แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลนาแห้ว พ.ศ. ๒๕๖๙

โรงพยาบาลนาแห้ว
อำเภอนาแห้ว จังหวัดเลย

บันทึกข้อความ

ส่วนราชการ กลุ่มงานสุขภาพดิจิทัลฯ โรงพยาบาลนาแห้ว อ.นาแห้ว จ.เลย โทร. ๐๔๒ ๘๙๗๐๓๙

ที่ ลย ๐๐๓๓.๓๐๑/พิเศษ **วันที่** ๑๒ มกราคม ๒๕๖๙

เรื่อง พิจารณาลงนามประกาศแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เรียน ผู้อำนวยการโรงพยาบาลนาแห้ว

๑. ความเป็นมา

ด้วยโรงพยาบาลนาแห้วเล็งเห็นความสำคัญของการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย มีประสิทธิภาพ และสอดคล้องกับกฎหมายที่เกี่ยวข้อง เพื่อป้องกันภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อการบริการและสิทธิของผู้ป่วย

๒. ข้อเท็จจริง

เพื่อให้บุคลากรทุกระดับและผู้เกี่ยวข้องมีแนวทางปฏิบัติที่ชัดเจนและเป็นไปในทิศทางเดียวกัน งานศูนย์เทคโนโลยีสารสนเทศจึงได้จัดทำร่างประกาศโรงพยาบาลนาแห้ว เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ โดยมีเนื้อหาครอบคลุมการควบคุมการเข้าถึงข้อมูล การรักษาความลับ และความรับผิดชอบต่อสินทรัพย์ของโรงพยาบาล

๓. ข้อเสนอเพื่อพิจารณา

เพื่อให้แนวปฏิบัติดังกล่าวมีผลบังคับใช้ในหน่วยงาน จึงเห็นควรเสนอผู้อำนวยการเพื่อโปรดพิจารณาลงนามในประกาศที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณาลงนาม

(นางสาวอรปรียา หุมคำ)
ตำแหน่ง นักวิชาการคอมพิวเตอร์
ผู้จัดทำและเสนอ

การพิจารณาและอนุมัติ

๑. หัวหน้ากลุ่มงาน	๒. ผู้บริหารสารสนเทศ (CISO)	๓. ผู้อำนวยการ
☑ ตรวจสอบแล้ว	☑ ตรวจสอบเนื้อหาแล้ว	☑ อนุมัติและลงนามแล้ว
☑ เห็นควรเสนอเพื่อพิจารณา	☑ เห็นควรอนุมัติ	☐ อื่นๆ.....
(นางสาวปัทมาวดี มูลที)	(นางสาววัชรวรรณ ขอบคุณ)	(นายอมร จันทร์ดำ)
หัวหน้ากลุ่มงานดิจิทัลทางการแพทย์และสุขภาพ	ผู้บริหารสารสนเทศ (CISO)	ผู้อำนวยการโรงพยาบาลนาแห้ว
วันที่ 12/01/2569	วันที่ 12/01/2569	วันที่ 12/01/2569

ประกาศโรงพยาบาลนาแห้ว
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปีงบประมาณ ๒๕๖๙

เพื่อให้การบริหารจัดการระบบสารสนเทศของโรงพยาบาลนาแห้ว มีความมั่นคงปลอดภัย มีประสิทธิภาพ และสอดคล้องกับกฎหมายที่เกี่ยวข้อง โรงพยาบาลนาแห้วจึงกำหนดแนวปฏิบัติให้บุคลากรและผู้เกี่ยวข้องถือปฏิบัติอย่างเคร่งครัด ดังนี้

๑. วัตถุประสงค์

ประกาศฉบับนี้มีวัตถุประสงค์เพื่อเผยแพร่แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลนาแห้ว พ.ศ. ๒๕๖๙ ให้บุคลากรทุกระดับในหน่วยงาน และผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบ เข้าใจ และถือปฏิบัติอย่างเคร่งครัด

๒. การยกเลิกและทดแทนระเบียบเดิม

บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ความในประกาศนี้แทน

๓. การบังคับใช้แนวปฏิบัติ

ให้บุคลากรทุกระดับของโรงพยาบาลนาแห้ว รวมถึงบุคคลภายนอกที่เข้ามาปฏิบัติงานเชื่อมต่อกับระบบสารสนเทศของโรงพยาบาล ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลนาแห้ว พ.ศ. ๒๕๖๙ ตามที่แนบท้ายประกาศนี้อย่างเคร่งครัด

๔. บทลงโทษ

หากมีการฝ่าฝืนหรือไม่ปฏิบัติตามแนวปฏิบัตินี้ จนก่อให้เกิดความเสียหายแก่ทางราชการ หรือละเมิดต่อสิทธิของผู้อื่น โรงพยาบาลจะพิจารณาโทษทางวินัยและดำเนินการตามกฎหมายที่เกี่ยวข้องต่อไป

๕. การมีผลบังคับใช้

ประกาศนี้ให้มีผลบังคับใช้ตั้งแต่วันที่ประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๒ มกราคม พ.ศ. ๒๕๖๙

นายอมร จันทร์ดำ
นายแพทย์เชี่ยวชาญ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลนาแห้ว

แบบฟอร์มการขอเผยแพร่ข้อมูลผ่านเว็บไซต์ของหน่วยงานในราชการบริหารส่วนกลาง
สำนักงานปลัดกระทรวงสาธารณสุข
ตามประกาศสำนักงานปลัดกระทรวงสาธารณสุข
เรื่อง แนวทางการเผยแพร่ข้อมูลต่อสาธารณะผ่านเว็บไซต์ของหน่วยงาน พ.ศ. ๒๕๖๑
สำหรับหน่วยงานในราชการบริหารส่วนกลางสำนักงานปลัดกระทรวงสาธารณสุข

แบบฟอร์มการขอเผยแพร่ข้อมูลผ่านเว็บไซต์ของหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

ชื่อหน่วยงาน.....โรงพยาบาลนาแห้ว.....

วัน/เดือน/ปี.....๑๒ มกราคม ๒๕๖๙.....

หัวข้อ.... เผยแพร่ประกาศโรงพยาบาลนาแห้ว เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปีงบประมาณ ๒๕๖๙

รายละเอียดข้อมูล

ตามเอกสารแนบ

Link ภายนอก..... https://nahaeo-hospital.blogspot.com/.....

หมายเหตุ.....

