แนวทางการจัดทำแผนการบริหารความเสี่ยง งบประมาณ บุคลากร และแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล ปีงบประมาณ พ.ศ. 2566-2568

สำนักงานปลัดกระทรวงสาธารณสุข

คำนำ

สำนักงานปลัดกระทรวงสาธารณสุข ได้จัดทำแนวทางการจัดทำแผนการบริหารความเสี่ยง งบประมาณ บุคลากรและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล ปีงบประมาณ พ.ศ. 2566-2568 โดยได้นำเนื้อหาสำคัญจาก นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 มาปรับแต่งให้มีความกระชับ เหมาะสำหรับผู้บริหารได้นำไปใช้ในการวางแผนบริหารจัดการด้านไซเบอร์ภายในองค์กร ตามนโยบายและข้อสั่งการของปลัดกระทรวงสาธารณสุข นายแพทย์โอภาส การย์กวินพงศ์ ที่ได้มอบไว้เมื่อวันที่ 12 เมษายน 2566

แนวทางฯ ฉบับนี้จัดทำขึ้นโดยมีวัตถุประสงค์ให้หน่วยงานในสังกัดกระทรวงสาธารณสุข ที่มีระบบเทคโนโลยีสารสนเทศที่มีความหลากหลายและแตกต่างกันค่อนข้างมาก สามารถนำแนวทางฯ นี้ไปใช้ประเมินความพร้อมด้านไซเบอร์ของตนเอง และนำไปประยุกต์ใช้ในการกำกับดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศได้อย่างเหมาะสมกับขนาดและความซับซ้อนของระบบไอทีของหน่วยงาน รวมถึงสามารถนำไปใช้ในการกำหนดมาตรการควบคุมความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข
Version 1.0

สารบัญ

แนวทางการจัดทำแผนการบริหารความเสี่ยง งบประมาณ บุคลากร
และแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
และการคุ้มครองข้อมูลส่วนบุคคล ปีงบประมาณ พ.ศ. 2566-2568

เพื่อให้หน่วยงานภายใต้สังกัดกระทรวงสาธารณสุขมีแนวทางในการจัดทำแผนการบริหารความเสี่ยง งบประมาณ บุคลากร และมีแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุขจึงได้จัดทำแนวทางการจัดทำแผนการบริหารความเสี่ยงในมิติการรักษาความมั่งคงปลอดภัยด้านไซเบอร์ และมิติการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ผู้บริหารของหน่วยงานใช้เป็นเครื่องมือช่วยในการบริหารหน่วยงานในด้านความมั่นคงปลอดภัยไซเบอร์ ด้านการปฏิบัติงานด้วยระบบสารสนเทศ การดูแลศูนย์ปฏิบัติการข้อมูลอิเล็กทรอนิกส์ (Data Center) ระบบเครือข่าย (Network) และเครื่องคอมพิวเตอร์แม่ข่าย (Server) รวมถึงการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ ซึ่งต้องทำอย่างต่อเนื่อง ประกอบด้วยคำแนะนำในการจัดทำแผนต่างๆ โดยแบ่งระยะการดำเนินงาน คำแนะนำสำหรับการกำหนดผู้รับผิดชอบไว้ จำนวน 30 ข้อหลัก ดังนี้

1. แผนด้านงบประมาณ จำนวน 8 ข้อย่อย
2. แผนด้านการบริหารทรัพยากรบุคคล 4 ข้อย่อย
3. แผนด้านการบริหารความเสี่ยงด้านดิจิทัล 14 ข้อย่อย
4. แผนด้านแนวทางปฏิบัติสำหรับบุคลากรด้านเทคโนโลยีสารสนเทศ/ดิจิทัล 46 ข้อย่อย

ผู้รับผิดชอบหลัก :

1. ผู้บริหาร หมายถึง CEO/CIO/CISO หรือเจ้าหน้าที่ระดับบริหาร ที่หัวหน้าหน่วยมอบหมายให้ดูแลงานด้านเครือข่ายคอมพิวเตอร์และสารสนเทศของหน่วยงาน
2. IT หมายถึง ผู้ปฏิบัติงานด้านระบบเครือข่ายคอมพิวเตอร์และสารสนเทศของหน่วยงาน

แนวทางการจัดทำแผนการบริหารความเสี่ยง งบประมาณ บุคลากร และแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลนี้ แบ่งหน่วยงานเป็น 2 กลุ่ม ประกอบด้วย

1. หน่วยงานระดับกอง : หน่วยงานในสำนักงานปลัดกระทรวงสาธารณสุขในระดับกอง สำนักงานเขตสุขภาพ สำนักงานสาธารณสุขจังหวัด โรงพยาบาลศูนย์และโรงพยาบาลทั่วไป (ในแนวทางนี้ใช้คำย่อว่า “กอง”)
2. หน่วยงานขนาดเล็ก : โรงพยาบาลชุมชน สำนักงานสาธารณสุขอำเภอ โรงพยาบาลส่งเสริมสุขภาพประจำตำบล (ในแนวทางนี้ใช้คำย่อว่า “รพช”)
3. แบ่งช่วงระยะเวลาการดำเนินการของแต่ละกลุ่มตามความเหมาะสม ดังนี้
    - ปีงบประมาณ พ.ศ. 2566 ระยะเร่งด่วน ประเด็นสำคัญที่สามารถดำเนินการได้โดยไม่ต้องรอการจัดสรรงบประมาณ
    - ปีงบประมาณ พ.ศ. 2567 ระยะเร่งด่วน แต่เป็นประเด็นสำคัญที่ต้องรอการจัดสรรงบประมาณในการดำเนินการ
    - ปีงบประมาณ พ.ศ. 2568 ระยะไม่เร่งด่วน แต่มีความสำคัญที่ต้องดำเนินการ

หลักปฏิบัติในการทำงาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล

“ทำทันที ทำต่อเนื่อง ทำและพัฒนา”

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
1	**สนับสนุนอุปกรณ์ป้องกันภัยคุกคามไซเบอร์ อย่างต่อเนื่อง**	งบประมาณ	/			/			/	
1.1	**Next-Gen Firewall (NGF)** หรือ ถ้ามี Firewall แล้ว ควรเพิ่มระบบ Intrusion Prevention System (IPS) สำหรับป้องกันการโจมตีผ่านช่องทาง Internet	งบประมาณ	/			/			/	
1.2	**Next-Gen Antivirus (NGAV)** รุ่นปัจจุบัน ที่สามารถตรวจจับไวรัสที่เกิดใหม่ได้อัตโนมัติและต่ออายุการใช้งานต่อเนื่อง หากยังจำเป็นต้องใช้ Antivirus ทั่วไป ต้องกำกับให้มีการอัปเดตเครื่องคอมพิวเตอร์อย่างน้อยทุกสัปดาห์	งบประมาณ	/			/			/	
1.3	**Extended Detection & Response (XDR)** อย่างน้อย XDR ต่อ 1 VLAN ตรวจจับการโจมตีของระบบทั้งหมด และต่ออายุการใช้งาน ถ้ามีอุปกรณ์การแพทย์ที่สามารถเชื่อมเครือข่ายไม่มากอาจใช้ Endpoint Detection & Response (EDR) ติดกับอุปกรณ์แต่ละชิ้นและมีผู้ดูแลรายเครื่องได้	งบประมาณ	/			/			/	
1.4	ระบบปฏิบัติการ (Operating System) สำหรับระบบสารสนเทศ/เครื่องแม่ข่าย และ Firmware สำหรับระบบเครือข่าย ที่มีลิขสิทธิ์และต่ออายุ	งบประมาณ	/			/			/	

