ด้านที่ 9 ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

พ.ศ. 2564

มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

01 รองรับตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

02 พรบ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

03 พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

04 พรบ.ว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2553

05 พรบ.ข้อมูลข่าวสารของทางราชการ พ.ศ.2540

01 พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

พระราชบัญญัติ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งคอมพิวเตอร์ที่ว่านี้ก็เป็นได้ทั้งคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์โน้ตบุ๊ค สมาร์ทโฟน รวมถึงระบบต่างๆ ที่ถูกควบคุมด้วยระบบคอมพิวเตอร์ด้วย ซึ่งเป็นพ.ร.บ.ที่ตั้งขึ้นมาเพื่อป้องกัน ควบคุมการกระทำผิดที่จะเกิดขึ้นได้จากการใช้คอมพิวเตอร์ หากใครกระทำความผิดตามพ.ร.บ.คอมพิวเตอร์นี้ ก็จะต้องได้รับการลงโทษตามที่พ.ร.บ.กำหนด

01 พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

1. เข้าถึงระบบ หรือข้อมูลของผู้อื่นโดยไม่ชอบ (มาตรา 5-8)

เช่น การเข้าไปเจาะข้อมูลทางคอมพิวเตอร์ของคนอื่น โดยที่เจ้าของข้อมูลไม่ได้อนุญาต (ละเมิด Privacy) การปล่อยไวรัส มัลแวร์เข้าคอมพิวเตอร์บุคคลอื่น เพื่อเจาะข้อมูลบางอย่าง หรือพวกแฮคเกอร์ ที่เข้าไปขโมยข้อมูลของบุคคลอื่นก็มีความผิดตามพ.ร.บ.

บทลงโทษ

เข้าถึงระบบคอมพิวเตอร์ : จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 1 หมื่นบาท หรือทั้งจำทั้งปรับ

เข้าถึงข้อมูลคอมพิวเตอร์ : จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์และนำไปเปิดเผย : จำคุกไม่เกิน 1 ปี ปรับไม่เกิน 2 หมื่นบาท หรือทั้งจำทั้งปรับ

ดักรับข้อมูลคอมพิวเตอร์ : จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

01

พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

2. แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย (มาตรา 9-10)

หมายถึง การทำให้ข้อมูลเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลของผู้อื่นโดยมิชอบ หรือจะเป็นในกรณีที่ทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ อย่างเช่น กรณีของกลุ่มคนที่ไม่ชอบใจกับการกระทำของอีกฝ่าย แล้วต่อต้านด้วยการเข้าไปขัดขวาง ทำร้ายระบบเว็บไซต์ของฝ่ายตรงข้าม ให้บุคคลอื่นๆ ใช้งานไม่ได้

บทลงโทษ ต้องระวางโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ

01 พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

3. ส่งข้อมูลหรืออีเมลก่อกวนผู้อื่น หรือส่งอีเมลสแปม (มาตรา 11)

เช่น การส่งอีเมลที่บุคคลอื่นไม่ยินดีที่จะรับ หรือที่รู้จักกันว่า อีเมลล์สแปม **หรือแม้แต่การข้อมูลต่าง ๆ ตาม Facebook กับ IG ก็เป็นสิ่งที่ไม่ควรทำ** และยังรวมถึงคนที่ขโมย Database จากบุคคลอื่น แล้วส่งอีเมลล์ขายเป็นต้น

บทลงโทษ ถ้าส่งโดยปกปิดหรือปลอมแปลงแหล่งที่มา ปรับไม่เกิน 1 แสนบาท และถ้าส่งโดยไม่เปิดโอกาสให้ปฏิเสธตอบรับได้โดยงาน ต้องได้รับโทษจำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

01

พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

4. เข้าถึงระบบ หรือข้อมูลทางด้านความมั่นคงโดยมิชอบ (มาตรา 12)