ผู้รับผิดชอบการให้ข้อมูล	**ผู้อนุมัติรับรอง**
(นางสาวปัทมาวดี มูลที)	(นายอมร จันทร์ดำ)
เจ้าพนักงานเวชสถิติชำนาญงาน	นายแพทย์เชี่ยวชาญ รักษาการในตำแหน่ง
หัวหน้ากลุ่มงานดิจิทัลทางการแพทย์และสุขภาพ	ผู้อำนวยการโรงพยาบาลนาแห้ว
วันที่ ๑๒ เดือน มกราคม พ.ศ. ๒๕๖๙	วันที่ ๑๒ เดือน มกราคม พ.ศ. ๒๕๖๙

ผู้รับผิดชอบการนำข้อมูลขึ้นเผยแพร่

(นางสาวอรปรียา หุมคำ)
นักวิชาการคอมพิวเตอร์
วันที่ ๑๒ เดือน มกราคม พ.ศ. ๒๕๖๙

คำนำ

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญอย่างยิ่งในการขับเคลื่อนระบบบริการสุขภาพของโรงพยาบาลนาแห้ว ข้อมูลสุขภาพของผู้ป่วยถือเป็นสินทรัพย์ดิจิทัลที่มีค่าและต้องได้รับความคุ้มครองสูงสุด ดังนั้นการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจึงไม่ใช่เพียงหน้าที่ของเจ้าหน้าที่ไอทีเท่านั้น แต่เป็นความรับผิดชอบร่วมกันของบุคลากรทุกระดับ เอกสารฉบับนี้จัดทำขึ้นเพื่อใช้เป็น "แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙" โดยมีเนื้อหาครอบคลุมทั้ง ๘ หมวดหลัก ตั้งแต่การควบคุมการเข้าถึงข้อมูล การบริหารจัดการสินทรัพย์ ไปจนถึงการรับมือกับภัยคุกคามทางไซเบอร์ เพื่อให้เป็นไปตามมาตรฐานสากลและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาลนาแห้วหวังเป็นอย่างยิ่งว่า แนวปฏิบัติฉบับนี้จะเป็นเครื่องมือสำคัญในการป้องกันความเสี่ยง และช่วยให้การดำเนินภารกิจของโรงพยาบาลเป็นไปอย่างต่อเนื่อง มั่นคงปลอดภัย และได้รับความไว้วางใจจากผู้รับบริการสืบไป

โรงพยาบาลนาแห้ว
มกราคม 2569

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของโรงพยาบาลนาแห้ว พ.ศ. ๒๕๖๙

ตามประกาศโรงพยาบาลนาแห้ว เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลนาแห้ว กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลนาแห้ว เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลนาแห้วเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาลนาแห้ว นั้น

โรงพยาบาลนาแห้ว จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

คำนิยาม

“หน่วยงาน” หมายถึง โรงพยาบาลนาแห้ว รวมถึงหน่วยงานภายในทุกกลุ่มงาน ที่อยู่ภายใต้สังกัดของโรงพยาบาลนาแห้ว

"ผู้ใช้งาน" หมายถึง ข้าราชการ ลูกจ้าง พนักงานราชการ พนักงานกระทรวงสาธารณสุข ผู้ดูแลระบบ ผู้รับบริการ หรือบุคคลใดก็ตามที่ได้รับอนุญาตให้เข้าใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

"ผู้บริหารระดับสูงสุด" หมายถึง ผู้อำนวยการโรงพยาบาลนาแห้ว หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติราชการแทนในขณะนั้น

"ผู้บริหาร" หมายถึง ผู้มีอำนาจในการบังคับบัญชาและสั่งการในหน่วยงาน ได้แก่ ผู้อำนวยการ, รองผู้อำนวยการ, หัวหน้ากลุ่มงาน, หัวหน้าฝ่าย และหัวหน้างาน

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO/CISO)" หมายถึง ผู้บริหารที่ได้รับมอบหมายให้รับผิดชอบการกำหนดนโยบาย วางแผน และกำกับดูแลความมั่นคงปลอดภัยสารสนเทศในภาพรวมขององค์กร

"ผู้ดูแลระบบ" (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีหน้าที่รับผิดชอบในการดูแลรักษา บริหารจัดการระบบคอมพิวเตอร์ ระบบฐานข้อมูล และระบบเครือข่ายของโรงพยาบาล

"เจ้าของข้อมูล" หมายถึง ผู้ที่ได้รับมอบอำนาจให้รับผิดชอบข้อมูลในแต่ละระบบงาน โดยเป็นผู้มีส่วนได้ส่วนเสียหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดความเสียหายหรือสูญหาย

"สิทธิของผู้ใช้งาน" หมายถึง ขอบเขตการอนุญาตในการเข้าถึงหรือใช้งานระบบสารสนเทศ ซึ่งอาจประกอบด้วยสิทธิทั่วไป สิทธิจำเพาะ หรือสิทธิพิเศษตามความจำเป็นในการปฏิบัติงาน

"สินทรัพย์" หมายถึง ข้อมูลอิเล็กทรอนิกส์ ระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และทรัพย์สินทางด้านเทคโนโลยีและการสื่อสารทั้งหมดที่หน่วยงานถือครอง

"ระบบเครือข่าย" หมายถึง ระบบเชื่อมต่อเพื่อการสื่อสารและส่งผ่านข้อมูลระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ทั้งในรูปแบบเครือข่ายแบบมีสาย (LAN) และเครือข่ายแบบไร้สาย (Wireless LAN)

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง กระบวนการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้ ทั้งในทางอิเล็กทรอนิกส์และทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การรักษาไว้ซึ่งความลับ(Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง สถานการณ์ที่บ่งชี้ว่าอาจมีการฝ่าฝืนนโยบายความปลอดภัย หรือเกิดความล้มเหลวของมาตรการป้องกันที่อาจส่งผลกระทบต่อระบบเครือข่ายและบริการ

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง เหตุการณ์ที่เกิดขึ้นโดยไม่ได้คาดการณ์ไว้ ซึ่งอาจส่งผลให้ระบบถูกบุกรุก โจมตี หรือทำให้ความมั่นคงปลอดภัยของข้อมูลถูกคุกคาม

หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมและบริหารจัดการการเข้าถึงข้อมูลและอุปกรณ์ประมวลผล โดยคำนึงถึงประสิทธิภาพการใช้งานและความมั่นคงปลอดภัยเป็นสำคัญ

๒. เพื่อกำหนดเกณฑ์และมาตรฐานในการอนุญาต การกำหนดสิทธิ์ และการมอบอำนาจให้แก่บุคลากรอย่างชัดเจน

๓. เพื่อสร้างความตระหนักและส่งเสริมให้ผู้ใช้งานปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัด เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในภาพรวม

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑ การอนุญาตเข้าใช้ระบบ

- ผู้ดูแลระบบจะดำเนินการเปิดสิทธิ์ให้ผู้ใช้งานเข้าถึงระบบสารสนเทศได้ต่อเมื่อได้รับการอนุมัติจากผู้บริหาร เจ้าของข้อมูล หรือผู้รับผิดชอบระบบตามความจำเป็นต่อภารกิจเท่านั้น

