(ร่าง) ประกาศกรมสนับสนุนบริการสุขภาพ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓

ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้องกับภารกิจของกรมสนับสนุนบริการสุขภาพ ในการเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) มีผลกระทบต่อประชาชนโดยตรง (Impact Security Risk และ Economics Public Health) จากการเชื่อมโยงข้อมูล (Interconnected Information System) และการเป็นหน่วยงานหลักในการควบคุม กำกับมาตรฐานสถานพยาบาล ด้านที่ ๙ การรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัลระดับกรม (Department Chief Information Officer) อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้และให้บริการได้อย่างต่อเนื่อง สามารถป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมสนับสนุนบริการสุขภาพและหน่วยงานในสังกัด รวมทั้งประชาชนผู้ใช้บริการ ประกอบกับกรมสนับสนุนบริการสุขภาพ ได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ จึงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ ๒๕๖๓ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ข้อ ๓ ได้กำหนดให้หน่วยงานรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ดังต่อไปนี้

ข้อ ๑ ยกเลิก ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๒

ข้อ ๒ ประกาศนี้ เรียกว่า “ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๓”

ข้อ ๓ ในประกาศนี้

(๑) “สบส.” หมายความว่า กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

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

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

(๔) “คณะกรรมการ” หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สบส.

(๕) “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

(๕.๑) พระราชบัญญัติ...

(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

(๕.๖) กฎหมายอื่นๆ ทั้งในและต่างประเทศที่เกี่ยวข้อง

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

(๗) “ผู้ดูแลระบบ” (System Administrator) หมายความว่า บุคลากร สบส. ผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ ของระบบเทคโนโลยีสารสนเทศ สบส.

(๘) “เจ้าของระบบ” (System Owner) หมายความว่า สำนัก/กอง/กลุ่ม/กลุ่มงาน/ศูนย์ ที่เป็นผู้รับผิดชอบในการพัฒนาระบบคอมพิวเตอร์ หรือ ระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อสนับสนุนภารกิจการปฏิบัติงานของหน่วยงานให้เกิดประสิทธิภาพ ต่อ สบส. ในภาพรวม หรือตามที่อธิบดีให้ดำเนินงาน หรือมีหน้าที่อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน (User)

(๙) “ผู้ใช้งาน” (User) หมายความว่า บุคลากร สบส.ทุกระดับ ซึ่งเป็นข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอก ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายและโปรแกรมประยุกต์หรือแอพพลิเคชั่นของ และ/หรือเกี่ยวข้องกับการใช้ประโยชน์จากระบบเทคโนโลยีสารสนเทศ สบส.

(๑๐) “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของ สบส.

(๑๑) “สินทรัพย์” (asset) หมายความว่า ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของ สบส. ประกอบด้วย

(๑๑.๑) ฮาร์ดแวร์ (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งแบบเครื่องแม่ข่ายปกติ (Rack Server) และเครื่องแม่ข่ายแบบชุด (Blade Server)

- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Laptop) อุปกรณ์สื่อสารแบบพกพา (Tablet/Smart phone) รวมถึงอุปกรณ์สนับสนุนเครื่องพิมพ์ (printer/Scanner) และอุปกรณ์สำรองข้อมูลของกรม สบส.

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

(๑๑.๒) โปรแกรมประยุกต์หรือแอพพลิเคชั่น (Program or Application) หมายความว่า ระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบ, System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ในหัวข้อ Hardware

(๑๑.๓) เครือข่าย...

(๑๑.๓) เครือข่าย (Network and Communication) หมายความว่า ระบบเทคโนโลยีด้านการสื่อสารโทรคมนาคม ของ สบส.

(๑๑.๔) “ระบบสารสนเทศ” หมายความว่า ระบบงานคอมพิวเตอร์ เช่น เว็บไซต์ (Website) เว็บพอร์ทัล (Portal Web) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น หรืออุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการพัฒนา หรือติดตั้ง หรือการนำมาประยุกต์ใช้ เพื่อสนับสนุนการปฏิบัติงานของ สบส.

(๑๑.๕) “ข้อมูลสารสนเทศ” หมายความว่า ข้อมูล (Data) หรือ สารสนเทศ (Information) ที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ เช่น แฟ้มข้อมูล (Files) ฐานข้อมูล (Database) หรือเอกสารที่มีการแปลงให้อยู่ในรูปแบบอิเล็กทรอนิกส์ (e-Document) เป็นต้น ของ สบส.

(๑๒) “พื้นที่ปฏิบัติงานทั่วไป” (General Working Area) หมายความว่า พื้นที่สำหรับการปฏิบัติงานภายใน สบส. ซึ่งได้มีการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์ลูกข่ายเสมือน เครื่องคอมพิวเตอร์พกพา อุปกรณ์ต่อพ่วงและเครือข่ายแบบมีสาย (LAN) และไร้สาย (Wireless)

(๑๓) “ศูนย์ข้อมูลและสารสนเทศ” หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะ เพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Devices) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบรักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ ระบบข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน ประกอบด้วย

(๑๓.๑) “ศูนย์กลางข้อมูล” (DC : Data Center) หมายความว่า ศูนย์กลางข้อมูลและสารสนเทศของ สบส. ตั้งอยู่ที่ชั้น ๒ อาคาร สบส.