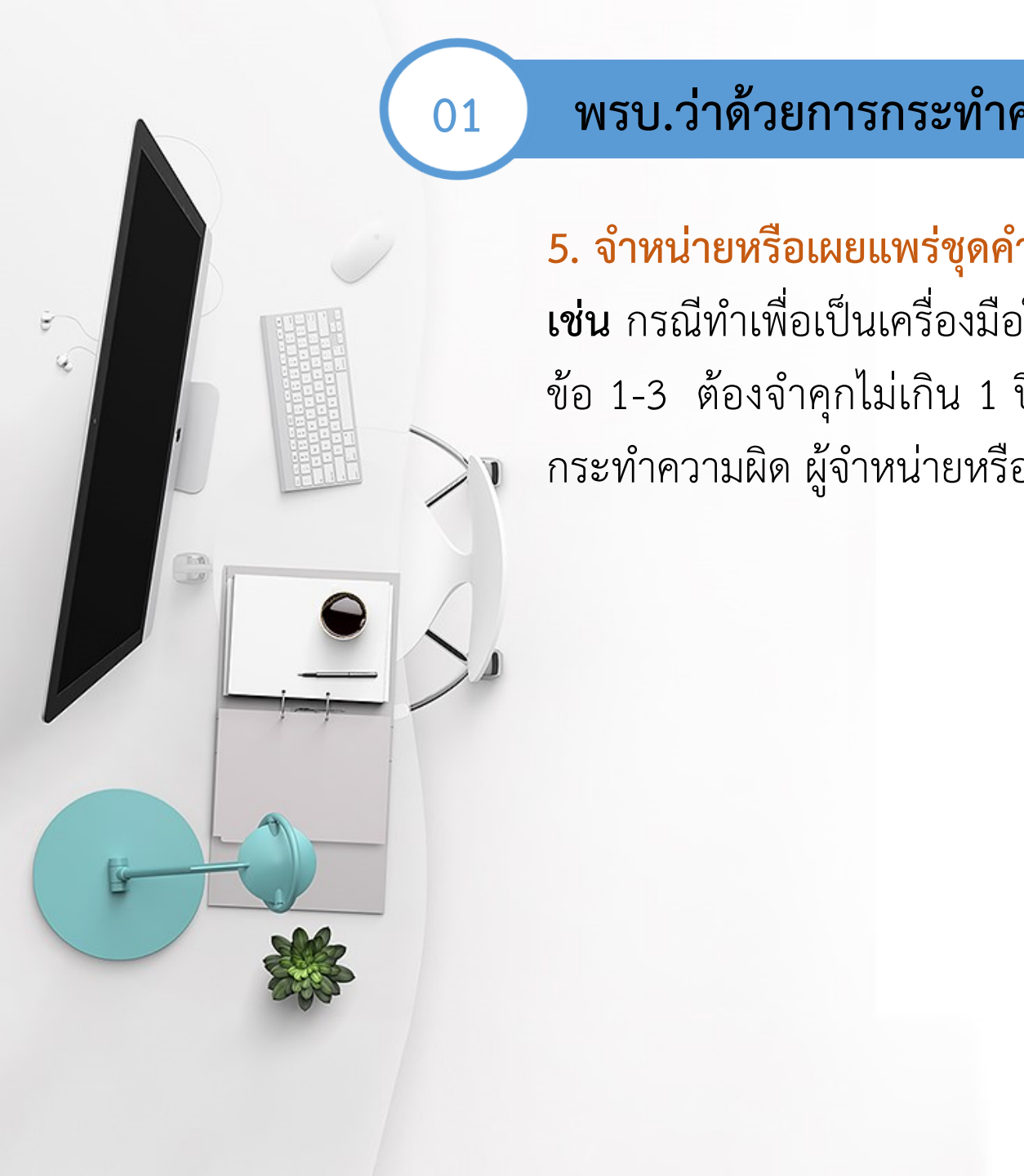
เช่น โพสต์เกี่ยวกับเรื่องการเมืองที่ส่งผลให้เกิดความเสียหายหรือความมั่นคงต่อประเทศ หรือโพสต์ที่เป็นการก่อกวน หรือการก่อการร้ายขึ้น ตามมาตรา 12 ได้บอกไว้ว่าการเข้าถึงระบบหรือข้อมูลทางด้านความมั่งคงโดยมิชอบ หรือการโพสต์ข้อความในโลกออนไลน์ที่เข่าข่ายข้อมูลเท็จที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ หรือทำให้ประชาชนเกิดอาการตื่นตระหนก และล่วงรู้ถึงมาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์และนำไปเปิดเผย

บทลงโทษ

กรณีไม่เกิดความเสียหาย: จำคุก 1-7 ปี และปรับ 2 หมื่น – 1.4 แสนบาท

กรณีเกิดความเสียหาย: จำคุก 1-10 ปี และปรับ 2 หมื่น – 2 แสนบาท

กรณีเป็นเหตุให้ผู้อื่นถึงแก่ความตาย: จำคุก 5-20 ปี และปรับ 1 แสน – 4 แสนบาท



01 พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

5. จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด (มาตรา 13)

