| ชื่อ-นามสกุล:                                  | ตำแหน่ง:  |
| ส่วนราชการ:                                    | เบอร์โทร: |
| e-Mail :                                       |           |

### ส่วนที่ 7 แจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPO เป็นผู้บันทึกข้อมูล)

|                                                                                                                                                                                                                                                           |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 5. แจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล*<br><input type="checkbox"/> แจ้งแล้ว เลขที่หนังสือ..... วันที่.....<br><input type="checkbox"/> ยังไม่แจ้ง<br><input type="checkbox"/> ไม่ต้องแจ้งเพราะการละเมิดไม่ใช่ข้อมูลส่วนบุคคล หรือไม่มีข้อมูลรั่วไหล |  |
| * หมายเหตุ หากเป็นกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล ต้องมีการแจ้งเจ้าของข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง                                                                                                          |  |
| <b>ผู้รายงาน (ผู้ควบคุมข้อมูลส่วนบุคคล)</b>                                                                                                                                                                                                               |  |

|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใ้ภายนอก</b>                                                                                            | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่ 7 ของ 10</b>        |

|                                                     |                              |
|-----------------------------------------------------|------------------------------|
| ชื่อ-นามสกุล: นายพันมิตร ย้อยสร้อยสุด               | ตำแหน่ง: เจ้าหน้าที่ DPO     |
| เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล                  |                              |
| ส่วนราชการ: รพ น้ำเกลี้ยง                           | เบอร์โทร: 045-609055 ต่อ 333 |
| e-Mail : nk10941.gmail.com      https : nkhos.go.th |                              |

|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใช้นายนอก</b>                                                                                           | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่ 8 ของ 10</b>        |

**ภาคผนวก**

**1. การพิจารณาปัจจัยความเสี่ยง เพื่อกำหนดคะแนนสำหรับระดับความเสี่ยงตามเกณฑ์ดังต่อไปนี้**

| คะแนนสำหรับระดับความเสี่ยง | ระดับความเสี่ยง   |
|----------------------------|-------------------|
| 0                          | ไม่มีความเสี่ยง   |
| 1-7                        | ความเสี่ยงน้อย    |
| 8-14                       | ความเสี่ยงปานกลาง |
| 15-21                      | ความเสี่ยงสูง     |

| หัวข้อประเมิน<br>ปัจจัยความเสี่ยง            | คะแนนความเสี่ยง                                                                                                                                                                                                                                                 |                                                                                                                                                              |                                                                                                       |                                                                                                                                                     |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | 0                                                                                                                                                                                                                                                               | 1                                                                                                                                                            | 2                                                                                                     | 3                                                                                                                                                   |
| 1. จำนวนเจ้าของข้อมูล<br>ที่อาจได้รับผลกระทบ | ไม่มีเจ้าของข้อมูลที่ได้รับผลกระทบ เช่น จำนวนข้อมูลที่รั่วไหลเป็นจำนวนสถิติ หรือข้อมูลที่ได้รับการแปลงแล้ว                                                                                                                                                      | ทราบจำนวนเจ้าของข้อมูลแน่นอนซึ่งไม่เกิน 50 คน                                                                                                                | คาดหมายว่าอาจมีเจ้าของข้อมูลที่ได้รับผลกระทบไม่เกิน 100 คน                                            | มากกว่า 100 คน<br>หรือไม่สามารถระบุจำนวนเจ้าของข้อมูลได้                                                                                            |
| 2. ลักษณะของข้อมูล ที่<br>รั่วไหล            | ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เช่น ข้อมูลนิรนามและข้อมูลภาพรวมเชิงสถิติ เป็นต้น และข้อมูลทั่วไปที่สามารถระบุตัวบุคคลได้ แต่เป็นข้อมูลที่ไม่อยู่ภายใต้กำกับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น ข้อมูลของผู้ถึงแก่กรรม ข้อมูลเพื่อกิจกรรมในครอบครัว เป็นต้น | ข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้ทันที (โดยไม่รวมถึงข้อมูลอ่อนไหว) ต้องประกอบกับข้อมูลอื่น เช่น รหัสพนักงาน ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น | ข้อมูลส่วนบุคคลที่สามารถระบุตัวเจ้าของข้อมูลได้ทันที เช่น ชื่อของเจ้าของข้อมูล ภาพถ่าย วิดีโอ เป็นต้น | ข้อมูลอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ ศาสนา ความเห็นทางการเมือง พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลชีวภาพ เป็นต้น |

