สำเนา

ประกาศองค์การเภสัชกรรม
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance
(Information Security Policy Practice Guideline and Data Governance)

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การเภสัชกรรม มีความน่าเชื่อถือ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่เหมาะสม หรือการถูกคุกคามจากภัยต่าง ๆ ที่ส่งผลเสียหายต่อองค์การเภสัชกรรม ซึ่งอาจเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้อง องค์การเภสัชกรรมจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance ขึ้น

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศองค์การเภสัชกรรม เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance”

ข้อ ๒. บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติใดที่ได้กำหนดไว้แล้ว ซึ่งขัดแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๓. ในประกาศนี้

๓.๑ นโยบาย (Policy) หมายความถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance

๓.๒ ผู้บริหารระดับสูง (CEO) หมายความถึง ผู้อำนวยการองค์การเภสัชกรรม

๓.๓ ผู้บริหาร (Manager) หมายความถึง ผู้อำนวยการองค์การเภสัชกรรม หรือ ผู้ที่ผู้อำนวยการองค์การเภสัชกรรมมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศขององค์การเภสัชกรรม

๓.๔ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หมายความถึง ผู้บริหารที่ได้รับการมอบหมายหน้าที่ให้กำกับดูแลการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปตามนโยบาย และทำหน้าที่ CDO (Chief Data Officer) โดยกำหนดทิศทาง ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติตามเกณฑ์คุณภาพ

๓.๕ หน่วยงาน (Section) หมายความถึง หน่วยงานในสังกัดองค์การเภสัชกรรมทุกระดับ

๓.๖ หน่วยงาน IT (IT Department) หมายความถึง กองเทคโนโลยีสารสนเทศองค์การเภสัชกรรม

๓.๗ ผู้ดูแลระบบ (System Administrator) หมายความถึง ผู้ที่ได้รับมอบหมายจากผู้อำนวยการกองเทคโนโลยีสารสนเทศ ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๓.๘ เจ้าของข้อมูล...

๓.๘ เจ้าของข้อมูล (Business Owner/ Data Owner) หมายความถึง หัวหน้าหน่วยงานในระดับฝ่ายหรือเทียบเท่าเป็นผู้รับผิดชอบ กำกับ ตรวจสอบ ดูแลและรักษาคุณภาพของข้อมูล โดยทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลและจัดให้มีบุคลากรที่เหมาะสมในการปฏิบัติงาน

๓.๙ ผู้ใช้งาน (User) หมายความถึงพนักงาน ลูกจ้าง หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การเภสัชกรรม

๓.๑๐ บัญชีผู้ใช้งาน (User Account) หมายความถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบสารสนเทศขององค์การเภสัชกรรม

๓.๑๑ สิทธิของผู้ใช้งาน (User Authorize) หมายความถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศขององค์การเภสัชกรรม

๓.๑๒ สินทรัพย์ (Asset) หมายความถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์การเภสัชกรรม

๓.๑๓ การเข้าถึงหรือการควบคุมการใช้งานระบบสารสนเทศ (Access and Control of Information System) หมายความถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก

๓.๑๔ ความมั่นคงปลอดภัยสารสนเทศ (Information Security) หมายความถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธการรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๓.๑๕ เหตุการณ์ความมั่นคงปลอดภัย (Information Security Event) หมายความถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๓.๑๖ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์การเภสัชกรรมถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๓.๑๗ ข้อมูลอิเล็กทรอนิกส์ (Electronic Data) หมายความถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๑๘ บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) หมายความถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบข้อกำหนดด้านคุณภาพ และความมั่นคงปลอดภัยของข้อมูล

๓.๑๙ บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) หมายความถึง เจ้าหน้าที่ IT หรือ ผู้ที่ได้รับมอบหมาย รับผิดชอบ รักษา และดูแลข้อมูลที่อยู่บนระบบเทคโนโลยีสารสนเทศต่าง ๆ ในหน่วยงานให้สนับสนุนด้านเทคโนโลยีสารสนเทศ แก่บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)

๓.๒๐ ระบบอินเทอร์เน็ต (Internet System) หมายความถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

๓.๒๑ ระบบสารสนเทศ...