เช่น กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทางคอมพิวเตอร์ตามมาตรา 5-11 หรือข้อ 1-3 ต้องจำคุกไม่เกิน 1 ปี ปรับไม่เกิน 2 หมื่นบาท หรือทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่ต้องรับผิดชอบร่วมด้วย

01 พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

6. นำข้อมูลที่ผิดพ.ร.บ.เข้าสู่ระบบคอมพิวเตอร์ (มาตรา 14)

ในความผิดมาตรา 14 จะระบุโทษการนำข้อมูลที่เปิดพ.ร.บ.เข้าสู่ระบบคอมพิวเตอร์ ซึ่งแบ่งออกเป็น 5 ข้อความผิดด้วยกันคือ

โพสต์ข้อมูลปลอม ทุจริต หลอกลวง (อย่างเช่น ข่าวปลอม โฆษณาธุรกิจลูกโซ่ที่หลอกลวงเอาเงินลูกค้า และไม่มีการส่งมอบของให้จริงๆ เป็นต้น)

โพสต์ข้อมูลความผิดเกี่ยวกับความมั่งคงปลอดภัย

โพสต์ข้อมูลความผิดเกี่ยวกับความมั่นคง ก่อการร้าย

โพสต์ข้อมูลลามก ที่ประชาชนเข้าถึงได้

เผยแพร่ ส่งต่อข้อมูล ที่รู้แล้วว่าผิด (อย่างเช่น กด Share ข้อมูลที่มีเนื้อหาเข้าข่ายความผิด พ.ร.บ.คอมพิวเตอร์)

บทลงโทษ หากเป็นการกระทำที่ส่งผลถึงประชาชน ต้องได้รับโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ และหากเป็นกรณีที่เป็นการกระทำที่ส่งผลต่อบุคลใดบุคคลหนึ่ง ต้องได้รับโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ

01

พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

7. ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจกับผู้ร่วมกระทำความผิด (มาตรา 15)

เช่น เว็บไซด์หน่วยงาน ที่เปิดให้มีการแสดงความคิดเห็น แล้วมีความคิดเห็นที่มีเนื้อหาผิดกฎหมายก็มีความผิดตาม พรบ. แต่ถ้าหากผู้ดูแลเว็บไซด์ตรวจสอบแล้วพบเจอ และลบออกจะถือว่าเป็นผู้ที่พ้นความผิด

บทลงโทษ

หากผู้ดูแลเว็บไซด์นั้น ๆ ไม่ดำเนินการใด ถือว่าเป็นผู้กระทำความผิดตามมาตรา 14 ต้องได้รับโทษเช่นเดียวกันผู้โพสต์ หรือแสดงความคิดเห็นทางออนไลน์ แต่ถ้าผู้ดูแลระบบพิสูจน์ได้ว่าตนได้ปฏิบัติตามขั้นตอนการแจ้งเตือนแล้วไม่ต้องรับโทษ

01 พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

8. ตัดต่อ เติม หรือดัดแปลงภาพ (มาตรา 16)

ความผิดข้อนี้ แบ่งออกเป็น 2 ประเด็นหลักคือ

- **การโพสต์ภาพของผู้อื่น** ที่เกิดจากการสร้าง ตัดต่อ หรือดัดแปลง ที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง อย่างเช่นกรณีที่เอาภาพดาราไปตัดต่อ และตกแต่งเรื่องขึ้นมาจนทำให้บุคคลนั้นเกิดความเสียหาย ก็ถือว่ามีความผิดตามพ.ร.บ.คอมพิวเตอร์
- **การโพสต์ภาพผู้เสียชีวิต** หากเป็นการโพสต์ที่ทำให้บิดามารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอาย

บทลงโทษ

หากกระทำผิดตามนี้ ต้องได้รับโทษจำคุกไม่เกิน 3 ปี และปรับไม่เกิน 2 แสนบาท

02 พรบ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

ทำไมต้องมี พ.ร.บ ไซเบอร์

เพื่อปกป้องระบบคอมพิวเตอร์และโครงข่าย IT ของโครงสร้างสำคัญพื้นฐานทางสารสนเทศ หรือ บริการที่สำคัญของประเทศที่มีความมั่นคงปลอดภัยสามารถให้บริการได้เป็นปกติและหน่วยงานสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

สาระสำคัญกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

1. กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐมีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
2. มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ
3. มีการร่วมมือและประสานงานกันและกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้ จนทำให้ประชาชนเดือดร้อน

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
Critical Information Infrastructure (CII)

คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) อำนาจหน้าที่ มาตรา 9

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) อำนาจหน้าที่ มาตรา 11

คณะกรรมการบริหารสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์(กบส.)
สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อำนาจหน้าที่ ม.22

Regulator

ประมวลแนวทางปฏิบัติ/ตรวจสอบการ ปฏิบัติ

มาตรา ๕๓ (หน่วยงานควบคุมหรือกำกับดูแล)
•ตรวจสอบมาตรฐานขั้นต่ำ
•สั่งให้แก้ไข
•รายงาน กกม. (ถ้าเพิกเฉย)

กรมสนับสนุนบริการสุขภาพ

CSO → กลุ่มงานความมั่นคงปลอดภัยสารสนเทศ ฯ

สถานพยาบาล

Operator

แผนรับมือ /COBIT/ISO27001

มาตรา ๕๔ (หน่วยงานโครงสร้างพื้นฐาน)
•ประเมินความเสี่ยง
•ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้ง

หน่วยงานเฝ้าระวัง ติดตาม ตรวจสอบ เผชิญเหตุ
- Health CERT
- ICS-CERT
- National Health-ISAC

มาตราที่เกี่ยวข้อง

ม.44,45,46,52
ม.53
ม.56,57
ม.59

ม.44, 45,46,52
ม.54
ม.56,57
ม.58

บทลงโทษ

ม.73,ม.77,ม.49(7) ด้านสาธารณสุข

หน่วยงานตรวจประเมินความเสี่ยงระบบ (Audit) ประมวลแนวทางปฏิบัติ (ตามแผนชาติ)

มาตรการ

การระบุ
IDENTIFY

หน่วยงานต้องทำการระบุว่า กระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้างที่มีความเสี่ยงต่อการถูกโจมตี ทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล ของหน่วยงานได้อย่างเหมาะสม

Framework for Improving
Critical Infrastructure Cybersecurity

มาตรการ

การป้องกัน
PROTECT

หน่วยงานต้องมีมาตรการป้องกันที่เหมาะสมเพื่อจำกัดผลกระทบของเหตุการณ์ภัยคุกคามไซเบอร์ ซึ่งครอบคลุมถึง เรื่องการควบคุมการเข้าถึง การฝึกอบรมและการสร้างความตระหนักให้แก่เจ้าหน้าที่และผู้ที่เกี่ยวข้อง ความปลอดภัยของ ข้อมูล และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี นอกจากนี้ หน่วยงานต้องทำการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบอิเล็กทรอนิกส์อย่างสม่ำเสมอเพื่อให้สามารถ รองรับการดำเนินงานได้อย่างต่อเนื่อง รวมทั้งการเปลี่ยนแปลงแก้ไข Patch หรือ update software

Framework for Improving
Critical Infrastructure Cybersecurity

มาตรการ

การตรวจจับ
DETECT

หน่วยงานต้องมีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง และ แจ้งเตือนถึงสิ่งที่ผิดปกติต่างๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคามที่เกิดขึ้น เพื่อเป็นข้อมูลประกอบในการพิจารณาทบทวนแนวทางการป้องกัน ความเสี่ยงและผลกระทบที่จะเกิดขึ้นกับหน่วยงานในอนาคต

Framework for Improving
Critical Infrastructure Cybersecurity

มาตรการ

ด้านการรับมือภัยคุกคาม(Response)

- มีการกำหนดมาตรการและกระบวนการรับมือภัยคุกคามไซเบอร์ที่ทันท่วงที
- มีความร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอกเกี่ยวกับแผนรับมือภัยคุกคามไซเบอร์
- มีการวิเคราะห์สาเหตุภัยคุกคามหรือตรวจพิสูจน์พยานหลักฐานดิจิทัล
- มีมาตรการป้องกันการลุกลามของภัยคุกคาม
- มีการทดสอบ ปรับปรุงกลยุทธ์และแผนรับมือภัยคุกคามไซเบอร์อย่างสม่ำเสมอ

Framework for Improving
Critical Infrastructure Cybersecurity

มาตรการ

การกู้คืนข้อมูลและระบบหลังเหตุภัยคุกคามไซเบอร์(Recover)

- มีแผนการกู้คืนระบบ ทั้งระหว่างเกิดเหตุและหลังเกิดเหตุภัยคุกคาม
- มีการปรับปรุงกลยุทธ์และแผนการกู้คืนอย่างสม่ำเสมอ
- มีการสื่อสารให้ผู้บริหารและ ผู้ที่เกี่ยวข้องทราบภายในองค์กรให้ทราบถึงกระบวนการกู้คืนข้อมูลหลังเกิดเหตุภัยคุกคามไซเบอร์