หมายเหตุ : เอกสารนี้ถูกควบคุมในระดับ [ลับมาก] เมื่อข้อมูลถูกกรอกลงในแบบฟอร์ม

|                                                                                   |                                                                                                                          |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------|
|  | <b>ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</b><br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                        | <b>เริ่มใช้</b><br>23 มี.ค. 69 |
|                                                                                   | <b>ชั้นความลับ : ใช้นายนอก</b>                                                                                           | <b>รหัสเอกสาร : F-PA-CL-02.01Rev01</b> | <b>หน้าที่ 9 ของ 10</b>        |

| หัวข้อประเมิน<br>ปัจจัยความเสี่ยง                                                                                                                  | คะแนนความเสี่ยง                                                                                              |                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                    | 0                                                                                                            | 1                                                                                                                                                                                                                                                                                        | 2                                                                                                                                                                                                                                                                                       | 3                                                                                                                                                                                |
| 3. ระยะเวลาการพบการ<br>รั่วไหล                                                                                                                     | ทราบเหตุทันทีที่เกิด<br>การรั่วไหล                                                                           | ทราบเหตุภายใน 24<br>ชั่วโมง นับแต่การ<br>รั่วไหล                                                                                                                                                                                                                                         | ทราบเหตุภายใน<br>24 ชั่วโมง แต่ไม่เกิน<br>72 ชั่วโมง นับแต่การ<br>รั่วไหล                                                                                                                                                                                                               | ทราบเหตุภายใน<br>72 ชั่วโมง นับแต่การ<br>รั่วไหล                                                                                                                                 |
| 4. การเข้าถึงข้อมูลของ<br>บุคลากรของหน่วยงาน<br>เมื่อถูกโจรกรรมข้อมูล                                                                              | บุคลากรสามารถเข้าถึง<br>ข้อมูลได้ปกติ                                                                        | บุคลากรไม่สามารถ<br>เข้าถึงข้อมูลบาง ส่วน<br>เป็นการชั่วคราว                                                                                                                                                                                                                             | บุคลากรไม่สามารถ<br>เข้าถึงข้อมูลทั้งหมด<br>เป็นการชั่วคราว                                                                                                                                                                                                                             | บุคลากรไม่สามารถ<br>เข้าถึงข้อมูลทั้งหมด<br>เป็นการถาวร                                                                                                                          |
| 5. ความเสียหายต่อ<br>ข้อมูล เมื่อถูก<br>โจรกรรมข้อมูล หรือ<br>ถูกเข้าโดย ไม่ได้รับ<br>อนุญาต หรือเกิดจาก<br>ความผิดพลาดของ<br>บุคลากรที่เกี่ยวข้อง | ข้อมูลไม่ได้ถูกแก้ไข/<br>เสียหายประการใด                                                                     | ข้อมูลถูกแก้ไข แต่ยังไม่<br>ถูกนำไปใช้งาน ซึ่ง<br>หน่วยงานยังมีข้อมูล<br>สำรอง และสามารถ<br>ใช้ข้อมูลสำรองได้                                                                                                                                                                            | ข้อมูลถูกแก้ไข และอาจ<br>ถูกนำไปใช้งานโดยไม่<br>ทราบว่ามีการแก้ไข<br>ข้อมูล ทั้งนี้ หน่วยงาน<br>ยังคงมีข้อมูลสำรองและ<br>สามารถใช้ข้อมูลสำรอง<br>ได้                                                                                                                                    | ข้อมูลถูกแก้ไข และอาจ<br>ถูกนำไปใช้งานโดยไม่<br>ทราบว่ามีการแก้ไข<br>ข้อมูลซึ่งหน่วยงานไม่มี<br>ข้อมูลสำรอง                                                                      |
| 6. ขอบเขตในการรั่วไหล<br>ของข้อมูล                                                                                                                 | ข้อมูลไม่ได้ถูกเปิดเผย<br>หรือถูกเข้าถึงโดยมิชอบ<br>โดยบุคคลที่ไม่ได้รับ<br>อนุญาต                           | ข้อมูลที่รั่วไหลอาจถูก<br>เปิดเผยต่อบุคคลที่ไม่<br>ได้รับอนุญาตภายใน<br>หน่วยงาน แต่ยังไม่พบ<br>หลักฐานว่าบุคคลที่<br>ไม่ได้รับอนุญาตดังกล่าว<br>มีการประมวลผลโดยมิ<br>ชอบเช่น เอกสารหาย<br>ภายในอาคารหน่วยงาน<br>หรืออุปกรณ์<br>อิเล็กทรอนิกส์ ถูกเลิก<br>ใช้งานโดยไม่ลบทำลาย<br>ข้อมูล | ข้อมูลถูกเปิดเผยต่อ<br>หรือเข้าถึงโดยบุคคล<br>ภายนอก โดยทราบ<br>บุคคลภายนอก<br>ดังกล่าว เช่น การส่ง<br>อีเมลผิดให้ผู้อื่น พร้อม<br>เอกสารแนบซึ่งเป็น<br>ข้อมูลส่วนบุคคล แต่<br>ผู้รับข้อมูลไม่สามารถ<br>เปิด หรือ อ่านข้อมูลได้<br>ต้องใช้มาตรการทาง<br>เทคนิคจึงจะเข้าถึง<br>ข้อมูลได้ | ข้อมูลถูกเปิดเผย หรือ<br>เข้าถึงโดยบุคคลภาย<br>นอกที่ไม่เกี่ยวข้องโดย<br>ไม่ทราบจำนวน เช่น<br>ถูกเปิด เผยสาธารณะ<br>หรือ มีการขายข้อมูล<br>ลูกค้า/ผู้ใช้บริการให้<br>บุคคลภายนอก |
| 7. ผลกระทบที่อาจ<br>เกิดขึ้นต่อเจ้าของ<br>ข้อมูลจากการรั่วไหล                                                                                      | ไม่มีผลกระทบต่อ<br>เจ้าของข้อมูลเนื่องจาก<br>เป็นข้อมูลที่เป็น<br>สาธารณะอยู่ก่อนการ<br>รั่วไหล หรือ ฝ่ายงาน | คาดว่าจะไม่เกิด<br>ผลกระทบต่อเจ้าของ<br>ข้อมูล แต่อาจก่อให้เกิด<br>ความรำคาญต่อเจ้าของ<br>ข้อมูล เช่น ต้องกรอก                                                                                                                                                                           | อาจก่อให้เกิด<br>ผลกระทบ โดยอ้อม ต่อ<br>สิทธิทรัพย์สิน และ<br>ร่างกายเช่น เกิดความ<br>กลัว หรือความกังวล                                                                                                                                                                                | อาจก่อให้เกิดผล<br>กระทบโดยตรงที่ไม่อาจ<br>แก้ไขได้โดยง่าย เช่น<br>ได้รับความเสียหายต่อ<br>ทรัพย์สิน ถูกเลิกจ้าง                                                                 |

