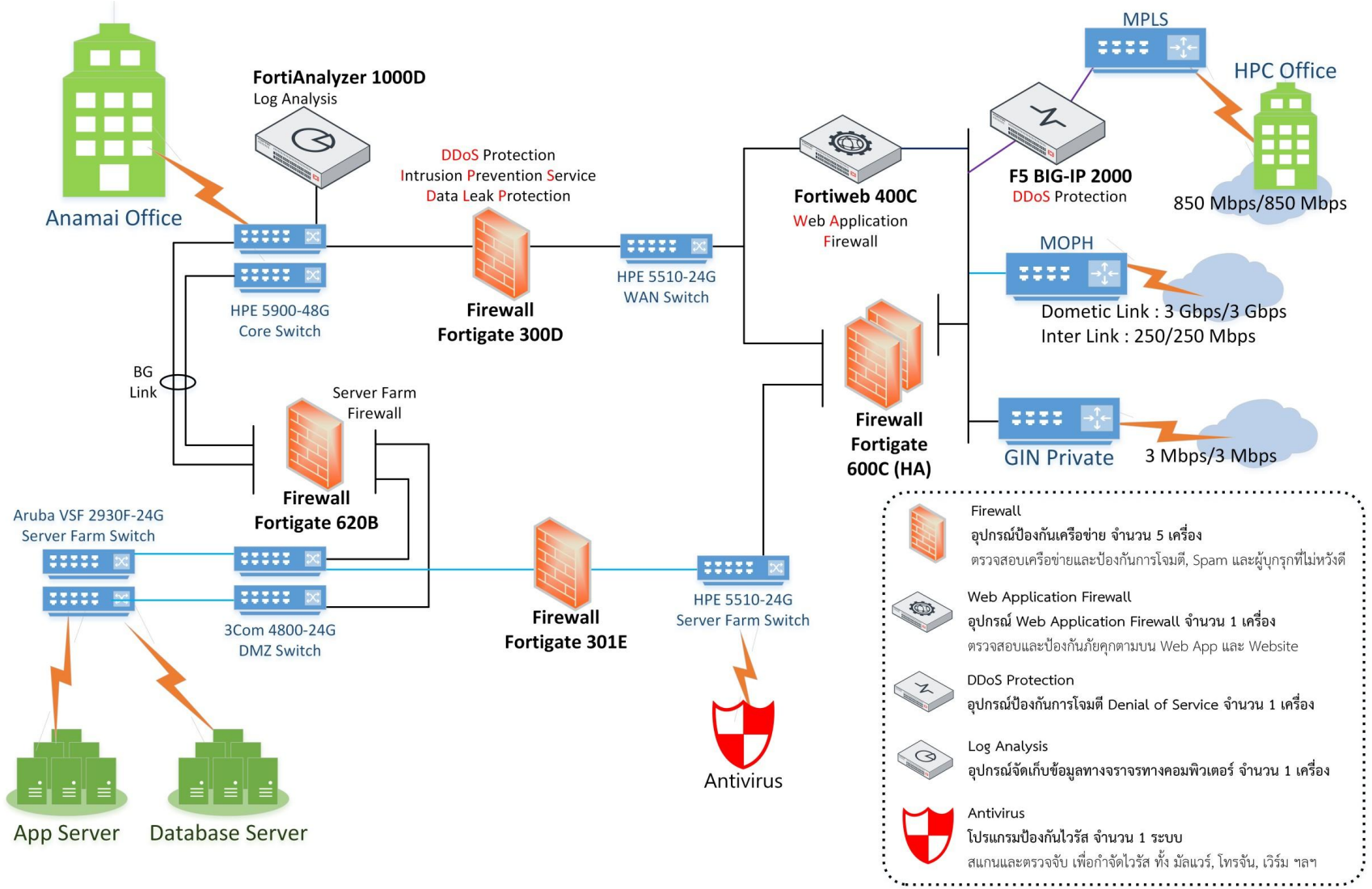
การดำเนินงาน
Cyber Security
กรมอนามัย