Framework for Improving
Critical Infrastructure Cybersecurity

03 พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

สาเหตุหลักที่ประเทศไทยต้องมี พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ความน่าเชื่อถือในมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศ มีผลกระทบต่อการค้าระหว่างประเทศ และการทำธุรกิจระหว่างประเทศ หากประเทศไทยไม่มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ย่อมทำให้เสียโอกาสและความเชื่อมั่นจากกลุ่มประเทศในสหภาพยุโรป และอาจรวมไปถึงประชาคมโลกที่กำลังตื่นตัวเรื่อง Data Protection เพราะเหตุการณ์ใหญ่ ๆ ที่เกิดขึ้นแล้ว เช่น การรั่วไหลของข้อมูลส่วนบุคคลของผู้ใช้ เป็นต้น

03 พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

สาระสำคัญของ พ.ร.บ. ฉบับนี้ มี 3 ประเด็นหลัก ดังนี้

1. เจ้าของข้อมูลต้องให้ความยินยอม ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ผู้ใช้ แจ้งไว้ตั้งแต่แรกแล้วเท่านั้น กล่าวคือ ต้องขออนุมัติจากเจ้าของข้อมูลก่อน เช่น หากแอปพลิชันหนึ่งจะเก็บข้อมูลบัตรเครดิตของเราไว้ในระบบ ก็ต้องมีข้อความให้เรากดยืนยันเพื่อยินยอม พร้อมแจ้งวัตถุประสงค์ในการเก็บรวบรวมและการใช้ หากเราไม่ยินยอมให้ใช้ข้อมูลบัตรเครดิต ผู้ให้บริการแอปพลิเคชันนั้นก็ไม่สามารถใช้ข้อมูลบัตรเครดิตของเราได้

2. ผู้เก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือถูกเข้าถึงโดยผู้ที่ไม่เกี่ยวข้องกับข้อมูล เช่น สถานพยาบาลจะต้องเก็บข้อมูลของผู้ป่วยให้เป็นความลับและไม่เปิดเผยให้กับผู้อื่น ธนาคารต้องเก็บรักษาข้อมูลเกี่ยวกับรายการถอน

3.เจ้าของข้อมูลมีสิทธิ์ถอนความยินยอม ขอให้ลบหรือทำลายข้อมูลเมื่อใดก็ได้ หากเป็นความประสงค์ของเจ้าของข้อมูล

03 พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

หน่วยงาน ที่ต้องมีการเก็บข้อมูลส่วนบุคคล สิ่งสำคัญคือ

1. ต้องรู้ขอบเขตของการเข้าถึงข้อมูลส่วนบุคคล
2. มีระบบควบคุมการเข้าถึงข้อมูลส่วนบุคคล
3. มีระบบยืนยันตัวตนของผู้ขอเข้าถึงข้อมูลส่วนบุคคล รวมไปถึงต้องมีการกำหนดนโยบายสำหรับบุคคลภายในองค์กรที่ต้องเกี่ยวข้องกับการใช้งานข้อมูลส่วนบุคคลที่ได้รับการยินยอมจากเจ้าของข้อมูลแล้ว เนื่องจากมีข้อบังคับต่าง ๆ ที่หากละเมิดแล้ว จะมีผลให้เกิดโทษอาญา โทษทางปกครอง ซึ่งมีโทษปรับมากถึง 5 ล้านบาท

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะออกระเบียบข้อบังคับ แนวทางด้านความมั่นคงปลอดภัยไซเบอร์ให้กับองค์กรต่าง ๆ ที่ต้องใช้ข้อมูลส่วนบุคคล (รวมถึงองค์กรที่ไม่ได้ใช้ข้อมูลส่วนบุคคล) ดังนั้นองค์กรควรปรับตัวและพัฒนาให้มีมาตรฐานความมั่นคงปลอดภัยไซเบอร์ในระดับสากล เพื่อให้ได้การรับรองตามมาตรฐาน ISO 27001 หรือ ISO 29100 เป็นต้น