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	การใช้งาน หรือ Open Source ที่น่าเชื่อถือ									
1.5	พื้นที่สำรองข้อมูล (อาจใช้ Cloud) ที่มีระบบรักษาความปลอดภัย 1) Offline backup 2) Isolated Environment backup	งบประมาณ			/	/			/	
1.6	กรณีใช้ Server ควรมี Data Center ที่มีระบบรักษาความปลอดภัย การวางแผนการบำรุงรักษาอุปกรณ์ตามอายุการใช้งาน	งบประมาณ	/			/			/	
1.7	**ติดตั้งอุปกรณ์สนับสนุนการรักษาความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์บริหารเครือข่าย และซ่อมบำรุงระบบสนับสนุนอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง ดังนี้** (1) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) หรืออุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าในระยะเวลาอย่างน้อย 30 นาที หรือที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย (2) อุปกรณ์ตรวจจับควัน (3) อุปกรณ์ดับเพลิงชนิดก๊าซ (4) ระบบระบายอากาศ ระบบควบคุมอุณภูมิ และระบบควบคุมความชื้น (5) ระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) มีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน	งบประมาณ			/	/			/	

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	ในกรณีที่เป็น Data Center ขนาดใหญ่									
2	หัวหน้าหน่วยงานทำหน้าที่เป็น Data controller มอบหมายหน้าที่ผู้ดูแลระบบสารสนเทศในลำดับถัดไปเป็นลายลักษณ์อักษรตามความเหมาะสมของขนาดและจำนวนบุคลากรโดยอาจแบ่งเป็น CIO, CDO, CISO, หัวหน้ากลุ่มงาน/ศูนย์คอมพิวเตอร์ หน้าที่และอำนาจของผู้ดูแลระบบ	บุคลากร	/	/					/	
3	จัดให้มีเจ้าหน้าที่ปฏิบัติงานเฝ้าระวังภัยคุกคามไซเบอร์เป็นประจำอย่างต่อเนื่อง อย่างน้อย 1 คน และสามารถประสานงานกับ Health CERT ได้ตลอดเวลา	บุคลากร	/	/					/	
4	สื่อสารสร้างความตระหนักในมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ และการรักษาความลับข้อมูลส่วนบุคคลให้บุคลากรทุกระดับรับทราบดังรายละเอียดในภาคผนวก ก	บุคลากร	/	/					/	
5	พัฒนาบุคลากรด้านสารสนเทศให้มีศักยภาพและความพร้อมในการปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมาย	บุคลากร			/	/			/	
6	คณะผู้บริหารของหน่วยงานมีนโยบายการบริหารความเสี่ยง/วางแผนการรักษาความมั่นคงปลอดภัยไซเบอร์จากภัยคุกคามไซเบอร์/เตรียมความพร้อมรองรับกรณีฉุกเฉิน อาจดำเนินการตาม NIST framework หรือ HAIT โดยให้ความสำคัญกับการใช้เทคโนโลยีและระบบสารสนเทศ	บริหารความเสี่ยง	/	/					/	

