

ตารางการประมาณความเสี่ยง (Risk estimation)

SIMPLE	ความเสี่ยง	โอกาสที่จะเกิด	ความรุนแรง
Personnel Safety Goals S :Security and Privacy of Information	GPS101 : เกิดอุบัติเหตุด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของ สถานพยาบาลรั่วไหล (Confidentiality Failure)	1	5
	GPS102 : เกิดอุบัติเหตุด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของ สถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure)	1	5
	GPS103 : เกิดอุบัติเหตุด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของ สถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	1	5
	GPS104 : เกิดอุบัติเหตุด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูล หรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	1	5
	GPS105 : เกิดอุบัติเหตุการละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของ บุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติเหตุด้านความมั่นคง ปลอดภัยไซเบอร์	2	4
	GPS106 : เกิดอุบัติเหตุการละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของ ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก ที่ไม่ใช่อุบัติเหตุด้านความมั่นคง ปลอดภัยไซเบอร์	2	4
	GPS201 : บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อ สาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่	2	3
	GPS202 : บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อ สาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	2	3
	GPS203 : บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	2	4
	GPS204 : เกิดอุบัติเหตุที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคน หนึ่งโดยตรง	2	4
Organization Safety Goals I : Information Technology & Communication, Internal control & Inventory	GOI101 : เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี-เทคนิค	2	3
	GOI102 : เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/ มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	2	5
	GOI103 : เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	2	3
	GOI104 : เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาท หน้าที่/ขาดความรู้และทักษะ	2	3

SIMPLE	ความเสี่ยง	โอกาสที่จะเกิด	ความรุนแรง
	GOI105 : เกิดปัญหาด้านข้อมูลสารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	5	3
	GOI106 : เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือ สื่อสารไม่ต่อเนื่อง/ไม่ครบถ้วน , ขาดการติดตาม ประเมินผลการสื่อสาร	2	2
	GOI201 : เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่ กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสาร หลักฐานกำกับ, ขาดการตรวจสอบหรือสอบทาน	2	3
	GOI202 : เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่ กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มี ทะเบียนคุม/การตรวจรับ/การบำรุงรักษา,ขาดการควบคุม การแจกจ่าย/การจำหน่าย	2	3
	GOI203 : เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกต้องตามมาตรฐาน/ บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้	2	3

3. การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้น ทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

$$\text{ระดับความเสี่ยง} = \text{โอกาสที่จะเกิดหรือความถี่ (P)} \times \text{ความรุนแรงหรือผลกระทบ (I)}$$

เกณฑ์ในการจัด แบ่งได้ดังนี้

ระดับคะแนนความเสี่ยง	สัญลักษณ์	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1-4	L	ต่ำ	ยอมรับความเสี่ยง	เขียว
5-9	M	ปานกลาง	ยอมรับความเสี่ยง(มีมาตรการ)	เหลือง
10-15	H	สูง	ควบคุมความเสี่ยง(มีแผนควบคุม)	ส้ม
16-25	HH	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

3.1 แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง



3.2 การประเมินความเสี่ยง

การวิเคราะห์ความเสี่ยงจากการวิเคราะห์ความเสี่ยงด้านสารสนเทศ สามารถแยกประเภทอุบัติการณ์ความเสี่ยงหลัก เป็น 2 ประเภท ปลาย 4 ประเภทย่อยดังนี้

- 1) รายการอุบัติการณ์ความเสี่ยงในกลุ่มอุบัติการณ์ความเสี่ยงทั่วไป (General Risk Incident : G)
หมวดอุบัติการณ์ความเสี่ยง Personnel Safety Goals : P

ประเภทอุบัติการณ์ความเสี่ยง S: Social Media and Communication มี 2 ประเภทย่อย ได้แก่ S1 : Security and Privacy of Information (ความปลอดภัยและความเป็นส่วนตัวของข้อมูล) S2 : Social Media and Communication Professionalism (ความเป็นมืออาชีพด้านโซเชียลมีเดียและการสื่อสาร)			
ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์ความเสี่ยง	SIMPER
1	GPS101	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล (Confidentiality Failure)	S1
2	GPS102	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure)	S1
3	GPS103	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	S1
4	GPS104	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	S1
5	GPS105	เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	S1

6	GPS106	เกิดอุบัติเหตุการละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก ที่ไม่ใช่อุบัติเหตุด้านความมั่นคงปลอดภัยไซเบอร์	S1
7	GPS201	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่	S2
8	GPS202	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	S2
9	GPS203	บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	S2
10	GPS204	เกิดอุบัติเหตุที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง	S2