04 พรบ.ว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2553

เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการทำธุรกรรมหรือสัญญา

05 พรบ.ข้อมูลข่าวสารของทางราชการ พ.ศ.2540

หน่วยงานของรัฐจะต้อง เปิดเผยข้อมูลข่าวสารและต้องนำข้อมูลข่าวสารตามมาตรา 7 มาตรา 9 ไปรวมไว้ให้ประชาชนเข้าตรวจดูได้ โดยมีแนวคิดหลักว่า รัฐบาลรู้อะไร อย่างไร ประชาชนต้องรู้อย่างนั้น และ เปิดเผยเป็นหลัก ปกปิดเป็น ข้อยกเว้น

ประเภทข้อมูลข่าวสาร

1. ข้อมูลข่าวสารของราชการ
2. ข้อมูลข่าวสารส่วนบุคคล

ลักษณะข้อมูลข่าวสารของราชการ

1. ข้อมูลข่าวสารที่ต้องเปิดเผย (มาตรา 7, 9, 11)
2. ข้อมูลข่าวสารที่ไม่ต้องเปิดเผย (มาตรา 14, 15)
3. ข้อมูลข่าวสารส่วนบุคคล (มาตรา 21, 22, 23, 24, 25)

05 พรบ.ข้อมูลข่าวสารของทางราชการ พ.ศ.2540

หน้าทีของหน่วยงานของรัฐ

1. ส่งข้อมูลลงพิมพ์ในราชกิจจานุเบกษา
2. จัดไว้ให้ประชาชนเข้าตรวจดู
3. จัดหาไว้ให้ประชาชนเป็นการเฉพาะราย
4. แนะนำแหล่งเก็บข้อมูล

สิทธิของประชาชน

1. ขอคำปรึกษา
2. ตรวจดูข้อมูล
3. ขอข้อมูลข่าวสารอื่นใดของราชการ
4. ทราบ / รู้ถึงข้อมูลส่วนบุคคลของตนเอง
5. ดำเนินการแทนผู้เยาว์
6. ร้องเรียน
7. อุทธรณ์

ประเมินมาตรฐานระบบบริการสุขภาพ ด้านที่ 9 ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ
2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ
3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ
4. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ
5. การจัดการห้อง Data Center

1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ

มีการจัดทีมดูแลระบบสารสนเทศของโรงพยาบาล
ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาล โดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม

มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย

มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดย
กำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ
ผู้รับผิดชอบ อย่างชัดเจน

มีการดำเนินการตามแผนจัดการความเสี่ยง

มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน

มีการนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT

มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้

มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วย มิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติ
ให้บุคลากรทุกคนได้รับทราบ

มีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด

มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

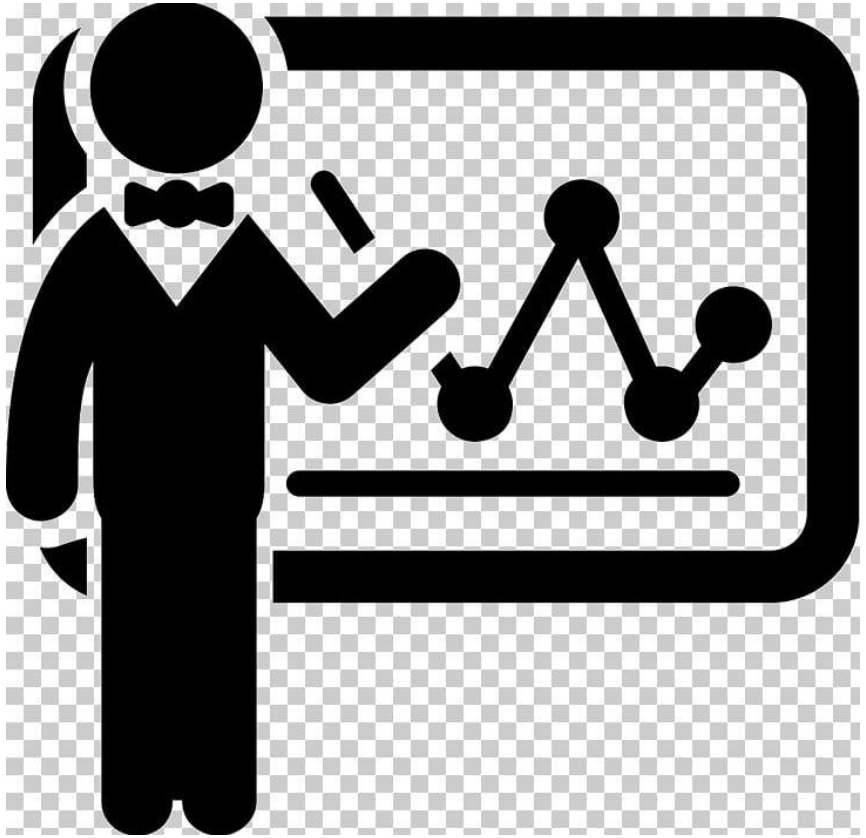
4. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร

มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากร ด้าน Hardware, Software, Network

มีการกำหนดสมรรถนะตามบทบาทหน้าที่ที่จำเป็น (Functional Competency) ของบุคลากรด้าน IT ทุกคน ประเมินสมรรถนะตามบทบาทหน้าที่ และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

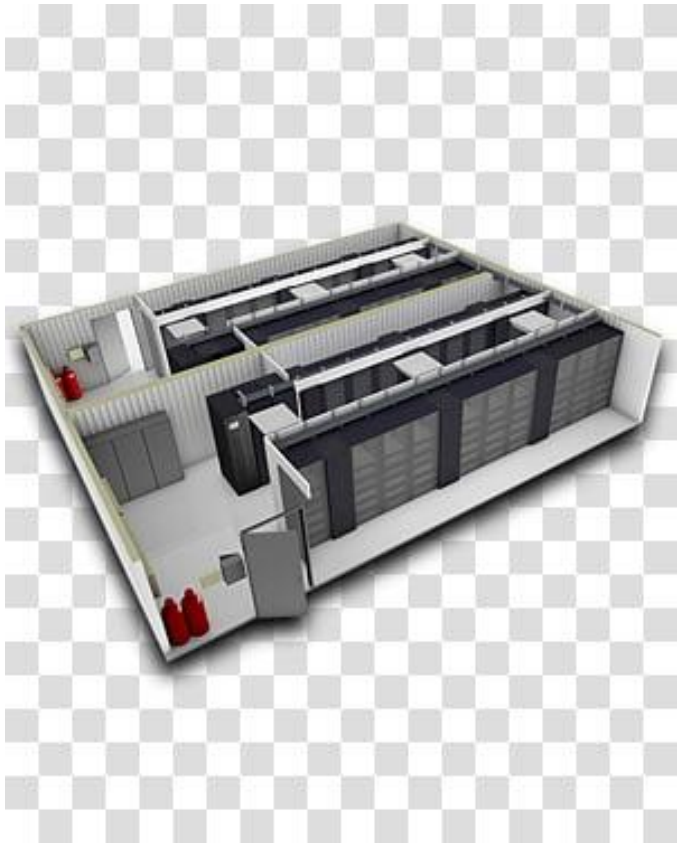
มีการดำเนินการตามแผนเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และมีการประเมิน วิเคราะห์ผลการดำเนินตามแผน



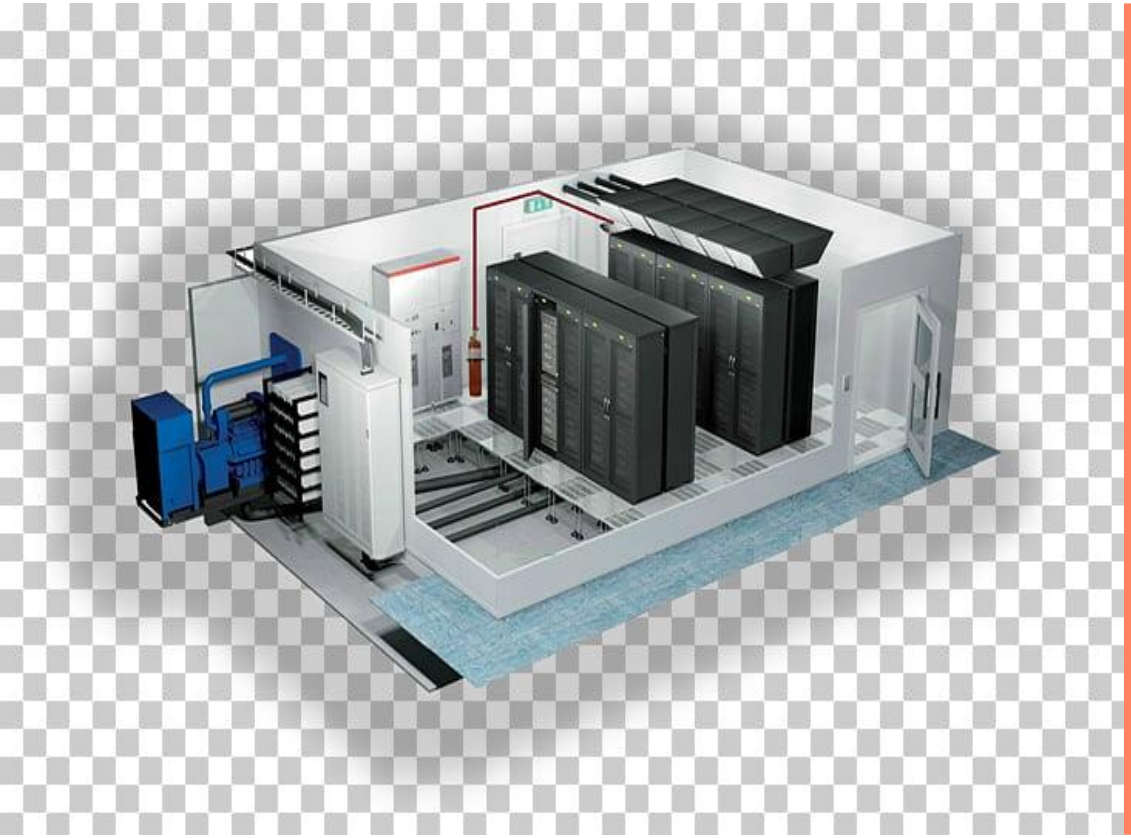
มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น