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	ดังต่อไปนี้ (1) Data-base, Server, Cloud, (2) Network, Internet, Intranet โครงข่ายอื่นๆ (3) ระบบสารสนเทศสำคัญสำหรับการบริการทางการแพทย์: HIS, ERP, LIS, PACS, HRIS, Telemedicine (4) Website, Web application, E-mail ของหน่วยงาน									
7	คณะผู้บริหารของหน่วยงานให้ความสำคัญกับการสื่อสาร และสร้างพฤติกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ และการรักษาความลับของข้อมูลส่วนบุคคลของบุคลากรทุกระดับ และควบคุมกำกับให้มีการปฏิบัติตามแนวทาง	บริหารความเสี่ยง	/	/					/	
8	กระบวนการจัดทำแผนบริหารความเสี่ยงจากภัยคุกคามไซเบอร์	บริหารความเสี่ยง			/	/			/	/
8.1	จัดทำแผนบริหารความเสี่ยง ประเมินและจัดลำดับความสำคัญของความเสี่ยงของหน่วยงาน กำหนดมาตรการ หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้อง	บริหารความเสี่ยง			/	/			/	/
8.2	ซ้อมแผนบริหารความเสี่ยง และการเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง	บริหารความเสี่ยง			/	/			/	/
8.3	ประเมินความเสี่ยงโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) ทบทวนเพื่อปรับปรุงแผนบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง	บริหารความเสี่ยง			/	/			/	/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
8.4	ประเมินความเสี่ยง โดยผู้ตรวจสอบภายนอก การเตรียมการสำหรับผู้ตรวจสอบภายนอก (1) สามารถเข้าถึงข้อมูลได้แบบอ่านได้อย่างเดียว ห้ามแก้ไขข้อมูลบันทึก Log (2) กรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ อาจสร้างสำเนาเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายเมื่อใช้เสร็จ หรือจัดเก็บไว้เป็นอย่างดี (2) ระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบ (3) กรณีที่มีเครื่องมือภายนอกสำหรับการตรวจสอบ ให้แยกการติดตั้งเครื่องมือนั้นออกจากระบบให้บริการจริง และต้องได้รับการอนุญาต	บริหารความเสี่ยง					/	/	/	/
9	จัดทำและเผยแพร่หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคลและคำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notices)	บริหารความเสี่ยง	/	/					/	/
10	จัดทำกระบวนการการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลภายในหน่วยงานกำหนดตัวบุคคลทำหน้าที่ต่างๆตามกระบวนการรับแจ้งเหตุของ DPO สป.สธ. (ภาคผนวก ข)	บริหารความเสี่ยง	/	/					/	/
11	จัดให้มีกระบวนการขอความเห็นชอบในการเผยแพร่ข้อมูลส่วนบุคคลผ่าน ระบบ Intranet และ Internet จากผู้ที่ได้รับมอบหมาย ในกรณีต่อไปนี้ (1) ข้อมูลส่วนบุคคลของประชาชนผู้มารับบริการ (CIO/CDO)	บริหารความเสี่ยง	/	/					/	/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	(2) ข้อมูลส่วนบุคคลของบุคลากรที่มีวัตถุประสงค์การใช้สื่อสารสาธารณะ (CIO/CDO) (3) ข้อมูลส่วนบุคคลของบุคลากรเพื่อการปฏิบัติงานภายในหน่วยงาน (หัวหน้ากลุ่มงาน หรือ CIO/CDO)									
12	มีกระบวนการควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์ และระบบระบบเครือข่าย Intranet และ Internet ที่หน่วยงานให้บริการ (Business Requirements for Access Control)	บริหารความเสี่ยง			/	/			/	/
12.1	มีกระบวนการจัดทำทะเบียนรายการบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management) เช่น ผู้ดูแลระบบ (System Administrator) ผู้ใช้งาน (User) ระบบเทคโนโลยีสารสนเทศสำคัญ ระบบเครือข่าย (Internet) จดหมายอิเล็กทรอนิกส์ของหน่วยงาน (E-Mail) เป็นต้น ให้เป็นลายลักษณ์อักษร	บริหารความเสี่ยง			/	/				
12.2	มีกระบวนการกำหนดสิทธิ์เพื่อควบคุมการเข้าถึงระบบสารสนเทศ และประมวลผล (1) กำหนดชั้นความลับ (2) กำหนดกลุ่มผู้เข้าใช้งานระบบ เช่น ผู้ดูแลฐานข้อมูล/โครงข่าย/ระบบสารสนเทศ, ผู้ใช้งาน (3) กำหนดสิทธิ์การเข้าถึง/ประมวลผล เช่น อ่านอย่างเดียว ป้อนข้อมูล แก้ไขข้อมูล/การบันทึก อนุมัติสิทธิ์	บริหารความเสี่ยง			/	/			/	/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
12.3	มีกระบวนการปรับปรุง/ทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง และกำหนดเกณฑ์การระงับสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) (1) สรุปทะเบียนรายชื่อของผู้ที่ยังมีสิทธิ์แยกตามหน่วยงาน (2) ส่งให้หัวหน้าหน่วยงานทบทวน ความถูกต้อง และทบทวนสำหรับผู้ที่มีสิทธิ์ในระดับสูงด้วยความถี่มากกว่าผู้ใช้งานทั่วไป (3) ฝ่ายบุคลากรแจ้งผู้กำกับระบบการให้สิทธิ์เมื่อบุคลากรเปลี่ยนตำแหน่งหน้าที่ความรับผิดชอบ หรือสิ้นสุดการปฏิบัติงานโดยเร็ว	บริหารความเสี่ยง			/	/			/	/
12.4	จัดทำระบบทะเบียนกลางเพื่อให้มีความสอดคล้องของการเข้าถึงข้อมูล โดยเฉพาะกรณีที่มีการเปิดสิทธิ์การเข้าถึงข้อมูลจากระบบหนึ่งไปอีกระบบหนึ่งอัตโนมัติ	แนวทางปฏิบัติ			/			/		/
13	มีการจัดทำทะเบียนรายการบัญชีสินทรัพย์ (Asset lists) การทำทะเบียนชื่อระบบ/เครื่อง (Computer Name) IP Address หรือ MAC Address (Media Access Control Address) สถานที่ติดตั้ง ผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์/ผู้ดูแลระบบ และการเก็บรักษาข้อมูล IP Address เป็นความลับ	แนวทางปฏิบัติ	/	/						/
13.1	ระบบสารสนเทศ	แนวทางปฏิบัติ	/	/						/
13.2	เว็บไซต์	แนวทางปฏิบัติ	/	/						/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
13.3	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย พร้อมระบบปฏิบัติการ	แนวทางปฏิบัติ	/	/						/
13.4	อุปกรณ์คอมพิวเตอร์ทั่วไป เช่น เครื่องคอมพิวเตอร์ Desktop, Notebook, Printer	แนวทางปฏิบัติ	/	/						/
13.5	เครื่องมือแพทย์ที่เชื่อมต่อกับระบบเครือข่าย	แนวทางปฏิบัติ			/	/				/
14	ติดตั้งอุปกรณ์รักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้	แนวทางปฏิบัติ	/	/						/
14.1	ติดตั้งอุปกรณ์ป้องกันภัยคุกคามไซเบอร์ ใช้งานอุปกรณ์ให้เต็มศักยภาพ ทำการตรวจติดตาม (Monitoring) การโจมตีอย่างน้อยเดือนละ 1 ครั้ง หรือตามระดับความเสี่ยง	แนวทางปฏิบัติ	/			/				/
	(1) ติดตั้งและกำหนดค่าเริ่มต้นของ Next-Gen Firewall หรือ Firewall ทุกการเชื่อมต่ออินเทอร์เน็ต ให้ครบทั้งหมด (Block/Deny) การปลดบล็อกต้องได้รับความเห็นชอบของ CISO (ผู้บริหารที่ได้รับมอบหมาย)	แนวทางปฏิบัติ	/			/				/
	(2) ติดตั้ง Next-Gen Antivirus หรือ Antivirus ทั่วไป อัปเดตเครื่องคอมพิวเตอร์ (เครื่องต้นทาง/ปลายทาง เครื่องส่วนตัวที่เชื่อมต่อกับระบบ) อย่างน้อยทุกสัปดาห์	แนวทางปฏิบัติ	/			/				/
	(3) ติดตั้งอุปกรณ์ป้องกันภัยคุกคามไซเบอร์อื่น ๆ ตามความเหมาะสม เช่น XDR, EDR ติดตามการโจมตีเครื่องคอมพิวเตอร์ปลายทาง	แนวทางปฏิบัติ	/			/				/
	(4) ทำการ Patch เพื่ออุดรูรั่วของระบบปฏิบัติการ (O/S) และ firmware อย่างสม่ำเสมอ	แนวทางปฏิบัติ	/	/						/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	(5) monitoring เว็บไซต์อย่างน้อยสัปดาห์ละ 1 ครั้ง	แนวทางปฏิบัติ	/	/						/
14.2	มีการสำรองข้อมูลตามความเหมาะสม	แนวทางปฏิบัติ	/	/						/
14.3	มีจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ Log File สามารถตรวจสอบ รายงานย้อนหลังได้อย่างน้อย 90 วัน หรือตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ	แนวทางปฏิบัติ	/	/						/
14.4	รายงานการขึ้นทะเบียนระบบสารสนเทศ และเว็บไซต์ไปยังศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ. (ศทส.) (1) แจ้ง ศทส. ขอเปลี่ยนชื่อโดเมนของเว็บไซต์และระบบงานที่ไม่ใช้ของ สธ. ให้เป็นของ สธ. รูปแบบ xxxx.moph.go.th (2) ปิดระบบงานที่ไม่ได้ใช้งานหรือที่พบความเสี่ยงทั้งหมด	แนวทางปฏิบัติ	/	/					/	/
15	ป้องกัน ค้นหา จัดการความเสี่ยงที่ทำให้เกิดช่องโหว่ทางไซเบอร์ที่พบบ่อย อย่างต่อเนื่อง ดังต่อไปนี้	แนวทางปฏิบัติ	/	/						/
	(1) ตรวจสอบและอัปเดตระบบปฏิบัติการ (Operating System) และ Environments ของระบบสารสนเทศทั้งหมดให้ทันสมัย เช่น Update Version Service Patch ให้เป็นปัจจุบัน	แนวทางปฏิบัติ	/	/						/
	(2) ค้นหา (scan) CMS Plugins ที่ไม่ได้ใช้งานแล้ว และถอนการติดตั้ง	แนวทางปฏิบัติ	/	/						/
	(3) ทำ Data Encryption ก่อนการส่งผ่าน internet	แนวทางปฏิบัติ	/	/						/
	(4) ปิดช่องทางการเข้าถึงไฟล์ เช่น หน้า Index Directory ที่	แนวทางปฏิบัติ	/	/						/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	สามารถเข้าถึงผ่านอินเทอร์เน็ตโดยไม่ผ่านการตรวจสอบ									
	(5) กำหนด IP Address ที่จะเข้าถึงระบบสารสนเทศสำคัญหรือมีความเสี่ยงสูง เช่น ระบบสารสนเทศที่ใช้ฐานข้อมูล open source: MySQL, SSH	แนวทางปฏิบัติ	/	/						/
	(6) กำหนด Rate-Limitation ในการเข้าถึงระบบสารสนเทศ หรือ Internet ที่หน่วยงานจัดให้บริการ หากเกิด login ผิดบ่อย ๆ จะต้องถูกปิดกั้น	แนวทางปฏิบัติ	/	/						/
	(7) ตรวจสอบและป้องกัน User Input ที่ทำให้เกิดช่องโหว่ที่ใช้โจมตีได้ เช่น SQL Injection, XSS Attack	แนวทางปฏิบัติ	/	/						/
	(8) ตรวจสอบและปิด Error ของระบบตอบกลับ ป้องกันผู้โจมตีตรวจพบ Payload ที่ใช้สามารถเจาะเข้าระบบได้	แนวทางปฏิบัติ	/	/						/
	(9) ปิดกั้นการ Exposed ของ Website Configuration, Database Configuration, Website Directory	แนวทางปฏิบัติ	/	/						/
	(10) ปิดให้เชื่อมต่อ port 3306 จากสาธารณะ โดยไม่ผ่าน VPN	แนวทางปฏิบัติ	/	/						/
	(11) ตรวจสอบ Username และ Permission บนระบบที่อยู่ภายใต้การดูแลให้ถูกต้อง หากพบความผิดปกติทำการแก้ไขโดยทันที	แนวทางปฏิบัติ	/	/						/
16	กำหนดแนวทางการระบุและยืนยันตัวตน ของผู้ใช้งาน (User Identification and Authentication) ก่อนการใช้งานระบบทุกครั้ง ควรใช้ Multi-factor Authentication หรืออย่างน้อย รหัสผ่านรายบุคคล	แนวทางปฏิบัติ			/			/	/	/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