2) รายการอุบัติเหตุความเสี่ยงในกลุ่มอุบัติเหตุความเสี่ยงทั่วไป (General Risk Incident : G)
หมวดอุบัติเหตุความเสี่ยง Organization Safety Goals: O

ประเภทอุบัติเหตุความเสี่ยง I: Information Technology & Communication, Internal control & Inventory มี 2 ประเภทย่อย ได้แก่			
I1 : Information Technology & Communication (เทคโนโลยีสารสนเทศและการสื่อสาร)			
I2 : Internal Control & Inventory (การควบคุมภายในและสินค้าคงคลัง)			
ลำดับ	รหัส อุบัติเหตุ	ชื่ออุบัติเหตุความเสี่ยง	มาตรฐาน
1	GOI101	เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี- เทคนิค	ตอนที่ I-4/ I1
2	GOI102	เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	ตอนที่ I-4/ I1
3	GOI103	เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	ตอนที่ I-4/ I1
4	GOI104	เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ	ตอนที่ I-4/ I1
5	GOI105	เกิดปัญหาด้านข้อมูล สารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	ตอนที่ I-4/ I1
6	GOI106	เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ไม่ครบถ้วน, ขาดการติดตามประเมินผลการสื่อสาร	ตอนที่ I-3/ I1
7	GOI201	เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ, ขาดการตรวจสอบหรือสอบทาน	ตอนที่ I-1/ I2
8	GOI202	เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา,ขาดการควบคุมการแจกจ่าย/การจำหน่าย	ตอนที่ I-1/ I2
9	GOI203	เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกต้องตามมาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้	ตอนที่ II-3/ I2

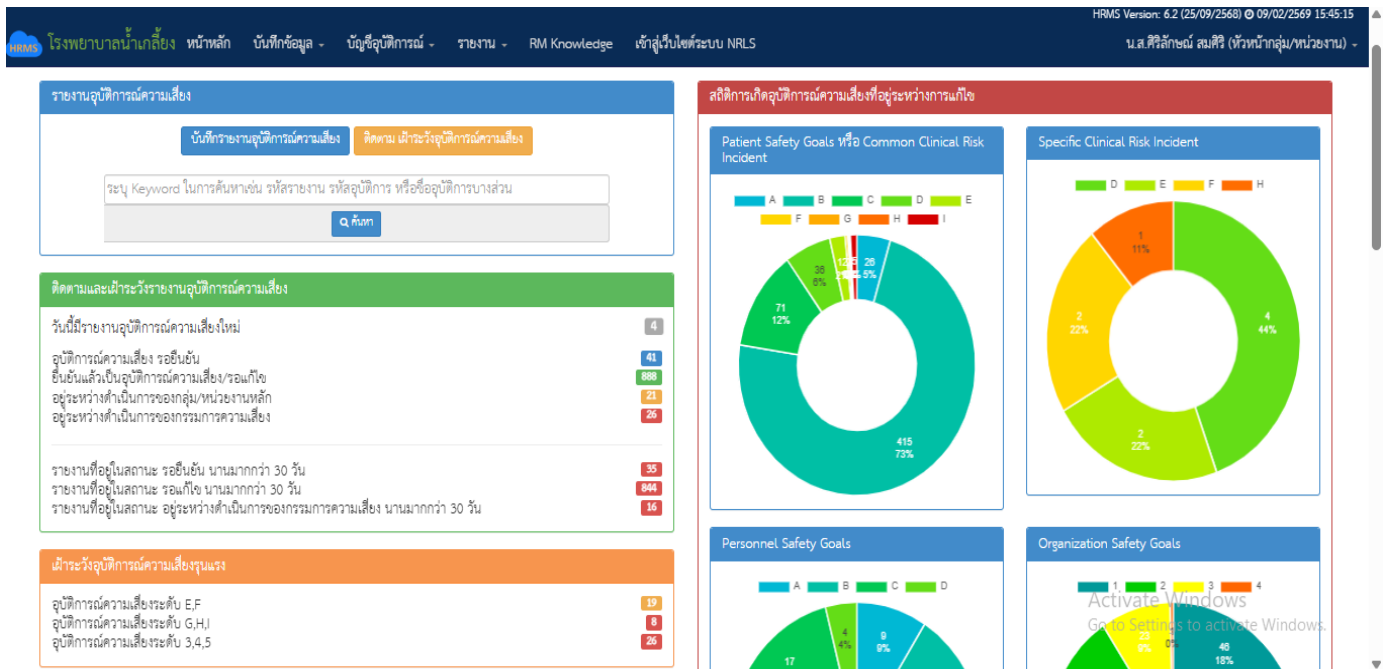
ตารางสรุปผลการประเมินค่าความเสี่ยง (Risk Evaluation)

