



โรงพยาบาลน้ำเกลี้ยง
ประกาศนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง ดำเนินไปอย่าง เหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลน้ำเกลี้ยง จึงกำหนดนโยบาย ดังนี้

๑. ส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนอง ต่อพันธกิจและนโยบายขององค์กร
๒. มีหน้าที่ควบคุม ดูแล ระวังภัยพิบัติหรือภัยธรรมชาติ หรือภัยจากเทคโนโลยี หากมีการละเมิด หรือฝ่าฝืนระเบียบปฏิบัติในกรณีสำคัญ งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ รายงานการฝ่าฝืนให้ต้นสังกัด หรือโรงพยาบาลเพื่อพิจารณาโทษ
๓. สนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ
๔. สนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษา ข้อมูลความลับของผู้ใช้ และข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๖๕

(นายแพทย์อริบ ลีธีระประเสริฐ)
ผู้อำนวยการโรงพยาบาลน้ำเกลี้ยง



โรงพยาบาลน้ำเกลี้ยง

ประกาศระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง ดำเนินไปอย่าง เหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจาก ภัยต่างๆ โรงพยาบาลน้ำเกลี้ยง จึงกำหนดระเบียบปฏิบัติ ดังนี้

ข้อ	ระเบียบปฏิบัติ
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรม Himpro ทุกๆ ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
๒	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม Himpro ให้มี ๖ ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน(Passward) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม
๔	ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่น ปริ้นเตอร์,อุปกรณ์กระจายสัญญาณต่างๆ ฯลฯ) มาเชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายของโรงพยาบาลโดยไม่ได้รับอนุญาต
๕	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตมาติดตั้งหรือการอัปเดตซอฟต์แวร์อื่นใด ในโรงพยาบาล นอกเหนือจากที่ผู้ดูแลระบบกำหนด
๖	ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่นดูหนัง เล่นเกมส์ เป็นต้น
๗	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
๘	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
๙	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้อนุญาตเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ
๑๐	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง

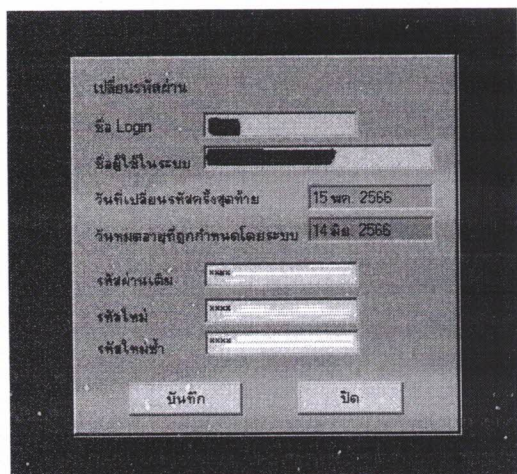
ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ.๒๕๖๓

(นายอธิป ลิธีระประเสริฐ)

ผู้อำนวยการโรงพยาบาลน้ำเกลี้ยง

ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ควรทำ



ควรทำการเปลี่ยนรหัสผ่านทุกๆ ๓๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

รหัสผ่านต้องมีความยาวอย่างน้อย ๖ ตัว ประกอบด้วยตัวเลขและอักษร

เก็บรักษาข้อมูลบัญชีของผู้ใช้งานและรหัสผ่าน ห้ามให้ผู้อื่นใช้

ไม่ควรกระทำ

ไม่ควรกระทำ	ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่น ปริ้นเตอร์, อุปกรณ์กระจายสัญญาณต่างๆ ฯลฯ) มาเชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายของโรงพยาบาลโดยไม่ได้รับอนุญาต
ไม่ควรกระทำ	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตมาติดตั้งหรือการอัปเดตซอฟต์แวร์อื่นใดในโรงพยาบาล นอกเหนือจากที่ผู้ดูแลระบบกำหนด
ไม่ควรกระทำ	ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น
ไม่ควรกระทำ	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
ไม่ควรกระทำ	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใดๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
ไม่ควรกระทำ	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ
ไม่ควรกระทำ	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์ หรือผู้รับผิดชอบโดยตรง

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติการรักษาความมั่นคง
ปลอดภัยของระบบเทคโนโลยีสารสนเทศ