ข้อ ๒ การเข้าถึงของบุคคลภายนอก

- บุคคลภายนอกที่ต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลนาแห้ว ต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรเสนอต่อผู้อำนวยการหรือผู้บริหารที่ได้รับมอบหมาย เพื่อพิจารณาให้ความเห็นชอบก่อนการดำเนินการใดๆ

ข้อ ๓ การกำหนดสิทธิ์และการทบทวนสิทธิ์

- กำหนดสิทธิ์การเข้าถึงข้อมูลให้สอดคล้องกับหน้าที่ความรับผิดชอบ (Role-based Access Control) และต้องมีการทบทวนสิทธิ์อย่างสม่ำเสมอ โดยแบ่งกลุ่มสิทธิ์ดังนี้

๑. สิทธิ์อ่านอย่างเดียว (Read Only): สำหรับการเรียกดูข้อมูลโดยไม่สามารถแก้ไขได้

๒. สิทธิ์สร้างและป้อนข้อมูล (Create/Input): สำหรับการบันทึกข้อมูลใหม่เข้าสู่ระบบ

๓. สิทธิ์แก้ไขและอนุมัติ (Edit/Approve): สำหรับผู้มีอำนาจตรวจสอบและยืนยันความถูกต้อง

๔. ไม่มีสิทธิ์ (No Access): สำหรับส่วนงานที่ไม่เกี่ยวข้องกับภารกิจ

- ผู้ดูแลระบบต้องติดตั้งระบบบันทึกเหตุการณ์ (Application Logs) เพื่อติดตามการใช้งานและตรวจสอบการละเมิดความปลอดภัยอย่างต่อเนื่อง

ข้อ ๔ การจัดชั้นความลับและประเภทข้อมูล

โรงพยาบาลนาแห้วยึดตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ในการจัดการข้อมูลดังนี้

- การจัดชั้นความลับ

๑. ลับที่สุด (Top Secret): ข้อมูลที่หากเปิดเผยจะก่อให้เกิดความเสียหายร้ายแรงที่สุด

๒. ลับมาก (Secret): ข้อมูลที่หากเปิดเผยจะก่อให้เกิดความเสียหายร้ายแรงมาก

๓. ลับ (Confidential): ข้อมูลที่หากเปิดเผยจะก่อให้เกิดความเสียหายต่อหน่วยงาน

๔. ทั่วไป: ข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้ตามความเหมาะสม

- การจัดประเภทข้อมูล

๑. ข้อมูลด้านการบริหาร: นโยบาย, แผนยุทธศาสตร์, ข้อมูลบุคลากร, งบประมาณและการเงิน

๒. ข้อมูลด้านการแพทย์และสาธารณสุข: ประวัติการรักษาพยาบาล, ผลตรวจทางห้องปฏิบัติการ และข้อมูลส่วนบุคคลของผู้ป่วย

ข้อ ๕ มาตรการควบคุมทางเทคนิค

- ผู้ใช้งานทุกคนต้องมีบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เฉพาะบุคคลในการเข้าถึงข้อมูลแต่ละชั้นความลับ

- การรับ-ส่งข้อมูลสำคัญผ่านเครือข่ายสารสนเทศ ต้องมีการเข้ารหัสข้อมูล (Encryption) ด้วยมาตรฐานสากล เช่น SSL หรือ VPN

ข้อ ๖ การบริหารจัดการสภาพแวดล้อมทางกายภาพ (Data Center)

- ระบบสนับสนุน: ต้องมีระบบสำรองไฟฟ้า (UPS), เครื่องกำเนิดไฟฟ้าสำรอง และระบบควบคุมอุณหภูมิ/ความชื้นที่เพียงพอ

- ความปลอดภัยทางกายภาพ: อุปกรณ์สำคัญต้องติดตั้งในพื้นที่หวงห้ามซึ่งจำกัดการเข้าถึงเฉพาะผู้ได้รับอนุญาต สายสัญญาณเครือข่ายต้องร้อยท่อเพื่อป้องกันความเสียหายจากสัตว์กัดแทะและการดักจับสัญญาณ ต้องจัดทำแผนผังสายสัญญาณ (Network Diagram) และจัดเก็บสายในตู้ Rack ที่ปิดล็อกอย่างมิดชิด

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๗ การลงทะเบียนและสิทธิ์ผู้ใช้งานใหม่

- จัดทำแบบฟอร์มลงทะเบียนขอเข้าใช้งานระบบเทคโนโลยีสารสนเทศอย่างเป็นทางการ

- ผู้ดูแลระบบต้องดำเนินการตรวจสอบความถูกต้องและป้องกันการลงทะเบียนซ้ำซ้อน

- การจัดสรรสิทธิ์ในการเข้าถึงข้อมูลต้องสอดคล้องกับบทบาทและหน้าที่ความรับผิดชอบ (Role-based Access) ผู้ใช้งานต้องได้รับเอกสารแจ้งสิทธิ์ หน้าที่ และความรับผิดชอบในการเข้าถึงระบบเป็นลายลักษณ์อักษร

ข้อ ๘ การควบคุมการใช้งานระบบสารสนเทศที่สำคัญ

- ครอบคลุมระบบคอมพิวเตอร์แอปพลิเคชัน (HIS), ระบบเครือข่ายไร้สาย (Wi-Fi) และอินเทอร์เน็ต การเปิดสิทธิ์การใช้งานต้องมุ่งเน้นเพื่อการปฏิบัติภารกิจในหน้าที่เท่านั้น และต้องได้รับความเห็นชอบจากผู้บริหารระดับสูงเป็นลายลักษณ์อักษร

ข้อ ๙ การทบทวนสิทธิ์การเข้าใช้งาน (Review of User Access Rights)

- จัดให้มีกระบวนการตรวจสอบและทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสถานะบุคลากร

- ผู้ดูแลระบบประสานงานกับหัวหน้ากลุ่มงานเพื่อตรวจสอบรายชื่อผู้ถือครองสิทธิ์และปรับปรุงข้อมูลให้เป็นปัจจุบัน

- ในกรณีเจ้าหน้าที่โอนย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้างงาน ต้องดำเนินการเพิกถอนสิทธิ์ภายใน ๑ – ๒ วันทำการ

ข้อ ๑๐ การบริหารจัดการรหัสผ่าน (Password Management)

- ชื่อผู้ใช้งาน (Username) ต้องมีความเฉพาะตัวและไม่ซ้ำกันในระบบ

- การส่งมอบรหัสผ่านชั่วคราวต้องดำเนินการผ่านช่องทางที่ปลอดภัยและมีการยืนยันการรับรหัสจากผู้ใช้งานโดยตรง

- กำหนดจำนวนครั้งในการใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง หากเกินกว่าที่กำหนดระบบจะทำการระงับการเข้าถึงชั่วคราว

- ผู้ใช้งานต้องไม่บันทึกหรือจดรหัสผ่านไว้ในรูปแบบที่บุคคลอื่นสามารถเข้าถึงได้ง่าย

