เรื่อง มาตรการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ของศูนย์อนามัยที่ ๔ สระบุรี

เพื่อให้ศูนย์อนามัยที่ ๔ สระบุรี สามารถปฏิบัติตามประกาศนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ กรมอนามัย พ.ศ.๒๕๖๗ เรื่อง การควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงาน ได้อย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน ศูนย์อนามัยที่ ๔ สระบุรี จึงได้วางแนวทางและใช้ในมาตการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ของศูนย์อนามัยที่ ๔ สระบุรี โดยสาระสำคัญของแนวทางปฏิบัติฉบับนี้ ประกอบด้วย

๑. มาตรการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
๒. มาตรการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม
๓. มาตรการสำรองข้อมูล และการเตรียมพร้อมกรณีฉุกเฉิน
๔. มาตรการตอบสนองเหตุการณ์ความมั่นคงปลอดภัย ทางระบบสารสนเทศ
๕. มาตรการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

มาตรการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของหน่วยงานของรัฐ

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแนวปฏิบัติ

แนวทางปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อ ๒. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่ กรณีเพื่อให้ความเห็นชอบและอนุญาตก่อน

ข้อ ๓. การกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูล ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๔. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึงเวลาเข้าถึงและช่องทางการเข้าถึงไว้ให้ชัดเจน โดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์

ข้อ ๕. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๑. กำหนดให้ผู้ใช้งานแต่ละรายมีบัญชีผู้ใช้งาน (user account) เป็นของตนเอง เพื่อใช้ตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (identification and authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ และจะต้องทำการเปลี่ยนรหัสผ่านทันทีหลังจากที่ได้รับรหัสผ่านเริ่มต้น ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น หน่วยงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

(๑) รหัสผ่านจะต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร

(๒) ต้องประกอบด้วยตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษ เช่น ! @ # $ % เป็นต้น

ข้อ ๒. การบริหารจัดการบัญชีผู้ใช้งาน

(๑) กำหนดชื่อบัญชีผู้ใช้งานต้องไม่ซ้ำกัน

(๒) มีระบบการเข้ารหัส (encryption) รหัสผ่านที่บันทึกลงในแฟ้มข้อมูลเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

(๓) ผู้ดูแลระบบต้องส่งมอบบัญชีผู้ใช้งานและรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือช่องทางที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๔) กำหนดให้ผู้ใช้งานจะต้องทำการเปลี่ยนรหัสผ่านหลังจากที่มีการเข้าระบบ (Login) ครั้งแรก หรือหลังจากที่มีการรีเซ็ตรหัสผ่าน

(๕) ผู้ดูแลระบบมีหน้าที่ยกเลิกบัญชีผู้ใช้งานเมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง

ข้อ ๓. มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือมีการโยกย้ายเปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้าง โดยปฏิบัติตามแนวทางดังนี้

(๑) เจ้าหน้าที่งานทรัพยากรบุคคลจะต้องปรับปรุงสถานะของบุคลากรผ่านระบบสารสนเทศของหน่วยงาน เมื่อมีการโยกย้ายเปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้าง

(๒) ผู้ดูแลระบบจะต้องเข้ามาสำรวจรายชื่อในระบบสารสนเทศของหน่วยงานและระงับบัญชีผู้ใช้งานของบุคลากรที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้าง

(๓) ผู้ดูแลระบบจะต้องรวบรวมรายชื่อบัญชีผู้ใช้งานระบบสารสนเทศ ของบุคลากรที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้าง นำส่งให้กองดิจิทัลเพื่อส่งเสริมสุขภาพกรมอนามัย เพื่อทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศกรมอนามัย

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑. การใช้บัญชีผู้ใช้งานระบบสารสนเทศและรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่ออผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษรพิมพ์ใหญ่ (Uppercase character) ตัวอักษรพิมพ์เล็ก (Lowercase character) และตัวอักษรพิเศษ (Special character)

(๓) ไม่ควรกำหนดรหัสผ่านที่มีข้อมูลเกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น และควรหลีกเลี่ยงการใช้คำที่ตรงกับคำในพจนานุกรม หรือมีบัญชีชื่อผู้ใช้งานอยู่ในรหัสผ่าน