**นโยบายและแนวปฏิบัติการรักษาความมั่นคง
ปลอดภัยของระบบเทคโนโลยีสารสนเทศ
(Information Security Policy)**

โรงพยาบาลน้ำเกลี้ยง
งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับองค์กรที่เข้ามาช่วยอำนวยความสะดวก ในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของหน่วยงานที่เชื่อมต่อในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสาร ต่างๆ เป็นต้น แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์ และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ แต่ในขณะเดียวกัน ก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูล ไปยังหน่วยงานต่างๆ ทำให้มีโอกาส ถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ ของหน่วยงาน ดังนั้นผู้ให้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแล บำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นอย่างยิ่ง

ดังนั้น โรงพยาบาลน้ำเกลี้ยง จึงจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบ เทคโนโลยีสารสนเทศขององค์กร เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคง ปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ จากทุกหน่วยงาน และต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยี ที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะกรรมการอำนวยการและกำกับดูแล ด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงหวังเป็นอย่างยิ่งว่า แนวปฏิบัติการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ ฉบับนี้ จะเป็นแนวทางให้กับผู้ให้บริการ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยงต่อไป

สารบัญ

หน้า

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ.....	๑
บทนำ.....	๑
หมวดทั่วไป.....	๑
หมวดที่ ๑ ว่าด้วยระเบียบการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ต.....	๒
หมวดที่ ๒ ว่าด้วยการใช้จดหมายอิเล็กทรอนิกส์ การสนทนาและการติดต่อสื่อสารทางอิเล็กทรอนิกส์.....	๓
หมวดที่ ๓ ว่าด้วยการใช้ Portal ขององค์กร และการเข้าใช้อินเทอร์เน็ต.....	๓
หมวดที่ ๔ ว่าด้วยการใช้งาน Application และโปรแกรมต่างๆ.....	๓
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ.....	๕
๑. หลักการและเหตุผล.....	๕
๒. วัตถุประสงค์.....	๕
๓. นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ.....	๕
๔. องค์ประกอบของแนวทางปฏิบัติ.....	๖
คำนิยาม.....	๗
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security).....	๑๐
๑. วัตถุประสงค์.....	๑๐
๒. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม.....	๑๐
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy).....	๑๑
๑. วัตถุประสงค์.....	๑๑
๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	๑๑
๒.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	๑๑
๒.๒ การบริหารจัดการ การเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	๑๑
๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ.....	๑๒
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy).....	๑๓
๑. วัตถุประสงค์.....	๑๓
๒. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย.....	๑๓
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy).....	๑๕
๑. วัตถุประสงค์.....	๑๕
๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย.....	๑๕

สารบัญ (ต่อ)

หน้า

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy).....	๑๖
๑. วัตถุประสงค์.....	๑๖
๒. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์.....	๑๖
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy).....	๑๘
๑. วัตถุประสงค์.....	๑๘
๒. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์.....	๑๘
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy).....	๑๙
๑. วัตถุประสงค์.....	๑๙
๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต.....	๑๙
นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy).....	๒๐
๑. วัตถุประสงค์.....	๒๐
๒. แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย.....	๒๐
นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy).....	๒๑
๑. วัตถุประสงค์.....	๒๑
๒. แนวทางปฏิบัติในการสำรองข้อมูล.....	๒๑
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ.....	๒๒
๑. วัตถุประสงค์.....	๒๒
๒. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ.....	๒๒

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

บทนำ

๑) นโยบายนี้จัดทำขึ้นสำหรับข้าราชการหรือเจ้าหน้าที่ในสังกัดโรงพยาบาลน้ำเกลี้ยง จะเข้าใช้งาน ระบบคอมพิวเตอร์ของโรงพยาบาลน้ำเกลี้ยง รวมไปถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต โดยผ่านทางเครือข่ายของโรงพยาบาลน้ำเกลี้ยง โดยให้ถือปฏิบัติโดยเคร่งครัด

๒) โรงพยาบาลน้ำเกลี้ยง สวสนสิทธิในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่ามี การละเมิดนโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ต

๓) นโยบายของระบบคอมพิวเตอร์และอุปกรณ์ประกอบของ โรงพยาบาลน้ำเกลี้ยง มีดังนี้

- ระบบคอมพิวเตอร์
- เครื่องคอมพิวเตอร์
- อุปกรณ์ประกอบ
- ซอฟต์แวร์
- เครือข่ายภายใน อินทราเน็ต
- เครือข่าย อินเทอร์เน็ต
- การใช้งานจากภายนอกองค์กร remote access
- โปรแกรมการใช้งาน Application