ข้อ ๑๑ การบริหารจัดการข้อมูลตามชั้นความลับ

- ผู้ดูแลระบบต้องกำหนดระเบียบปฏิบัติในการจัดเก็บ การเข้าถึง และการทำลายข้อมูลตามประเภทความลับอย่างชัดเจน

- การรับ-ส่งข้อมูลที่มีความสำคัญสูงผ่านเครือข่ายภายนอก ต้องได้รับการเข้ารหัสข้อมูล (Encryption) ตามมาตรฐานสากล

- เจ้าของข้อมูล (Data Owner) มีหน้าที่ร่วมทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลในความรับผิดชอบอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ การเชื่อมโยงระบบสารสนเทศกับหน่วยงานภายนอก

- การเชื่อมโยงข้อมูลกับหน่วยงานภายนอก หรือระดับกระทรวงฯ ต้องผ่านการประเมินความเสี่ยงและจุดอ่อนด้านความปลอดภัยก่อนการดำเนินการ

- ต้องมีมาตรการควบคุมข้อมูลส่วนบุคคลและข้อมูลลับอย่างรัดกุม โดยไม่อนุญาตให้เข้าถึงหรือใช้งานร่วมกันหากระบบไม่มีมาตรฐานการป้องกันที่เพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๓ แนวปฏิบัติเกี่ยวกับการใช้รหัสผ่าน

- ความรับผิดชอบส่วนบุคคล ผู้ใช้งานต้องเก็บรักษาบัญชี (Username) และรหัสผ่าน (Password) เป็นความลับส่วนบุคคล ห้ามเผยแพร่หรือใช้งานร่วมกับผู้อื่นโดยเด็ดขาด

- มาตรฐานความปลอดภัย รหัสผ่านต้องมีความยาวไม่น้อยกว่า ๑๒ ตัวอักษร ประกอบด้วย ตัวเลข ตัวอักษรภาษาอังกฤษตัวเล็ก ตัวอักษรภาษาอังกฤษตัวใหญ่ และอักขระพิเศษ และหลีกเลี่ยงข้อมูลที่เดาได้ง่าย เช่น ชื่อ-นามสกุล

- ข้อห้าม ห้ามจดบันทึกรหัสผ่านไว้ในที่เปิดเผย และห้ามใช้ระบบจดจำรหัสผ่านอัตโนมัติ (Save Password) บนเครื่องคอมพิวเตอร์ที่ใช้งาน

- การปรับปรุง ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อมีการแจ้งเตือนจากระบบ

ข้อ ๑๔ การรักษาความลับและความรับผิดชอบทางกฎหมาย

- การเข้ารหัสข้อมูล การจัดการข้อมูลที่เป็นความลับต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสากล

- ความรับผิดส่วนบุคคล การกระทำใดๆ ที่เกิดขึ้นภายใต้บัญชีผู้ใช้งาน (Username) ของบุคคลใด ให้ถือเป็นความรับผิดชอบของบุคคลนั้นตามกฎหมาย แม้การกระทำนั้นจะไม่ได้เกิดจากเจ้าของบัญชีก็ตาม

ข้อ ๑๕ การพิสูจน์ตัวตนและการใช้งานเครื่องคอมพิวเตอร์

- การเข้าใช้งาน ต้องทำการพิสูจน์ตัวตน (Login) ทุกครั้งก่อนเข้าใช้ระบบปฏิบัติการ ระบบเครือข่ายและอินเทอร์เน็ต

- การล็อกหน้าจอ ผู้ใช้งานต้องล็อกหน้าจอ (Lock Screen) ทุกครั้งเมื่อไม่อยู่ที่โต๊ะ

ข้อ ๑๖ การจัดการเอกสารและสื่ออิเล็กทรอนิกส์

- เอกสารความลับ เอกสารที่พิมพ์ออกจากเครื่องพิมพ์หรือไฟล์อิเล็กทรอนิกส์ที่มีความสำคัญ ต้องจัดเก็บในที่ปลอดภัย และทำลายทันทีเมื่อหมดความจำเป็นในการใช้งาน

- การคุ้มครองข้อมูล โรงพยาบาลนาแห้วเคารพในสิทธิส่วนบุคคล แต่ขอสงวนสิทธิ์ในการตรวจสอบข้อมูลหากคาดว่ามีความเกี่ยวข้องกับความปลอดภัยของหน่วยงานได้ตลอดเวลาโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

ข้อ ๑๗ ข้อห้ามในการใช้งานสินทรัพย์สารสนเทศ

- โปรแกรมต้องห้าม ห้ามใช้งานโปรแกรมประเภท Peer-to-Peer (เช่น BitTorrent)

- การใช้งานผิดวัตถุประสงค์ ห้ามใช้สินทรัพย์ของโรงพยาบาลเพื่อประโยชน์ทางการค้า หรือกระทำการที่ขัดต่อศีลธรรม กฎหมาย และความมั่นคงของประเทศ

- การละเมิดระบบ ห้ามลักลอบใช้งานรหัสของผู้อื่น ห้ามดักจับข้อมูลในเครือข่าย และห้ามติดตั้งอุปกรณ์ใดๆ เพิ่มเติมเพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๑๘ การควบคุมพื้นที่หวงห้าม

- ผู้ใช้งานต้องไม่เข้าไปในศูนย์ปฏิบัติการข้อมูลอิเล็กทรอนิกส์ (Data Center) หรือสถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

- ห้ามนำอุปกรณ์หรือชิ้นส่วนใด ๆ ออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๑๙ การใช้งานและลิขสิทธิ์

- ห้ามนำเครื่องมือหรืออุปกรณ์ส่วนตัวมาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานเพื่อประกอบธุรกิจส่วนตัวโดยเด็ดขาด

- ผู้ใช้งานต้องไม่ทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาต และห้ามเข้าถึง ใช้งาน หรือลบแฟ้มข้อมูลของผู้อื่นในทุกกรณี

ข้อ ๒๐ การทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูล

- ก่อนการกำจัดอุปกรณ์หรือส่งต่อให้ผู้อื่นใช้งาน ผู้ใช้งานต้องทำลายข้อมูลสำคัญด้วยเทคนิคการลบหรือเขียนทับข้อมูล (Wiping) เพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบ โดยกำหนดวิธีการทำลายตามประเภทสื่อบันทึกดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายข้อมูล
กระดาษ	ใช้เครื่องหั่นทำลายเอกสาร
Flash Drive	ทำลายข้อมูลตามมาตรฐาน DOD 5220.22-M หรือใช้วิธีการทุบ/บดให้เสียหาย
แผ่น CD/DVD	ใช้เครื่องหั่นทำลายเอกสาร
เทปบันทึกข้อมูล	ใช้วิธีการทุบ บดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์ (Hard Disk)	ทำลายข้อมูลตามมาตรฐาน DOD 5220.22-M หรือใช้วิธีการทุบ/บดให้เสียหาย