16.1	ระบบสารสนเทศที่ใช้การยืนยันตัวตนด้วยรหัสผ่าน (Password) ต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้ (1) กำหนดรหัสผ่านเริ่มต้นที่ยากต่อการคาดเดา และการส่งมอบให้กับผู้ใช้งานอย่างปลอดภัย (2) สามารถจัดการการสร้างชื่อผู้ใช้งานที่ไม่ซ้ำกันและคาดเดาได้ยาก (3) จำกัดจำนวนครั้งที่ยอมให้ผู้ใช้งาน ใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน 3 ครั้ง	แนวทางปฏิบัติ			/			/		/
16.2	การบริหารจัดการรหัสผ่าน (Password) อย่างน้อยดังต่อไปนี้ (1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบพ้นจากตำแหน่ง (2) กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนด (3) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจาก ผู้ที่ได้รับมอบหมาย โดยมีการกำหนดระยะเวลา และกำหนดให้รหัสต่างจากปกติ	แนวทางปฏิบัติ			/			/		/
16.3	กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน Password (Session Time-out) เมื่อมีการว่างเว้นจากการใช้งานเป็นเวลานานกว่า 30 นาที หรือตามความเหมาะสม	แนวทางปฏิบัติ			/			/	/	/
17	จัดทำและปฏิบัติตามแนวทางการเข้าถึงระบบสารสนเทศของ	แนวทางปฏิบัติ			/			/		/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	หน่วยงาน ด้วยอุปกรณ์คอมพิวเตอร์ส่วนบุคคล (1) การขออนุมัติ/ปรับปรุง/ยกเลิกสิทธิ์การเข้าถึง ตามหน้าที่ความรับผิดชอบ ระบุ ระบบงานที่อนุญาต ช่วงเวลาการทำงาน (2) การขึ้นทะเบียนอุปกรณ์คอมพิวเตอร์ส่วนบุคคลที่สามารถเข้าถึงระบบสารสนเทศสำคัญ ตรวจสอบ O/S และ antivirus ที่ถูกต้องมีลิขสิทธิ์ (3) ตั้งค่า Firewall ของหน่วยงานให้เปิดรับอุปกรณ์ที่ขึ้นทะเบียนเท่านั้น (4) ผู้ใช้งานจากระยะไกลต้อง Login และพิสูจน์ยืนยันตัวตน (Authentication) อย่างน้อยด้วยการใช้รหัสผ่านทุกครั้ง และจำกัดระยะเวลาของการพักใช้งาน (Limitation of Connection Time)									
18	จัดทำและปฏิบัติตามแนวทางการยืมอุปกรณ์คอมพิวเตอร์ของหน่วยงานออกไปใช้นอกสถานที่ (1) เตรียมอุปกรณ์ให้มีข้อมูลที่จำเป็น จัดเก็บสำรองข้อมูล ติดตั้งระบบล็อกการใช้งานจากบุคคลภายนอก (2) ผู้ใช้งานต้องเก็บอุปกรณ์ไว้กับตัว ไม่อนุญาตให้บุคคลภายนอกใช้งาน (3) ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไขหรือทำสำเนาข้อมูล เพื่อนำไปใช้งานที่อื่นๆ ยกเว้นได้รับการอนุญาต (4) ผู้ใช้งานต้องนำส่งคืนอุปกรณ์เมื่อหมดความจำเป็นต้องใช้ (5) ผู้ดูแลต้องตรวจสอบการ	แนวทางปฏิบัติ			/			/		/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	ละเมิดความปลอดภัยและความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์ที่รับคืน									
19	จัดให้มีการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : ROPA) โดยอาจพิจารณาจัดทำกิจกรรมสำคัญ เช่น กิจกรรมที่มีการเก็บ รวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคลอ่อนไหว	แนวทางปฏิบัติ			/	/			/	/
20	จัดทำและปฏิบัติตามแนวทางการทำข้อกำหนดและขอบเขตการพัฒนา (TOR) ซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development) (1) แยกประเภทความต้องการให้ชัดเจน - จัดซื้อ ได้กรรมสิทธิ์การใช้งาน - จ้างพัฒนา ได้ลิขสิทธิ์ ทรัพย์สินทางปัญญา และกรรมสิทธิ์การใช้งาน - ซื้อหรือพัฒนาต่อยอด ได้กรรมสิทธิ์ ได้ลิขสิทธิ์บางส่วนที่พัฒนาเพิ่มเติม - จ้างเหมาบริการต้องกำหนดให้ข้อมูลเป็นของผู้จ้าง ใช้ Source Code ตามที่ผู้จ้างกำหนด มีการเก็บ Source Code, Library ไว้ที่ผู้จ้าง เพื่อให้สามารถประมวลผลได้ (2) กำหนดให้ผู้ขาย/ผู้พัฒนา/ผู้ให้บริการ ต้องดำเนินการด้านความปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคลและอื่น ๆ ที่สอดคล้องกับ พ.ร.บ.ที่เกี่ยวข้อง และคำนึงถึงหลักการ ITIL, OWASP TOP 10, NIST, CIS และ API Security Standard และปฏิบัติตาม	แนวทางปฏิบัติ			/	/			/	/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	มาตรการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข (3) ผู้ให้บริการระบบดิจิทัลหรือผู้พัฒนาระบบต้องลงนามและปฏิบัติตามข้อตกลงไม่เปิดเผยข้อมูล/Non-Disclosure Agreement (NDA) และข้อตกลงการประมวลผลข้อมูลส่วนบุคคล/Data Processing Agreement (DPA) ก่อนดำเนินการ (4) ต้องมีการขออนุมัติจากผู้ดูแลระบบก่อนการทดสอบ ติดตั้ง ถ่ายโอน เชื่อมต่อข้อมูล (5) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องสามารถดำเนินการเปลี่ยนรหัสผ่านต่างๆ ได้เอง									
21	จัดทำและปฏิบัติตามแนวทางการเชื่อมต่อระบบสารสนเทศ เช่น HIS, LIS, PACS ที่มีการให้บริการจากบุคคลภายนอกกับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และแพลตฟอร์ม (1) ระบบสารสนเทศที่ขอเชื่อมโยงมี การดำเนินการตาม พ.ร.บ. PDPA และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ไม่น้อยกว่าที่หน่วยงานได้ทำการไว้ (2) ระบบที่รับ-ส่งข้อมูลสำคัญหรืออ่อนไหวต้องมีกระบวนการแฝงข้อมูลส่วนบุคคลเข้ารหัส	แนวทางปฏิบัติ			/	/				/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	(Encryption) ที่เป็นมาตรฐานสากล (3) ระบบสามารถรับ-ส่งข้อมูลผ่าน API ที่มีมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (4) มีการอนุญาตเชื่อมแพลตฟอร์มสารสนเทศ และการเข้าถึงฐานข้อมูลของหน่วยงานเป็นลายลักษณ์อักษร (5) ผู้เชื่อมต่อต้องลงนามและปฏิบัติตามข้อตกลง NDA, DPA, อาจรวมถึงข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล/Data Sharing Agreement (DSA) แล้วแต่กรณี (6) กำหนดสิทธิ์การเข้าถึงข้อมูลตามภารกิจของผู้ใช้งานจากภายนอกและตามชั้นความลับ (7) มีการบันทึกการจราจรข้อมูลคอมพิวเตอร์ (Log Files) ทุกธุรกรรม (Transaction)									
22	หน่วยงานภายนอกต้องจัดทำแผนและวิธีการดำเนินงาน เพื่อขออนุญาตเข้าถึงโครงสร้างพื้นฐานระบบสารสนเทศ หรือฐานข้อมูล เป็นรายกิจกรรม เช่น การพัฒนาระบบ การทดสอบระบบ การประมวลผลการดูแลระบบและจะเข้าถึงได้เมื่อได้รับการอนุญาตแล้วเท่านั้น	แนวทางปฏิบัติ			/	/				/
23	จัดทำและปฏิบัติตามแนวทางด้านสถานที่และระบบสนับสนุนสำหรับ Data Center สถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์บริหารเครือข่าย ดังนี้ (1) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญของ	แนวทางปฏิบัติ			/	/				/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	แต่ละส่วนจัดทำแผนผังแสดงตำแหน่งของพื้นที่ ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบ (1) IT Equipment Area พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) พื้นที่ที่ให้บุคคลภายนอกเข้าถึง เป็นต้น (2) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก (3) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว เพราะเป็นปัจจัยเสี่ยงที่อาจถูกคุกคามได้ (4) จัดเก็บสายสัญญาณต่างๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิทเพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง (5) ต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่าง เมื่อไม่มีเจ้าหน้าที่ประจำอยู่ (6) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว (7) ควรเป็นพื้นที่ที่ไม่มีน้ำท่วมถึง ไม่มีน้ำรั่วซึมจากหลังคาหรือกำแพง หากมีความเสี่ยงจะต้องมีแนวทางการเฝ้าระวังและการแก้ปัญหา									
24	จัดทำและปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยของพื้นที่เขตหวงห้ามโดยเด็ดขาด ให้	แนวทางปฏิบัติ					/	/		/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	ทำการกำหนดในแต่ละส่วนพื้นที่ดังนี้ (1) กำหนดชื่อผู้มีหน้าที่ในการกำกับดูแล Data Center (2) กำหนดชื่อผู้มีหน้าที่ในการปฏิบัติงานแต่ละพื้นที่ สิทธิ์ผ่านเข้า-ออก และมีการพิสูจน์ตัวตน ควบคุมการเข้า-ออกในพื้นที่สำคัญ (3) ห้ามบุคคลอื่นเข้าไปใน Data Center โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้กำกับดูแล Data Center (4) บุคคลภายนอกที่ได้รับอนุญาต จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตน ที่ออกโดยราชการ และมีการลงบันทึกข้อมูลบัตรในสมุดบันทึกการเข้า-ออกจัดเก็บบันทึกการเข้า-ออกพื้นที่สำคัญ (5) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาและต้องปฏิบัติตามแนวทางการรักษาความปลอดภัยไซเบอร์ (6) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกที่เข้ามาปฏิบัติงานในพื้นที่สำคัญ ห้ามนำอุปกรณ์หรือชิ้นส่วนใดออกจาก Data Center เว้นแต่ได้รับอนุญาต (7) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด										
25	จัดทำและปฏิบัติตามแนวทางการบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครือข่าย (Network) (1) กำหนดผู้รับผิดชอบดูแลระบบคอมพิวเตอร์แม่ข่าย	แนวทางปฏิบัติ			/	/				/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	(Server) เครือข่าย (Network) และการเข้าถึง Firewall (2) จัดทำแผนผังสายสัญญาณสื่อสาร (Network Diagram) ระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ (3) การติดตั้ง Firewall ระบบรักษาความปลอดภัย เช่น Next-Gen Firewall, Virus Scanning เป็นต้นจะต้องมีการบันทึกการเปลี่ยนแปลง ปรับปรุงการตั้งค่าและการเชื่อมต่อสัญญาณ โดยพิจารณาตั้งค่าให้ใช้เท่าที่จำเป็นเพื่อป้องกันการโจมตีจนส่งผลให้ระบบ Internet ช้าเกินไป (4) ดำเนินการตรวจสอบ Log File หรือรายงาน (Report) ของระบบป้องกันหรือรักษาความมั่นคงปลอดภัยเป็นประจำและสม่ำเสมอ หากพบความผิดปกติให้รายงานผู้บังคับบัญชาโดยทันที (5) สำรองข้อมูลการกำหนดค่าต่างๆ (Configuration) ของอุปกรณ์ป้องกันและรักษาความมั่นคงปลอดภัยเป็นประจำทุกเดือนและทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า (6) แบ่ง Intranet เครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ แยกจาก Internet เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน (7) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลางโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ เช่น อุปกรณ์ที่เชื่อมต่อกับระบบ									