หมวดทั่วไป

๑) ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์ต่อเชื่อมของโรงพยาบาลน้ำเกลี้ยง จัดหาเพื่อ ให้บริการที่ เกี่ยวข้องกับกิจการของโรงพยาบาลน้ำเกลี้ยงเท่านั้น ไม่อนุญาตให้ใช้ในกิจการ ที่ไม่เกี่ยวข้องกับกิจการของโรงพยาบาลน้ำ เกลี้ยง และหากไม่ได้รับอนุญาตห้ามนำบุคคลภายนอก มาใช้งานเครื่องคอมพิวเตอร์ และเครือข่ายของโรงพยาบาลน้ำ เกลี้ยง

๒) การเข้าใช้งานระบบคอมพิวเตอร์ และการต่อเชื่อมทางอินเทอร์เน็ต ของโรงพยาบาลน้ำเกลี้ยง จะต้องปฏิบัติ ตามระเบียบในการขออนุญาตเข้าใช้โดยจะมีการลงทะเบียนการเข้าใช้งานตามขั้นตอนของโรงพยาบาลน้ำเกลี้ยง

๓) บัญชีผู้ใช้งาน (USER ACCOUNT) ที่ให้ผู้ใช้งานไว้นั้น ผู้ใช้งานต้องรับผิดชอบผลต่างๆ อันอาจเกิดขึ้นรวมถึง ผลเสียหายต่างๆ ที่เกิดขึ้นจากบัญชีผู้ใช้งาน (USER ACCOUNT) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการ กระทำของผู้อื่น

๔) บัญชีผู้ใช้งาน (USER ACCOUNT) ให้เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกสิทธินั้นให้กับ ผู้อื่นไม่ได้

๕) ในการขออนุญาตเข้าใช้งาน ให้ผู้ที่ขอใช้บริการเป็นผู้ขอโดยปฏิบัติตามขั้นตอนการขอเข้าใช้ระบบที่กำหนด ไว้

๖) ผู้เข้าใช้งานจะต้องทำความเข้าใจและลงนามเพื่อยืนยันว่าจะปฏิบัติตามนโยบายการใช้งานระบบคอมพิวเตอร์ และการเชื่อมต่อกับอินเทอร์เน็ต และจะต้องทำความเข้าใจในส่วนเปลี่ยนแปลงแก้ไข (หากมี) โดยลงนามเพื่อยืนยันทุกรอบ ปี

๗) ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่กำหนดขึ้นโดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้

๘) นโยบายการใช้ระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตนี้ ถือเป็นส่วนหนึ่งของข้อกำหนดในการปฏิบัติงานของข้าราชการและเจ้าหน้าที่ทุกคน และจะถือเป็นการผิดวินัยหรือระเบียบในการปฏิบัติงานเช่นเดียวกันหากไม่ปฏิบัติตาม

๙) หากพบว่าข้าราชการหรือเจ้าหน้าที่มีการละเมิดนโยบายการใช้งานระบบคอมพิวเตอร์และ การเชื่อมต่อกับอินเทอร์เน็ต จะถูกลงโทษตามกฎหมายของการเป็นข้าราชการหรือเจ้าหน้าที่ รวมไปถึงอาจจะส่งตัวเพื่อดำเนินคดีตามกฎหมาย หากการละเมิดนั้นมีความผิดตามกฎหมาย หรือพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐

๑๐) ผู้ใช้งานต้องต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแลระบบคอมพิวเตอร์

หมวดที่ ๑ ว่าด้วยระเบียบการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ต

๑) โรงพยาบาลน้ำเกลี้ยง ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบคอมพิวเตอร์และ การเชื่อมต่อทางอินเทอร์เน็ต จะถือปฏิบัติตามพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้องโดยข้าราชการหรือเจ้าหน้าที่ สามารถศึกษาข้อกฎหมายจาก พรบ.ดังกล่าวได้

๒) โรงพยาบาลน้ำเกลี้ยง ไม่สนับสนุนหรือยินยอมให้ข้าราชการหรือเจ้าหน้าที่ของโรงพยาบาลน้ำเกลี้ยง กระทำผิดต่อพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง

๓) โรงพยาบาลน้ำเกลี้ยง จะจัดให้มีชื่อผู้ใช้ (USERID) และรหัสผ่าน (Password) ให้กับข้าราชการหรือ เจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตเป็น รายบุคคล และมีกฎในการใช้งานรหัสผ่าน เช่น ความยาวของตัวอักษร หรือระยะเวลาที่ต้องเปลี่ยนรหัส ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม

๔) รหัสผ่านของข้าราชการหรือเจ้าหน้าที่ถือเป็นทรัพย์สินของโรงพยาบาลน้ำเกลี้ยง และไม่อนุญาตให้มี การแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และข้าราชการหรือเจ้าหน้าที่ทุกคนมีหน้าที่ในการ ป้องกันรหัสผ่านขององค์กรอย่างเคร่งครัด

๕) โรงพยาบาลน้ำเกลี้ยง ไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน

๖) ข้าราชการหรือเจ้าหน้าที่อาจจะได้รับมอบหมายให้เข้าใช้ระบบงานอื่นๆ ที่โรงพยาบาลน้ำเกลี้ยง กำหนดให้ใช้ ข้าราชการหรือเจ้าหน้าที่จะต้องปฏิบัติตามกฎการใช้ระบบเก็บรักษาชื่อและรหัสผ่านไว้ ห้ามมิให้เปิดเผยกับผู้อื่น ยกเว้นได้รับอนุมัติจากผู้บังคับบัญชาโดยตรงเป็นลายลักษณ์อักษร

๗) หากจะต้องมีการเลิกใช้ชื่อและรหัสผ่านให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอลีกใช้ โดยจะต้องกระทำทันทีที่จะเลิกใช้งาน หรือบัญชีผู้ใช้งานใดๆ ที่มิได้มีการใช้งานภายในระยะที่กำหนดไว้ จะถูกระงับหรือยกเลิกการใช้งาน

๘) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของโรงพยาบาลน้ำเกลี้ยง ข้าราชการหรือ เจ้าหน้าที่ที่เป็นผู้รับผิดชอบจะต้องมีหน้าที่ดูแลบำรุงรักษาเบื้องต้น

๙) ไม่อนุญาตให้ใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มีใช้ของโรงพยาบาลน้ำเกลี้ยง ในการ เชื่อมต่อเข้ากับเครือข่ายของโรงพยาบาลน้ำเกลี้ยง เว้นแต่ได้มีการขออนุญาตเข้าใช้ระบบเครือข่าย คอมพิวเตอร์จากงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

หมวดที่ ๒ ว่าด้วยการใช้จดหมายอิเล็กทรอนิกส์, การสนทนา และการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่นๆ (E-mail), chat, social network and others digital communication เช่น การส่ง file หรือการส่งโทรสาร

๑) ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์ หรือการติดต่อสื่อสารใดๆ ให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือ หรือจดหมายของโรงพยาบาลน้ำเกลี้ยง ได้แก่ การรักษาความลับของเอกสาร ห้ามส่งเอกสารความลับ โดยจดหมายอิเล็กทรอนิกส์ ยกเว้นได้รับการเข้ารหัส และรับรองจากหน่วยงานคอมพิวเตอร์

๒) ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อโรงพยาบาลน้ำเกลี้ยง หรือบุคคลอื่นๆ

๓) ห้ามส่งรูปหรือข้อความที่เกี่ยวข้องกับเรื่องลามกอนาจาร

๔) การส่งข้อมูลใดๆ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๕) หากพบว่ามีการส่งข้อมูลที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือผิดต่อกฎระเบียบของโรงพยาบาลน้ำเกลี้ยง ให้แจ้งต่อผู้บังคับบัญชาโดยตรง หรือเจ้าหน้าที่ หน่วยงานคอมพิวเตอร์

๖) ให้ใช้ข้อความสุภาพในการส่งจดหมายอิเล็กทรอนิกส์ การสนทนา chat หรือการสื่อสารทาง อิเล็กทรอนิกส์อื่นๆ

๗) ห้ามส่งจดหมายอิเล็กทรอนิกส์หรือการสื่อสารทางอิเล็กทรอนิกส์ใดๆ โดยไม่ระบุชื่อผู้ส่ง (SPAM (E-mail))

๘) ไม่อนุญาตให้ข้าราชการหรือเจ้าหน้าที่ใช้ (E-mail) อื่นใดที่โรงพยาบาลน้ำเกลี้ยง ไม่ได้กำหนดให้ใช้

หมวดที่ ๓ ว่าด้วยการใช้ Portal ขององค์กร และการเข้าใช้อินเทอร์เน็ต

๑) ห้ามข้าราชการหรือเจ้าหน้าที่ post และ/หรือ download file รูป หรือข้อมูลใดๆ บน Portal ของโรงพยาบาลน้ำเกลี้ยง หรือ Portal อื่นๆ ที่เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยเรื่องการทำ ความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐

๑.๑ มีไวรัส หรือชุดคำสั่งไม่พึงประสงค์

๑.๒ ไม่เกี่ยวข้องกับกิจการขององค์กร

๒) การเปิดให้บริการการเข้าถึงเว็บไซต์

๒.๑ ให้บริการเว็บไซต์ที่เกี่ยวข้อง การให้บริการและกิจการของโรงพยาบาลน้ำเกลี้ยงเป็นหลัก หากตรวจพบว่าความเร็วอินเทอร์เน็ตของระบบช้า จะงดให้บริการอินเทอร์เน็ตในกิจการอื่นๆ ที่มีใช้ของโรงพยาบาลน้ำเกลี้ยงก่อน

๒.๒ กำหนดช่วงเวลาหรือระดับการเข้าใช้งานของเว็บไซต์ ที่กำหนดโดยงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์

หมวดที่ ๔ ว่าด้วยการใช้งาน Application และโปรแกรมต่างๆ

๑) การใช้งาน Application ต่างๆ จะต้องได้รับอนุญาตจากเจ้าของระบบ

๒) ให้ข้าราชการหรือเจ้าหน้าที่ใช้โปรแกรมและ Application ที่โรงพยาบาลน้ำเกลี้ยง กำหนดให้ใช้ เท่านั้น

๓) ห้ามข้าราชการหรือเจ้าหน้าที่นำโปรแกรม หรือ Application ใดๆ มาติดตั้งบนเครื่องคอมพิวเตอร์หรือ ระบบคอมพิวเตอร์รวมถึงอุปกรณ์ประกอบอื่นๆ โดยไม่ได้รับความยินยอมจากหน่วยงานคอมพิวเตอร์ โดยตรง

๔) ห้ามข้าราชการหรือเจ้าหน้าที่ใช้โปรแกรม หรือ Application ที่ไม่ถูกลิขสิทธิ์ หากก่อให้เกิดความเสียหาย หรือ มีการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

๕) ผู้ที่ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามนโยบายนี้ โดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่างๆ เป็นไปตามมาตรฐานและไม่เกิดผลกระทบกับระบบ เครือข่ายคอมพิวเตอร์ส่วนรวมของ โรงพยาบาลน้ำเกลี้ยง

๖) การขออนุญาตนำเครื่องคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายและหมายเลขไอพี (IP ADDRESS) ของหน่วยงานใดๆ หน่วยงานนั้นจะต้องทำหนังสือขออนุญาต มายังงานประกันสุขภาพ ยุทธศาสตร์และ สารสนเทศทางการแพทย์ เพื่อพิจารณาดำเนินการ

๗) ห้ามบุคคลใดกระทำการเคลื่อนย้ายหรือทำการใดๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการเพราะ อาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของโรงพยาบาลน้ำเกลี้ยงได้

๘) ในกรณีที่ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติของระบบเครือข่ายหลักของ โรงพยาบาลน้ำเกลี้ยง งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ อาจจะพิจารณา ระงับการให้บริการ จากระบบ เครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ ทำงานได้เป็นปกติก่อน

๙) ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับการอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบ ไร้สาย

๑๐) โรงพยาบาลน้ำเกลี้ยง จะติดตั้งโปรแกรมควบคุมการใช้งานผ่านเครือข่าย (REMOTE ACCESS) เพื่อติดตาม ช่วยเหลือ แก้ไข และควบคุมการใช้งานเครื่องคอมพิวเตอร์

๑๑) ผู้ใช้งานห้ามทำการเก็บหรือสำรองข้อมูลส่วนบุคคลไว้ในเครื่องคอมพิวเตอร์ ของโรงพยาบาลน้ำเกลี้ยง หาก เกิดปัญหาจำเป็นต้องมีการซ่อมบำรุงหรือมีการติดตั้งระบบปฏิบัติการใหม่ อาจมีการ ล้างข้อมูลในเครื่องคอมพิวเตอร์ ทั้งหมด งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ จะไม่รับผิดชอบต่อการสูญหายของข้อมูลส่วนบุคคล นั้นๆ

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. หลักการและเหตุผล

ตามพระราชบัญญัติกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลน้ำเกลี้ยงจึงเห็นสมควรกำหนดนโยบายและแนวทาง ปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความ มั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

๒. วัตถุประสงค์

๒.๑ การจัดทำนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อ้างอิงตาม มาตรฐาน HA และมีการปรับปรุงอย่างต่อเนื่อง

๒.๓ นโยบายและแนวทางปฏิบัตินี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและ เจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบ เทคโนโลยีสารสนเทศขององค์กร ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๕ นโยบายและแนวทางปฏิบัตินี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา อย่างน้อย ๑ ครั้ง ต่อปี