ข้อ ๒๑ ความรับผิดชอบต่อสินทรัพย์

- ผู้ใช้งานต้องดูแลรักษาความปลอดภัยของสินทรัพย์ที่ได้รับมอบหมายเสมือนเป็นทรัพย์สินของตนเอง
- การรับหรือคืนสินทรัพย์ต้องมีการบันทึกและตรวจสอบโดยเจ้าหน้าที่ที่ได้รับมอบหมายทุกครั้ง
- ห้ามให้บุคคลอื่นยืมสินทรัพย์ เว้นแต่จะได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน
- กรณีปฏิบัติงานนอกสถานที่ ผู้ใช้งานต้องรับผิดชอบดูแลสินทรัพย์ที่นำออกไปใช้งานอย่างเข้มงวด

ข้อ ๒๒ การชดใช้ความเสียหายและบทลงโทษ

- ผู้ใช้งานมีสิทธิใช้สินทรัพย์และระบบสารสนเทศเพื่อวัตถุประสงค์ในงานราชการของหน่วยงานเท่านั้น
- หากเกิดความชำรุดเสียหายหรือสูญหายของทรัพย์สินเนื่องจากความประมาทเลินเล่อ ผู้ใช้งานต้องชดใช้ค่าเสียหายตามมูลค่าทรัพย์สินนั้น
- ความเสียหายใด ๆ ที่เกิดจากการนำสินทรัพย์ไปใช้ในกิจกรรมที่ไม่ได้กำหนด ให้ถือเป็นความผิดส่วนบุคคลที่ผู้ใช้งานต้องรับผิดชอบ

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๒๓ มาตรการควบคุมการเข้า-ออกศูนย์ข้อมูล (Data Center)

(๑) ผู้ติดต่อภายนอก: ต้องแลกบัตรแสดงตน (เช่น บัตรประชาชน) กับเจ้าหน้าที่เพื่อรับบัตรผู้ติดต่อ (Visitor) และลงบันทึกในสมุด "บันทึกการเข้าออกพื้นที่" ทุกครั้ง

(๒) การนำอุปกรณ์เข้าพื้นที่: กรณีนำอุปกรณ์คอมพิวเตอร์เข้าปฏิบัติงานในห้องควบคุมเครือข่าย ต้องลงบันทึกรายละเอียดอุปกรณ์ในแบบฟอร์มขออนุญาตให้ชัดเจน

(๓) การตรวจสอบ: ผู้ดูแลระบบต้องตรวจสอบความถูกต้องของบันทึกการเข้า-ออกเป็นประจำ

ข้อ ๒๔ การขอเชื่อมต่อและใช้งานระบบเครือข่าย

- การนำอุปกรณ์มาเชื่อมต่อกับเครือข่ายของโรงพยาบาลนาแห้ว ต้องได้รับอนุมัติจากหัวหน้าหน่วยงานและกรอกแบบฟอร์ม "การขอเชื่อมต่อเครือข่าย" อย่างเคร่งครัด
- การขอใช้พื้นที่ Web Server หรือโดเมนย่อย (Sub Domain) ต้องทำเป็นหนังสือขออนุญาต และห้ามติดตั้งซอฟต์แวร์ที่ส่งผลกระทบต่อระบบส่วนรวม
- ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือดำเนินการใดๆ ต่ออุปกรณ์เครือข่ายส่วนกลาง (เช่น Router, Switch) โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๒๕ หน้าที่ของผู้ดูแลระบบในการควบคุมเครือข่าย

(๑) การจำกัดสิทธิ์: กำหนดสิทธิ์ให้ผู้ใช้งานเข้าถึงเฉพาะเครือข่ายที่ได้รับอนุญาต และจำกัดเส้นทางการเข้าถึงเครื่องแม่ข่าย (Server) ให้เป็นไปตามภารกิจ

(๒) ระบบป้องกันความปลอดภัย: เครือข่ายที่เชื่อมต่อภายนอกต้องผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall) และติดตั้งระบบตรวจจับมัลแวร์และระบบ IPS/IDS เพื่อเฝ้าระวังพฤติกรรมผิดปกติ

(๓) การพิสูจน์ตัวตน: การเข้าเครือข่ายผ่านอินเทอร์เน็ตต้อง Login และยืนยันตัวตนด้วยรหัสผ่านเพื่อตรวจสอบความถูกต้องก่อนทุกครั้ง

(๔) ข้อมูลโครงสร้างเครือข่าย: ต้องป้องกันไม่ให้บุคคลภายนอกมองเห็นหมายเลข IP Address ภายใน และจัดทำแผนผังเครือข่าย (Network Diagram) ให้เป็นปัจจุบันเสมอ

(๕) การจัดการอุปกรณ์: เก็บบัญชีการเชื่อมต่อ ระบุหมายเลข IP และตรวจสอบ IP Address ต้นทาง-ปลายทางของอุปกรณ์บนเครือข่ายได้

ข้อ ๒๖ การบริหารจัดการเครื่องแม่ข่ายและซอฟต์แวร์ระบบ

- ผู้ดูแลระบบรับผิดชอบการกำหนดค่าและเปลี่ยนแปลงซอฟต์แวร์ระบบ (Systems Software) บนเครื่องแม่ข่าย

- การติดตั้งหรือปรับปรุงซอฟต์แวร์ระบบงานต้องได้รับอนุมัติ และจัดเก็บซอร์สโค้ด (Source Code) ในที่ปลอดภัย

- ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ให้ระบุตัวบุคคลได้ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๒๗ การควบคุมเครือข่ายสำหรับผู้ใช้งานภายนอกและการเชื่อมต่อระยะไกล

- ผู้ใช้งานภายนอกที่ต้องการเข้าถึงเครื่องแม่ข่ายต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

- การเชื่อมต่อจากระยะไกล (Remote Login) ต้องระบุเหตุผลความจำเป็น ควบคุมช่องทาง (Port) อย่างรัดกุม และต้องพิสูจน์ตัวตนด้วยรหัสผ่านทุกครั้ง

- การใช้เครื่องมือตรวจสอบระบบ (Network Tools) ต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้เท่าที่จำเป็นเท่านั้น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๒๘ มาตรการด้านรหัสผ่านและการเข้าใช้งาน

- ผู้ใช้งานต้องลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง และห้ามให้ผู้อื่นใช้บัญชีร่วมกันโดยเด็ดขาด

- ผู้ใช้งานต้องลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่โต๊ะทำงาน

ข้อ ๒๙ การจัดการซอฟต์แวร์และลิขสิทธิ์

- ซอฟต์แวร์ที่โรงพยาบาลจัดเตรียมไว้ให้ถือเป็นทรัพย์สินราชการ ห้ามคัดลอก ติดตั้ง หรือถอดถอนโดยไม่ได้รับอนุญาต