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	เครือข่ายหลัก (Core switch) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์จัดเส้นทาง (Router) โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (8) ทำป้ายชื่อ (Label) สำหรับสายสัญญาณและบนอุปกรณ์ (9) พิจารณาใช้งานสาย Fiber optic หรือ สายสัญญาณแบบ Coaxial Cable สำหรับระบบสารสนเทศที่สำคัญ (10) ร้อยท่อสายสัญญาณ สายไฟและสายเคเบิลอื่นที่แยกจากกัน ป้องกันการแทรกแซง/รบกวนสัญญาณกัน การตัดสายสัญญาณผิดพลาด และการกัดแทะของสัตว์ เช่น หนู									
26	จัดทำและปฏิบัติตามแนวทางการควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) (1) ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ แบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier) โดยเฉพาะระบบงานที่เป็นชั้นความลับ (2) กำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) หรือที่ดีกว่า ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN	แนวทางปฏิบัติ	/			/				/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	Client) และ อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าโดยไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย									
27	จัดทำและปฏิบัติตามแนวทางการดูแลระบบจัดการฐานข้อมูล (Database Management Operation) (1) กำหนดสิทธิ์และรายชื่อผู้บริหารระบบฐานข้อมูล (Database Administrator) ตามลำดับ (2) การบันทึกการจราจรข้อมูลคอมพิวเตอร์ (Log Files) ทุกธุรกรรม (Transaction) ที่มีการเข้าถึงระบบจัดการฐานข้อมูลให้สามารถตรวจสอบย้อนหลังได้อย่างน้อย 90 วัน (3) ปรับปรุง / กำหนดค่า ระบบจัดการฐานข้อมูลให้เหมาะสมทันสมัย หรือป้องกันการเกิดปัญหาเป็นประจำ (4) กำหนดเกณฑ์การสำรอง / สำเนา / ทดสอบกู้คืนข้อมูล/ระบบ (Restore Test)	แนวทางปฏิบัติ			/	/			/	/
28	จัดทำและปฏิบัติตามแนวทางการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ทุกชนิด (Equipment Maintenance) (1) ให้มีการบำรุงรักษาอุปกรณ์ตามคำแนะนำในการบำรุงรักษาของผู้ผลิต (2) จัดเก็บบันทึกปัญหาและกิจกรรมการบำรุงรักษาอุปกรณ์ทุกครั้งเพื่อใช้ในการประเมินจัดซื้อทดแทน (3) การนำอุปกรณ์ที่มีการเก็บข้อมูลออกไป ซ่อมบำรุงรักษา ให้	แนวทางปฏิบัติ					/	/		/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	ดำเนินการสำรองหรือเข้ารหัสข้อมูลส่วนบุคคล หรือการจำหน่ายขายซากให้ดำเนินการลบข้อมูลสำคัญและข้อมูลส่วนบุคคล ก่อนนำออกไป									
29	จัดให้มีกระบวนการลบหรือทำลายข้อมูล เมื่อสิ้นสุดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ/ถอนความยินยอม	แนวทางปฏิบัติ	/	/					/	/
30	จัดทำและปฏิบัติตามแนวทางการทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญและข้อมูลอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์นั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้ (1) กระดาษ ควรใช้เครื่องทำลายเอกสาร หรือพิจารณาวิธีอื่นๆ ที่ดีกว่า (2) Flash Drive ควรใช้วิธีการทุบหรือบดให้เสียหาย หรือพิจารณาการทำลายตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา (3) แผ่น CD/DVD ควรใช้เครื่องทำลายเอกสารที่สามารถทำลายแผ่น CD/DVD ได้	แนวทางปฏิบัติ			/	/				/