(๑๓.๒) “ศูนย์สำรองข้อมูล” (DR Site : Disaster Recovery Site) หมายความว่า ศูนย์กลางสำรองข้อมูลและสารสนเทศ ของ สบส. ตั้งอยู่ที่ ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง จังหวัดชลบุรี

(๑๓.๓) “ศูนย์บริการธุรกิจสุขภาพ” (OSS” One Stop Service) หมายความว่า หน่วยให้บริการข้อมูลด้านระบบบริการสุขภาพแบบเบ็ดเสร็จครบวงจร ณ จุดเดียว ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒ ตั้งอยู่ที่ชั้น ๑ อาคาร สบส.

(๑๓.๔) “ห้องเซิร์ฟเวอร์” (Server Room) หมายความว่า ศูนย์ข้อมูลและสารสนเทศของ สบส. ตั้งอยู่ที่ศูนย์สนับสนุนบริการสุขภาพ หรือ ศูนย์พัฒนาการสาธารณสุขมูลฐาน ของ สบส. จำนวน ๑๒ แห่ง

(๑๔) “เครือข่าย” (Network System) หมายความว่า ระบบเครือข่ายที่เชื่อมโยงกับอุปกรณ์ในหัวข้อ Hardware, Software และระบบเทคโนโลยีสารสนเทศของ สบส. ทั้งแบบใช้สายและไร้สาย

(๑๕) “ระบบงาน” หมายความว่า ระบบฐานข้อมูลที่สนับสนุนการดำเนินงานของ สบส.

(๑๕.๑) งานคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ

(๑๕.๒) งานสนับสนุนการบริหารจัดการและกำกับมาตรฐานระบบบริการสุขภาพ

(๑๕.๓) งานวิศวกรรมการแพทย์และเครื่องมือแพทย์

(๑๕.๔) งานแบบมาตรฐานอาคารด้านระบบบริการสุขภาพ

(๑๕.๕) งานการมีส่วนร่วมภาคประชาชน

(๑๕.๕.๑) งานสุขศึกษา

(๑๕.๕.๒) งานสนับสนุนสุขภาพภาคประชาชน

(๑๖) “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดแนวปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๑๗) “ความมั่นคง...

(๑๗) “ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (Reliability)

(๑๘) “เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๙) “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ สบส. ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษร ตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๖ ถึง ข้อ ๑๐

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของ สบส.

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติฯ ดังกล่าวให้ชัดเจน

(๔) ต้องทบทวนและปรับปรุงนโยบาย อย่างน้อย ปีละ ๑ ครั้ง

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ (Access Control) มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่เปิดเผย (Business Requirements for Access Control)

(๑.๑) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๑.๒) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(๑.๓) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๒) ศูนย์ข้อมูลและสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยแยกประเภทและจัดเก็บเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และสภาพพร้อมใช้งาน และมีแผนฉุกเฉินเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องดำเนินการอย่างสม่ำเสมอ โดยกำหนดให้ต้องตรวจสอบ ควบคุมคุณภาพและดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๔) การกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการรายงานเหตุการณ์ที่เสี่ยงต่อความมั่นคงปลอดภัยที่เกิดขึ้น

(๕) การสร้างความรู้...

(๕) การสร้างความรู้ ความเข้าใจการใช้งานระบบสารสนเทศหรือระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ ความเข้าใจ โดยการจัดทำคู่มือ การฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ผู้ใช้งาน

ข้อ ๖ 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) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(๗) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management)

โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๗ สบส. ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการใดวิธีการหนึ่ง ให้ผู้ใช้งาน (User) และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าใจ เข้าถึงและปฏิบัติตาม ด้วยหนังสือเวียนภายในองค์กร ระบบเครือข่ายภายใน (Intranet) หนังสือเวียนอิเล็กทรอนิกส์ หรือเว็บไซต์ภายในและภายนอก สบส.

ข้อ ๘ หน่วยงานภายใน สบส. ที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศ สามารถกำหนดแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานได้เอง ทั้งนี้ต้องให้สอดคล้องกับ “ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓”

ข้อ ๙ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ ของ สบส. เกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ต้องรายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับกรม สั่งการตรวจสอบผู้ละเลยที่ก่อให้เกิดความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ สบส. เพื่อรายงานต่อผู้บริหารระดับสูงสุด

ข้อ ๑๐ สบส. กำหนดให้ผู้บริหารระดับสูงสุด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ ระบบสารสนเทศและข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่ สบส. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับนี้

ข้อ ๑๑ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ กันยายน พ.ศ. ๒๕๖๓