- ห้ามติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ หากตรวจพบถือเป็นความผิดส่วนบุคคล

- ห้ามใช้ทรัพยากรทุกประเภทของโรงพยาบาลเพื่อประโยชน์ทางการค้าหรือกิจกรรมที่ผิดกฎหมาย

ข้อ ๓๐ การใช้โปรแกรมยูทิลิตี้ (System Utilities)

- การใช้งานโปรแกรมยูทิลิตี้ที่ส่งผลต่อระบบต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องจำกัดสิทธิ์เฉพาะผู้ที่จำเป็นเท่านั้น

ข้อ ๓๑ การกำหนดเวลาสิ้นสุดการใช้งาน (Session Time-out)

ระบบทั่วไปจะตัดการเชื่อมต่ออัตโนมัติเมื่อไม่มีการใช้งานเกิน ๓๐ นาที

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application Access Control)

ข้อ ๓๒ การจัดการสิทธิ์และข้อมูลตามชั้นความลับ

- การเข้าถึงข้อมูลผู้ป่วยและข้อมูลส่วนบุคคลต้องผ่านการพิสูจน์ตัวตนอย่างเข้มงวด
- ข้อมูลสำคัญที่ส่งผ่านเครือข่ายสาธารณะหรืออุปกรณ์พกพาต้องมีการเข้ารหัส (Encryption) ตามมาตรฐาน
- ต้องสำรองข้อมูลและทดสอบการกู้คืนระบบอย่างสม่ำเสมอตามรอบที่กำหนด

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และการป้องกันมัลแวร์ (Malware Prevention)

ข้อ ๓๓ มาตรการป้องกันไวรัสและโปรแกรมไม่ประสงค์ดี

- คอมพิวเตอร์ทุกเครื่องต้องติดตั้งโปรแกรม Antivirus และ Update Patch ให้เป็นปัจจุบันเสมอ
- ห้ามเชื่อมต่อเครื่องที่ติดไวรัสเข้าสู่เครือข่าย และต้องแจ้งผู้ดูแลระบบทันที
- ห้ามพัฒนาหรือเผยแพร่โปรแกรมที่มีลักษณะทำลายกลไกรักษาความปลอดภัยของระบบ

ข้อ ๓๔ การจ้างหน่วยงานภายนอกพัฒนาซอฟต์แวร์ (Outsource)

- ผู้รับจ้างต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (NDA) และต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยของโรงพยาบาลนาแห้วอย่างเคร่งครัด

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๓๕ มาตรการทำงานระยะไกล

- การเข้าถึงระบบจากภายนอกต้องผ่านการพิสูจน์ตัวตนและเชื่อมต่อผ่านช่องทางที่ปลอดภัย
- อุปกรณ์ส่วนตัวที่นำมาใช้ต้องผ่านการตรวจสอบมาตรฐานความปลอดภัยตามที่หน่วยงานกำหนด

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN)

ข้อ ๓๖ ความปลอดภัยของ Wi-Fi

- ผู้ดูแลระบบต้องซ่อนชื่อเครือข่าย (SSID) สำหรับระบบงานสำคัญ และเข้ารหัสข้อมูลด้วยมาตรฐาน WPA2/WPA3 หรือสูงกว่า
- ต้องลงทะเบียนอุปกรณ์ (MAC Address) และมีระบบ Firewall กั้นระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน

ส่วนที่ ๑๑ การควบคุมอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๓๗ นโยบายการกำหนดค่า Firewall

- กำหนดค่าเริ่มต้นเป็น "ปฏิเสธทั้งหมด" (Deny All) และอนุญาตเฉพาะบริการที่จำเป็นต่อภารกิจเท่านั้น

- จัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) จาก Firewall ไม่น้อยกว่า ๙๐ วัน ตามที่กฎหมายกำหนด

- การขอเปิดพอร์ต (Port) พิเศษ ต้องทำเป็นหนังสือขออนุมัติต่อ CIO/CISO โดยระบุวัตถุประสงค์และหมายเลข IP ให้ชัดเจน

- ตรวจสอบและปิดพอร์ตที่ไม่มีความจำเป็นอย่างน้อยสัปดาห์ละ ๑ ครั้ง

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

ข้อ ๓๘ มาตรการความปลอดภัยในการใช้ E-Mail

(๑) การเข้าใช้งาน: ต้องลงทะเบียนขอใช้บัญชีอย่างเป็นทางการ รหัสผ่านต้องไม่ปรากฏเป็นตัวอักษรขณะพิมพ์ และต้องเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน

(๒) การส่งข้อมูล: ห้ามระบุความลับลงในหัวข้อจดหมาย หากเป็นข้อมูลสำคัญต้องเข้ารหัส (Encryption) และระบุชื่อผู้ส่งในจดหมายทุกฉบับ

(๓) ข้อห้าม: ห้ามส่งจดหมายขยะ (Spam), จดหมายลูกโซ่ (Chain Letter), ข้อมูลละเมิดกฎหมาย หรือเจตนาส่งไวรัส

(๔) การป้องกันมัลแวร์: ต้องตรวจสอบเอกสารแนบด้วยโปรแกรม Antivirus ก่อนเปิดเสมอ ห้ามเปิดจดหมายจากผู้ส่งที่ไม่รู้จัก

(๕) จดหมายอิเล็กทรอนิกส์ภาครัฐ: ให้ใช้ E-Mail ภาครัฐ (เช่น @moph.go.th หรือ Mailgo.th) ในการติดต่อราชการตามมติคณะรัฐมนตรี

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๓๙ แนวปฏิบัติการใช้เครือข่ายอินเทอร์เน็ต

(๑) ช่องทางเชื่อมต่อ: ต้องผ่านระบบรักษาความปลอดภัย (Firewall) ของโรงพยาบาลเท่านั้น ห้ามเชื่อมต่อผ่านช่องทางอื่นโดยไม่ได้รับอนุญาต

(๒) ข้อห้ามการใช้งาน: ห้ามใช้เพื่อธุรกิจส่วนตัว หรือกระทำการที่ส่งผลกระทบต่อความมั่นคงของชาติและสถาบันพระมหากษัตริย์

(๓) สื่อสังคมออนไลน์: ให้ปฏิบัติตามนโยบาย Social Media Policy ของโรงพยาบาล ไม่โพสต์ข้อมูลเท็จหรือข้อมูลที่ทำให้หน่วยงานเสื่อมเสียชื่อเสียง

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ ๔๐ มาตรการดูแลคอมพิวเตอร์ส่วนบุคคล

(๑) ลิขสิทธิ์ซอฟต์แวร์: ห้ามคัดลอกหรือติดตั้งโปรแกรมที่ไม่มีลิขสิทธิ์ หากตรวจซ่อมต้องดำเนินการโดยเจ้าหน้าที่ศูนย์ไอทีเท่านั้น

(๒) การป้องกัน: ต้องสแกนไวรัสสื่อบันทึกพกพา (Flash Drive) ก่อนใช้งานทุกครั้ง

(๓) การสำรองข้อมูล: เจ้าหน้าที่ศูนย์ไอทีมีหน้าที่สำรองข้อมูลสำคัญ (Backup) ลงสื่อบันทึกภายนอก และทดสอบการกู้คืนอย่างสม่ำเสมอ

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ ๔๑ การดูแลและรักษาความปลอดภัยคอมพิวเตอร์แบบพกพา

(๑) การดูแลทางกายภาพ: ระมัดระวังการตกกระแทก ความร้อน และความชื้น ไม่วางเครื่องทิ้งไว้ในที่สาธารณะเพื่อป้องกันการสูญหาย

(๒) การเข้าถึง: ต้องกำหนดรหัสผ่านในการเข้าเครื่อง และทำการ Logout ทุกครั้งเมื่อเลิกใช้งาน

ส่วนที่ ๑๖ การตรวจจับการบุกรุก (IDS/IPS Policy)

ข้อ ๔๒ ระบบเฝ้าระวังและการตอบสนองต่อเหตุการณ์

- ระบบที่เชื่อมต่ออินเทอร์เน็ตทั้งหมดต้องผ่านการตรวจสอบจาก IDS/IPS และมีการ Update Signature ให้เป็นปัจจุบันเสมอ

-ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ผิดปกติทุกวัน และเก็บบันทึกข้อมูล (Logs) ไว้ไม่น้อยกว่า ๙๐ วัน

- สิทธิ์ในการระงับ โรงพยาบาลมีสิทธิ์ยุติการเชื่อมต่อเครื่องที่มีพฤติกรรมเสี่ยงทันทีโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Configuration)

ข้อ ๔๓ มาตรฐานการติดตั้งระบบและฐานข้อมูล

(๑) ระบบปฏิบัติการ: ต้องกำหนดชื่อเครื่อง, IP Address และ Update Patch ความปลอดภัยทันทีหลังติดตั้ง

(๒) ระบบฐานข้อมูล: จำกัดสิทธิ์ผู้บริหารฐานข้อมูล (DBA) และเชื่อมต่อระบบงานให้ทำงานได้อย่างมีประสิทธิภาพพร้อมเกณฑ์การสำรองข้อมูลที่ชัดเจน

ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๔๔ มาตรการจัดเก็บ Log File

(๑) ความถูกต้อง: ต้องจัดเก็บ Log ในสื่อที่รักษาความครบถ้วน ถูกต้อง และห้ามแก้ไขเปลี่ยนแปลงข้อมูลโดยเด็ดขาด

(๒) ระยะเวลา: เก็บบันทึก Application Logs และการเข้า-ออกระบบไว้ไม่น้อยกว่า ๙๐ วัน ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(๓) การเข้าถึง: จำกัดสิทธิ์การเข้าถึง Log เฉพาะบุคคลที่เกี่ยวข้องเพื่อป้องกันการรั่วไหลหรือการแก้ไข

หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

- เพื่อให้ระบบสารสนเทศสามารถให้บริการได้อย่างต่อเนื่องและข้อมูลมีความถูกต้องแม่นยำตามมาตรฐานความปลอดภัย

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑ การบริหารจัดการสิทธิ์: ผู้ดูแลระบบต้องจัดทำบัญชีฐานข้อมูลและกำหนดสิทธิ์การใช้งาน (เช่น อ่านอย่างเดียว, แก้ไข, อนุมัติ) ตามหน้าที่ความรับผิดชอบ และต้องมีการขออนุญาตเป็นลายลักษณ์อักษร

ข้อ ๒ การจัดชั้นความลับ: แบ่งระดับความสำคัญของข้อมูลตามระเบียบสำนักนายกรัฐมนตรี (ลับที่สุด, ลับมาก, ลับ, ทั่วไป) และจำแนกประเภทข้อมูล (ข้อมูลบริหาร และ ข้อมูลทางการแพทย์) ให้ชัดเจน

ข้อ ๓ การตรวจสอบ: เจ้าของฐานข้อมูลต้องจัดให้มีแฟ้มลงบันทึกการใช้งาน (Log File) เพื่อใช้ตรวจสอบความถูกต้องและป้องกันการเข้าถึงโดยมิชอบ

ข้อ ๔ การใช้ข้อมูลร่วมกับหน่วยงานภายนอก: ต้องจัดทำข้อตกลง (MOU/Contract) กำหนดมาตรฐานทางเทคนิคและหน้าที่ความรับผิดชอบในการป้องกันข้อมูลสูญหาย

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๕ การจัดทำระบบสำรอง คัดเลือกระบบงานที่สำคัญเพื่อทำระบบสำรองให้พร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ มาตรฐานการสำรองข้อมูล ต้องกำหนดความถี่ รูปแบบ และมีการบันทึกกิจกรรมการสำรองข้อมูลทุกครั้ง โดยจัดเก็บสื่อบันทึกข้อมูลไว้ นอกสถานที่ (Off-site Storage) ในระยะที่ปลอดภัยจากภัยพิบัติ

ข้อ ๗ การกู้คืนข้อมูล: ต้องทดสอบประสิทธิภาพการกู้คืนข้อมูล (Restore Test) อย่างน้อยปีละ ๑ ครั้ง และเข้ารหัสข้อมูลลับที่ได้สำรองไว้

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินระดับความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ

๒. เพื่อป้องกันและลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

๓. เพื่อให้หน่วยงานมีแนวทางปฏิบัติที่ชัดเจนในการจัดการภัยคุกคามด้านเทคโนโลยี

แนวปฏิบัติ

ข้อ ๑ การประเมินความเสี่ยงประจำปี

- ให้ผู้ตรวจสอบภายใน (Internal Auditor) ดำเนินการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง ครอบคลุมภัย ๔ ประเภทหลัก ได้แก่ ภัยจากบุคคล (Human Error), ภัยจากซอฟต์แวร์ (Malware), ภัยจากระบบไฟฟ้า/อัคคีภัย และภัยจากอุทกภัย
- จัดทำรายงานสรุปผลพร้อมข้อเสนอแนะในการลดระดับความเสี่ยงเสนอต่อผู้บริหาร

ข้อ ๒ มาตรการและข้อจำกัดในการตรวจประเมิน

- กำหนดสิทธิ์ให้ผู้ตรวจสอบเข้าถึงข้อมูลที่จำเป็นในรูปแบบ "อ่านได้อย่างเดียว (Read Only)" เท่านั้น
- กรณีต้องใช้เครื่องมือพิเศษในการตรวจสอบ (Audit Tools) ต้องแยกการติดตั้งออกจากระบบที่ให้บริการจริง (Production System) เพื่อไม่ให้กระทบต่อการทำงานตามปกติของโรงพยาบาล