๓. นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลน้ำเกลี้ยง

๓.๑ โรงพยาบาลน้ำเกลี้ยงส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยี สารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๓.๒ โรงพยาบาลน้ำเกลี้ยงมีหน้าที่จำกัด ระบุ เพิกถอนสิทธิหรือบทลงโทษตามความเหมาะสมหากมี การละเมิดหรือฝ่าฝืนระเบียบปฏิบัติ ในกรณีสำคัญงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศ ทางแพทย์ รายงานการฝ่าฝืนให้ต้นสังกัดหรือโรงพยาบาลเพื่อพิจารณาโทษ

๓.๓ โรงพยาบาลน้ำเกลี้ยงสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๕ โรงพยาบาลน้ำเกลี้ยงสนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

๔. องค์ประกอบของแนวทางปฏิบัติ

๔.๑ คำนินยาม

๔.๒ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๔.๓ การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

๔.๔ การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔.๕ การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

๔.๖ การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

๔.๗ การรักษาความมั่นคงปลอดภัยของอีเมล

๔.๘ การรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต

๔.๙ การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

๔.๑๐ ความมั่นคงปลอดภัยของการสำรองข้อมูล

๔.๑๑ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ แต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ (Objective) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กร มีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความ ปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลน้ำเกลี้ยง

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุม ดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ หมายถึง ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในโรงพยาบาลน้ำเกลี้ยง

หัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการ ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในโรงพยาบาลน้ำเกลี้ยง

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศของโรงพยาบาลน้ำเกลี้ยง

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตาม วัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแล รักษา ระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งโรงพยาบาลน้ำเกลี้ยงกำหนดไว้ดังนี้

- **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลน้ำเกลี้ยง เช่น ผู้อำนวยการ โรงพยาบาลน้ำเกลี้ยง รองผู้อำนวยการโรงพยาบาล หัวหน้าตึก หัวหน้ากลุ่มงาน เป็นต้น
- **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจาก ผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่น เพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น
- **เจ้าหน้าที่** หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ ประจำโครงการต่างๆ ของโรงพยาบาลน้ำเกลี้ยง

- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลน้ำเกลี้ยง อนุญาต ให้มีสิทธิ ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ ในการใช้ระบบตาม อำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบ คอมพิวเตอร์ใน สภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรม อิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการ กำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดย อัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่ง ข้อมูลและ สารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบ คอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อ การติดต่อสื่อสารแลกเปลี่ยนข้อมูลและ สารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่าย คอมพิวเตอร์ ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอา เทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้าง สารสนเทศที่หน่วยงานสามารถนำมาใช้ ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้ บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมี องค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

- **พื้นที่ทำงานทั่วไป (General working area)** หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
- **พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)** หมายถึง พื้นที่ติดตั้งอุปกรณ์ ระบบ เทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
- **พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)** หมายถึง พื้นที่ใช้งานระบบเครือข่าย ไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดย เจ้าของข้อมูล เป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบ เทคโนโลยีสารสนเทศ

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของ หน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบ อำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความ ถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืน นโยบาย ด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POPm และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของ ข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ให้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๒. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เป็นผู้กำหนดพื้นที่ผู้ให้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน และประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้ง และจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒.๒ ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓ ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ กำหนดมาตรการควบคุม การเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกัน การบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคล ที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่าย ของหน่วยงานได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง

๒.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑.๑ โรงพยาบาลน้ำเกลี้ยงกำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงาน หน่วยงานภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน จะต้องขออนุญาต เป็นลายลักษณ์อักษรต่อหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทาง การแพทย์

๒.๑.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึง อย่างสม่ำเสมอ

๒.๑.๓ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

๒.๑.๔ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิ ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒ การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๒.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลน้ำเกลี้ยง กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒.๒ ผู้ดูแลระบบต้องกำหนดการเข้าใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างสม่ำเสมอ

๒.๒.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

๒.๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลากออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๒.๓.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ให้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยง การใช้ บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันใน การส่งรหัสผ่าน

๒.๒.๓.๓ ควรกำหนดให้ผู้ให้บริการตอบยืนยันการได้รับรหัสผ่าน

๒.๒.๓.๔ ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบ ที่ ไม่ได้ป้องกันการเข้าถึง