๓.๒๑ ระบบสารสนเทศ (Information System) หมายความถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีระบบ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศ ให้หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้บริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นองค์ประกอบ

๓.๒๒ หน่วยงานภายนอก (Outside Section) หมายความถึง องค์กรหรือหน่วยงานภายนอก ที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๓.๒๓ จดหมายอิเล็กทรอนิกส์ (E-Mail) หมายความถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน โดยใช้มาตรฐาน SMTP, POP3, IMAP

๓.๒๔ สื่อบันทึกพกพา (Recording Media) หมายความถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล

๓.๒๕ ชื่อผู้ใช้ (Username) หมายความถึง ชุดของตัวอักษรหรือตัวเลข ที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิการใช้งานไว้

๓.๒๖ รหัสผ่าน (Password) หมายความถึง ตัวอักษร หรือตัวอักขระพิเศษ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๓.๒๗ การเข้ารหัส (Encryption) หมายความถึง การนำข้อมูลมาเข้ารหัส เพื่อป้องกันการลักลอบการเข้าถึงข้อมูล ผู้ที่สามารถเปิดข้อมูลที่เข้ารหัสไว้ จะต้องมีโปรแกรมในการถอดรหัส เพื่อให้ข้อมูลกลับมาใช้งานได้ปกติ

๓.๒๘ อุปกรณ์จัดเส้นทาง (Router) หมายความถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทาง เพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๓.๒๙ การพิสูจน์ยืนยันตัวตน (Authentication) หมายความถึง กระบวนการในการยืนยันความถูกต้องของผู้ใช้ที่แสดงตน ว่าเป็นบุคคลที่กล่าวอ้างตามสิทธิที่กำหนดไว้

๓.๓๐ SSID (Service Set Identifier) หมายความถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยทุก ๆ เครื่องในระบบ ต้องตั้งค่า SSID ค่าเดียวกัน

๓.๓๑ WPA (Wi-Fi Protected Access) หมายความถึง ระบบการเข้ารหัสเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในการแลกเปลี่ยนข้อมูลในระบบเครือข่ายไร้สาย

๓.๓๒ MAC Address (Media Access Control Address) หมายความถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่ายโดยจะมีหมายเลขที่ไม่ซ้ำกัน

๓.๓๓ SSL-VPN (Secure Socket Layer Virtual Private Network) หมายความถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริง จะทำโดยการเข้ารหัสเฉพาะ แล้วทำการรับส่งผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถเข้าถึงข้อมูลที่เข้ารหัสไว้ได้

๓.๓๔ แผนผังระบบเครือข่าย (Network Diagram) หมายความถึง แผนผัง ซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

ข้อ ๔. นโยบาย...

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance องค์การเภสัชกรรม

(๑) มีวัตถุประสงค์ ดังนี้

๑.๑ เพื่อให้เกิดความเชื่อมั่นว่า ระบบเทคโนโลยีสารสนเทศขององค์การเภสัชกรรม มีความมั่นคงปลอดภัย สามารถให้บริการได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อกำหนดแนวทางการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC 27001

๑.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์การเภสัชกรรมได้รับทราบและปฏิบัติตามอย่างเคร่งครัด

๑.๔ เพื่อกำหนดแนวทางปฏิบัติ หรือวิธีปฏิบัติที่เป็นมาตรฐานเดียวกัน ให้ผู้ใช้งานได้ยึดถือปฏิบัติและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์การเภสัชกรรม

(๒) การจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance

๒.๑ ผู้บริหาร เจ้าหน้าที่ด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการจัดทำ

๒.๒ จัดทำนโยบายเป็นลายลักษณ์อักษร และประกาศให้ผู้ใช้งานได้ทราบผ่านเว็บไซต์ของหน่วยงานหรือช่องทางอื่นใดที่สามารถเข้าถึงได้อย่างสะดวก

๒.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติให้ชัดเจน

๒.๔ มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง

(๓) รายละเอียดของนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance

๓.๑ การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

๓.๑.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

๓.๑.๒ การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๓.๑.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓.๑.๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๑.๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๓.๑.๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓.๑.๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๓.๑.๘ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑.๙ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

๓.๑.๑๐ การควบคุม...