ประเภท อุบัติการณ์ ความเสี่ยง	รหัส อุบัติการณ์ ความเสี่ยง	ชื่ออุบัติการณ์	โอกาส/ ความถี่	ความ รุนแรง	ระดับ คะแนน
S1 : Security and Privacy of Information (ความปลอดภัย และความเป็น ส่วนตัวของข้อมูล)	GPS101	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล(Confidentiality Failure)	2	5	10
	GPS102	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure)	2	5	10
	GPS103	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	2	5	10
	GPS104	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	2	5	10
	GPS105	เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	2	4	8
	GPS106	เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	2	4	8
S2 : Social Media and Communication Professionalism (ความเป็นมืออาชีพด้านโซเชียล)	GPS201	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่	2	3	6
	GPS202	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	2	3	6
	GPS203	บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	2	4	8
	GPS204	เกิดอุบัติการณ์ที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง	2	4	8

ประเภท อุบัติการณ์ ความเสี่ยง	รหัส อุบัติการณ์ ความเสี่ยง	ชื่ออุบัติการณ์	โอกาส/ ความถี่	ความ รุนแรง	ระดับ คะแนน
I1 : Information Technology & Communication (เทคโนโลยี สารสนเทศและ การสื่อสาร)	GOI101	เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี-เทคนิค	2	3	6
	GOI102	เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	2	5	10
	GOI103	เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	2	3	6
	GOI104	เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ	2	3	6
	GOI105	เกิดปัญหาด้านข้อมูล สารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	5	3	15
	GOI106	เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ไม่ครบถ้วน, ขาดการติดตามประเมินผลการสื่อสาร	2	2	4
I2 : Internal Control & Inventory (การ ควบคุมภายใน และสินค้าคงคลัง)	GOI201	เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ, ขาดการตรวจสอบหรือสอบทาน	2	3	6
	GOI202	เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา, ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา, ขาดการควบคุมการแจกจ่าย/การจำหน่าย	2	3	6
	GOI203	เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกตามมาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้	2	3	6

โรงพยาบาลน้ำเกลี้ยงได้มีการนำระบบบริหารจัดการความเสี่ยง NRLSเข้ามาใช้งานโดยทุกหน่วยงานสามารถเข้ามำบันทึกรายงานอุบัติการณ์ความเสี่ยง ตามภาพด้านล่างต่อไปนี้

1. หน้าระบบแสดงรายงาน



2. หน้าบันทึกรายงานอุบัติการณ์ความเสี่ยง

รายงานอุบัติการณ์ความเสี่ยง

บันทึกรายงานอุบัติการณ์ความเสี่ยง ติดตาม เฝ้าระวังอุบัติการณ์ความเสี่ยง

ระบุ Keyword ในการค้นหาเช่น รหัสรายงาน รหัสอุบัติการณ์ หรือชื่ออุบัติการณ์บางส่วน

ค้นหา

ติดตามและเฝ้าระวังรายงานอุบัติการณ์ความเสี่ยง

วันนี้มีรายงานอุบัติการณ์ความเสี่ยงใหม่ 4

อุบัติการณ์ความเสี่ยง รอยืนยัน 41

ยืนยันแล้วเป็นอุบัติการณ์ความเสี่ยง/รอแก้ไข 888

อยู่ระหว่างดำเนินการของกลุ่ม/หน่วยงานหลัก 21

อยู่ระหว่างดำเนินการของกรรมการความเสี่ยง 26

รายงานที่อยู่ในสถานะ รอยืนยัน นานมากกว่า 30 วัน 35

รายงานที่อยู่ในสถานะ รอแก้ไข นานมากกว่า 30 วัน 844

รายงานที่อยู่ในสถานะ อยู่ระหว่างดำเนินการของกรรมการความเสี่ยง นานมากกว่า 30 วัน 16

เฝ้าระวังอุบัติการณ์ความเสี่ยงรุนแรง

อุบัติการณ์ความเสี่ยงระดับ E,F 19

อุบัติการณ์ความเสี่ยงระดับ G,H,I 8

อุบัติการณ์ความเสี่ยงระดับ 3,4,5 26