5. การจัดการห้อง Data Center

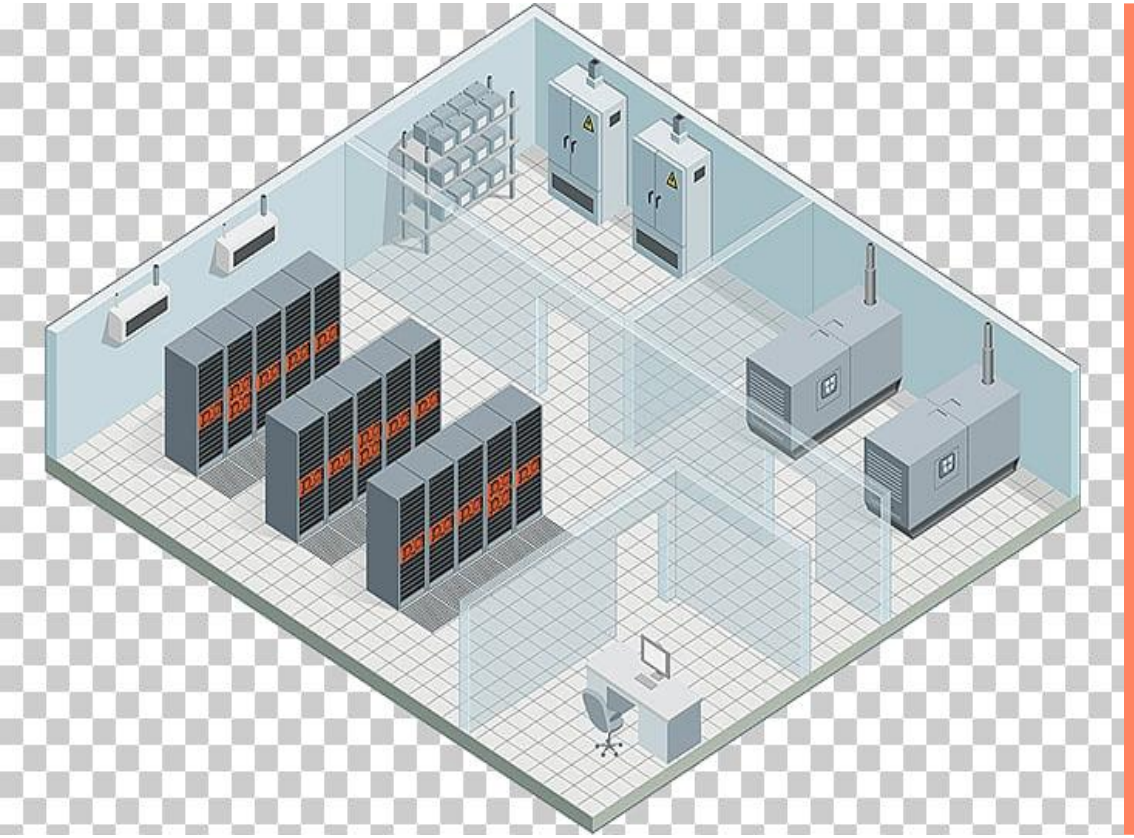
มีการจัดการ Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย



ห้อง สถานที่ และสิ่งแวดล้อมต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก



มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ



มีระบบป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server

มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยง และความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center


Thank
you!