๒.๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๒.๓.๖ ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้อง ได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้ งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ ถึงระดับใดบ้าง และต้องกำหนดให้ รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุม การเข้าถึง ข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๒.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและ การ เข้าถึงผ่านระบบงาน

๒.๒.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการ ตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๒.๔.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

๒.๒.๔.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๒.๒.๔.๕ ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของ ข้อมูล

๒.๒.๔.๖ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำ เครื่อง คอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ ไปตรวจซ่อม ควรสำรองและลบ ข้อมูลที่ เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

๒.๓.๑ ผู้ให้บริการต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของ เครื่อง คอมพิวเตอร์ของหน่วยงาน

๒.๓.๒ ผู้ให้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่านของตน ในการเข้าใช้งาน เครื่อง คอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๓.๓ ผู้ให้บริการควรตั้งค่าการใช้งานโปรแกรมถนัดหน้าจอ เพื่อทำการล๊อคหน้าจอภาพ เมื่อไม่มี การ ใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ให้บริการ ต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

๒.๓.๔ ผู้ให้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็น เวลานานมากกว่า ๑ ชม.

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้บริการได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์ และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตาม เพื่อเป็นการป้องกันทรัพยากร และข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อม ใช้งานอยู่เสมอ

๒. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายโรงพยาบาลน้ำเกลี้ยง

กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

๒.๑ ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุม ป้องกัน การบุกรุกได้อย่างเป็นระบบ

๒.๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบ เครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้างาน ประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ และต้องปฏิบัติตามนโยบายนี้ โดยเคร่งครัด

๒.๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงาน รับผิดชอบ อยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้างาน ประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผล กระทบต่อการกระทำของระบบและผู้ใช้บริการ อื่นๆ

๒.๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย หลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๒.๕ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๒.๕.๑ มีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งาน เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๒.๕.๒ ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยัง เครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ

๒.๕.๓ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๒.๕.๔ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๒.๕.๕ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๒.๕.๖ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมี การป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๒.๕.๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็น ปัจจุบันอยู่เสมอ

๒.๕.๘ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๕.๙ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการ ดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ ระบบ (Systems Software)

๒.๖ โรงพยาบาลน้ำเกลี้ยง กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตาม แนวทาง ดังต่อไปนี้

๒.๖.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้อง กำหนดขึ้นความลับในการเข้าถึงข้อมูล และผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูล ที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๒.๖.๒ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึก การพยายามเข้าสู่ระบบบันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๒.๖.๓ ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๒.๖.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึก เหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๒.๗ โรงพยาบาลน้ำเกลี้ยง กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๒.๗.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขอ อนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

๒.๗.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๒.๗.๓ วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากกระยะไกลต้องได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และ สารสนเทศทางการแพทย์

๒.๗.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นใน การดำเนินงานกับหน่วยงานอย่างเพียงพอ

๒.๗.๕ การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบ ในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ต้องปฏิบัติ ดังนี้

๒.๑ การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา ในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งานเพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๒.๒ ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

๒.๓ ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

๒.๔ กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

๒.๔.๑ ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสมโดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายในที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

๒.๔.๒ ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่อง คอมพิวเตอร์ ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๒.๔.๓ ให้เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งานและต้องปิดคุณสมบัติการ Auto Broadcast SSID ด้วย

๒.๔.๔ ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

๒.๔.๕ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๒.๔.๖ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งาน ระบบเครือข่ายไร้สาย ในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๒.๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบ เครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่าย ไร้สาย และจัดส่งรายงานผลการตรวจสอบ ทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานให้หัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทราบทันที

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

๑. วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

๒. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของโรงพยาบาลน้ำเกลี้ยง มีหน้าที่และ ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑ งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของโรงพยาบาลน้ำเกลี้ยง

๒.๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๒.๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๒.๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

๒.๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อ ที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๒.๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแล จัดการเท่านั้น

๒.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บ ข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อย กว่า ๓๐ วัน

๒.๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ต การเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลน้ำเกลี้ยง อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากหัวหน้างาน ประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ก่อน

๒.๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ โดยต้องระบุข้อมูลดังนี้

๒.๙.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๒.๙.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๒.๙.๓ วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้นๆ

๒.๙.๔ วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

๒.๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๒.๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็น กรณี ไป

๒.๑๒ โรงพยาบาลน้ำเกลี้ยง มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาลน้ำเกลี้ยง หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

๒.๑๓ ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาลน้ำเกลี้ยง หรือกฎหมาย หรืออาจจะทำให้เกิดความเสียหายด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ จะยกเลิกการให้บริการทันที