ข้อ	รายการ	แผนด้าน	ปีงบประมาณ / หน่วยปฏิบัติ						ผู้รับผิดชอบหลัก	
			2566		2567		2568		ผู้บริหาร	IT
			กอง	รพช	กอง	รพช	กอง	รพช		
	(4) เทป ควรใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย (5) ฮาร์ดดิสก์ ควรใช้วิธีการทุบหรือบดให้เสียหาย หรือพิจารณาการทำลายตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา									

ภาคผนวก ก

สื่อสารมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ และการรักษาความลับของข้อมูลส่วนบุคคล สำหรับผู้ใช้งานระบบสารสนเทศทั่วไป

คณะผู้บริหารของหน่วยงานให้ความสำคัญกับการสื่อสาร และสร้างพฤติกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ และการรักษาความลับของข้อมูลส่วนบุคคล และควบคุมกำกับให้บุคลากรปฏิบัติตามมาตรการที่กำหนด ผู้ใช้ทุกคนควรรับทราบและปฏิบัติตามมาตรการ เพราะปัญหาการรั่วไหลหรือถูกโจมตีมาจากข้อผิดพลาดของบุคลากรผู้ใช้งานระบบ (Human Errors) เป็นปัญหาที่สามารถแก้ไขได้โดยการฝึกวินัยการใช้งานระบบสารสนเทศซึ่งไม่ต้องลงทุนสูง ควรทบทวนและซักซ้อมความเข้าใจอย่างสม่ำเสมอ อย่างน้อยปีละครั้ง เช่นเดียวกับการซ้อมแผนอัคคีภัย

1. **ผู้ใช้งานให้ทราบถึงความสำคัญของการรักษาความลับและการปกป้องข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**
2. **ผู้ใช้งานเข้าใจเข้าถึงข้อมูลส่วนบุคคล ข้อมูลตามชั้นความลับ**
    - ระบุวิธีการเข้าถึงข้อมูลที่เหมาะสมและเฉพาะเจาะจงเพื่อป้องกันการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต ตัวอย่างเช่นให้ใช้ระบบรหัสผ่านที่แข็งแกร่งและการกำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทและความจำเป็นของผู้ใช้
3. **การจัดเก็บและการดำเนินการกับข้อมูล:**
    - ระบุวิธีการจัดเก็บข้อมูลให้เป็นระเบียบเรียบร้อยและปลอดภัย รวมถึงการดำเนินการกับข้อมูลอย่างถูกต้อง เช่น การรักษาความถูกต้องของข้อมูล เป็นต้น
4. **การทำสำเนาข้อมูล (Backup):**
    - อธิบายถึงความสำคัญของการสำรองข้อมูล (Backup) และการดำเนินการสำรองข้อมูลอย่างเป็นระบบ รวมถึงการทดสอบและการกู้คืนข้อมูลเพื่อให้ผู้ใช้รับทราบถึงวิธีการดำเนินการเมื่อเกิดข้อผิดพลาดหรือภัยคุกคามที่อาจทำให้ข้อมูลสูญหาย
5. **การปรับปรุงและการอัปเดตข้อมูล:**
    - เน้นความสำคัญของการปรับปรุงและการอัปเดตข้อมูลเพื่อให้ข้อมูลเป็นปัจจุบันและปลอดภัย รวมถึงการอัปเดตซอฟต์แวร์และระบบปฏิบัติการให้มีเวอร์ชันล่าสุด
6. **การฝึกอบรมและการเผยแพร่ข้อมูล:**
    - อธิบายถึงการจัดหาการฝึกอบรมและการเผยแพร่ข้อมูลเกี่ยวกับการรักษาความปลอดภัยข้อมูลสำหรับผู้ใช้ทั่วไป เช่น การจัดหาคอร์สเรียนออนไลน์เกี่ยวกับความปลอดภัยทางไซเบอร์ การเผยแพร่คู่มือหรือเอกสารที่เกี่ยวข้อง เป็นต้น
7. **การรายงานการละเมิดความปลอดภัย:**
    - ระบุวิธีการรายงานความผิดปกติหรือการละเมิดความปลอดภัยของข้อมูลที่ผู้ใช้พบเจอ รวมถึงการรายงานช่องโหว่ในระบบสารสนเทศที่อาจส่งผลกระทบต่อความปลอดภัย

ตัวอย่าง : เอกสารสื่อสารมาตรการ
สำหรับผู้ใช้ทั่วไป ใช้ในการรับทราบและปฏิบัติ
เรื่อง “การป้องกันภัยคุกคามทางไซเบอร์” ในระบบสารสนเทศของโรงพยาบาล

1. **การสร้างความตระหนักรู้และการฝึกอบรม:**
    - หลักสำคัญในการป้องกันภัยคุกคามทางไซเบอร์คือการเพิ่มความตระหนักรู้ในเรื่องความปลอดภัยทางไซเบอร์ จัดกิจกรรมอบรมและการฝึกอบรมเพื่อเพิ่มความรู้เกี่ยวกับการตรวจจับและป้องกันการโจมตีทางไซเบอร์ เช่น การรู้จักกับการโจมตีแบบพยายามเข้าสู่ระบบ (Brute Force Attacks), การโจมตีแบบฟิชชิ่ง (Phishing Attacks), และการรู้จักกับเทคนิคการเข้ารหัส (Encryption Techniques)
2. **การสร้างความมีสติและปฏิบัติตามนโยบายความปลอดภัย:**
    - เพื่อให้ผู้ใช้ทราบถึงความสำคัญของความปลอดภัยทางไซเบอร์ ให้กำหนดนโยบายความปลอดภัยที่เข้มงวดและชัดเจน เช่น การใช้รหัสผ่านที่แข็งแกร่ง, การไม่เปิดเผยข้อมูลส่วนตัว, และการปฏิบัติตามขั้นตอนและนโยบายที่กำหนดไว้
3. **การรักษาความปลอดภัยของอุปกรณ์:**
    - อุปกรณ์ที่ใช้ในการเชื่อมต่อกับระบบสารสนเทศควรรักษาความปลอดภัยอย่างเหมาะสม เช่น การปรับแต่งการตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย (Network Devices) และการปรับค่าความปลอดภัยของอุปกรณ์เครื่องคอมพิวเตอร์ส่วนบุคคล เช่น คอมพิวเตอร์โน้ตบุ๊ค (Laptop) และสมาร์ทโฟน (Smartphone)
4. **การประเมินและการอัปเดตระบบ:**
    - ควรประเมินและอัปเดตระบบสารสนเทศและซอฟต์แวร์เป้าหมายตลอดเวลา เพื่อรับมือกับช่องโหว่ใหม่ที่คาดไม่ถึง และใช้ชุดแก้ไขปัญหาที่มีอัปเดตล่าสุดเพื่อป้องกันการโจมตีที่อาจเกิดขึ้น
5. **การสำรวจและการตรวจสอบ:**
    - ควรสำรวจและตรวจสอบระบบสารสนเทศเพื่อตรวจหาความผิดปกติและภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ การตรวจสอบเหล่านี้อาจรวมถึงการตรวจสอบการเข้าถึงที่ไม่ได้รับอนุญาต และการบันทึกกิจกรรมการใช้งานที่เกี่ยวข้องกับระบบสารสนเทศ
6. **การสำรวจและการสำรองข้อมูลสำคัญ:**
    - ควรมีการสำรวจและสำรองข้อมูลสำคัญอย่างสม่ำเสมอเพื่อป้องกันการสูญหายของข้อมูลและการโจมตีทางไซเบอร์ที่อาจทำให้ข้อมูลสำคัญถูกเข้าถึงหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
7. **การใช้งานออนไลน์อย่างปลอดภัย:**
    - ควรใช้เทคนิคการรักษาความปลอดภัยทางไซเบอร์ในการใช้งานออนไลน์ เช่น การตรวจสอบเว็บไซต์ที่เชื่อถือได้ (Trusted Websites) และการใช้งานอีเมลล์และสื่อสังคมออนไลน์อย่างระมัดระวัง เพื่อป้องกันการเป็นเหยื่อของการฉ้อโกงทางอินเทอร์เน็ต (Online Scams) หรือการแอบแฝงเข้าสู่ระบบของผู้ไม่ประสงค์ดี