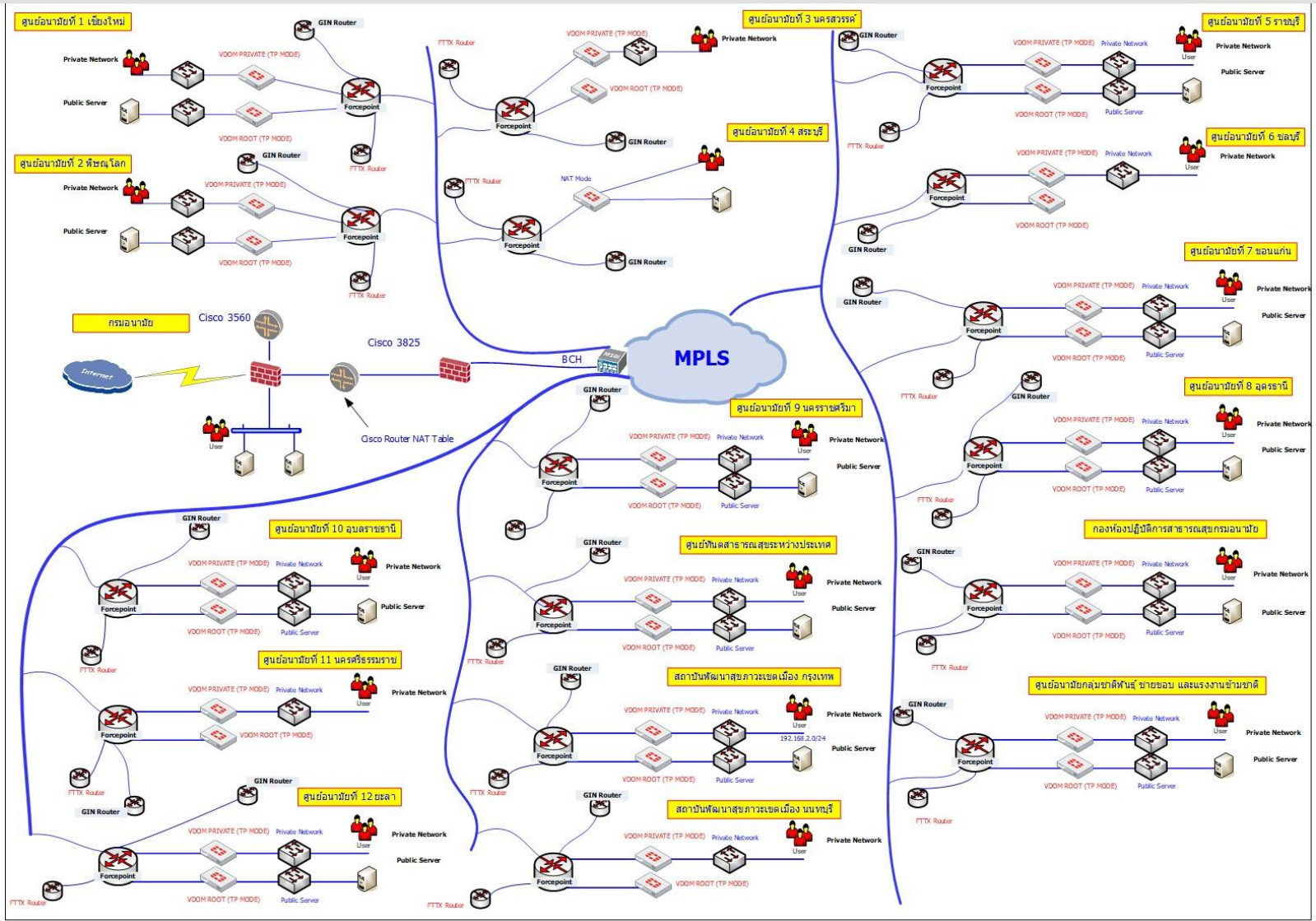
โครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมอนามัย

หน่วยงานส่วนกลาง



โครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมอนามัย

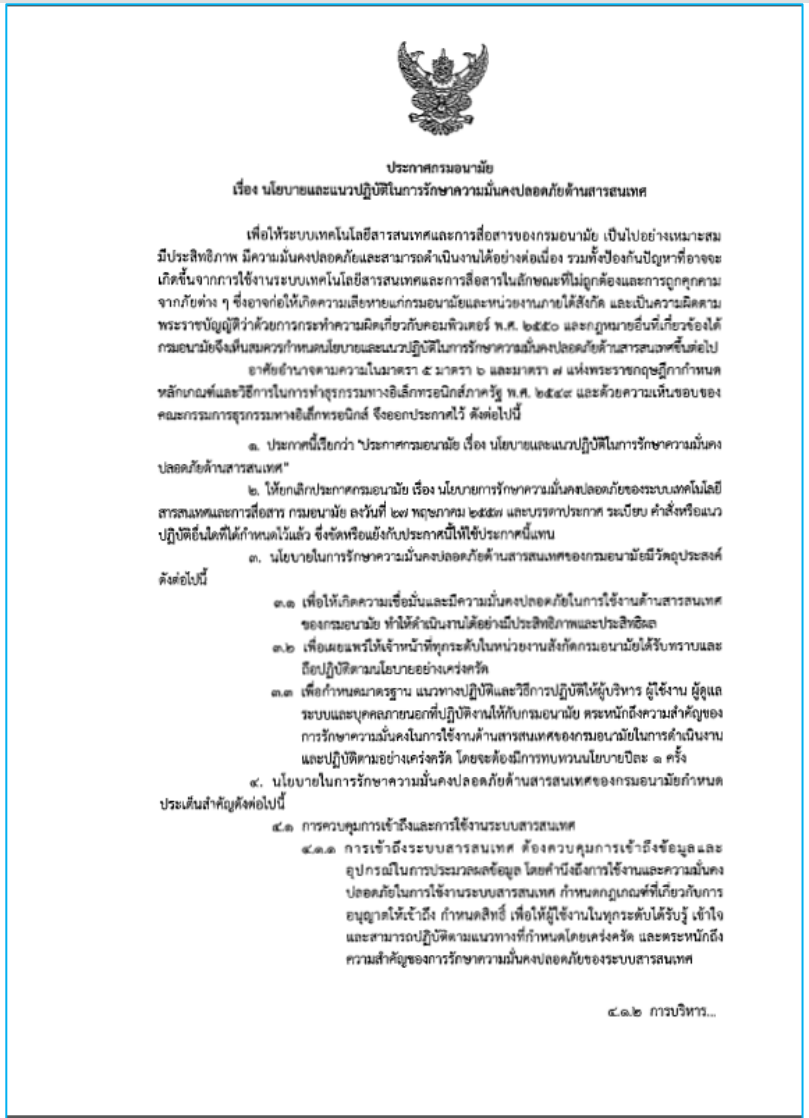
หน่วยงานส่วนภูมิภาค



แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

จัดทำนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมอนามัย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมอนามัย โดยปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001



ประกาศกรมอนามัย
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอนามัย เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมอนามัยและหน่วยงานภายใต้สังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ กรมอนามัยจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๙ และด้วยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ ดังต่อไปนี้

๑. ประกาศนี้เรียกว่า "ประกาศกรมอนามัย เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ"

๒. ให้ยกเลิกประกาศกรมอนามัย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย ลงวันที่ ๒๗ พฤษภาคม ๒๕๕๗ และบรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอนามัยมีวัตถุประสงค์ดังต่อไปนี้

๓.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของกรมอนามัย ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๓.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานสังกัดกรมอนามัยได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมอนามัย ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของกรมอนามัยในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอนามัยกำหนดประเด็นสำคัญดังต่อไปนี้

๔.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๔.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๔.๑.๒ การบริหาร...

การดำเนินงานรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

เฝ้าระวังภัยคุกคามและแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ (1/2)