๒.๑๔ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากโรงพยาบาลน้ำเกลี้ยงก่อน

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้ จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่าย เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของโรงพยาบาลน้ำเกลี้ยง มีหน้าที่และความรับผิดชอบ ที่ต้องปฏิบัติ ดังนี้

๒.๑ ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลคำขอ เข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ โรงพยาบาลน้ำเกลี้ยง

๒.๒ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที

๒.๓ ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

๒.๔ ควรเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน

๒.๕ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

๒.๖ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของโรงพยาบาลน้ำเกลี้ยง ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลน้ำเกลี้ยง เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ ของโรงพยาบาลน้ำเกลี้ยง ขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๒.๗ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๒.๘ การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยุ่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของโรงพยาบาลน้ำเกลี้ยง หรือก่อให้เกิดความเสียหายต่อโรงพยาบาลน้ำเกลี้ยง

๒.๙ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลน้ำเกลี้ยง เพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของโรงพยาบาลน้ำเกลี้ยง ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของโรงพยาบาลน้ำเกลี้ยง

๒.๑๐ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๑๑ การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน ๑๐ เมกะไบต์

๒.๑๒ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตของโรงพยาบาลน้ำเกลี้ยง ซึ่งผู้ใช้งานต้องให้ ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต

ผู้ใช้งานเครือข่ายอินเทอร์เน็ตของโรงพยาบาลน้ำเกลี้ยง มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑ การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ หรือทำการสมัครผ่านระบบอินเทอร์เน็ตของโรงพยาบาลน้ำเกลี้ยง โดยรอการตรวจสอบตัวบุคคลและอนุมัติการใช้งานโดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลน้ำเกลี้ยง สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากหัวหน้างานเทคโนโลยีและสารสนเทศทางการแพทย์ หรือผู้ที่ได้รับมอบหมาย

๒.๒ ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๒.๓ ผู้ใช้งานอินเทอร์เน็ต พึงใช้ข้อมูลความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่าน ระบบเครือข่าย

๒.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๒.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒.๖ รับผิดชอบการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลด การอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมี ความจำเป็นให้แจ้งผู้ที่ได้รับมอบหมาย

๒.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ Facebook โปรแกรมอื่นๆ ที่มีลักษณะคล้ายกัน ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อมูลที่ยั่ว ยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๒.๘ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควร (Logout) ออกจากระบบทุกครั้ง

นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

๑. วัตถุประสงค์

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัย ของเครือข่าย เพื่อป้องกันทรัพยากรระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในโรงพยาบาลน้ำเกลี้ยง ให้มีความมั่นคงปลอดภัย

๒. แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

๒.๑ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของโรงพยาบาลน้ำเกลี้ยง และเครือข่าย ข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๒.๒ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ต หรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๒.๓ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้ง และเปิดให้บริการ

๒.๔ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๒.๕ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

๒.๖ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งานกิจกรรม และปริมาณข้อมูลเข้าใช้งาน เครือข่ายเป็นประจำโดยผู้ดูแลระบบ

๒.๗ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบ เทคโนโลยีสารสนเทศตามปกติ

๒.๘ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๒.๙ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จ และไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๒.๑๐ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

๒.๑๑ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้นานอย่างน้อย ๓๐ วัน

๒.๑๒ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจ เกิดอีกในอนาคต และดำเนินการตามแผน

๒.๑๓ โรงพยาบาลน้ำเกลี้ยง มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๒.๑๔ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาลน้ำเกลี้ยง การพยายามเข้าถึงระบบโดยไม่ชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของ ระบบเทคโนโลยีสารสนเทศ จะถูก

ระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็น การกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของโรงพยาบาลน้ำเกลี้ยง จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. แนวทางปฏิบัติในการสำรองข้อมูล

๒.๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูล ระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

๒.๒ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบ ซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศ แต่ละระบบ

๒.๓ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดง ถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรอง ซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๔ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหา แนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละ ไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดรวมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มี ประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวัง ในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจ ความต้องการ ของ ผู้ใช้บริการ

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้ผ่าน การพิจารณาจาก คณะกรรมการอำนวยการและกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของโรงพยาบาลน้ำเกลี้ยง เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความ มั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทราบ และถือปฏิบัติอย่างเคร่งครัดต่อไป



(นายแพทย์อชิบ ลีธีระประเสริฐ)
ผู้อำนวยการโรงพยาบาลน้ำเกลี้ยง