ประกาศกรมสนับสนุนบริการสุขภาพ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องกับภารกิจของกรมสนับสนุนบริการสุขภาพ ในการเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII :Critical Information Infrastructure) และการเป็นหน่วยงานหลักในการควบคุมกำกับ มาตรฐานสถานพยาบาล ด้านที่ ๙ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัลระดับกรม (Department Chief Information Officer) อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้และให้บริการได้อย่างต่อเนื่อง สามารถป้องกันภัยคุกคามไซเบอร์ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมสนับสนุนบริการสุขภาพและหน่วยงานในสังกัด จึงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ดังต่อไปนี้

ข้อ ๑ ยกเลิกประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๓

ข้อ ๒ ประกาศนี้ เรียกว่า “ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๔”

ข้อ ๓ ในประกาศนี้

(๑) “กรม สบส.” หมายความว่า กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

(๒) “ผู้บริหารระดับสูงสุด” (Chief Executive Officer : CEO) หมายความว่า อธิบดีกรม สบส.

(๓) “ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม” (Department Chief Information Officer: DCIO) หมายความว่า รองอธิบดีหรือผู้ซึ่งได้รับมอบหมายให้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศกรม สบส.

(๔) “คณะกรรมการ” หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรม สบส.

(๕) “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

(๕.๑) พระราชบัญญัติว่า...

(๕.๑) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

(๕.๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๕.๓) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๕.๔) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และและที่แก้ไขเพิ่มเติม

(๕.๕) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๖) "แนวปฏิบัติ" หมายความว่า ขั้นตอน วิธีการหรือข้อกำหนดให้ผู้ใช้งาน (User) และผู้ดูแลระบบ (Administrator) รวมทั้งบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ กรม สบส. ได้ถือปฏิบัติตามนโยบาย ข้อ ๓ (๕)

(๗) "เจ้าของระบบ" (System Owner) หมายความว่า สำนัก/กอง/กลุ่ม/กลุ่มงาน/ศูนย์ที่เป็นเจ้าของระบบคอมพิวเตอร์ หรือ ระบบสารสนเทศ

(๘) "ผู้ดูแลระบบ" (System Administrator) หมายความว่า บุคลากร กรม สบส. ผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบเทคโนโลยีสารสนเทศ กรม สบส.

(๙) "ผู้ใช้งาน" (User) หมายความว่า บุคลากร กรม สบส. ทุกระดับ ซึ่งเป็นข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอก ที่ได้รับอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศ กรม สบส.

(๑๐) "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรม สบส.

(๑๑) "สินทรัพย์" (asset) หมายความว่า ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของกรม สบส. ประกอบด้วย

(๑๑.๑) ฮาร์ดแวร์ (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งแบบเครื่องแม่ข่ายปกติ (Rack Server) และเครื่องแม่ข่ายแบบชุด (Blade Server)
- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) และคอมพิวเตอร์พกพา (Laptop)
- เครื่องพิมพ์ (Printer/Scanner) และอุปกรณ์สำรองข้อมูลของกรม สบส.
- อุปกรณ์โครงข่าย (Network) หรือ อุปกรณ์รักษาความมั่นคงปลอดภัย

- อุปกรณ์โครงข่าย ...

- อุปกรณ์โครงข่าย (Network) หรือ อุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

(๑๑.๒) โปรแกรมประยุกต์หรือแอปพลิเคชัน (Program or Application) หมายความว่า ระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบ, System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ฮาร์ดแวร์

(๑๒) "ศูนย์ข้อมูลและสารสนเทศ" หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะเพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Devices) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบรักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ ระบบข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน ประกอบด้วย

(๑๒.๑) "ศูนย์ข้อมูล" (Data Center) หมายความว่า ศูนย์ข้อมูลและสารสนเทศของกรม สบส. ตั้งอยู่ที่ชั้น ๒ อาคาร กรม สบส.

(๑๒.๒) "ศูนย์สำรองข้อมูล" (DR Site: Disaster Recovery Site) หมายความว่า ศูนย์กลางสำรองข้อมูล ของกรม สบส. ตั้งอยู่ที่ ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง จังหวัดชลบุรี

(๑๒.๓) "ศูนย์บริการธุรกิจสุขภาพ" (OSS" One Stop Service ) หมายความว่า หน่วยให้บริการ

(๑๓) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

(๑๔) "ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน(Availability) ของสารสนเทศ รวมทั้ง คุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (nonrepudiation) และความน่าเชื่อถือ (Reliability)

(๑๕) "เหตุการณ์ด้านความมั่นคงปลอดภัย" (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๖) "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ กรม สบส. ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๕ นโยบายในการ...

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

(๑) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบ

(๒) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติฯ ดังกล่าวให้ชัดเจน

(๓) ต้องทบทวนและปรับปรุงนโยบาย อย่างน้อย ปีละ ๑ ครั้ง

ข้อ ๖ กรม สบส. ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งได้กำหนดให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศเป็นผู้กำกับ ดูแล และติดตามผู้ใช้งาน (User) ปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวไว้อย่างชัดเจน ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

(๔) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

(๗) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management)

(๙) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๗ กรม สบส. ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการใดวิธีการหนึ่ง ให้ ผู้ใช้งาน (User) และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าใจ เข้าถึงและปฏิบัติตาม ด้วยหนังสือเวียนภายในองค์กร ระบบ เครือข่ายภายใน (Intranet) หนังสือเวียนอิเล็กทรอนิกส์ หรือเว็บไซต์ภายในและภายนอก กรม สบส.

ข้อ ๘ หน่วยงานภายใน กรม สบส. ที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศ สามารถกำหนดแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานได้เอง ทั้งนี้ต้องให้สอดคล้องกับ “ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔”

ข้อ ๙ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของกรม สบส. เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ต้องรายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับกรม

สั่งการตรวจสอบ...

สั่งการตรวจสอบผู้ละเลยที่ก่อให้เกิดความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกรม สบส. เพื่อรายงานต่อผู้บริหารระดับสูงสุด

ข้อ ๑๐ กรม สบส. กำหนดให้ผู้บริหารระดับสูงสุด เป็นผู้รับผิดชอบในการบริหารความเสี่ยง ควบคุมความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม สบส.

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๘ มิถุนายน พ.ศ. ๒๕๖๔

(นายธเรศ กรัษนัยรวิวงศ์)
อธิบดีกรมสนับสนุนบริการสุขภาพ