หมายเหตุ : เอกสารนี้ถูกควบคุมในระดับ [ลับมาก] เมื่อข้อมูลถูกกรอกลงในแบบฟอร์ม

|                                                                                   |                                                                                                                   |                                                                                                                    |   |                                                                                                              |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------|
|  | ชื่องาน : แบบบันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล<br>(สำหรับหน่วยงานที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล) |                                                                                                                    |   | เริ่มใช้<br>23 มี.ค. 69                                                                                      |
|                                                                                   | ชั้นความลับ : ใช้นอก                                                                                              | รหัสเอกสาร : F-PA-CL-02.01Rev01                                                                                    |   | หน้าที่10ของ<br>10                                                                                           |
| หัวข้อประเมิน<br>ปัจจัยความเสี่ยง                                                 | คะแนนความเสี่ยง                                                                                                   |                                                                                                                    |   |                                                                                                              |
|                                                                                   | 0                                                                                                                 | 1                                                                                                                  | 2 | 3                                                                                                            |
|                                                                                   | สามารถป้องกันเหตุที่<br>อาจเกิดขึ้นแล้ว                                                                           | ข้อมูลในระบบใหม่<br>หรือลักษณะของ ข้อมูล<br>ที่รั่วไหลไม่สามารถ<br>กระทบต่อการ<br>ดำรงชีวิตของเจ้าของ<br>ข้อมูลได้ |   | การถูกปฏิเสธในการรับ<br>บริการถูกดำเนินคดี<br>เสียสุขภาพ หรือ<br>เจ็บป่วยรุนแรง หรือ<br>ระยะยาวหรือเสียชีวิต |

หมายเหตุ : เอกสารนี้ถูกควบคุมในระดับ [ลับมาก] เมื่อข้อมูลถูกกรอกลงในแบบฟอร์ม