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

๑. เพื่อกำหนดมาตรการควบคุมการเข้าถึงพื้นที่ติดตั้งอุปกรณ์สำคัญและระบบเครือข่าย

๒. เพื่อป้องกันความเสียหายต่อสินทรัพย์สารสนเทศจากสภาพแวดล้อมและบุคคลที่ไม่ได้รับอนุญาต

แนวปฏิบัติ

ข้อ ๑ มาตรฐานความปลอดภัยศูนย์ข้อมูล (Data Center)

- กำหนดให้ห้องควบคุมระบบเครือข่ายเป็นเขตหวงห้ามเด็ดขาด ต้องปิดล็อกประตูเสมอ
- ห้ามบันทึกภาพ และห้ามมีป้ายสัญลักษณ์ที่บ่งบอกความสำคัญของระบบเพื่อป้องกันการตกเป็นเป้าหมาย

ข้อ ๒ การควบคุมการเข้า-ออกพื้นที่สำคัญ

- บุคคลภายนอกหรือผู้มาติดต่อต้องแลกบัตรและลงบันทึกรายละเอียดการเข้า-ออกในสมุดบันทึกพื้นที่หวงห้ามอย่างละเอียด โดยต้องมีเจ้าหน้าที่กำกับดูแลตลอดระยะเวลาปฏิบัติงานจนเสร็จสิ้นภารกิจ

ข้อ ๓ ระบบสนับสนุนและโครงสร้างสายสัญญาณ

- ต้องติดตั้งระบบสำรองไฟฟ้า (UPS) และเครื่องกำเนิดไฟฟ้าสำรอง (Generator) ที่มีประสิทธิภาพ
-สายสัญญาณสื่อสารต้องร้อยท่อเพื่อป้องกันสัตว์กัดแทะและการดักจับสัญญาณ และต้องจัดทำแผนผังสายสัญญาณ (Network Diagram) ให้เป็นปัจจุบัน

หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัย

วัตถุประสงค์

๑. เพื่อเฝ้าระวังและวิเคราะห์รูปแบบการบุกรุกโจมตีระบบสารสนเทศ

๒. เพื่อให้สามารถระงับเหตุและแก้ไขสถานการณ์ความไม่ปลอดภัยได้อย่างทันท่วงที

แนวปฏิบัติ

ข้อ ๑ การเฝ้าระวังและตรวจสอบระบบ

- ผู้ดูแลระบบต้องตรวจสอบ Log File ของ Firewall และระบบ IDS/IPS อย่างน้อยเดือนละ ๑ ครั้ง เพื่อวิเคราะห์ความถี่และรูปแบบการโจมตี รวมถึงหมายเลขไอพีที่ต้องสงสัย

ข้อ ๒ การจัดการมัลแวร์และภัยคุกคามอินเทอร์เน็ต

- หากพบเครื่องคอมพิวเตอร์ติดมัลแวร์หรือมีพฤติกรรมส่งข้อมูลผิดปกติออกสู่ภายนอก ให้ระงับการเชื่อมต่อเครือข่ายทันที และดำเนินการล้างข้อมูลหรือแก้ไขโดยเจ้าหน้าที่ไอทีก่อนอนุญาตให้กลับมาใช้งาน

หมวดที่ ๖ การสร้างความตระหนัก (Security Awareness)

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบคอมพิวเตอร์อย่างปลอดภัยแก่บุคลากร

๒. เพื่อลดความเสี่ยงจากการกระทำความผิดที่เกิดจากความรู้เท่าไม่ถึงการณ์

แนวปฏิบัติ

ข้อ ๑ การฝึกอบรมและเผยแพร่ความรู้

- จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างน้อยปีละ ๑ ครั้ง และติดประกาศเกร็ดความรู้ด้าน IT Security เช่น วิธีการตั้งรหัสผ่านที่ปลอดภัย หรือการสังเกตอีเมลหลอกลวง (Phishing)

ข้อ ๒ ความตระหนักและความรับผิดชอบทางกฎหมาย

- ผู้ใช้งานต้องตระหนักถึงความรับผิดชอบส่วนบุคคลตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎระเบียบของโรงพยาบาล โดยความผิดที่เกิดขึ้นถือเป็นความรับผิดชอบส่วนบุคคล

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดบทบาทหน้าที่ของผู้เกี่ยวข้องทุกระดับในการรักษาความมั่นคงปลอดภัยสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ ระดับนโยบาย(CIO/CISO)

- รับผิดชอบกำหนดทิศทางนโยบาย อนุมัติงบประมาณด้านความปลอดภัย และกำกับดูแลภาพรวมความเสี่ยงของโรงพยาบาล

ข้อ ๒ ระดับบริหาร (หัวหน้ากลุ่มงาน/หัวหน้าศูนย์ IT)

- รับผิดชอบกำกับดูแลการปฏิบัติงานในหน่วยงาน วางแผนบริหารความเสี่ยง และควบคุมการเข้าถึงระบบฐานข้อมูลให้เป็นไปตามสิทธิ์ที่กำหนด

ข้อ ๓ ระดับปฏิบัติการ (เจ้าหน้าที่ IT)

- รับผิดชอบงานเชิงเทคนิค ได้แก่ การสำรองข้อมูล การเฝ้าระวังการเจาะระบบ ดูแลรักษาความสะอาดและอุณหภูมิในห้อง Server และให้การสนับสนุนผู้ใช้งาน

หมวดที่ ๘ การบริหารจัดการการใช้บริการจากหน่วยงานภายนอก (Outsource)

วัตถุประสงค์

- เพื่อให้การใช้บริการจากบริษัทภายนอกเป็นไปอย่างมั่นคงปลอดภัยและไม่กระทบต่อความลับขององค์กร

แนวปฏิบัติ

ข้อ ๑ การควบคุมการเข้าถึงระบบ

- ก่อนอนุญาตให้เข้าปฏิบัติงาน ต้องมีการประเมินความเสี่ยงและจัดทำสัญญาการรักษาความลับ (Non-Disclosure Agreement: NDA) ระหว่างโรงพยาบาลและหน่วยงานภายนอกเสมอ

ข้อ ๒ ข้อกำหนดในสัญญาจ้างและสิทธิ์การใช้งาน

- ในสัญญาจ้างต้องระบุรายละเอียดการให้บริการ (SLA), หน้าที่ความรับผิดชอบ และความเป็นเจ้าของลิขสิทธิ์ซอฟต์แวร์ที่พัฒนาขึ้นให้ชัดเจน

- ผู้ดูแลระบบต้องให้สิทธิ์เข้าถึงข้อมูลแก่หน่วยงานภายนอกเท่าที่จำเป็นต่อการปฏิบัติงานและกำหนดระยะเวลาการใช้งานให้ชัดเจน เมื่อเสร็จสิ้นภารกิจต้องยกเลิกสิทธิ์ทันที