การป้องกันภัยคุกคามทางไซเบอร์เป็นกระบวนการที่ต้องมีการปรับปรุงและอัปเดตอย่างต่อเนื่อง ควรระมัดระวังและปฏิบัติตามแนวทางที่เหมาะสมเพื่อปกป้องข้อมูลส่วนบุคคลและความปลอดภัยของระบบสารสนเทศในทุก ๆ ช่วงเวลา

ตัวอย่าง : เอกสารสื่อสารมาตรการ
สำหรับผู้ใช้ทั่วไป ใช้ในการรับทราบและปฏิบัติ
เรื่อง “การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)” ในโรงพยาบาล

1. **การรักษาความลับ:**
    - กรุณาเปลี่ยนรหัสผ่าน (Password) โดยทันที เมื่อมีการเข้าสู่ระบบในครั้งแรก และเก็บรักษารหัสผ่านไว้เป็นความลับ ไม่อนุญาตให้ผู้อื่นใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) เพื่ออ่าน รับ หรือส่งข้อความ และหลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้อง Logout ทุกครั้ง
    - การส่งข้อมูลที่เป็นความลับควรใช้วิธีการเข้ารหัสข้อมูล E-Mail ที่หน่วยงานกำหนดไว้ และให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-Mail ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิด
2. **การใช้งานให้มีความปลอดภัย:**
    - ต้องตรวจสอบเอกสารแนบจาก E-Mail ก่อนการเปิดทุกครั้ง โดยอาจใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น
    - ต้องตรวจสอบลิงก์ที่แนบมากับ E-Mail ก่อนการกดลิงก์ทุกครั้ง โดยให้คิดเสมอว่าเป็นลิงก์ที่ไม่มีความปลอดภัย
    - ไม่ส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น เช่น จดหมายขยะ (Spam Mail) จดหมายลูกโซ่ (Chain Letter) จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา เป็นต้น และต้องไม่ใช้ข้อความที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน
3. **การจัดการพื้นที่จัดเก็บและการทำสำเนาข้อมูล (Backup):**
    - บริหารจัดการ E-Mail ให้มีความเหมาะสมตามพื้นที่จัดเก็บ
    - ทำการสำรองข้อมูล E-Mail ตามความจำเป็นอย่างสม่ำเสมอ
4. **การแจ้งเตือนและรายงานปัญหา:**
    - หากท่านสงสัยหรือพบปัญหาที่เกี่ยวข้องกับความปลอดภัยของ E-mail กรุณาแจ้งเรื่องให้ทีมงานความปลอดภัยหรือบุคคลที่รับผิดชอบตามนโยบายของโรงพยาบาล

การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ควรระมัดระวังและปฏิบัติตามแนวทางที่เหมาะสมเพื่อป้องกับภัยคุกคามทางไซเบอร์ที่แฝงมากับ E-Mail

ตัวอย่าง : เอกสารสื่อสารมาตรการ
สำหรับผู้ใช้ทั่วไป ใช้ในการรับทราบและปฏิบัติ
เรื่อง “การปฏิบัติทั่วไป” ของการใช้งานระบบสารสนเทศของโรงพยาบาล

1. **ปฏิบัติตามนโยบายและข้อกำหนด**:
    - กรุณาปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการใช้ระบบสารสนเทศของโรงพยาบาล ตรวจสอบว่าท่านเข้าใจและปฏิบัติตามข้อกำหนดเหล่านี้อย่างถูกต้อง
2. **การเข้าถึงและการใช้งาน:**
    - กรุณาใช้ระบบสารสนเทศเฉพาะเพื่อการทำงานที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของท่านเท่านั้น หลีกเลี่ยงการเข้าถึงหรือใช้งานข้อมูลที่ไม่ได้รับอนุญาต
3. **การแจ้งเตือนและรายงานปัญหา:**
    - หากท่านสงสัยหรือพบปัญหาที่เกี่ยวข้องกับความปลอดภัยของระบบสารสนเทศ กรุณาแจ้งเรื่องให้ทีมงานความปลอดภัยหรือบุคคลที่รับผิดชอบตามนโยบายของโรงพยาบาล
4. **การรักษาความลับ:**
    - กรุณารักษาความลับของข้อมูลที่คุณเข้าถึงในระบบสารสนเทศ ห้ามเปิดเผยหรือแจกจ่ายข้อมูลให้แก่บุคคลภายนอกที่ไม่มีอำนาจ
5. **การปฏิบัติตามคำแนะนำ**:
    - กรุณาปฏิบัติตามคำแนะนำที่ให้มาจากทีมงานความปลอดภัย โปรดอัปเดตและติดตั้งซอฟต์แวร์ป้องกันไวรัสและแก้ไขช่องโหว่เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

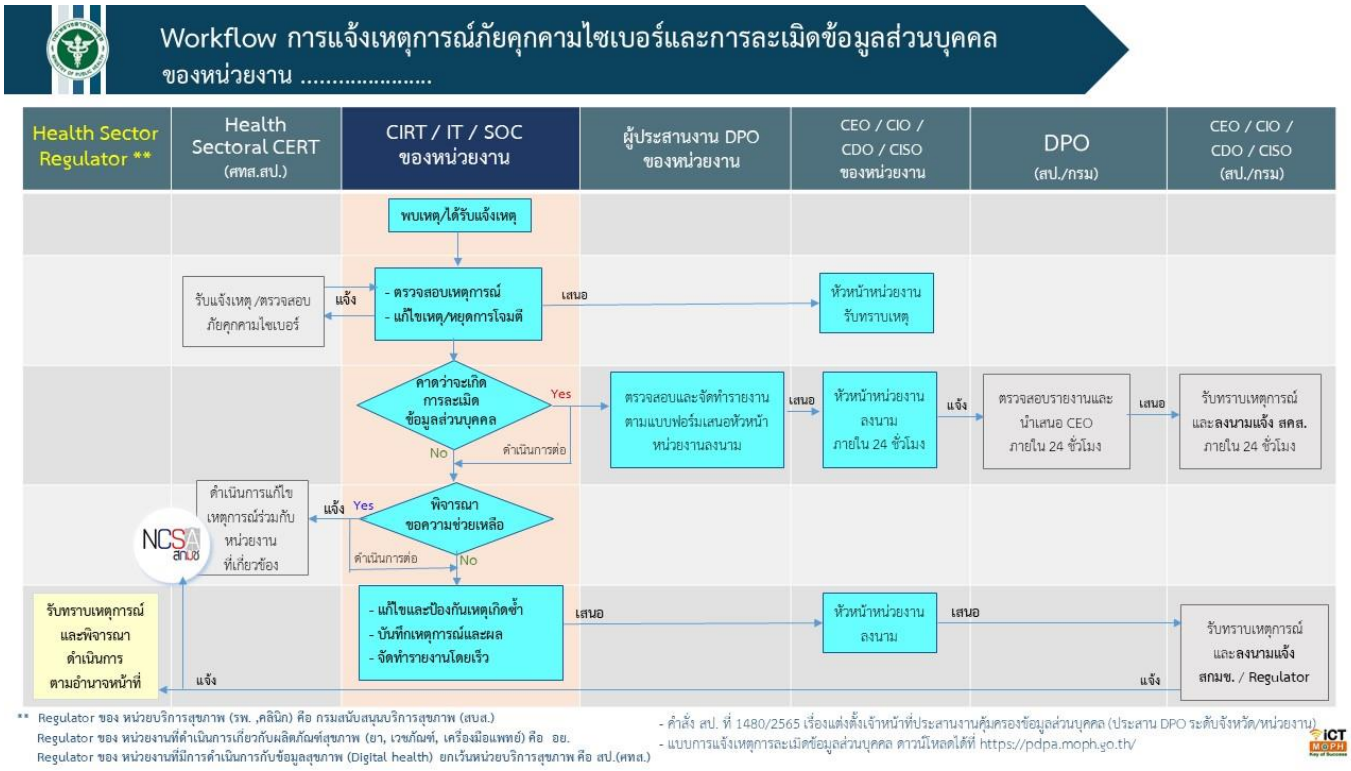
การปฏิบัติตามมาตรการด้านความปลอดภัยเป็นสิ่งสำคัญที่ช่วยให้ระบบสารสนเทศของโรงพยาบาลมีความมั่นคงปลอดภัยและมีประสิทธิภาพ ทางทีมงานของเราจะพยายามรักษาความปลอดภัยของระบบสารสนเทศของโรงพยาบาลเพื่อให้ท่านมีประสบการณ์การใช้งานที่ดีที่สุด