แนวทางการป้องกัน	รายละเอียดดำเนินการ
1. ตรวจสอบช่องโหว่อยู่เสมอ (Vulnerability Assessment : VA SCAN)	บริษัท ดาต้าฟาร์ม เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านไซเบอร์ ตรวจสอบและแนะนำการแก้ไขช่องโหว่ระบบงานของหน่วยงานที่ติดตั้ง Cloud กรมอนามัย โดยดำเนินการเป็นประจำทุกปีและแจ้งผู้รับผิดชอบระบบงานดำเนินการแก้ไขช่องโหว่ที่ตรวจพบในระบบงาน
2. เฝ้าระวังและแจ้งภัยคุกคามทางไซเบอร์	กรมอนามัย มอบหมายให้ทีม Anamai CIRT ดำเนินการเฝ้าระวัง ประมวลผล วิเคราะห์ข้อมูลการโจมตีทางไซเบอร์ และแจ้งเตือนภัยคุกคามกับหน่วยงานที่เกี่ยวข้อง เช่น สกมช., สป.สธ. เป็นต้น *** Anamai CIRT : เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย
3. ประเมินความเสี่ยงด้านระบบสารสนเทศ	ดำเนินการประเมินความเสี่ยงระบบงาน/ระบบสารสนเทศ และรายงาน CIO กรมอนามัย โดยดำเนินการเป็นประจำทุกปี
4. ความปลอดภัยด้านคอมพิวเตอร์และเครือข่าย	มีอุปกรณ์ป้องกันและเฝ้าระวังความปลอดภัยทางเครือข่าย - อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย เช่น Firewall, IPS, DDOS, Web Application firewall เป็นต้น - การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ โดยการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น - ซอฟต์แวร์เฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น PRTG Network Monitor เป็นต้น
5. สำรองข้อมูลอย่างสม่ำเสมอ	มีระบบสำรองข้อมูลแบบอัตโนมัติ (Veeam Backup) เพื่อสามารถนำข้อมูลกลับมาใช้งานได้อย่างต่อเนื่อง ด้วยการกู้คืนข้อมูล (Restore) รวมทั้งสำรองข้อมูลไปยัง GDCC Cloud Service ภายนอกกรมอนามัย และมีการทดสอบกู้คืนระบบสารสนเทศ โดยดำเนินการเป็นประจำทุกปี
6. ติดตั้งซอฟต์แวร์รักษาความปลอดภัย (Anti Virus)	มีการติดตั้ง/สแกน/อัพเดทฐานข้อมูล ซอฟต์แวร์ป้องกันไวรัส (Antivirus) : Kaspersky อย่างสม่ำเสมอ

การดำเนินงานรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

เฝ้าระวังภัยคุกคามและแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ (2/2)

แนวทางการป้องกัน	รายละเอียดดำเนินการ
7. การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อมห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย	การควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล
8. แยกสัญญาณ Wi-Fi จากสาธารณะ	แยกสัญญาณ Wi-Fi และแยกกลุ่มผู้ใช้งานภายในองค์กรและผู้ใช้งานภายนอก ออกจากกัน
9. ติดตั้งเฉพาะโปรแกรมที่มีความน่าเชื่อถือ	ติดตั้งซอฟต์แวร์ที่มีลิขสิทธิ์ และป้องกันการติดตั้งโปรแกรม โดยใช้ Active Directory บริหารจัดการเครื่องคอมพิวเตอร์และบัญชีชื่อผู้ใช้งานของกรมอนามัย
10. อุปกรณ์มีการอัพเดทโปรแกรมและระบบปฏิบัติการอยู่เสมอ	มีการอัพเดทโปรแกรมและระบบปฏิบัติการที่ล่าสุด
11. การตั้งรหัสผ่านให้มีความ ปลอดภัย	มีการแจ้งบุคลากรของทุกหน่วยงาน ในการกำหนดรหัสผ่านอย่างน้อย 8 ตัวอักษร (พิมพ์เล็ก, พิมพ์ใหญ่, อักขระพิเศษ และตัวเลข) และเปลี่ยนรหัสผ่านทุก 6 เดือน
12. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Awareness) ให้กับบุคลากรในองค์กร	การสร้างความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยให้กับบุคลากรในองค์กร โดยมีการจัดประชุม Digital Literacy และ การประชุมภาคีเครือข่ายไอซีที
13. ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบงาน/ระบบสารสนเทศ และกำหนดสิทธิการเข้าถึงข้อมูลต้องปฏิบัติตามกฎหมาย	- กฎหมายด้านเทคโนโลยีสารสนเทศ เช่น พรบ.คุ้มครองข้อมูลส่วนบุคคล, พรบ.ไซเบอร์, พรบ.คอมพิวเตอร์, พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และประกาศกรมอนามัย นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นต้น - เจ้าหน้าที่และผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของกรมอนามัย

การประสานงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย

จัดตั้งคณะเจ้าหน้าที่ประสานงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กระทรวงสาธารณสุข (Health CIRT)