(๔) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕๖” เป็นต้น

(๕) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๖) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๗) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๘) ผู้ใช้งานทั่วไปควรเปลี่ยนรหัสผ่าน (Password) อย่างน้อยทุก ๆ ๖ เดือน ส่วนผู้ดูแลระบบควรเปลี่ยนรหัสผ่าน (Password) อย่างน้อยทุก ๆ ๓ เดือน

(๙) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำกับรหัสผ่านครั้งสุดท้าย

ข้อ ๒. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๓. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของหน่วยงาน และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย นำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๔. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึงวิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน แต่ละเครื่องต่าง ๆ มีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (BitTorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๕. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของหน่วยงาน

ข้อ ๖. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของหน่วยงาน

ข้อ ๗. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของหน่วยงาน โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๘. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ ๙. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๑๐. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

ข้อ ๑. ผู้ใช้งานต้องเป็นบุคลากรของหรับบุคคลภายศูนย์อนามัยที่ ๔ สระบุรี นอกจะต้องได้รับอนุญาตจากผู้บริหาร หรือผู้ที่ได้รับมอบหมาย

ข้อ ๒. ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (User Account) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อใช้งานระบบเครือข่ายของศูนย์อนามัยที่ ๔ สระบุรี และต้องไม่ให้ผู้อื่นใช้งานบัญชีผู้ใช้งาน (User Account) ของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้งาน (User Account) ต้องเป็นผู้รับผิดชอบ

ข้อ ๓. ผู้ใช้งานต้องรับผิดชอบต่อข้อมูลของตนเอง ไม่ว่าจะเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือการส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์

ข้อ ๔. ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์สินของหน่วยงานไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ เพื่อป้องกันการโจมตีจากแฮกเกอร์ (Hacker)

ข้อ ๕. ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของหน่วยงาน และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และที่แก้ไขเพิ่มเติม

ข้อ ๖. ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมที่ใช้สำหรับการควบคุมเครื่องคอมพิวเตอร์จากระยะไกล (Remote) เช่น AnyDesk, TeamViewer , RealVNC , LogMeIn , RemotePC เป็นต้น หากมีความจำเป็นต้องใช้งาน ให้แจ้งผู้ดูแลระบบมาติดตั้งโปรแกรมทุกครั้งและให้ถอนการติดตั้งทุกครั้งเมื่อใช้งานเรียบร้อยแล้ว

๕. แนวปฏิบัติการใช้งานอินเตอร์เน็ต (Internet Policy)

ข้อ ๑. ผู้ใช้งานต้องใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิ์ภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่ไม่ใช้งานระบบที่มีการใช้แบนด์วิดท์ (Bandwidth) สูงที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ ได้แก่ รายการบันเทิงต่าง ๆ ในเวลาราชการ

ข้อ ๒. ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาเกี่ยวกับทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย

ข้อ ๓. ห้ามแสดงความคิดเห็นในลักษณะที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากหน่วยงาน และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

ข้อ ๔. หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งานต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

มาตรการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบเครือข่าย อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลง ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูล และระบบข้อมูลของศูนย์อนามัยที่ ๔ สระบุรี และป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ

แนวทางปฏิบัติ

๑. การรักษาความมั่นคงปลอดภัยห้องควบคุมระบบเครือข่าย

ข้อ ๑. กำหนดให้ห้องควบคุมระบบเครือข่ายเป็นเขตหวงห้ามเด็ดขาด ห้ามผู้ที่ไม่มีหน้าที่เกี่ยวข้องเข้าพื้นที่โดยไม่ได้รับอนุญาต

ข้อ ๒. เป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า – ออก ของบุคคลเป็นจำนวนมาก มีทางเข้าออกได้ทางเดียว

ข้อ ๓. มีการปกปิดหรือปิดบังไม่ให้มองเห็นภายในห้องได้จากภายนอก

ข้อ ๔. ไม่ให้มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

ข้อ ๕. มีการปิดล็อกประตูและหน้าต่างตลอดเวลาที่ไม่มีผู้ปฏิบัติงานภายในห้อง

ข้อ ๖. มีการจัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณห้องควบคุมระบบเครือข่ายเพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๒. การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