ขอขอบคุณท่านที่มีส่วนร่วมในการรักษาความปลอดภัยของระบบสารสนเทศของโรงพยาบาลของเรา หากท่านมีคำถามหรือข้อสงสัยเพิ่มเติม กรุณาติดต่อทีมงานด้านความปลอดภัยของเรา

ขอแสดงความนับถือ
[ชื่อหน่วยงานหรือผู้ลงนาม]
[วันที่]

ภาคผนวก ข

Workflow การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์และการละเมิดข้อมูลส่วนบุคคล



- Computer Emergency Response Team (CERT)
- Computer Incident Response Team (CIRT)
- Security Operations Center (SOC)
- Data Protection Officer (DPO)

ภาคผนวก ค
หน้าที่และอำนาจของผู้ดูและระบบสารสนเทศของหน่วยงาน เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

1. ผู้รับผิดชอบการบริหารเทคโนโลยีสารสนเทศและข้อมูล (CIO & CDO) ทำหน้าที่บริหารเทคโนโลยีสารสนเทศและระบบสุขภาพดิจิทัล กำกับและสนับสนุน ให้เกิดความพร้อมใช้งานของระบบสารสนเทศที่สำคัญอย่างต่อเนื่อง (SLA 99.9%) จัดทำแผนงบประมาณ/โครงการ กำกับดูแล กำหนดมาตรการที่เกี่ยวข้องกับการบริหาร ตามแนวทางการคุ้มครองข้อมูลส่วนบุคคล และ พ.ร.บ. ต่าง ๆ รวมถึงการพัฒนานวัตกรรม
หมายเหตุ หน่วยงานขนาดใหญ่ แยกผู้ที่ทำหน้าที่บริหารเทคโนโลยีสารสนเทศ (Chief Information Officer) จากผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ได้

2. ผู้รับผิดชอบการรักษาความปลอดภัยไซเบอร์ (CISO) ทำหน้าที่จัดทำแผนบริหารความเสี่ยง (Risk Management Plan) ป้องกัน เฝ้าระวัง รับมือการโจมตีและภัยคุกคามตามแนวทางของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ จัดให้มี Computer Incident Response Team (CIRT) และ Security Operations Center (SOC) และระบบตรวจสอบภายในของหน่วยงาน (Internal Auditor)

3. หัวหน้ากลุ่มงาน/หัวหน้าศูนย์/หัวหน้างานเทคโนโลยีสารสนเทศ มีหน้าที่ความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้ (สำหรับหน่วยงานที่มีนักวิชาการคอมพิวเตอร์หลายคน อาจมอบหมายหน้าที่ในลำดับถัดไป โดยทำเป็นลายลักษณ์อักษร)

3.1 จัดทำหนังสือขออนุมัติสิทธิ์และระบบจัดการสิทธิ์การเข้าถึงระบบสารสนเทศ เครื่องคอมพิวเตอร์แม่ข่าย การเชื่อมระบบเครือข่าย การนำทรัพย์สินออกไปนอกหน่วยงาน และอื่น ๆ เสนอ CIO

3.2 จัดการความเสี่ยงตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยตามแนวทางคำแนะนำในเอกสารนี้ ร่วมกับผู้เกี่ยวข้องเสนอ CISO ดูแล CIRT/SOC ให้เกิดความพร้อมใช้งานของระบบสารสนเทศอย่างต่อเนื่อง (SLA 99.9%) เฝ้าระวังภัยคุกคามทางไซเบอร์ และประสานงานกับ Health CERT, DPO

3.3 บริหารจัดการให้มีการระบุและยืนยันตัวตนของผู้ใช้งานตามสิทธิ์ (User Identification and Authentication) และทะเบียนรายชื่อผู้มีสิทธิ์เข้าใช้งาน ระบบสารสนเทศ เครื่องแม่ข่าย เครือข่าย และอื่น ๆ

3.4 จัดทำทะเบียนทรัพย์สิน แผนผังโครงสร้างระบบสารสนเทศ แผนผัง Data Center และเครือข่าย

3.5 จัดทำทะเบียนบัญชีผู้ใช้งาน สิทธิ์การเข้าใช้งานระบบสารสนเทศ เครื่องคอมพิวเตอร์แม่ข่าย การเชื่อมระบบเครือข่าย การนำทรัพย์สินออกไปนอกหน่วยงาน และอื่น ๆ

3.6 จัดทำหรือให้คำแนะนำโครงการขออนุมัติจัดหาระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์ของหน่วยงาน ให้เป็นไปตามแนวทางการรักษาความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล

3.7 มอบหมายและกำกับดูแลผู้มีหน้าที่ควบคุมพื้นที่ Data Center ระบบเครือข่าย (Network) และเครื่องคอมพิวเตอร์แม่ข่าย (Server) เป็นลายลักษณ์อักษร

3.8 ตรวจสอบทบทวนความถูกต้อง ทันสมัย ของมาตรการแนวทาง สิทธิต่าง ๆ อย่างสม่ำเสมอ (อย่างน้อยปีละ 1 ครั้ง)

3.9 ปฏิบัติงานอื่นๆ ที่ได้รับมอบหมาย

ภาคผนวก ง
แบบฟอร์มที่เกี่ยวข้องกับการเชื่อมต่อระบบสารสนเทศ

- ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล (DSA : Data Sharing Agreement)
- ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA : Data Processing Agreement)

https://pdpa.moph.go.th/pdpa/law_ops.php

หรือ https://moph.cc/lOKrqKOW_

คณะผู้จัดทำ
แนวทางการจัดทำแผนการบริหารความเสี่ยง งบประมาณ บุคลากร
และแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
และการคุ้มครองข้อมูลส่วนบุคคล ปีงบประมาณ พ.ศ. 2566-2568

ที่ปรึกษา

1. แพทย์หญิงปฐมพร ศิรประภาศิริ นายแพทย์ทรงคุณวุฒิ (ด้านเวชกรรม)
   ผู้บริหารข้อมูลระดับสูง (CDO) ประจำกระทรวงสาธารณสุข
2. นายแพทย์อนันต์ กนกศิลป์ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ.
   ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ประจำสำนักงานปลัดกระทรวงสาธารณสุข
3. นายแพทย์กิตติ โล่สุวรรณรักษ์ ผู้อำนวยการโรงพยาบาลคูเมือง จังหวัดบุรีรัมย์
   รองผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ.
4. นายแพทย์ภาณุพงศ์ ตันติรัตน์ ผู้ช่วยผู้อำนวยการด้านสารสนเทศโรงพยาบาลสระบุรี
5. นายแพทย์ทรงยศ ชญานินปรเมศ โรงพยาบาลเกาะสมุย จังหวัดสุราษฎร์ธานี
6. นายธีรยศถ์ ทองศรี สำนักงานเขตสุขภาพที่ ๑๑ จังหวัดสงขลา
7. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คณะทำงาน

1. นายราชิ ปาลือชา ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ.
2. นางสาวสุธาทิพย์ คล้ายเหล็ง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ.
3. นางรุ่งนิภา อมาตยคง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ.
4. นางสาวศิริพร เภรีฤกษ์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ.

ผลิตเอกสาร : เมษายน - มิถุนายน 2566

เผยแพร่ : มิถุนายน 2566

สำนักงานปลัดกระทรวงสาธารณสุข