๓.๑.๑๐ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๓.๑.๑๑ การใช้ห้องศูนย์ข้อมูลหลัก (Data Center) และ DR-Site

๓.๒ ระบบสารสนเทศและระบบสำรองของสารสนเทศ

กำหนดให้มีการจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง พร้อมทั้งทบทวนและทดสอบอย่างน้อยปีละ ๑ ครั้ง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

กำหนดให้มีการตรวจสอบประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓.๔ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

กำหนดให้มีการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือการใช้งานและการฝึกอบรม

ข้อ ๕. ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) มีอย่างน้อย ดังนี้

(๑) ให้มีการควบคุม การเข้าถึงข้อมูลและอุปกรณ์ ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ให้มีการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงาน

(๓) ให้มีการกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนัก เรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) ให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตแล้ว ดังกล่าว

(๓) การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) ให้มีการควบคุมจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิ์อื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Rights) ให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๗. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Use) ให้กำหนดแนวปฏิบัติที่ดี สำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน การเปลี่ยนแปลงรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ให้มีการควบคุมไม่ให้สินทรัพย์สารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) การใช้งานอุปกรณ์คอมพิวเตอร์พกพา การปฏิบัติงานจากภายนอกหน่วยงานและการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน (Mobile Device, Teleworking and BYOD Policy)

ข้อ ๘. มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้งานบริการเครือข่าย กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) กำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์ของเครือข่าย (Equipment Identification in Networks) ให้มีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ให้มีการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (Segregation in Networks) ให้ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้มีการควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกัน หรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้มีการควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอน...

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการให้มีการควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๐. มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Information Access Control) อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดข้อปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๑. จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ให้มีการพิจารณาคัดเลือกจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ให้มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ให้มีการกำหนด...

(๓) ให้มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ และทบทวนแนวทางจัดทำระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) ความถี่ของการปฏิบัติในแต่ละข้อ ให้มีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

ข้อ ๑๒. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) ให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ตรวจสอบและประเมินความเสี่ยง ให้ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Audit) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๓. องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์การเภสัชกรรม โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศเรื่อง **“แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance”** เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระบบที่เกี่ยวข้อง

ข้อ ๑๔. กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศ ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้ใดผู้หนึ่งอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance หรือกรณีอื่นใดตามประกาศ กฎระเบียบหรือกฎหมายที่เกี่ยวข้องกำหนด

ข้อ ๑๕. กำหนดบทบาทหน้าที่ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติ ดังนี้

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO & CDO) เป็นผู้กำกับดูแลการใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance ของหน่วยงาน โดยมีหน้าที่ดังนี้

(๑.๑) นำข้อมูลและวิเคราะห์ข้อมูล เพื่อสร้างและส่งมอบเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานมีคุณค่าและเกิดประโยชน์สูงสุดต่อหน่วยงาน

(๑.๒) วิเคราะห์และร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการกำกับดูแลข้อมูลคุณภาพและการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูล

(๑.๓) นำแนวปฏิบัติและมาตรฐานของหน่วยงานไปปรับปรุงข้อมูลและยุทธศาสตร์ของประเทศ

(๑.๔) เป็นตัวกลาง...

(๑.๔) เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการแลกเปลี่ยน เชื่อมโยงข้อมูล รวมไปถึงการจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงานภาครัฐ

(๑.๕) ส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์ปัญหา

(๑.๖) วิเคราะห์หาเทคโนโลยีใหม่ ๆ มาใช้ในการวิเคราะห์ข้อมูล

(๒) ผู้อำนวยการกองเทคโนโลยีสารสนเทศ มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance ของหน่วยงาน

(๓) ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบ การใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance ของหน่วยงาน

(๔) ผู้ใช้งาน หรือผู้ใช้ข้อมูล เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศขององค์การเภสัชกรรมตามที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance ขององค์การเภสัชกรรม

(๕) เจ้าของข้อมูล (Data Owner) เป็นผู้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย โดยมีหน้าที่ดังนี้

(๕.๑) ตรวจสอบ ดูแล และรักษาคุณภาพของข้อมูล

(๕.๒) ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล

(๖) บริกรข้อมูลด้านธุรกิจ (Business Data Steward) มีหน้าที่ดังนี้

(๖.๑) นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย

(๖.๒) นิยามเมทาดาตา (Metadata)

(๖.๓) ร่างนโยบายข้อมูล มาตรฐาน และแนวทางปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล

(๖.๔) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ

(๖.๕) ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล การวิเคราะห์คุณภาพข้อมูล

(๗) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) โดยมีหน้าที่ดังนี้

(๗.๑) ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ

(๗.๒) รักษาและดูแลข้อมูลที่อยู่บนระบบเทคโนโลยีสารสนเทศต่าง ๆ ในหน่วยงาน

ข้อ ๑๖. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและ Data Governance ตามเอกสารแนบท้ายประกาศฉบับนี้

ประกาศนี้ให้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๕ กันยายน พ.ศ. ๒๕๖๕

(นายวิฑูรย์ ด่านวิบูลย์)
ผู้อำนวยการองค์การเภสัชกรรม