ข้อ ๑. ผู้ที่เกี่ยวข้อง บทบาท และหน้าที่รับผิดชอบ

(๑) หัวหน้ากลุ่มขับเคลื่อนยุทธศาสตร์และพัฒนากำลังคน

- อนุมัติสิทธิเข้าออกพื้นที่ห้องควบคุมระบบเครือข่าย
- อนุมัติกระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

(๒) ผู้ดูแลห้องควบคุมระบบเครือข่าย

- ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบเครือข่าย ให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด
- ตรวจสอบความเรียบร้อยของสถานที่ การทำงานของระบบเครือข่าย และอุปกรณ์ที่เกี่ยวข้อง ภายหลังจากที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่ายเสร็จสิ้นแล้ว

ข้อ ๒. กระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

(๑) บุคคลที่ไม่ใช่ผู้ดูแลห้องควบคุมระบบเครือข่าย ที่มีความจำเป็นต้องเข้าปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย จะต้องแจ้งต่อผู้ดูแลห้องควบคุมระบบเครือข่าย และกรอกแบบฟอร์มขอเข้าห้องควบคุมระบบเครือข่ายก่อนเข้าปฏิบัติงานทุกครั้ง

(๒) ผู้ที่จะเข้าปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย สามารถเข้าปฏิบัติงานได้ในวันและเวลาราชการที่มีการทำงานตามปกติ (จันทร์-ศุกร์ เวลา ๘.๓๐ – ๑๖.๓๐ น. ยกเว้นวันหยุดราชการ) หากมีความจำเป็นต้องปฏิบัติงานนอกเวลาราชการ ให้แจ้งต่อหัวหน้ากลุ่มขับเคลื่อนยุทธศาสตร์และพัฒนากำลังคน เป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อย ๕ วันทำการ

(๓) กรณีที่มีเหตุฉุกเฉิน ที่มีความจำเป็นจะเข้าห้องควบคุมระบบเครือข่ายเร่งด่วน ให้แจ้งผู้ดูแลห้องควบคุมระบบเครือข่าย ทราบถึงเหตุผลและความจำเป็นในการเข้าไปใช้งาน

(๔) ห้ามนำอาหารและน้ำดื่ม เข้าห้องควบคุมระบบเครือข่าย

(๕) ห้ามถ่ายรูปภายในห้องก่อนได้รับอนุญาตจากผู้ดูแล

(๖) กรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าห้องควบคุมระบบเครือข่าย ผู้ดูแลห้องจะต้องมีการควบคุมอย่างรัดกุม

๓. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

ข้อ ๑. มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ดังต่อไปนี้

(๑) ระบบสำรองกระแสไฟฟ้า (UPS)

(๒) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

(๓) ระบบระบายอากาศ

(๔) ระบบปรับอากาศ ๒ ชุด ทำงานสลับกันตลอดเวลา

ข้อ ๒. มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสียงจากการล้มเหลวในการทำงานของระบบ

ข้อ ๓. มีถังดับเพลิงชนิดสารสะอาดสำหรับห้อง Data Center หรือห้องเซิร์ฟเวอร์ เพื่อใช้สำหรับการดังเพลิงเบื้องต้น โดยมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

มาตรการสำรองข้อมูล และการเตรียมพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

การสำรองข้อมูล และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบสารสนเทศสำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพในเวลาที่ต้องการ (availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูล รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

แนวทางปฏิบัติ

๑. การสำรองข้อมูล

ข้อ ๑. ผู้ที่เกี่ยวข้อง บทบาท และหน้าที่รับผิดชอบ

(๑) นายอนุพงศ์ กันธิมา ตำแหน่งนักวิชาการคอมพิวเตอร์ปฏิบัติการ
มีหน้าที่รับผิดชอบการสำรองข้อมูลระบบสารสนเทศของหน่วยงาน ครอบคลุมทุกขั้นตอน ตั้งแต่การจัดทำบัญชีระบบสารสนเทศ การทำแผนสำรองข้อมูล การจัดทำขั้นตอนการสำรองข้อมูล การสำรองข้อมูล การเก็บรักษาข้อมูล การทดสอบการกู้คืนระบบ และการจัดทำรายงานต่าง ๆ ที่เกี่ยวข้อง