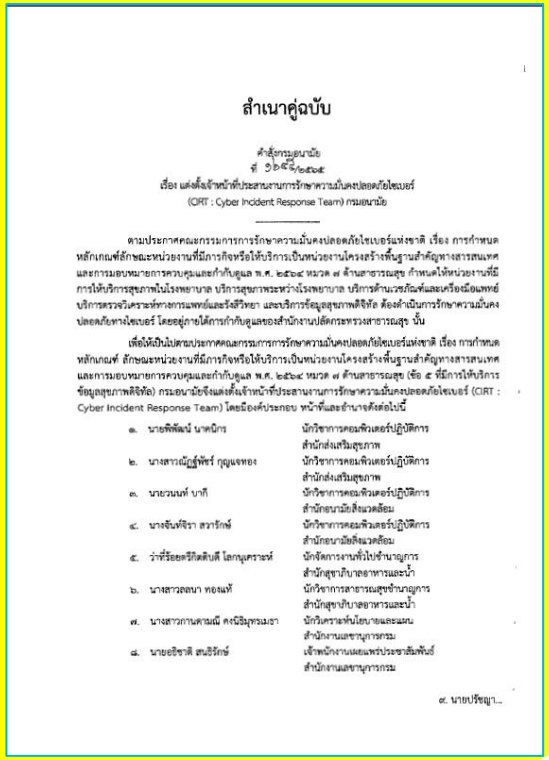
ศูนย์เทคฯ สป.สธ. ดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Health CIRT) ในหน่วยงานสังกัดกระทรวงสาธารณสุข

กองดิจิทัลฯ โดยกรมอนามัย ได้ส่งตัวแทน จำนวน 2 ท่าน

ระดับขีดความสามารถของ Health CIRT	อัตรากำลัง (ทีมงาน) ขั้นต่ำจำเป็น
1. ระดับเบื้องต้น เพื่อเป็นผู้ติดต่อ (Point of Contact: POC) สำหรับประสานแจ้งเหตุและ แก้ไขเหตุภัยคุกคาม มีกฎ ระเบียบ และข้อบังคับ สำหรับการแจ้งเตือนและรายงานไปยังองค์กรที่เกี่ยวข้องต่าง ๆ	2 อัตรา

กรมอนามัย (Anamai CIRT)

กองดิจิทัลฯ โดยกรมอนามัย ดำเนินการจัดตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Anamai CIRT) ในหน่วยงานสังกัดกรมอนามัยทุกหน่วยงาน ทั้งส่วนกลางและส่วนภูมิภาค



สำเนาคู่ฉบับ

คำสั่งกรมอนามัย
ที่ ๖๒๕๕/๒๕๖๕
เรื่อง แต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์
(CIRT : Cyber Incident Response Team) กรมอนามัย

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีการกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และชันสูตร และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข นั้น

เพื่อให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีการกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข (ข้อ ๕ ที่มีการให้บริการข้อมูลสุขภาพดิจิทัล) กรมอนามัยจึงแต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CIRT : Cyber Incident Response Team) โดยมีองค์ประกอบ หน้าที่และอำนาจดังต่อไปนี้