(๒) นายเอกพจน์ ผดุงศักดิ์ ตำแหน่งเจ้าหน้าที่คอมพิวเตอร์
มีหน้าที่รับผิดชอบการสำรองข้อมูลระบบสารสนเทศของโรงพยาบาล (HIS) ครอบคลุมทุกขั้นตอนตั้งแต่การทำแผนสำรองข้อมูล การจัดทำขั้นตอนการสำรองข้อมูล การสำรองข้อมูล การเก็บรักษาข้อมูล การทดสอบการกู้คืนระบบ และการจัดทำรายงานต่าง ๆ ที่เกี่ยวข้อง

ข้อ ๒. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ ๑ ครั้ง

ข้อ ๓. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดวิธีการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลโดยอัตโนมัติ การทำ Storage Snapshot หรือการสำรองข้อมูลโดยผู้ดูแลระบบ

(๓) กำหนดให้มีแหล่งเก็บข้อมูลสำรองไว้อย่างน้อย ๒ แหล่ง โดยมีทั้งแหล่งจัดเก็บที่อยู่บนระบบเครือข่าย (Network Storage) และบนอุปกรณ์จัดเก็บข้อมูลที่ไม่เชื่อมต่อกับระบบเครือข่าย (Offline Storage)

(๔) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศ แบบเต็ม (full backup) ตามเงื่อนไขต่อไปนี้

- ตามระยะเวลาที่กำหนดไว้
- ก่อนที่จะดำเนินการปรับปรุงระบบสารสนเทศหรืออุปกรณ์ที่เกี่ยวข้อง
- หลังจากที่ดำเนินการปรับปรุงระบบและทดสอบการใช้งานจนมั่นใจว่าระบบดังกล่าวสามารถทำงานได้โดยไม่มีปัญหา
- เมื่อมีเหตุการณ์ความเสี่ยงด้านสารสนเทศ โดยประเมินจากสถานการณ์ปัจจุบัน ข่าวสาร การแจ้งเตือนจากกองดิจิทัลเพื่อสุขภาพ กรมอนามัย การแจ้งเตือนจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) เป็นต้น

(๕) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ

(๖) ตรวจสอบข้อมูลทั้งหมดระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน (configuration) ข้อมูลในฐานข้อมูล ฯลฯ

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่และอุปกรณ์ที่ใช้จัดเก็บข้อมูล

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการสำรองข้อมูลและการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๒. การทดสอบกู้คืนข้อมูลและระบบสารสนเทศ

ข้อ ๑. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

ข้อ ๒. ต้องทดสอบกู้คืนระบบจากข้อมูลสำรอง อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

ข้อ ๓. จัดทำรายงานการทดสอบกู้คืนระบบทุกครั้งที่ได้ดำเนินการทดสอบ โดยให้มีการรายงานข้อมูล ได้แก่ ชื่อข้อมูลที่สำรอง ผู้ดำเนินการ รายละเอียดของทรัพยากรที่ใช้ วัน/เวลาที่เริ่มทดสอบ วัน/เวลาที่เสร็จสิ้นการทดสอบ ผลการทดสอบ สำเร็จ/ไม่สำเร็จ ปัญหาและอุปสรรค และข้อเสนอแนะ

ข้อ ๔. ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

๓. การเตรียมพร้อมกรณีฉุกเฉิน

ข้อ ๑. ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการจัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้คืนแต่ละระบบงาน

(๓) มีการประเมินความเสี่ยงและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้นและต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

(๔) มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะ ของเครื่องคอมพิวเตอร์ (specification) ขั้นต่ำ ค่า configuration และอุปกรณ์เครือข่าย เป็นต้น

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

ข้อ ๒. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๔. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

มาตรการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวทางปฏิบัติ

๑. ระบบป้องกันผู้บุกรุก (Network Firewall)

ข้อ ๑. กำหนดให้เครื่องคอมพิวเตอร์และอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายของหน่วยงาน จะต้องกำหนดชื่อที่สอดคล้องกับผู้ใช้งานหรือจุดที่ใช้งาน สามารถระบุตัวผู้ใช้งานหรือสถานที่ติดตั้งได้

ข้อ ๒. ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

(๑) Packet ที่ Firewall ได้ทำการ Block

(๒) ลักษณะของ Packet ที่ถูก Block

(๓) Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

(๔) ชื่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ผิดปกติ พบหรือสงสัยว่ามีความเสี่ยง ไม่สามารถระบุตัวผู้ใช้งานหรือสถานที่ติดตั้งได้