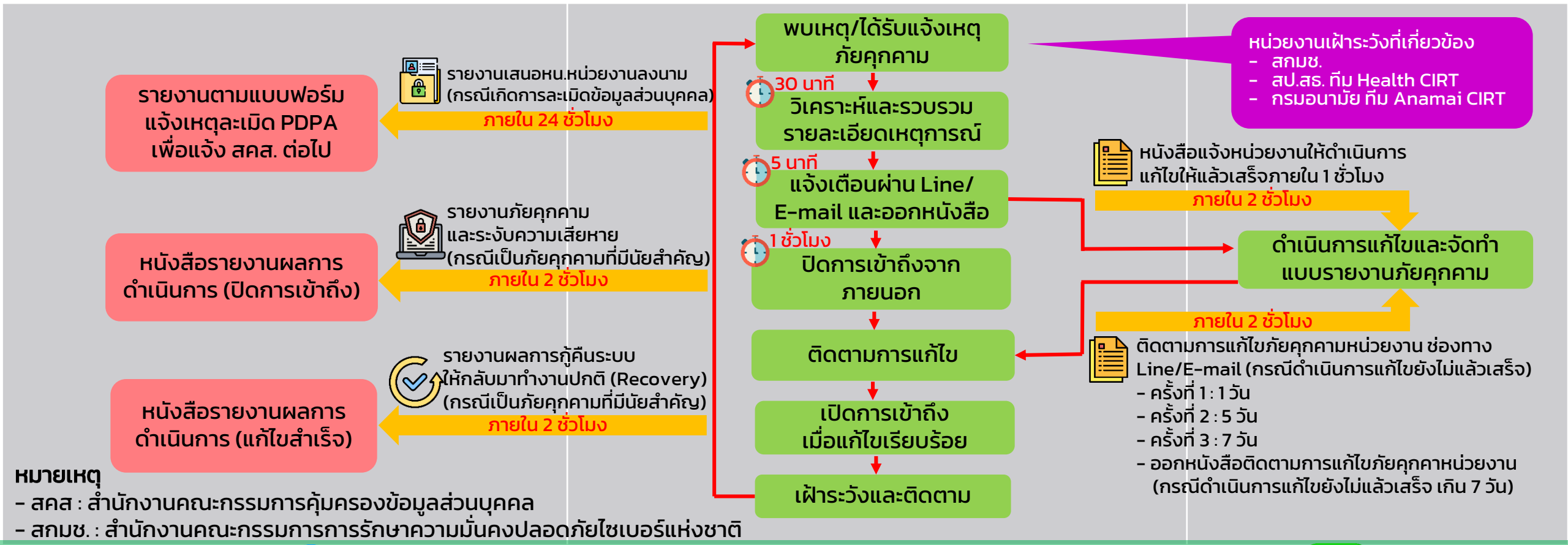
๑. นายพิพัฒน์ นาคนิกร — นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักส่งเสริมสุขภาพ
๒. นางสาวผัญญ์พัชร์ กุญแจทอง — นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักส่งเสริมสุขภาพ
๓. นายวนนท์ บาที — นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักอนามัยสิ่งแวดล้อม
๔. นางจันทิรา สวารักษ์ — นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักอนามัยสิ่งแวดล้อม
๕. ว่าที่ร้อยตรีกิตติบดี โลกนุเคราะห์ — นักจัดการงานทั่วไปชำนาญการ สำนักสุขาภิบาลอาหารและน้ำ
๖. นางสาวลลนา ทองแท้ — นักวิชาการสาธารณสุขชำนาญการ สำนักสุขาภิบาลอาหารและน้ำ
๗. นางสาวกานต์ณี คงนิธิมุทรเมธา — นักวิเคราะห์นโยบายและแผน สำนักงานเลขานุการกรม
๘. นายอธิชาติ สนธิรักษ์ — เจ้าพนักงานเผยแพร่ประชาสัมพันธ์ สำนักงานเลขานุการกรม

๙. นายปรัชญา...

การประสานงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย

การจัดการและตอบสนองต่อภัยคุกคามทางไซเบอร์

อธิบดีกรม/CIO/สป.สธ.(Regulator)/สกมช.	กองดิจิทัลเพื่อส่งเสริมสุขภาพ	หน่วยงานผู้รับผิดชอบเว็บไซต์/ระบบงาน



หมายเหตุ
- สคส : สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- สกมช. : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

02 590 4310
02 590 4290
https://cybersec.anamai.moph.go.th
cybersec@anamai.mail.go.th
LINE AnamaiCIRT

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย

Timeline การปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

ต.ค. 68

วิเคราะห์/ทบทวน
สถานการณ์

พ.ย. – ธ.ค. 68

การให้ความรู้และทำความเข้าใจกับบุคลากร
- ประชุมแนวทางดำเนินงานด้านความปลอดภัยไซเบอร์ตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์
- การสแกนช่องโหว่บนเครือข่าย และตรวจสอบเฝ้าระวังสถานะเครื่องแม่ข่าย

ม.ค. – ก.พ. 69

ตรวจสอบการดำเนินงานตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของหน่วยงานสังกัดกรมอนามัย

มี.ค. – เม.ย. 69

ติดตามและประเมินผลการดำเนินงานตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์

พ.ค. 69

ฝึกซ้อมเพื่อรับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ กิจกรรมแผนเผชิญเหตุ

มิ.ย. 69

การประชุมแนวทางดำเนินงานด้านความปลอดภัยไซเบอร์ของกรมอนามัย

ส.ค. 69

ทบทวนแผนและแนวทางการปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ประจำปี 2566

02 590 4310
02 590 4290
https://cybersec.anamai.moph.go.th
cybersec@anamai.mail.go.th
LINE AnamaiCIRT