(๕) เครื่องคอมพิวเตอร์หรือชื่อผู้ใช้งานที่มีการถ่ายโอนข้อมูลจำนวนมาก

๒. ติดตามสถานการณ์ด้านความมั่นคงปลอดภัยทางระบบสารสนเทศ

ให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายของหน่วยงาน ติดตามสถานการณ์ด้านความมั่นคงปลอดภัยทางระบบสารสนเทศ (Cyber Security) อย่างสม่ำเสมอจากช่องทางต่าง ๆ ได้แก่ การแจ้งเตือนจากกองดิจิทัลเพื่อสุขภาพ กรมอนามัย ผ่านไลน์กลุ่ม “AnamaiCIRT” , การแจ้งเตือนจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) หรือเว็บไซต์อื่น ๆ ที่เกี่ยวข้อง เพื่อเตรียมความพร้อมหรือประเมินความเสี่ยงทางระบบสารสนเทศของหน่วยงาน

๓. แนวทางปฏิบัติเมื่อเกิดเหตุร้ายแรงขึ้นต่อคอมพิวเตอร์หรือระบบสารสนเทศ

เมื่อเกิดเหตุการณ์ร้ายแรงขึ้นกับเครื่องคอมพิวเตอร์ ข้อมูล ระบบสารสนเทศ หรือระบบเครือข่าย มีสาเหตุจากปัจจัยภายนอกหรือภายในหน่วยงาน จนเกิดความเสียหายหรือสงสัยว่าจะสามารถสร้างความเสียหายต่อระบบเครือข่ายของหน่วยงาน ผู้ที่มีหน้าที่เกี่ยวข้องหรือผู้ประสบเหตุควรปฏิบัติดังต่อไปนี้

ข้อ ๑. กรณีที่ไม่สามารถประเมินความรุนแรงของเหตุการณ์ได้ หรือประเมินได้ว่ามีความรุนแรงและสามารถกระจายไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่ายได้ ให้ปิดเครื่องคอมพิวเตอร์ดังกล่าว หรือตัดการทำงานของเครื่องคอมพิวเตอร์นั้นออกจากระบบเครือข่ายของหน่วยงาน ด้วยวิธีที่รวดเร็วและสร้างความเสียหายน้อยที่สุด ได้แก่

- การถอดสายแลนออกจากเครื่องคอมพิวเตอร์
- การปิดเน็ตเวิร์คสวิตช์ตัวที่อยู่ใกล้ที่สุด
- การปิดเครื่องคอมพิวเตอร์ หากในกรณีที่ไม่สามารถสั่งปิดเครื่องได้ตามปกติ ให้กดปุ่มเปิดเครื่องค้างไว้จนกว่าเครื่องจะดับ

ข้อ ๒. แจ้งต่อหัวหน้ากลุ่มขับเคลื่อนยุทธศาสตร์และพัฒนากำลังคน โดยช่องทางที่รวดเร็ว เช่น ในเวลาราชการ โทรศัพท์ภายใน ต่อ ๑๒๔, Social Network

ข้อ ๓. งานเทคโนโลยีสารสนเทศดำเนินการตรวจสอบและแก้ไขปัญหาที่เกิดขึ้นจนแล้วเสร็จ และทำบันทึกข้อความรายงานปัญหา วิเคราะห์หาสาเหตุ วิธีแก้ไขและแนวทางป้องกัน เพื่อประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต เสนอต่อหัวหน้ากลุ่มขับเคลื่อนยุทธศาสตร์และพัฒนากำลังคน

ข้อ ๔. กรณีตรวจสอบพบว่าปัญหาที่เกิดขึ้นมีสาเหตุมาจากภัยคุกคามทางไซเบอร์ ให้แจ้งต่อกองดิจิทัลเพื่อสุขภาพ กรมอนามัย โดยบันทึกรายละเอียดตามแบบฟอร์มรายงานผลการตรวจสอบภัยคุกคามทางไซเบอร์ ส่งทางอีเมล์ cybersec@anamai.mail.go.th

มาตรการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของหน่วยงาน ช่วยให้สามารถป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด ทำให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน หรือการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๓. ประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๔. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๕. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดี ว่าต้องดำเนินการอย่างไร

ข้อ ๖. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ข้อ ๗. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของกรมอนามัย และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง