การสัมมนา
เรื่องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลสำหรับสหกรณ์
27 พฤษภาคม 2565
โรงแรมลองบีช ชะอำ จังหวัดเพชรบุรี
เวลา 13:00-16:00 น.

บรรยายโดย ดร.ดวงกมล ทรัพย์พิทยากร
Senior IT Security Specialist
บริษัท ที-เน็ต จำกัด

แนะนำตัวผู้บรรยาย

บจ. ที-เน็ต จำกัด

ดร.ดวงกมล ทรัพย์พิทยากร

ชื่อเล่น: เกด

- ตำแหน่งปัจจุบัน Senior IT Security Specialist
  บจ. ที-เน็ต จำกัด
- ใบประกาศ, วุฒิบัตร (CERTIFICATE)
- CISA (Certified Information Systems Auditor)
- EXIN Privacy and Data Protection Foundation
- EXIN Information Security Foundation based on ISO/IEC 27001
- ISO/IEC 27701, PIMS Implementer
- ISO/IEC 27001 ISMS Lead Auditor
- ISO/IEC 20000 SMS Lead Auditor
- ISO/IEC 22301 BCMS Lead Auditor
- CompTIA Security +
- บทบาทหน้าที่ในปัจจุบัน เป็นที่ปรึกษาด้าน Information Security และด้าน PDPA ให้กับองค์กรชั้นนำทั้งภาครัฐและเอกชน และหน่วยงานกำกับดูแล

วัตถุประสงค์การอบรม

- เพื่อให้บุคลากรของชุมนุมสหกรณ์ออมทรัพย์ประเทศไทยมีความรู้ความเข้าใจในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และรอบรู้ถึงภัยคุกคามทางไซเบอร์ที่อาจส่งผลต่อการละเมิดข้อมูลส่วนบุคคล รวมถึงมาตรการรักษาความมั่นคงปลอดภัยที่จำเป็น

ประเภทของภัยคุกคามทางไซเบอร์

Cyber crime อาชญากรรมไซเบอร์ มุ่งหวังผลประโยชน์ทางการเงิน

Cyber attack การโจมตีทางไซเบอร์ มุ่งหวังข้อมูล/สารสนเทศ

Cyber terrorist การก่อการร้ายทางไซเบอร์ เพื่อทำลายระบบ IT หรือทำให้ระบบมั่นคงปลอดภัย

Cyber Security เกี่ยวข้องกับเราอย่างไร?

อาจตกเป็นเหยื่อ หรือ ทำให้องค์กรตกเป็นเหยื่อ

ผลกระทบที่ตามมา

องค์กร

ส่วนตัว

การเงิน

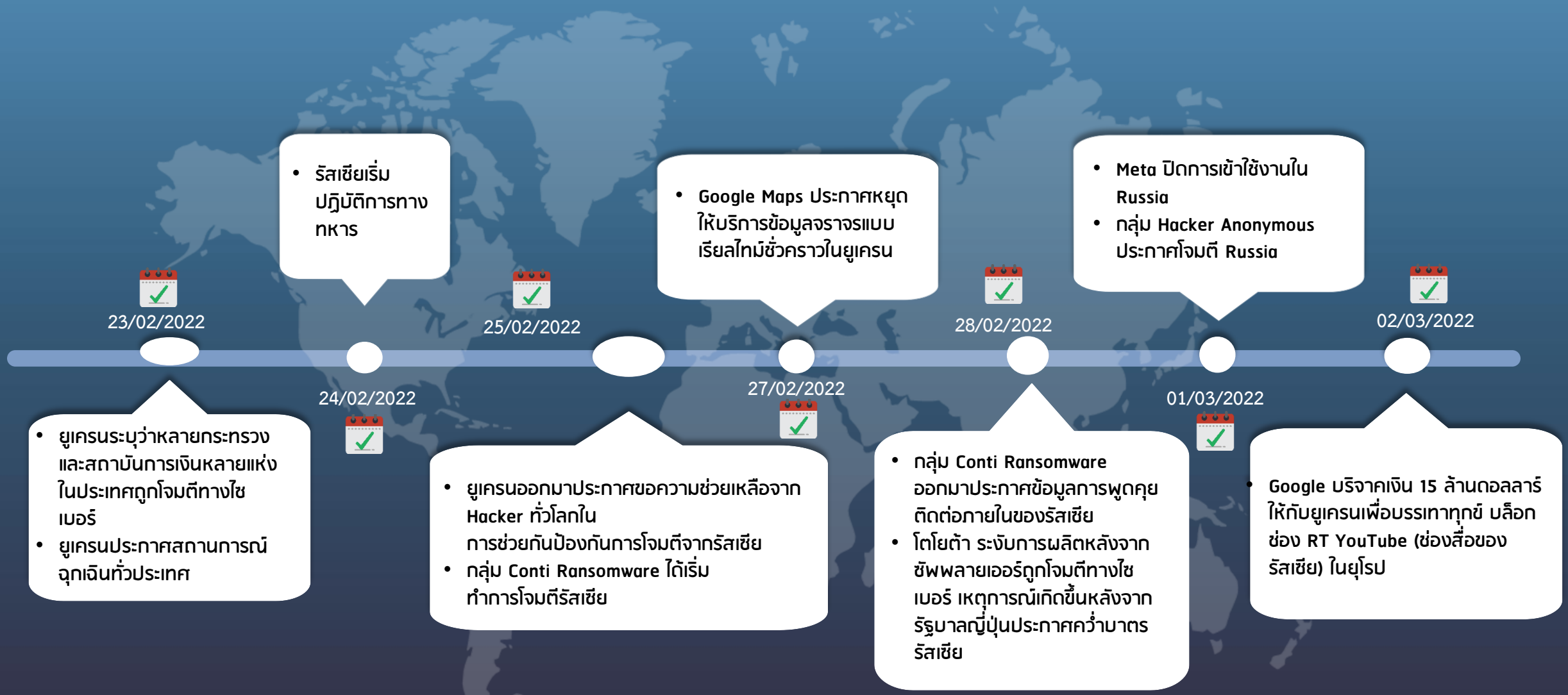
การดำเนินงาน

กฎหมาย ข้อบังคับ นโยบาย

ภาพลักษณ์ ชื่อเสียง

ข้อมูลส่วนบุคคล

Cyber attack between Russia and Ukraine



THE CYBER KILL CHAIN

01 RECONNAISSANCE

HARVESTING EMAIL ADDRESS, CONFERENCE INFORMATION, ETC.

02 WEAPONIZATION

COUPLING EXPLOIT WITH BACKDOOR INTO DELIVERABLE PAYLOAD

03 DELIVERY

DELIVERING WEAPONIZED BUNDLE TO THE VICTIM VIA EMAIL, WEB, USB, ETC.

04 EXPLOITATION

EXPLOITING A VULNERABILITY TO EXECUTE CODE ON VICTIM'S SYSTEM

05 INSTALLATION

INSTALLING MALWARE ON THE ASSET

06 COMMAND & CONTROL

COMMAND CHANNEL FOR REMOTE MANIPULATION OF VICTIM

07 ACTION ON OBJECTIVES

WITH 'HANDS ON KEYBOARD' ACCESS, INTRUDERS ACCOMPLISH THEIR ORIGINAL GOAL

AIS แจงคอมพิวเตอร์พนักงานถูกแฮ็ก ตรวจพบข้อมูลลูกค้ารั่ว 1 แสนราย ถูกนำไปปล่อยใน Dark Web

โดย THE STANDARD WEALTH
19.02.2022

347

AIS

เอไอเอส แจ้ง พบมีผู้ละเมิดข้อมูลผู้ใช้บริการ และได้ดำเนินการแก้ไขเรียบร้อยแล้ว โดยไม่กระทบกับระบบรักษาความปลอดภัยและการดำเนินธุรกิจ

18 กุมภาพันธ์ 2565 เวลา 15.05 น.: **นายปรัธนา ลีลพนัง หัวหน้าคณะผู้บริหาร กลุ่มลูกค้าทั่วไป เอไอเอส** กล่าวว่า "บริษัทฯได้ตรวจพบว่า มีผู้ละเมิดข้อมูลผู้ใช้บริการ ประมาณ 100,000 รายการ อันประกอบด้วย ชื่อ-นามสกุล, เลขบัตรประจำตัวประชาชน, วัน-เดือน-ปีเกิด,หมายเลขโทรศัพท์ โดยไม่มีข้อมูลเกี่ยวกับธุรกรรมทางการเงินใดๆ และนำไปเผยแพร่อยู่บน Dark Web ซึ่งหลังจากพบกรณีนี้ บริษัทฯได้ร่วมกับผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เร่งตรวจสอบหาสาเหตุอย่างเร่งด่วน พร้อมกับแจ้งไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)และ กสทช. รวมถึงแจ้งไปยังลูกค้ากลุ่มดังกล่าวผ่านทาง SMS เพื่อให้รับทราบและระมัดระวังต่อไป โดยกรณีดังกล่าว ไม่กระทบกับระบบรักษาความปลอดภัยและการดำเนินธุรกิจของบริษัท"

"จากการตรวจสอบสาเหตุในเบื้องต้นพบว่า กรณีนี้เกิดจากการถูกบุกรุกด้วย Ransomware เข้ามาที่เครื่องคอมพิวเตอร์ Stand Alone บางเครื่องของพนักงานที่ใช้ข้อมูลดังกล่าวในการปฏิบัติงานในช่วงระหว่างการ Work From Home และนำข้อมูลดังกล่าวออกไปเผยแพร่ ซึ่ง เอไอเอส ได้ดำเนินการตรวจสอบและให้พนักงานที่เกี่ยวข้องทั้งหมดปรับปรุงเวอร์ชั่นของซอฟต์แวร์ และระบบรักษาความปลอดภัยให้เป็นเวอร์ชั่นปัจจุบันเรียบร้อยแล้ว ทั้งนี้การให้บริการของบริษัทไม่ได้รับผลกระทบใดๆจากเหตุการณ์ดังกล่าว"

นายปรัธนา กล่าวต่อไปว่า "บริษัทฯใคร่ขออภัยจากเหตุการณ์นี้ ที่อาจจะก่อให้เกิดความไม่สะดวกแก่ลูกค้า และขอเรียนแนะนำให้ลูกค้าเพิ่มความระมัดระวังในการทำธุรกรรมต่างๆที่ต้องใช้ข้อมูลดังกล่าว รวมถึงตรวจสอบเพิ่มเติมกรณีอาจมีผู้แอบอ้างในการติดต่อเพื่อขอข้อมูลและทำธุรกรรมใดๆ กับท่าน"

"บริษัทฯ ในฐานะผู้ให้บริการโครงสร้างระบบสื่อสารของประเทศ เราให้ความสำคัญสูงสุดกับนโยบายด้านการรักษาความปลอดภัยไซเบอร์ตามมาตรฐานสากล และกฎระเบียบที่เกี่ยวข้อง ทั้งนี้บริษัทฯกำลังเร่งตรวจสอบผู้ที่

โตโยต้าหยุดโรงงานในญี่ปุ่นทั้งหมด หลังผู้ผลิตชิ้นส่วนถูกโจมตีไซเบอร์

By: lew on 28 February 2022 - 21:48 Tags: Toyota Security

โตโยต้าและโรงงานในเครือบางส่วน เช่น Hino และ Daihatsu ต้องหยุดสายการผลิตในญี่ปุ่น หลังซัพพลายเออร์รายหนึ่งถูกโจมตีไซเบอร์

บริษัทที่ถูกโจมตีคือ Kojima Industries Corp เป็นซัพพลายเออร์รายใหญ่ให้กับเครือโตโยต้า ทำหน้าที่ผลิตชิ้นส่วนอิเล็กทรอนิกส์และชิ้นส่วนพลาสติก คาดว่าคนร้ายโจมตีโดยส่งมัลแวร์เข้ามาทางอีเมล แต่ตอนนี้ยังไม่สามารถยืนยันได้แน่ชัดเนื่องจากบริษัทปิดเซิร์ฟเวอร์ทั้งหมดป้องกันปัญหาลุกลาม ทำให้ตอนนี้ระบบคอมพิวเตอร์ของ Kojima เชื่อมต่อข้อมูลกับทางโตโยต้าไม่ได้ และไม่สามารถมอนิเตอร์การทำงานของเครื่องจักรได้เลย

โตโยต้ามีโรงงานในญี่ปุ่นทั้งหมด 14 แห่ง มีกำลังผลิต 1 ใน 3 ของโรงงานทั้งโลก การหยุดสายการผลิตแต่ละวันกระทบรถยนต์วันละประมาณ 13,000 คัน

ปีที่ผ่านมาอุตสาหกรรมยานยนต์มีปัญหากำลังผลิตค่อนข้างมากจากเหตุการณ์ชิปขาดแคลน การหยุดสายการผลิตขนานใหญ่เช่นนี้น่าจะทำให้ปัญหาร้ายแรงไปอีกขั้น

ที่มา - Fox19, Reuters, Wall Street Journal

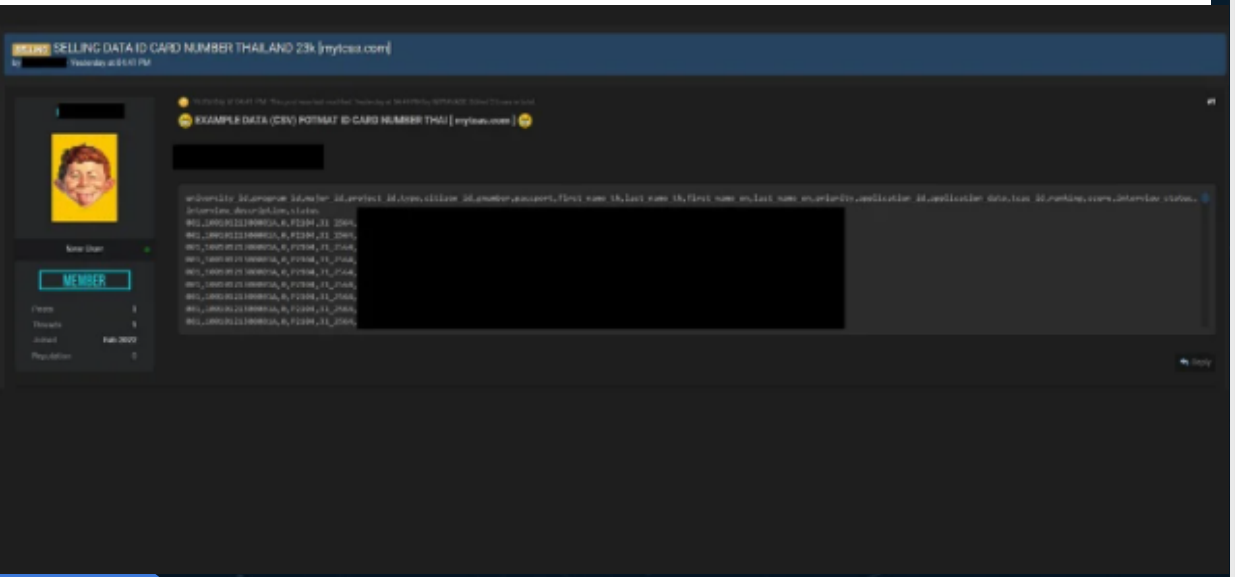
ภาระเด็กไทย ชื่อ นามสกุล เลขบัตรประชาชน หลุดจากระบบ mytcas.com กว่า 23,000 รายการ

By: mheevariety on 2 February 2022 - 22:21 Tags: Thailand TCAS Data Breach

แฮกเกอร์ประกาศขายข้อมูลที่หลุดจากเว็บไซต์หน่วยงานไทยอีกครั้ง บนฟอรั่มเดิมที่เคยพบการขายข้อมูลโรงพยาบาลเพชรบูรณ์ และแจกเลขบัตรประชาชนไทยจากฐานข้อมูลโรงพยาบาลก่อนหน้านี้

ครานี้ที่ข้อมูลที่หลุดมีส่วนสำคัญเป็นชื่อ นามสกุล และหมายเลขบัตรประชาชนของผู้ที่อยู่ในระบบ mytcas.com หรือเว็บไซต์ระบบการคัดเลือกกลางบุคคลเข้าศึกษาในสถาบันอุดมศึกษา แฮกเกอร์ระบุว่ามีกว่า 23,000 รายการ นอกนั้นเป็นข้อมูลเช่นรหัสมหาวิทยาลัยที่เลือก รหัสคณะที่เลือก และสถานะในระบบการสอบอื่นๆ

ส่วนรายละเอียดอื่นและมาตรการแก้ไขป้องกัน คงต้องรอแถลงการจากหน่วยงานที่เกี่ยวข้องต่อไป

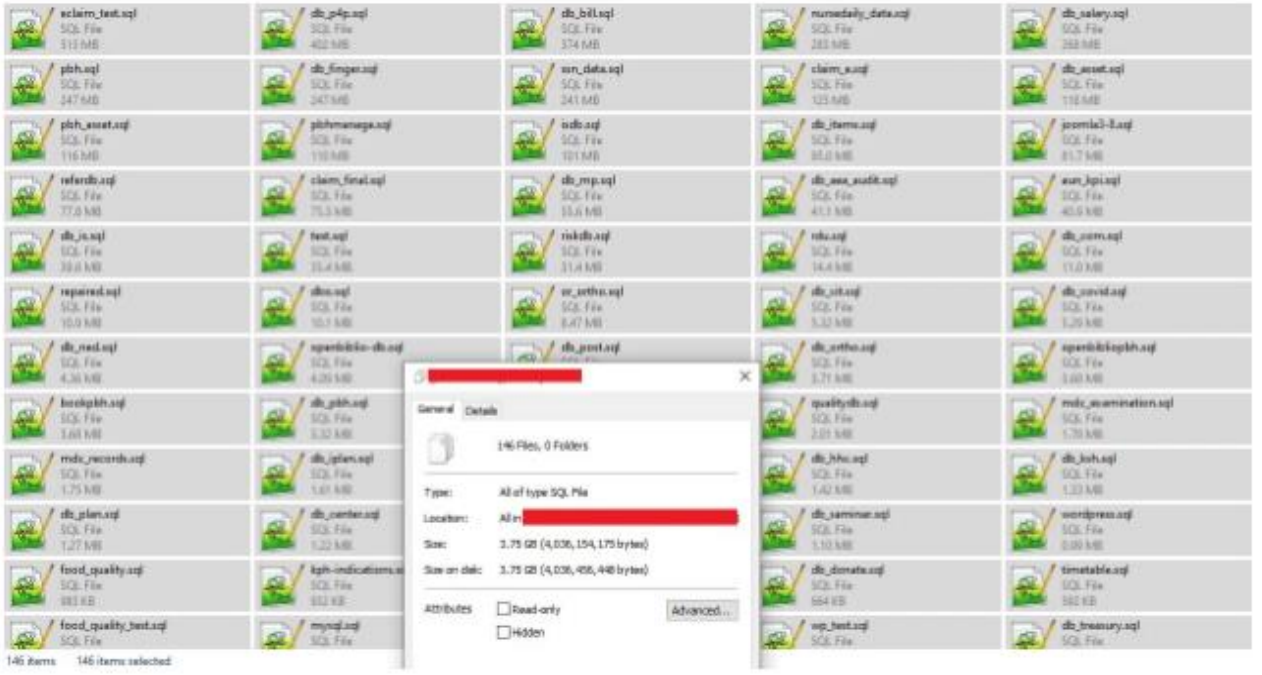


[อัพเดต: ประกาศจาก รพ.เพชรบูรณ์] คนร้ายวางขายข้อมูลส่วนตัวผู้ป่วยและโรงพยาบาล กว่า 16 ล้านรายการ ระบุมาจากกระทรวงสาธารณสุขไทย

By: mheevariety on 6 September 2021 - 19:24 Tags: Security Thailand

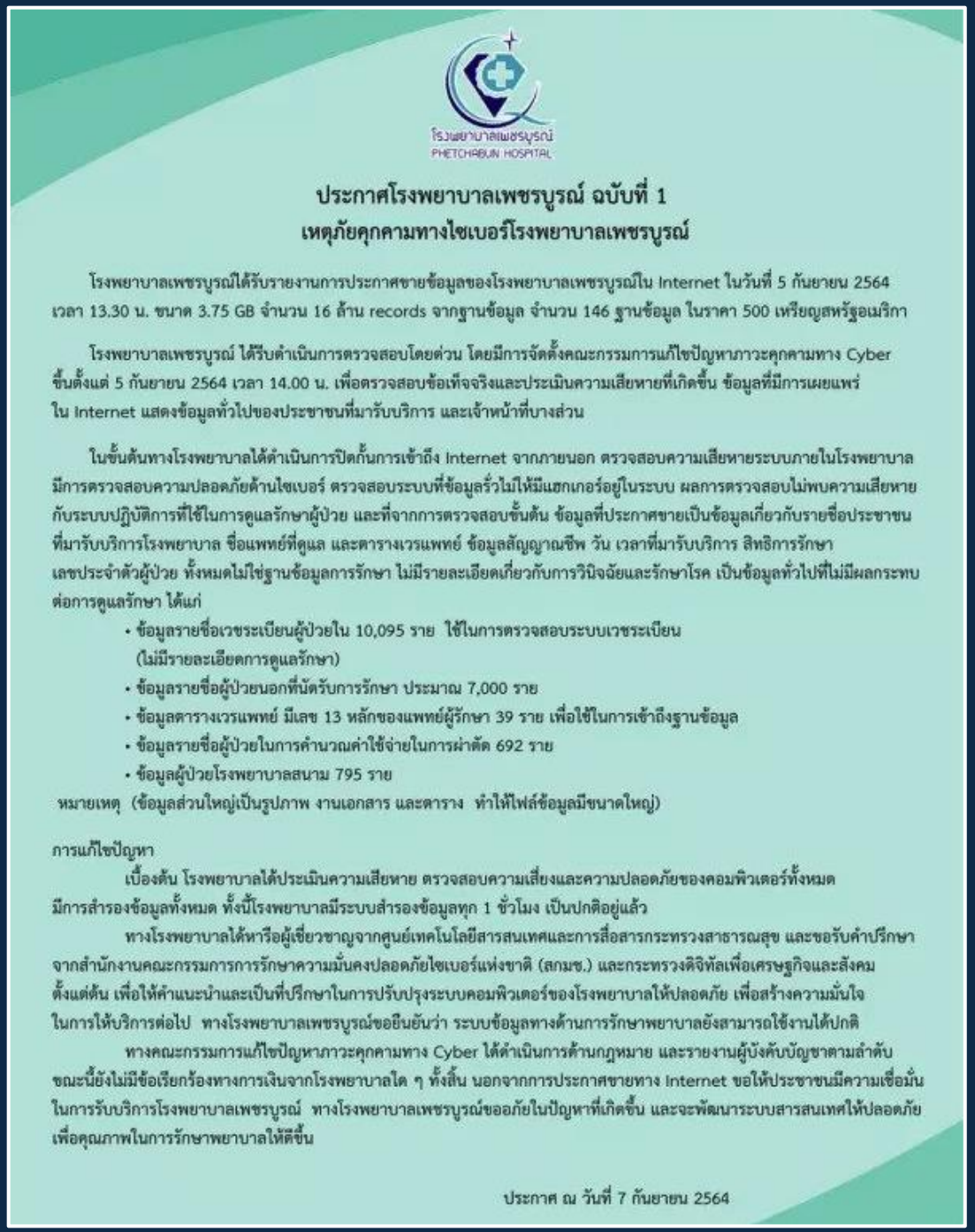
ผู้ที่ใช้ชื่อว่า Inanimate บนเว็บบอร์ด Raidforums ลงขายข้อมูลในรูปแบบไฟล์ SQL ที่อ้างว่านำมาจากระบบของกระทรวงสาธารณสุขประเทศไทย ขนาด 3.75GB กว่า 16 ล้านรายการ ระบุวันที่ล่าสุดของฐานข้อมูล วันอาทิตย์ที่ 5 กันยายน 2021 ที่ผ่านมา

ข้อมูลประกอบด้วย ชื่อผู้ป่วย ที่อยู่ เบอร์โทร หมายเลขประจำตัวประชาชน วันเกิด ชื่อโรงพยาบาล แพทย์ประจำตัว รหัสเข้าใช้ระบบโรงพยาบาล และอื่นๆ โดยลงขายในราคาเพียง 500 ดอลลาร์ หรือราว 16,300 บาทเท่านั้น (แต่ระบุเป็นราคาพิเศษช่วงสองวันแรก)



ที่มา: Raidforums

โรงพยาบาลเพชรบูรณ์



โรงพยาบาลเพชรบูรณ์
PHETCHABUN HOSPITAL

ประกาศโรงพยาบาลเพชรบูรณ์ ฉบับที่ 1
เหตุภัยคุกคามทางไซเบอร์โรงพยาบาลเพชรบูรณ์

โรงพยาบาลเพชรบูรณ์ได้รับรายงานการประกาศขายข้อมูลของโรงพยาบาลเพชรบูรณ์ใน Internet ในวันที่ 5 กันยายน 2564 เวลา 13.30 น. ขนาด 3.75 GB จำนวน 16 ล้าน records จากฐานข้อมูล จำนวน 146 ฐานข้อมูล ในราคา 500 เหรียญสหรัฐอเมริกา

โรงพยาบาลเพชรบูรณ์ ได้รีบดำเนินการตรวจสอบโดยด่วน โดยมีการจัดตั้งคณะกรรมการแก้ไขปัญหาภาวะคุกคามทาง Cyber ขึ้นตั้งแต่ 5 กันยายน 2564 เวลา 14.00 น. เพื่อตรวจสอบข้อเท็จจริงและประเมินความเสียหายที่เกิดขึ้น ข้อมูลที่มีการเผยแพร่ใน Internet แสดงข้อมูลทั่วไปของประชาชนที่มารับบริการ และเจ้าหน้าที่บางส่วน

ในขั้นต้นทางโรงพยาบาลได้ดำเนินการปิดกั้นการเข้าถึง Internet จากภายนอก ตรวจสอบความเสียหายระบบภายในโรงพยาบาล มีการตรวจสอบความปลอดภัยด้านไซเบอร์ ตรวจสอบระบบที่ข้อมูลรั่วไม่ให้มีแฮกเกอร์อยู่ในระบบ ผลการตรวจสอบไม่พบความเสียหายกับระบบปฏิบัติการที่ใช้ในการดูแลรักษาผู้ป่วย และที่จากการตรวจสอบขั้นต้น ข้อมูลที่ประกาศขายเป็นข้อมูลเกี่ยวกับรายชื่อประชาชนที่มารับบริการโรงพยาบาล ชื่อแพทย์ที่ดูแล และตารางเวรแพทย์ ข้อมูลสัญญาณชีพ วัน เวลาที่มารับบริการ สิทธิการรักษา เลขประจำตัวผู้ป่วย ทั้งหมดไม่ใช่ฐานข้อมูลการรักษา ไม่มีรายละเอียดเกี่ยวกับการวินิจฉัยและรักษาโรค เป็นข้อมูลทั่วไปที่ไม่มีผลกระทบต่อการดูแลรักษา ได้แก่

- ข้อมูลรายชื่อเวชระเบียนผู้ป่วยใน 10,095 ราย ใช้ในการตรวจสอบระบบเวชระเบียน (ไม่มีรายละเอียดการดูแลรักษา)
- ข้อมูลรายชื่อผู้ป่วยนอกที่นัดรับการรักษา ประมาณ 7,000 ราย
- ข้อมูลตารางเวรแพทย์ มีเลข 13 หลักของแพทย์ผู้รักษา 39 ราย เพื่อใช้ในการเข้าถึงฐานข้อมูล
- ข้อมูลรายชื่อผู้ป่วยในการคำนวณค่าใช้จ่ายในการผ่าตัด 692 ราย
- ข้อมูลผู้ป่วยโรงพยาบาลสนาม 795 ราย

หมายเหตุ (ข้อมูลส่วนใหญ่เป็นรูปภาพ งานเอกสาร และตาราง ทำให้ไฟล์ข้อมูลมีขนาดใหญ่)

การแก้ไขปัญหา

เบื้องต้น โรงพยาบาลได้ประเมินความเสียหาย ตรวจสอบความเสี่ยงและความปลอดภัยของคอมพิวเตอร์ทั้งหมด มีการสำรองข้อมูลทั้งหมด ทั้งนี้โรงพยาบาลมีระบบสำรองข้อมูลทุก 1 ชั่วโมง เป็นปกติอยู่แล้ว

ทางโรงพยาบาลได้หารือผู้เชี่ยวชาญจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกระทรวงสาธารณสุข และขอรับคำปรึกษาจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตั้งแต่ต้น เพื่อให้คำแนะนำและเป็นที่ปรึกษาในการปรับปรุงระบบคอมพิวเตอร์ของโรงพยาบาลให้ปลอดภัย เพื่อสร้างความมั่นใจในการให้บริการต่อไป ทางโรงพยาบาลเพชรบูรณ์ขอยืนยันว่า ระบบข้อมูลทางด้านการรักษาพยาบาลยังสามารถใช้งานได้ปกติ

ทางคณะกรรมการแก้ไขปัญหาภาวะคุกคามทาง Cyber ได้ดำเนินการด้านกฎหมาย และรายงานผู้บังคับบัญชาตามลำดับ ขณะนี้ยังไม่มีข้อเรียกร้องทางการเงินจากโรงพยาบาลใด ๆ ทั้งสิ้น นอกจากการประกาศขายทาง Internet ขอให้ประชาชนมีความเชื่อมั่นในการรับบริการโรงพยาบาลเพชรบูรณ์ ทางโรงพยาบาลเพชรบูรณ์ขออภัยในปัญหาที่เกิดขึ้น และจะพัฒนาระบบสารสนเทศให้ปลอดภัย เพื่อคุณภาพในการรักษาพยาบาลให้ดีขึ้น

ประกาศ ณ วันที่ 7 กันยายน 2564

Bangkok Airways ถูกแฮก อาจมีการเข้าถึงข้อมูลผู้ใช้บริการ

By: ZiiT on 26 August 2021 - 23:22 Tags: Bangkok Airways Security Hacking Aviation

บางกอกแอร์เวย์สประกาศผ่านหน้าเว็บไซต์ของบริษัทว่า เมื่อวันที่ 23 สิงหาคม 2564 บริษัทถูกโจมตีทางไซเบอร์ เป็นผลให้อาจมีข้อมูลผู้ใช้บริการถูกเข้าถึงโดยไม่ได้รับอนุญาติ ซึ่งข้อมูลที่โดนเข้าถึงนั้นได้แก่ ชื่อ นามสกุล สัญชาติ เพศ หมายเลขโทรศัพท์ อีเมล ที่อยู่ ช่องทางการติดต่อสื่อสาร ข้อมูลหนังสือเดินทาง ประวัติการเดินทาง ข้อมูลอาหารพิเศษของผู้โดยสาร รวมถึงข้อมูลบัตรเครดิตบางส่วนด้วย

บริษัทแนะนำให้ผู้โดยสารติดต่อไปยังธนาคารหรือผู้ให้บริการบัตรเครดิตเพื่อดำเนินการตามมาตรการรักษาความปลอดภัย ทำการเปลี่ยนรหัสผ่าน รวมถึงระวังการแอบอ้างโดยใช้ข้อมูลดังกล่าวจากผู้ไม่ประสงค์ดี

ทั้งนี้ทางบางกอกแอร์เวย์สอยู่ระหว่างดำเนินการสืบสวนเพื่อหาผู้ที่ได้รับผลกระทบและข้อมูลที่ได้รับความเสียหาย และยืนยันว่าไม่มีผลกระทบต่อความปลอดภัยด้านการบิน

ที่มา: ประกาศจากบางกอกแอร์เวย์ส

กระทรวงกลาโหมเบลเยียมถูกแฮกด้วยช่องโหว่ Log4j

By: lew on 21 December 2021 - 19:56 Tags: Log4j Security Belgium

กระทรวงกลาโหมเบลเยียมถูกคนร้ายแฮกด้วยช่องโหว่ Log4j ตั้งแต่วันพฤหัสที่ผ่านมา จนระบบหลายส่วนใช้งานไม่ได้ และผู้เกี่ยวข้องต้องแก้ไขปัญหาตลอดสุดสัปดาห์ที่ผ่านมา

แถลงการไม่เปิดเผยว่าระบบใดถูกโจมตีบ้าง และถูกโจมตีโดยกลุ่มใด แต่ระบุเพียงว่าจำกัดความเสียหายได้แล้ว

ช่องโหว่ Log4j ที่พบเมื่อต้นเดือนที่ผ่านมา หรือ CVE-2021-44228 มีความร้ายแรงสูง โจมตีได้ง่าย และมีซอฟต์แวร์ได้รับผลกระทบเป็นวงกว้าง ทำให้แฮกเกอร์กลุ่มต่างๆ พัฒนามัลแวร์ทั้งมับแวร์เรียกค่าไถ่, botnet สำหรับยิงทราฟิก, หรือแม้แต่ worm ที่แพร่กระจายตัวเองได้ไม่หยุด ออกมาเรื่อยๆ ศูนย์ความมั่นคงไซเบอร์ของเบลเยียมเองก็ออกมาเตือนว่าหากยังไม่ป้องกันแล้ว ก็เตรียมเจอการแฮกได้ภายในไม่กี่วันหรือไม่กี่สัปดาห์

ที่มา - ZDNet, The Register

MAILCHIMP ยอมรับถูกโจมตี แฮ็กเกอร์เข้าถึงข้อมูลลูกค้า

April 5, 2022 Security, Threats Update

Mailchimp ได้ยอมรับเหตุถูกโจมตีจากบัญชีของพนักงานภายใน ส่งผลให้แฮ็กเกอร์สามารถเข้าถึงข้อมูลที่ให้บริการลูกค้าและนำไปก่อเหตุ Phishing ต่อได้

credit : logowik

แจ้งเตือนผู้ลงทะเบียนบน Thailand Pass

28 ม.ค. 2565 1,681 view

แจ้งเตือนผู้ลงทะเบียนบน Thailand Pass

ผู้ลงทะเบียนบน Thailand Pass ที่ได้อีเมลรูปแบบตามภาพ **โปรดอย่า!!** ดำเนินการตามข้อความในอีเมลดังกล่าว
เนื่องจากเป็นข้อมูลเท็จ ซึ่งไม่ได้มาจากระบบ Thailand Pass และอาจส่งผลต่อความปลอดภัยของข้อมูลส่วนตัวของท่าน

Notice;

Applicants on Thailand Pass who have received the following email, **DO NOT!!** scan the QR Code or follow the instructions described.
The email does not come from Thailand Pass, and could compromise the security and privacy of your personal information.

THAILAND PASS

There is a problem related to the request, please download the attachment and update the information

Thailand Pass Registration System (for air travel only)

[redacted]

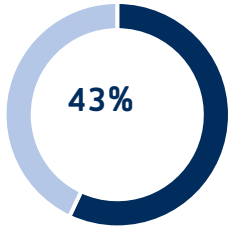
Download Document

important note. You must open the document from a PC and not from the phone

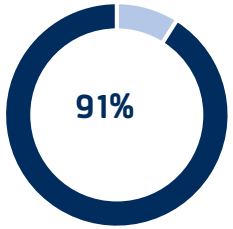
THAILAND PASS

Embassy, Consulate General ,

Cyber Security Statistics

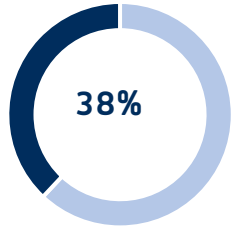


43% of all cyber attacks are aimed at small businesses.



91% of attacks launch with a phishing email.

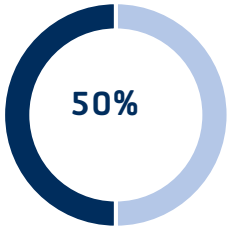
A business falls victim to a ransomware attack every 14 seconds.



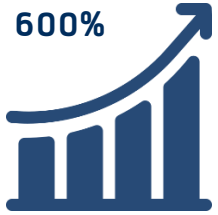
38% of malicious attachments are masked as one Microsoft Office type of file or another.

Companies faced an average of 22 security breaches in 2020.

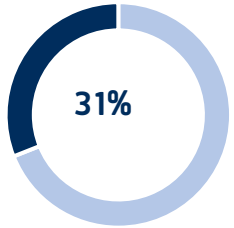
The global cost of online crime is expected to reach $6 trillion by 2021



Around 50% of the risk companies face come by way of having multiple security vendors



IoT attacks were up by 600% in 2017. In 2019, the attacks reached 2.9 billion events



31% of organizations have experienced cyber attacks on operational infrastructure

The app stores block over 24,000 malicious mobile apps each day.

Social Media

Smart Home

Wearable Device

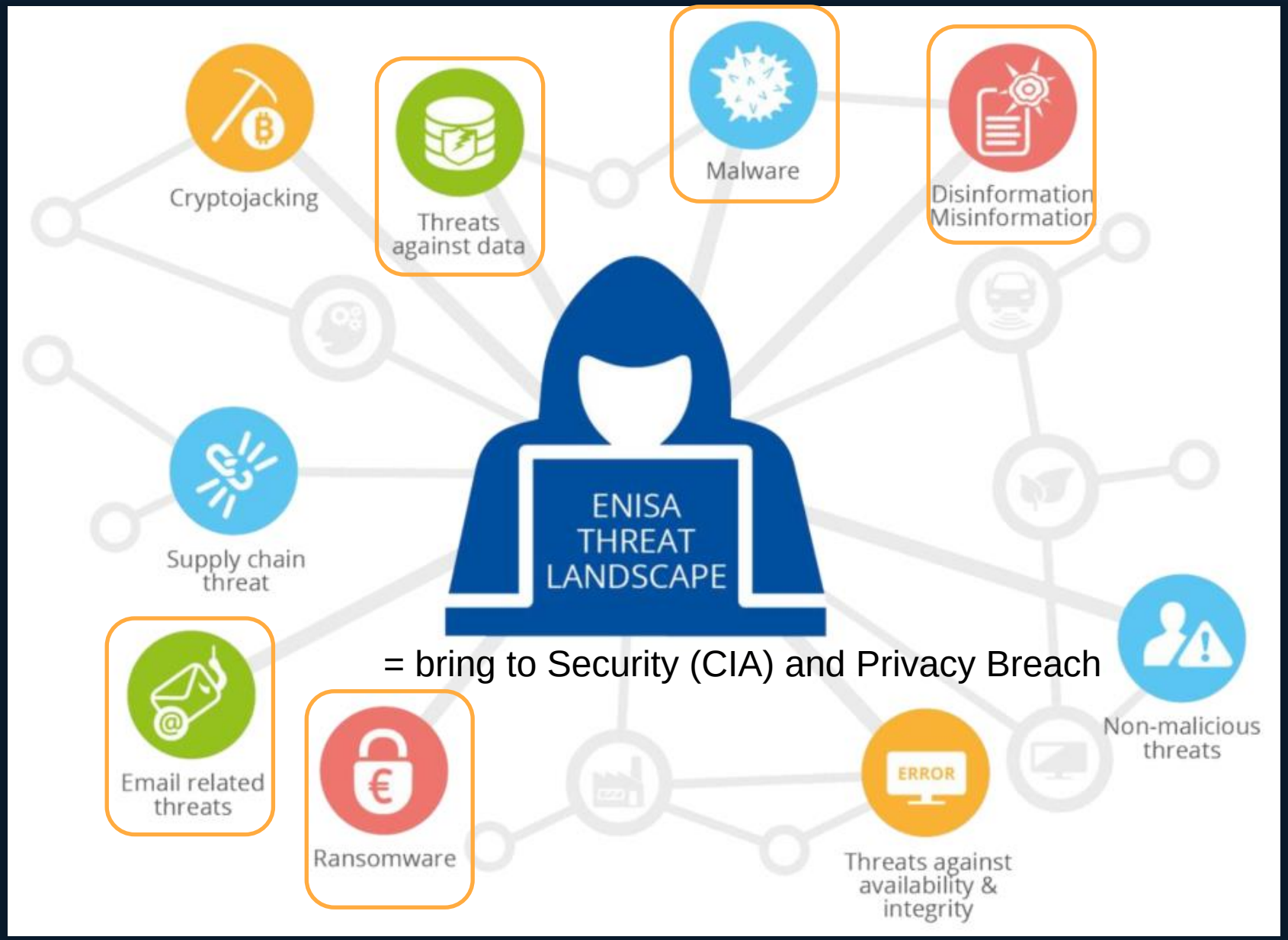
Internet Cafe

Shopping Online

Scan QR Codes

Online Movie

Prime threats



= bring to Security (CIA) and Privacy Breach

Data Privacy Risk

โครงสร้างของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

บททั่วไป (มาตรา ๑ – มาตรา ๗)

หมวด ๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๘ – มาตรา ๑๘)

หมวด ๒ การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑ บททั่วไป (มาตรา ๑๙ – มาตรา ๒๑)

ส่วนที่ ๒ การเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา ๒๒ – มาตรา ๒๖)

ส่วนที่ ๓ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา ๒๗ – มาตรา ๒๙)

หมวด ๓ สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา ๓๐ – มาตรา ๓๖)

หน้าที่ของผู้ควบคุมข้อมูล มาตรา ๓๗

หน้าที่ของผู้ประมวลผลข้อมูล มาตรา ๔๐

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มาตรา ๔๑ – มาตรา ๔๒

หมวด ๔ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๓ – มาตรา ๗๐)

หมวด ๕ การร้องเรียน (มาตรา ๗๑ – มาตรา ๗๖)

หมวด ๖ ความรับผิดทางแพ่ง (มาตรา ๗๗ - มาตรา ๗๘)

หมวด ๗ บทกำหนดโทษ

ส่วนที่ ๑ โทษอาญา (มาตรา ๗๙ – มาตรา ๘๑)

ส่วนที่ ๒ โทษทางปกครอง (มาตรา ๘๒ – มาตรา ๙๐)

บทเฉพาะกาล (มาตรา ๙๑ – มาตรา ๙๕)

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๓) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(๔) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

(๕) ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

โดยที่มาตรา ๓ วรรคสอง แห่งพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ กำหนดให้ผู้ควบคุมข้อมูลซึ่งเป็นหน่วยงานหรือกิจการตามบัญชีท้ายพระราชกฤษฎีกาดังกล่าวต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

อาศัยอำนาจตามความในมาตรา ๓ วรรคสอง แห่งพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงออกประกาศไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาจนถึงวันที่ ๓๑ พฤษภาคม ๒๕๖๔

ข้อ ๓ ในประกาศนี้

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานหรือกิจการตามบัญชีท้ายพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓

“ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามประกาศนี้ ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ รวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

ข้อ ๕ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical

safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วยการดำเนินการ ดังต่อไปนี้

(๑) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

(๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

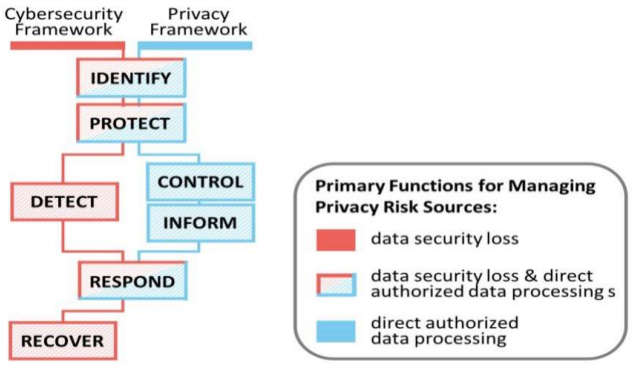
(๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(๕) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ ๖ ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในประกาศนี้

ข้อ ๗ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามประกาศนี้ และให้มีอำนาจตีความและวินิจฉัยปัญหาอันเกิดจากการปฏิบัติตามประกาศนี้

ประกาศ ณ วันที่ ๒๔ มิถุนายน พ.ศ. ๒๕๖๓
พุทธิพงษ์ ปุณณกันต์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



https://www.nist.gov/privacy-framework.

ISO 27001

องค์ประกอบของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

1

การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูล

2

การกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

3

การเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว (User access management)

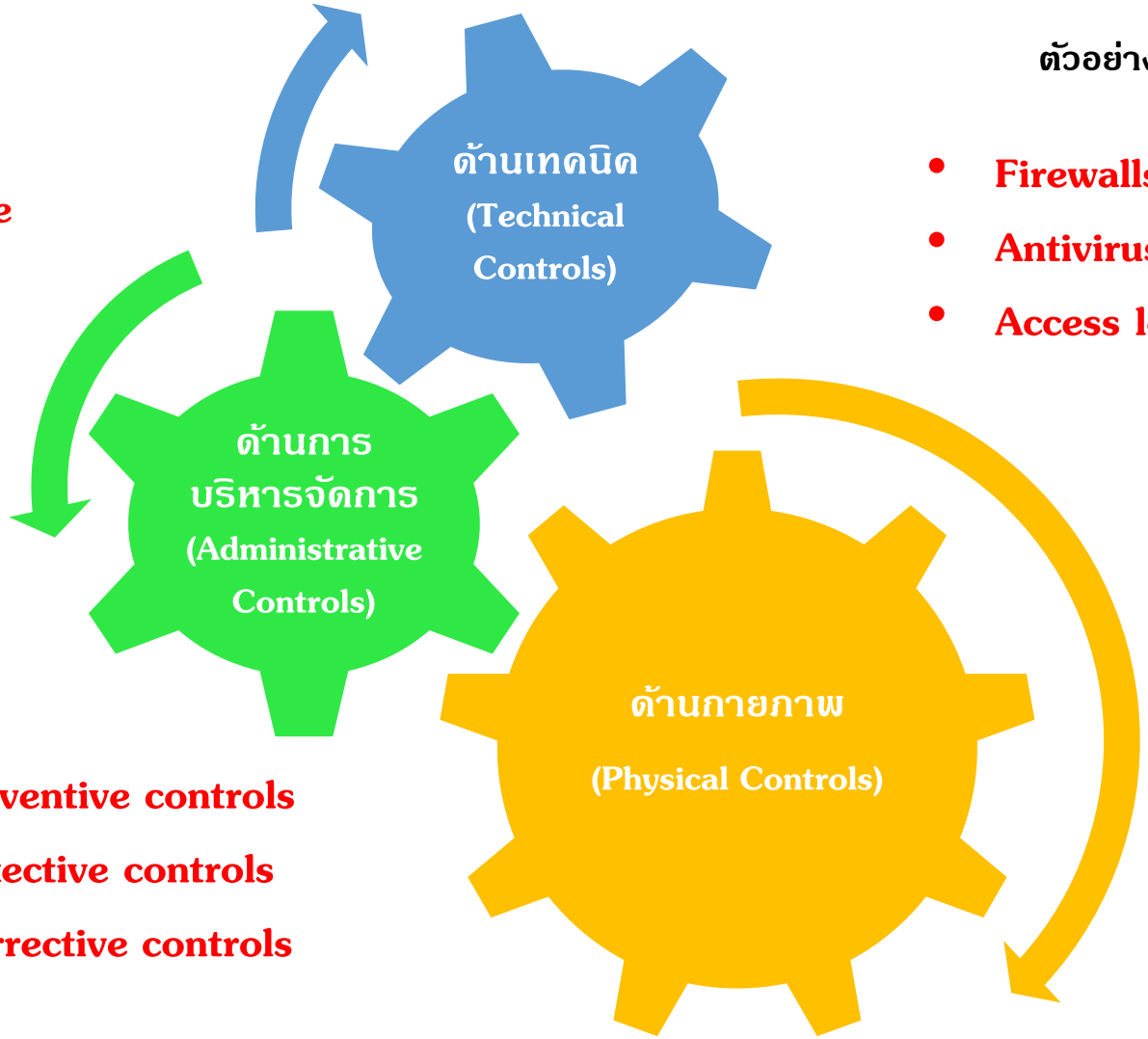
4

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

5

การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลัง

องค์ประกอบของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล



ตัวอย่าง

Incident response procedures and training

ตัวอย่าง

- Firewalls
- Antivirus Software
- Access logs

- Preventive controls
- Detective controls
- Corrective controls

ตัวอย่าง

- Locks
- CCTV
- Fences

Privacy v$ Security

Privacy

- Collection of Personal Information
- Using and disclosing personal information in authorized manner
- Data quality
- Access to personal information

Protection of personal information

Security

- **Confidentiality**: data being stored is safe from unauthorized access and use
- **Integrity**: data is reliable and accurate
- **Availability**: data is available for use when it is needed

วงจรชีวิตข้อมูลส่วนบุคคล

Data Storage
(รูปแบบการจัดเก็บ แหล่งที่จัดเก็บ)
2

Data Disclosure
(องค์กรภายนอกที่มีการเปิดเผยข้อมูล)
4

Data Archival
(มีการสำรองข้อมูลไว้ที่ไหนหรือไม่)
6

Physical/Electronic | (Handling of Data Subject Request/Response of Request) | Retention Period

(มีการสำรองข้อมูลไว้ที่ไหนหรือไม่)

1
Data Collection
(Lawful basis, Notice requirement purpose limitation, data minimization)

3
Data Use Access to Personal Data
(ภายในองค์กร: ใครบ้าง ที่ใช้และเข้าถึงข้อมูล)

5
Data Transfer
(Rules for international transfer)
(มีการโอนข้อมูลฯไปต่างประเทศหรือไม่ รูปแบบ, วิธีการโอน)

7
Data Disposal
(การลบและทำลายข้อมูล)

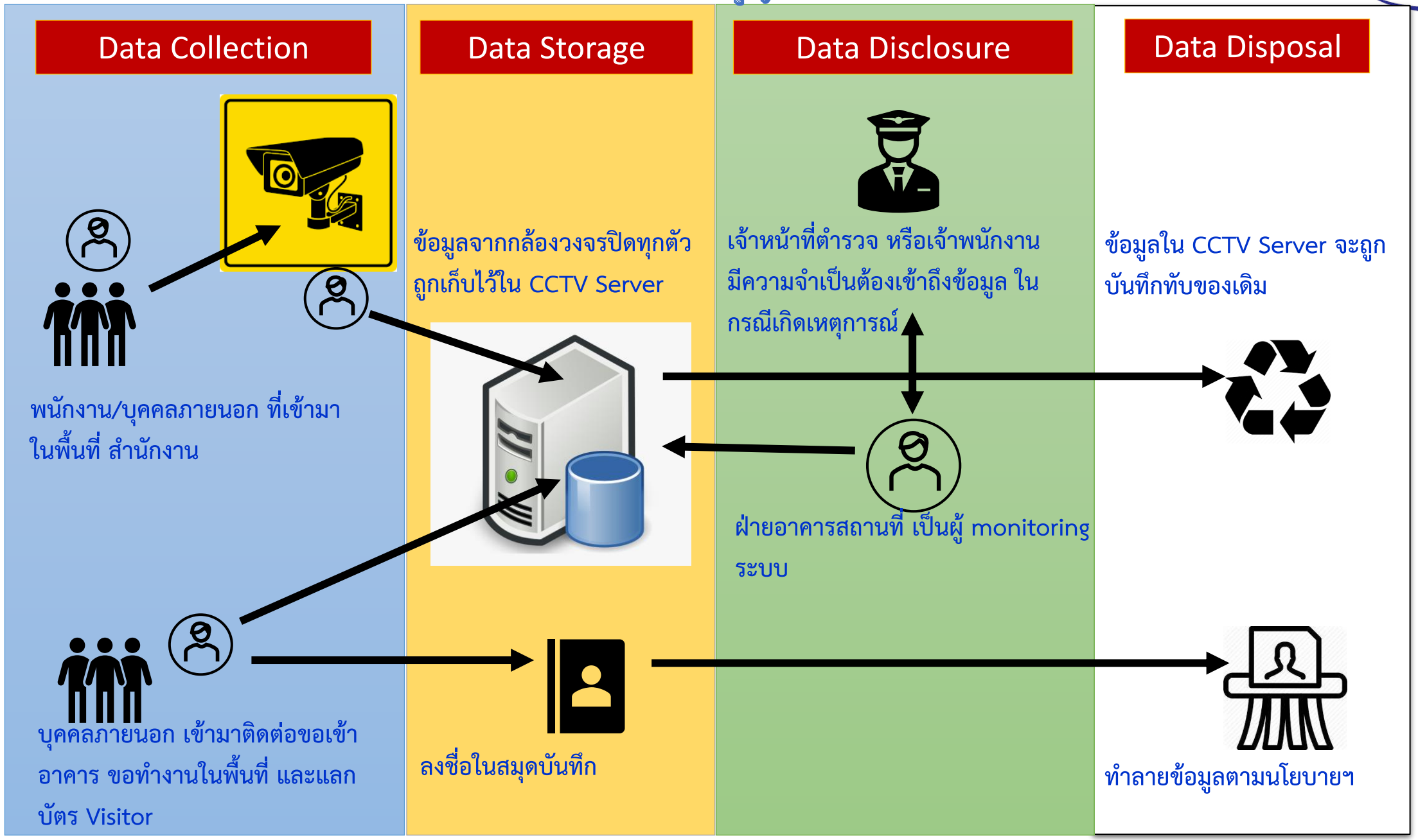
(ฐานทางกฎหมาย, การแจ้ง, วัตถุประสงค์จำกัด, ใช้ข้อมูลน้อยที่สุด)

Data Collection
1. Lawful basis
2. Notice requirement
3. Purpose limitation
4. Data minimization

1.ฐานทางกฎหมาย (7 ฐานตามมาตรา 24 และ 26)
2.การแจ้ง (ม.23 Privacy Notice)
3.วัตถุประสงค์จำกัด (ม.21)
4.ใช้ข้อมูลน้อยที่สุด (ม.22)

Ensure Security Measures

ตัวอย่าง Data map, Data Flow



ตัวอย่าง Data map, Data Flow

- CIA ของ CCTV
- Equipment Siting
- ความชัดเจนของภาพ การเก็บภาพได้ถูกต้องเหมาะสม และสภาพความพร้อมใช้ของกล้อง CCTV
- ไม่ไปละเมิด Privacy ของบุคคลอื่น
- + MA

ection

Data Storage

- CIA ของสายสัญญาณที่ส่งข้อมูล
- อยู่ในตำแหน่งที่ถูกดักจับสัญญาณได้ง่ายหรือไม่
- สัญญาณ loss หรือไม่
- สายถูกหนูกัดแทะง่ายหรือไม่

Data Disclosure

เหตุละเมิดข้อมูลส่วนบุคคล (Breach)
ข้อมูลส่วนบุคคลรั่วไหล (Leak)

Data Disposal

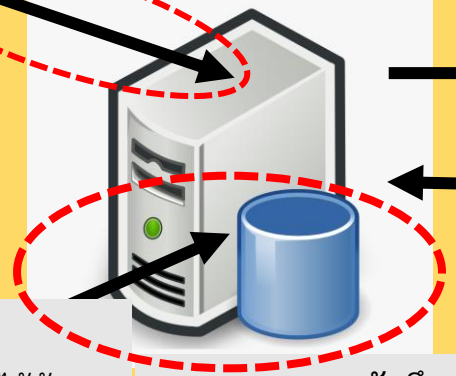
- Incident Management Process

ายนอก ที่เข้ามา

- Privacy Notice

เจ้าหน้าที่ตำรวจ หรือเจ้าพนักงาน มีความจำเป็นต้องเข้าถึงข้อมูล ในกรณีเกิดเหตุการณ์

ข้อมูลใน CCTV Server จะถูกบันทึกทับของเดิม



ฝ่ายอาคารสถานที่ เป็นผู้ monitoring

กรณีฮาร์ดดิสก์เสื่อมสภาพ

บุคคลภา
อาคาร ข
บัตร Vis

- C ของระบบบันทึกภาพ
- ใครสามารถเข้าถึงภาพในระบบได้บ้าง
- การพิสูจน์ตัวตนทำอย่างไร
- มีขั้นตอนกระบวนการ กรณีที่มีบุคคลภายนอกขอเข้าถึงภาพในระบบหรือไม่
- USR management มีหรือไม่อย่างไร
- มีการจัดเก็บล็อกเพื่อพิสูจน์ตัวตนไหม

- I ของระบบบันทึกภาพ
- ภาพที่ถูกจัดเก็บเข้าไปมีความถูกต้องสมบูรณ์หรือไม่
- มีการแก้ไขเปลี่ยนแปลงภาพโดยไม่ได้รับอนุญาตหรือไม่
- เวลาของกล้องกับเวลาของฐานข้อมูลหลังบ้านตรงกันหรือไม่

- A ของระบบบันทึกภาพ
- ระบบสามารถบันทึกภาพทั้งหมดได้ครบตามกำหนดระยะเวลาหรือไม่
- ทรัพยากรเพียงพอหรือไม่
- ต้องมีการแบคอัพหรือสำเนาไว้อีกชุดหรือไม่

- CIA ของการลบ
- ใครเข้าถึงข้อมูลในระหว่างที่ลบได้บ้าง
- ลบได้สิ้นซากจริงหรือไม่
- ใช้วิธีการลบแบบไหน
- Clear, Purge, Physical Destroy (NIST 800-88)

*** สิ่งที่ควรดำเนินการเมื่อองค์กรจะต้องมีการประมวลผล (เก็บ รวบรวม ใช้ เปิดเผย) ข้อมูลส่วนบุคคล ***

- ร่าง Data map, Data flow สำหรับกิจกรรมที่จะมีการประมวลผลข้อมูลส่วนบุคคล
- DPIA ประเมินผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล (สิ่งที่เราจะเก็บรวบรวมใช้เปิดเผย มันกระทบกับตัวเจ้าของข้อมูลส่วนบุคคลไหม) ประเมินว่าจะใช้ฐานไหน เหมาะสมหรือไม่
- Risk Assessment +Risk Option (Reduce, Accept, Transfer, Avoid) +Budget
- วาง Security Measures (Organizational Measures and Technical Measures) ในแต่ละจังหวะให้ครบถ้วน ถ้าจะต้องไป design ระบบก็เพิ่มเรื่อง Data Protection by Design and by Default
- Consult DPO ขอความเห็นจาก DPO
- เริ่มลงมือทำกิจกรรมนั้น

หมายเหตุ ข้อมูลที่กล่าวมาข้างต้นเป็นแนวคิดและความคิดเห็นส่วนบุคคล บางรายการไม่ได้มีการบังคับตาม PDPA

ISO/IEC 27001 Framework

Annex A

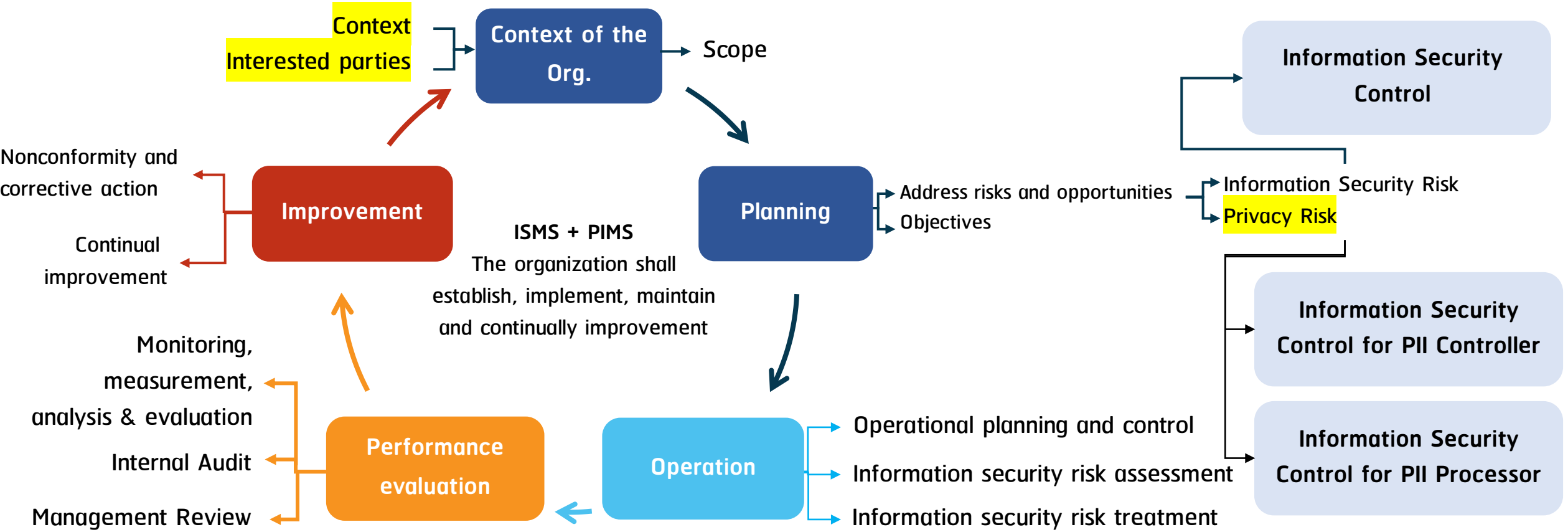
- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

ISMS + PIMS

Security + Privacy
(C-I-A)

PIMS =
Privacy Information
Management
System

Leadership
[Leadership and commitment, Policy, Roles responsibilities and Authorities]



Support

ISMS + PIMS

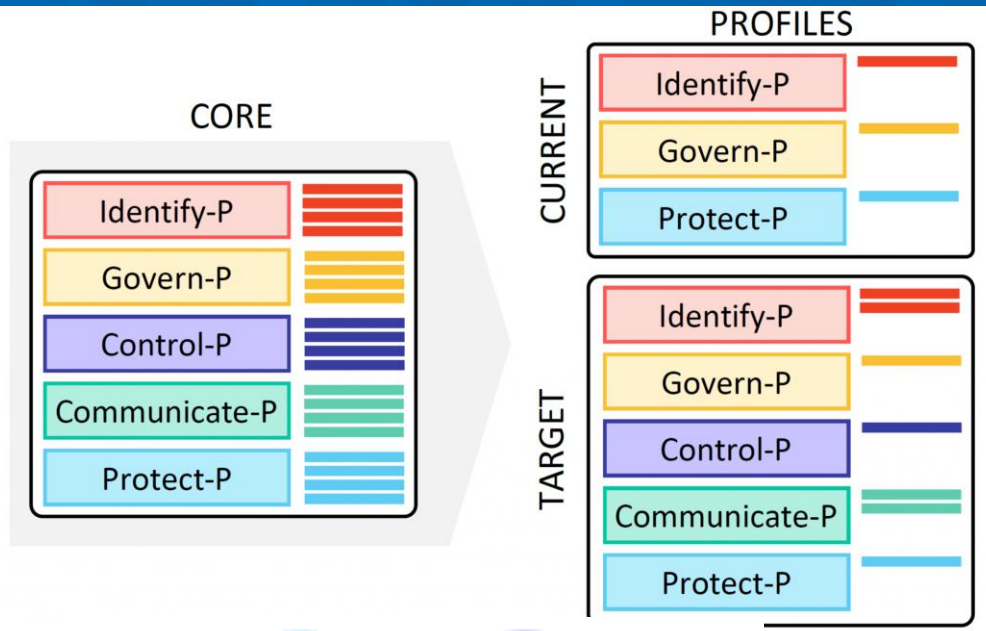
Requirements	Information Security Control	Information Security Control for PII Controller	Information Security Control for PII Processor
1. Context of the organization	1. Information security policies	1. Conditions for collection and processing	1. Conditions for collection and processing
2. Leadership	2. Organization of information security	2. Obligations to PII principals	2. Obligations to PII principals
3. Planning	3. Human resource security	3. Privacy by design and privacy by default	3. Privacy by design and privacy by default
4. Support	4. Asset management	4. PII sharing, transfer, and disclosure	4. PII sharing, transfer, and disclosure
5. Operation	5. Access control		
6. Performance evaluation	6. Cryptography		
7. Physical and environmental security	7. Physical and environmental security		
8. Improvement	8. Operations security		
	9. Communications security		
	10. Systems acquisition, development and maintenance		
	11. Supplier relationships		
	12. Information security incident management		
	13. Information security aspects of business continuity management		
	14. Compliance		

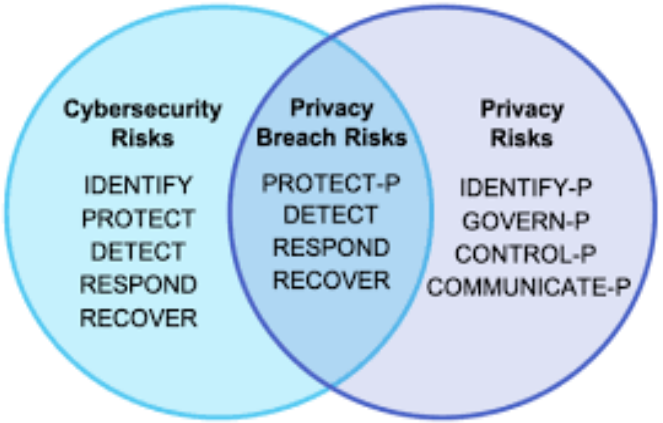
= ขยายข้อกำหนดเพิ่มเติมของ ISO/IEC 27001:2013 เพื่อคำนึงถึงการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูล PII ที่อาจได้รับผลกระทบจากการประมวลผลข้อมูล PII

PII = personally identifiable information

= ข้อแนะนำเพิ่มเติมของ ISO/IEC 27002 สำหรับผู้ควบคุมข้อมูล PII และสำหรับผู้ประมวลผลข้อมูล PII

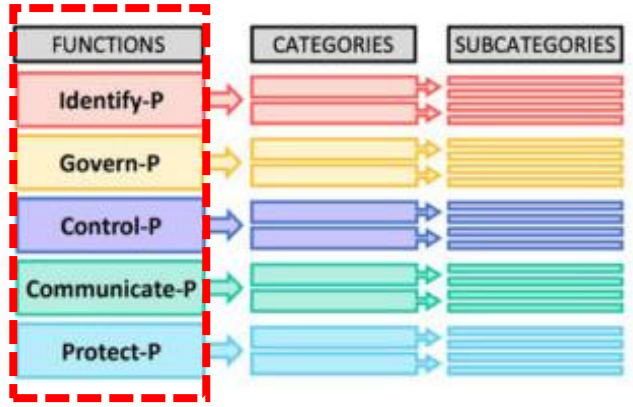
NIST PRIVACY FRAMEWORK





อ้างอิง https://www.nist.gov/system/files/documents/2021/05/05/NIST-Privacy-Framework-V1.0-Core-PDF.pdf

NIST Privacy Framework:
A Tool for Improving Privacy through Enterprise Risk Management
(Preliminary Draft)



The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk

Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

NIST PRIVACY FRAMEWORK

IDENTIFY

Function	Category	Subcategory
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
		ID.IM-P4: Data actions of the systems/products/services are inventoried.
		ID.IM-P5: The purposes for the data actions are inventoried.
		ID.IM-P6: Data elements within the data actions are inventoried.
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.
	Business Environment (ID.BE-P): The organization's mission, objectives,	**ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified and communicated.
	stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P2:** Priorities for organizational mission, objectives, and activities are established and communicated.
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.
		ID.RA-P3: Potential problematic data actions and associated problems are identified.
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.
		ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.
		ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.
		ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.

อ้างอิง https://www.nist.gov/system/files/documents/2021/05/05/NIST-Privacy-Framework-V1.0-Core-PDF.pdf

NIST

PRIVACY FRAMEWORK

T-NET

GOVERN

Function	Category	Subcategory
		ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations.
GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P)**: The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PO-P1**: Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.
		GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
		GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.
		GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
		GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**GV.RM-P1**: Risk management processes are established, managed, and agreed to by organizational stakeholders.
		GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.
		GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.
	Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with	**GV.AT-P1**: The workforce is informed and trained on its roles and responsibilities.
		GV.AT-P2: Senior executives understand their roles and responsibilities.
		GV.AT-P3: Privacy personnel understand their roles and responsibilities.

CONTROL

Function	Category	Subcategory
	related policies, processes, procedures, and agreements and organizational privacy values.	**GV.AT-P4**: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.
	Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1**: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
		GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.
		GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
		GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
		GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).
		GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.
		GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.
CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with	**Data Processing Policies, Processes, and Procedures (CT.PO-P)**: Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the	**CT.PO-P1**: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
		CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).

อ้างอิง https://www.nist.gov/system/files/documents/2021/05/05/NIST-Privacy-Framework-V1.0-Core-PDF.pdf

NIST PRIVACY FRAMEWORK

Function	Category	Subcategory
sufficient granularity to manage privacy risks.	organization's risk strategy to protect individuals' privacy.	**CT.PO-P3:** Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
		CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.
	Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P1:** Data elements can be accessed for review.
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.
		CT.DM-P3: Data elements can be accessed for alteration.
		CT.DM-P4: Data elements can be accessed for deletion.
		CT.DM-P5: Data are destroyed according to policy.
		CT.DM-P6: Data are transmitted using standardized formats.
		CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
		CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.
		CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.
	Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).
		CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).
		CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).
		CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.
		CT.DP-P5: Attribute references are substituted for attribute values.

COMMUNICATE

Function	Category	Subcategory
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
		CM.AW-P3: System/product/service design enables data processing visibility.
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.
		CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.

PROTECT

PROTECT-P (PR-P): Develop and implement	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles	**PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).

อ้างอิง https://www.nist.gov/system/files/documents/2021/05/05/NIST-Privacy-Framework-V1.0-Core-PDF.pdf

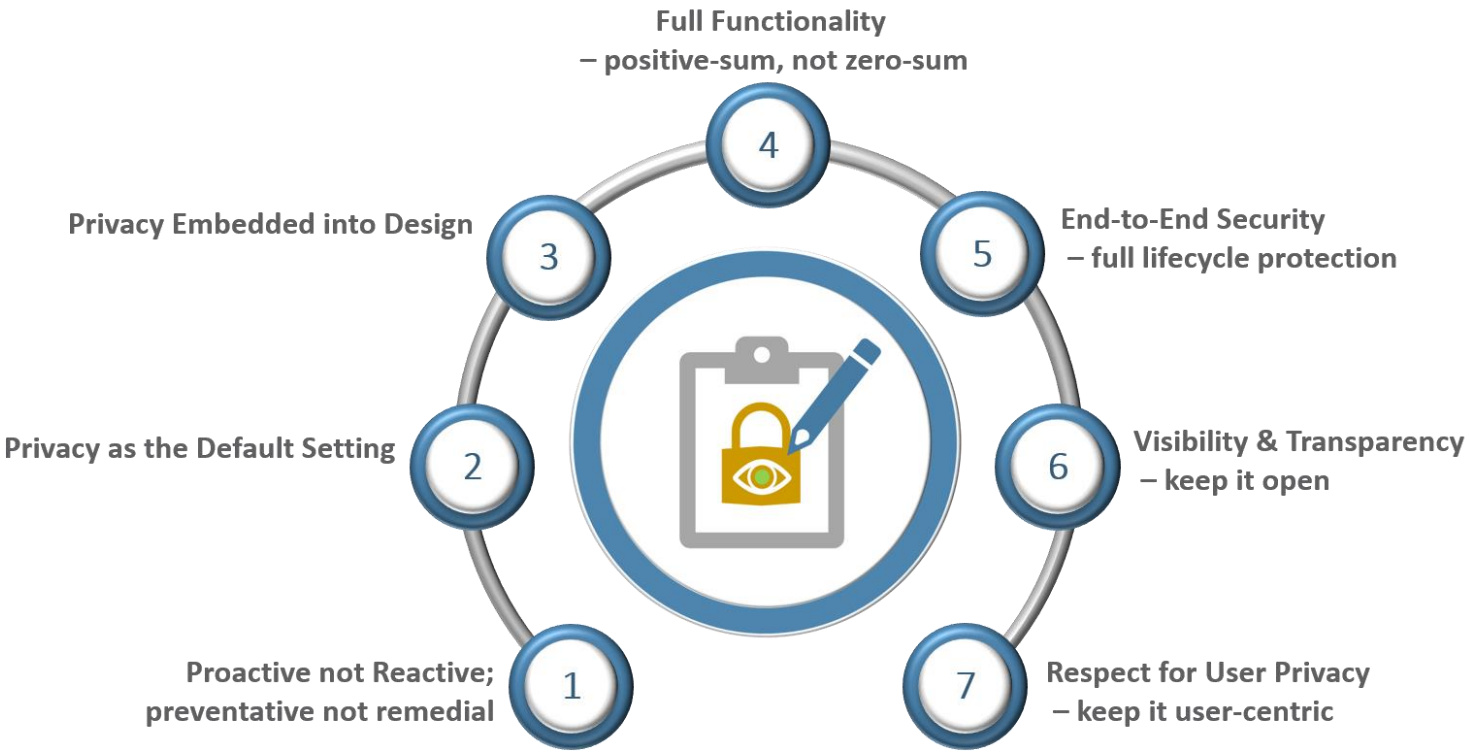
NIST PRIVACY FRAMEWORK

Function	Category	Subcategory
appropriate data processing safeguards.	and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**PR.PO-P2:** Configuration change control processes are established and in place.
		PR.PO-P3: Backups of information are conducted, maintained, and tested.
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.
		PR.PO-P5: Protection processes are improved.
		PR.PO-P6: Effectiveness of protection technologies is shared.
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.
		PR.PO-P8: Response and recovery plans are tested.
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
		PR.PO-P10: A vulnerability management plan is developed and implemented.
	Identity Management, Authentication, and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
		PR.AC-P2: Physical access to data and devices is managed.
		PR.AC-P3: Remote access is managed.
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
	Data Security (PR.DS-P): Data are managed consistent with the	**PR.DS-P1:** Data-at-rest are protected.
		PR.DS-P2: Data-in-transit are protected.

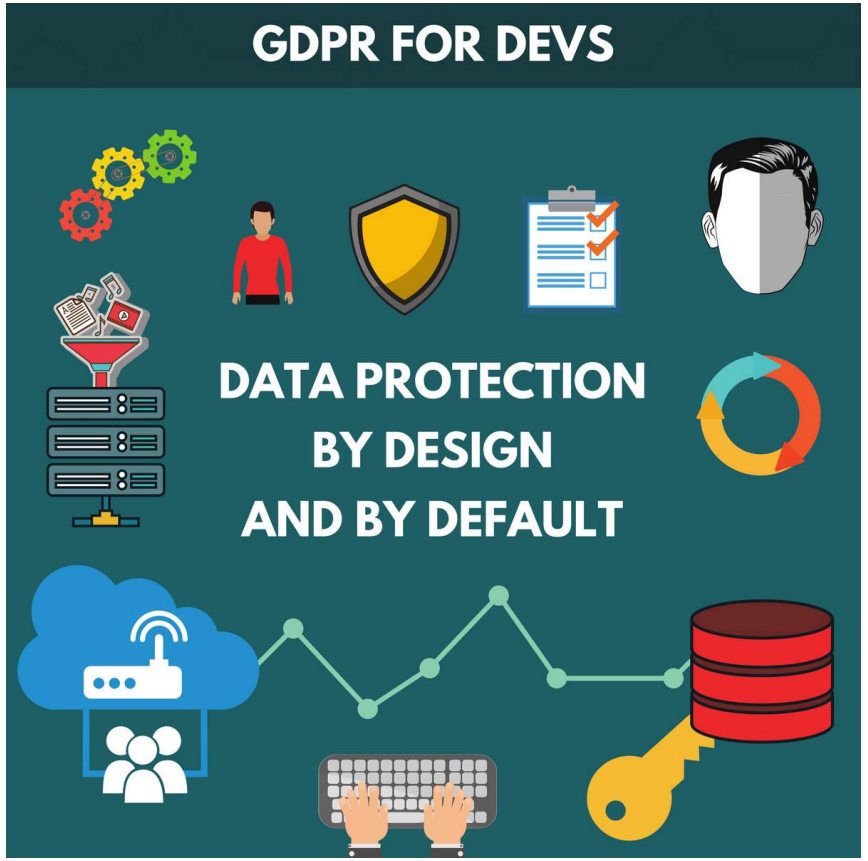
Function	Category	Subcategory
	organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P3:** Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
		PR.DS-P4: Adequate capacity to ensure availability is maintained.
		PR.DS-P5: Protections against data leaks are implemented.
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		PR.PT-P3: Communications and control networks are protected.
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

อ้างอิง https://www.nist.gov/system/files/documents/2021/05/05/NIST-Privacy-Framework-V1.0-Core-PDF.pdf

Privacy by design and by default



Ref: https://www.coreio.com/gdpr-makes-a-compelling-case-for-privacy-by-design/



Picture by GDPR for developers

STRIDE Model

Category	Description	Controls
Spoofing (การปลอมแปลง)	**Pretending to be someone else**	**Authentication**
Tampering (การแก้ไข เปลี่ยนแปลง)	**Changing data to be inaccurate**	**Integrity controls**
Repudiation (การปฏิเสธ)	**Denying that you did a thing you did**	**Accountability controls**
Information Disclosure (การเปิดเผย)	**Revealing information that should not be otherwise accessible**	**Confidentiality controls**
Denial of Service (การปฏิเสธการให้บริการ)	**Trying to stop someone else from using a system**	**Availability controls**
Elevation of Privilege (การเลื่อนระดับสิทธิ)	**Trying to get a higher level of access than you are currently assigned**	**Authorization controls**

An effective privacy program that includes:

- Privacy governance and accountability.
- Written policies and procedures.
- Controls and processes.
- Roles and responsibilities.
- Training and education of employees.
- Monitoring and auditing.
- Information security practices.
- Incident response plans.
- Plans for responding to detected problems and corrective action.

อ้างอิง เอกสาร พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล สำหรับผู้ตรวจสอบ (PDPA for Auditors)

PDPA Security Checklist

(37) หน้าที่ของผู้ควบคุม (1) มาตรการรักษาความมั่นคงปลอดภัย

ท่านได้กำหนด DPO สำหรับหน่วยงานท่านแล้วหรือไม่

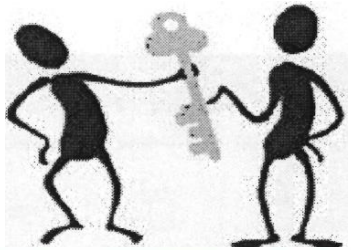
ท่านได้กำหนด R&R (Role & Responsibility) สำหรับ DPO ที่ชัดเจน เป็นลายลักษณ์อักษร หรือไม่ ท่านมั่นใจว่า DPO มีความรู้ ความสามารถ เพียงพอที่จะปฏิบัติตามข้อกำหนด ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่

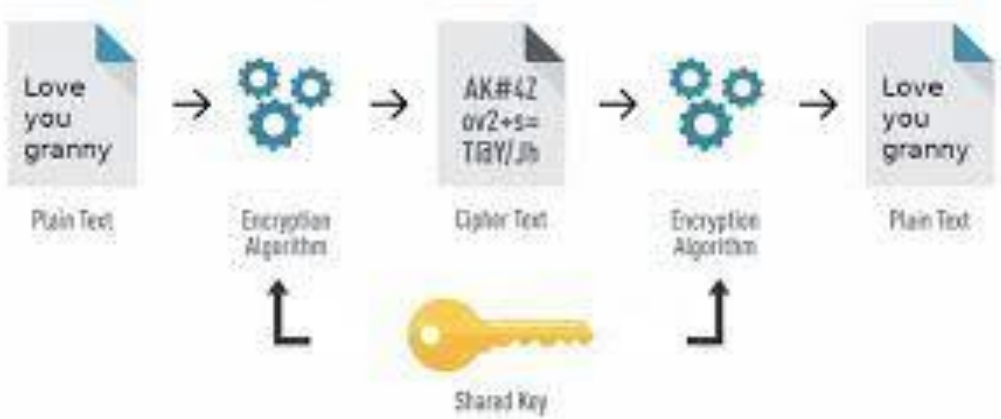
PDPA Security Checklist

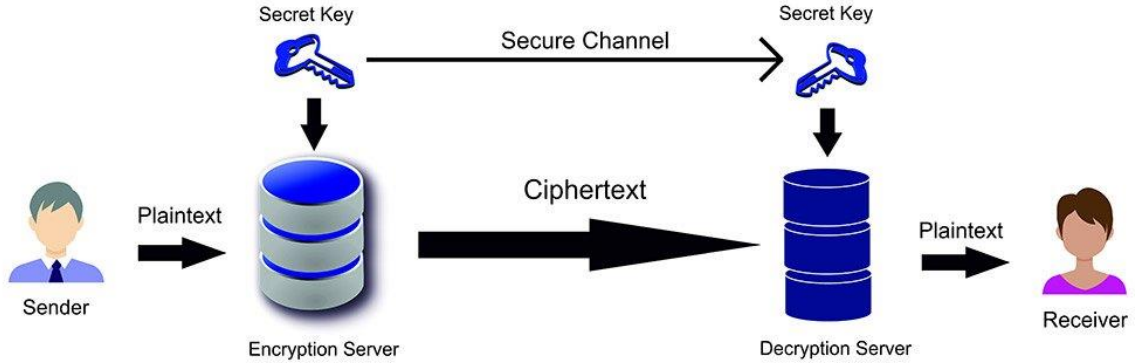
มาตรการในการปกป้องข้อมูลรั่วไหล

- ท่านใดใช้การประทับตรา "ข้อมูลส่วนบุคคล" (Personal data label) ไว้ในเอกสารที่เป็น Hard copy หรือทำ Watermark ไว้ใน File เอกสารที่เป็น Soft file หรือไม่
- ท่านได้ทำการเข้ารหัส หรือ ใส่ Password ข้อมูลส่วนบุคคลตลอดเวลาในการจัดเก็บ และการส่งข้อมูลหรือไม่
- ท่านจำกัดให้พนักงานที่ได้รับอนุญาตเท่านั้นที่สามารถใช้ Thumb drive / External Hard disk มาใช้กับเครื่องคอมพิวเตอร์ขององค์กรหรือไม่
- ท่านมีนโยบาย BYOD (Bring your own device) ในการควบคุมการใช้งานอุปกรณ์ที่เคลื่อนย้ายได้ (Portable computing device) ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่
- ท่านมีนโยบายการใช้เครื่องพิมพ์ที่รัดกุมหรือไม่
- ท่านมีนโยบายการเข้ารหัส (Encryption policy) ที่กำหนดมาตรฐาน / Algorithm สำหรับองค์กรที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่
- ท่านกำหนดให้มีการเข้าและข้อมูลหรือ ใส่รหัสผ่าน ก่อนที่จะเก็บข้อมูลบนคลาวด์หรือไม่
- ท่านใดใช้การเข้ารหัส หรือรหัสผ่านที่แข็งแกร่งสอดคล้องกับระดับความสำคัญของข้อมูลหรือไม่
- ท่านมีนโยบายป้องกันข้อมูลรั่วไหล (Data leak protection) ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่
- ท่านมีนโยบาย Data classification ที่กำหนดระดับความสำคัญของข้อมูลและการควบคุมที่ต้องการในแต่ละระดับข้อมูลที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่

Disk encryption

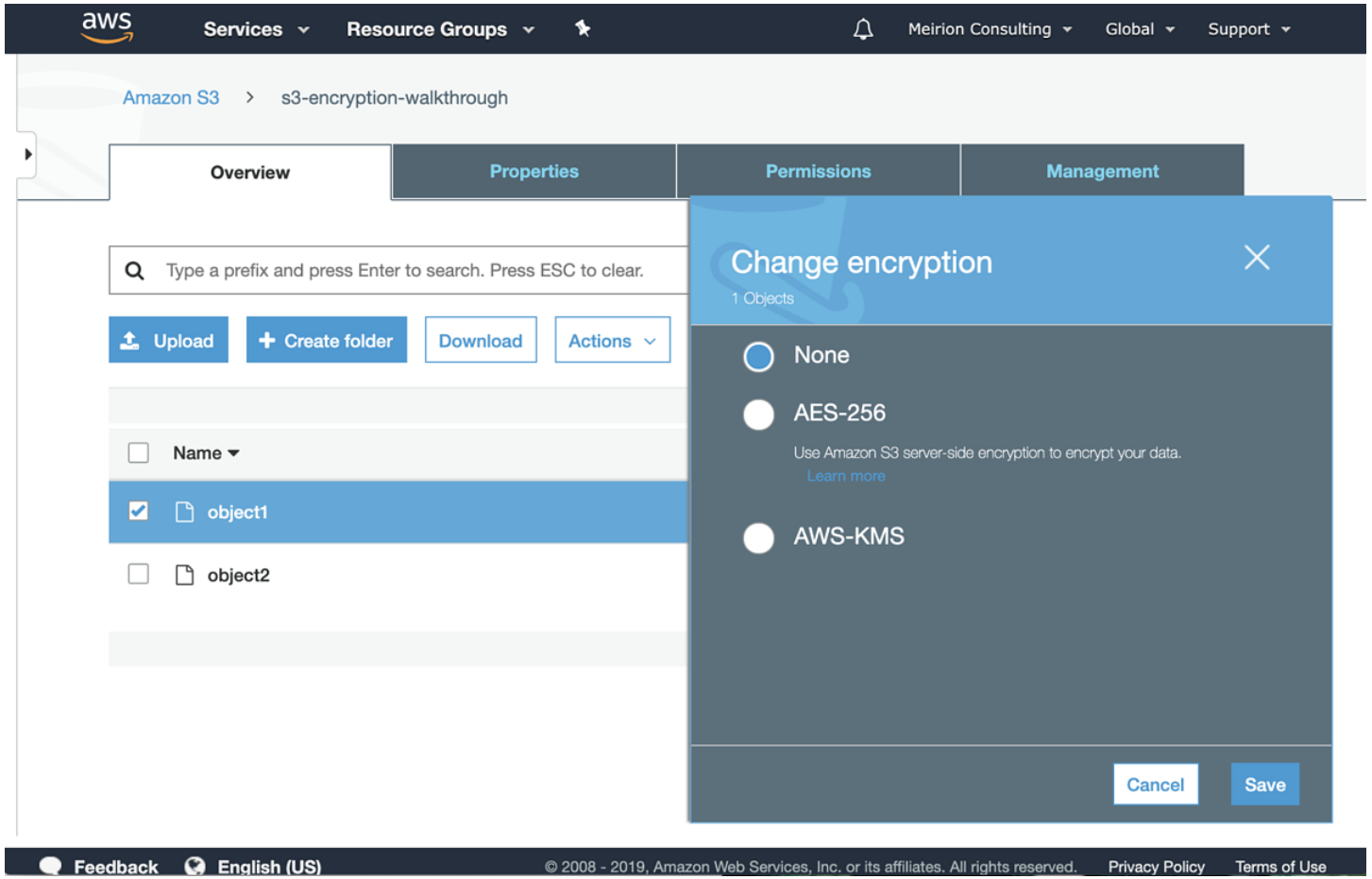




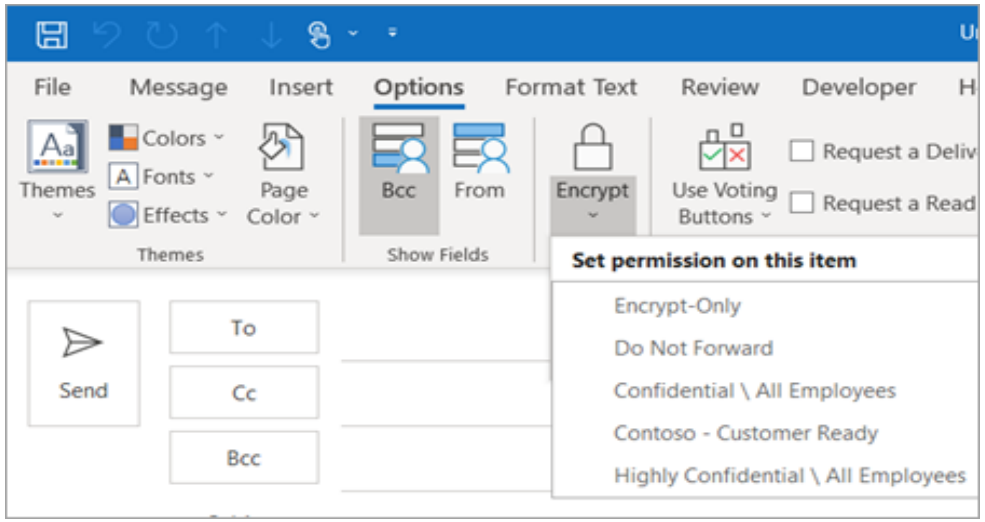


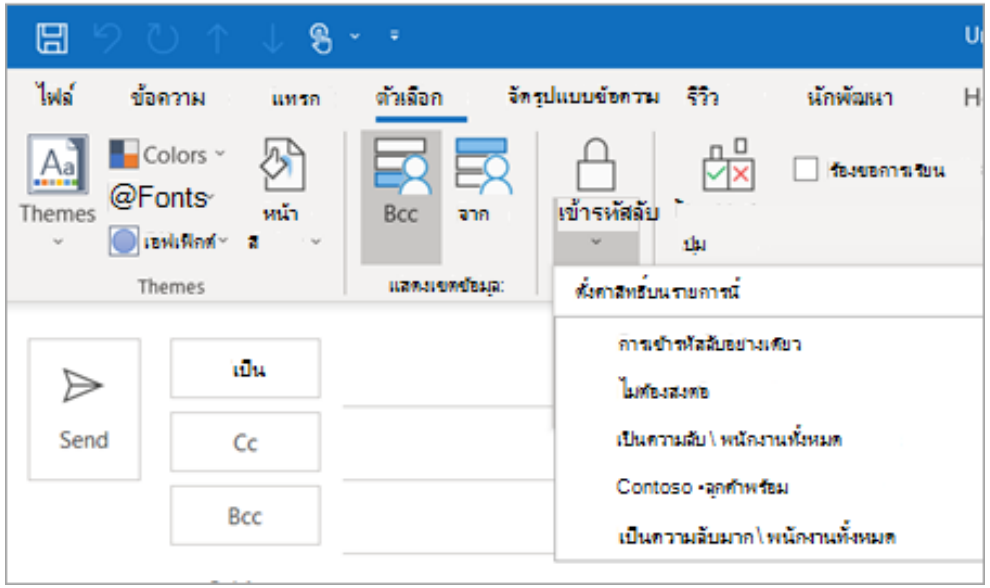
Symmetric Cryptography

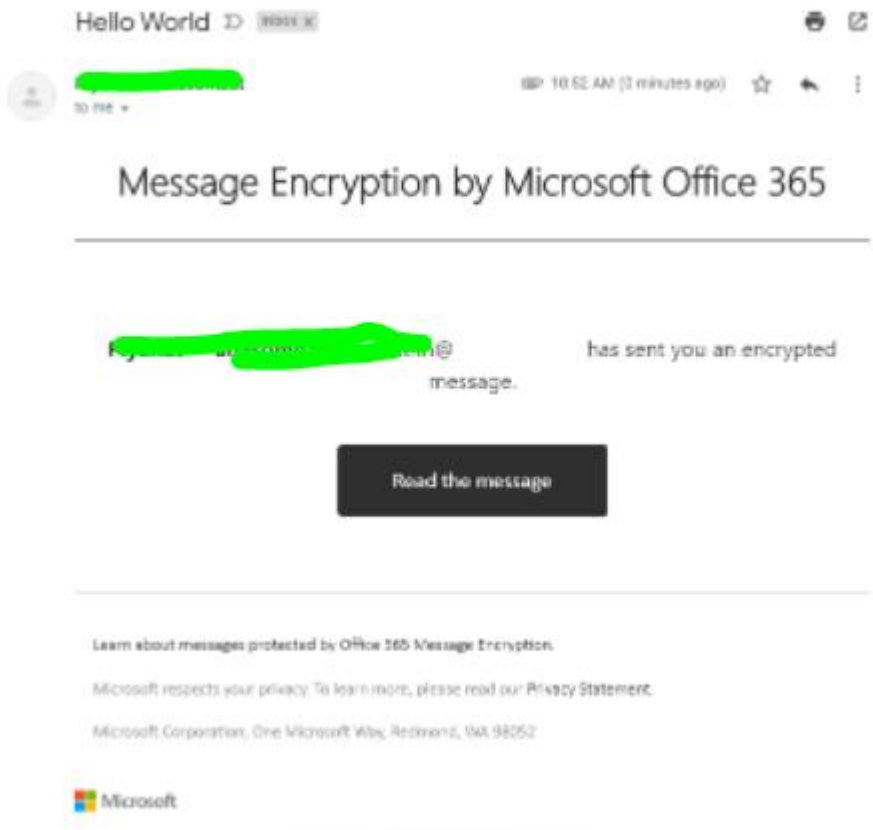
Amazon s3 encryption



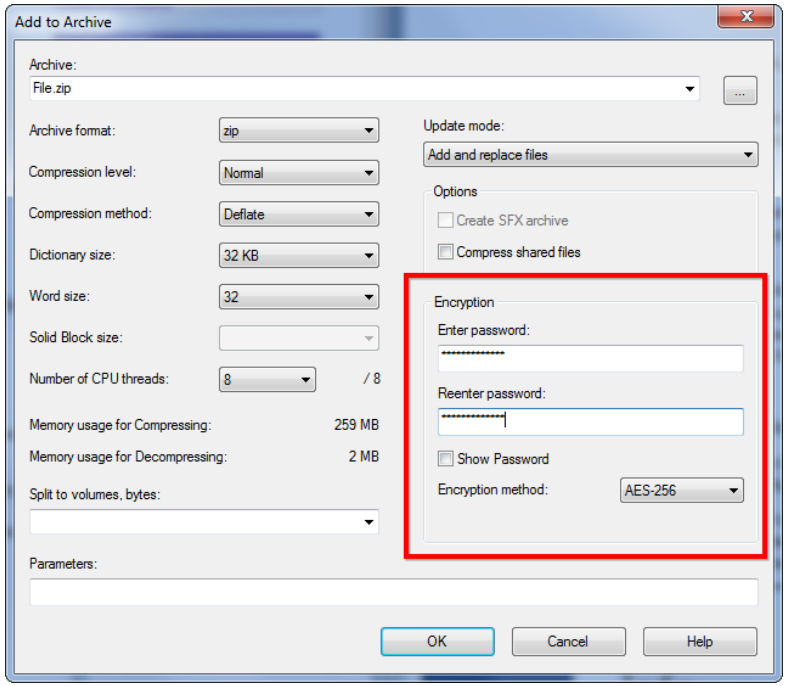
Email encryption



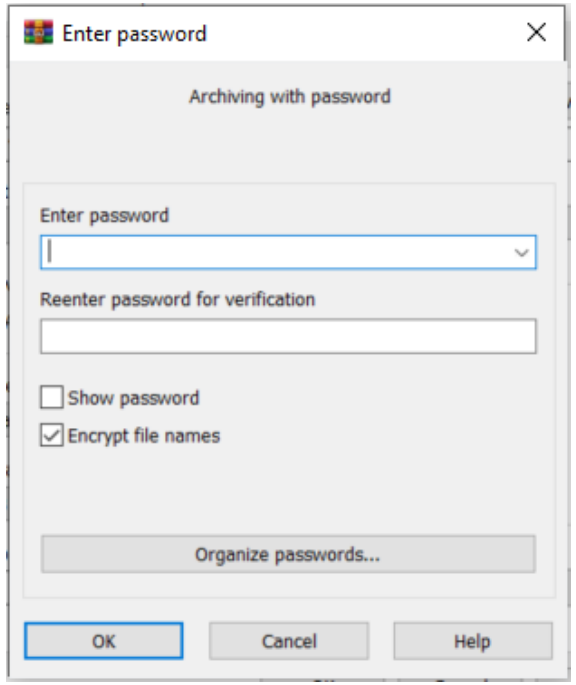




File encryption

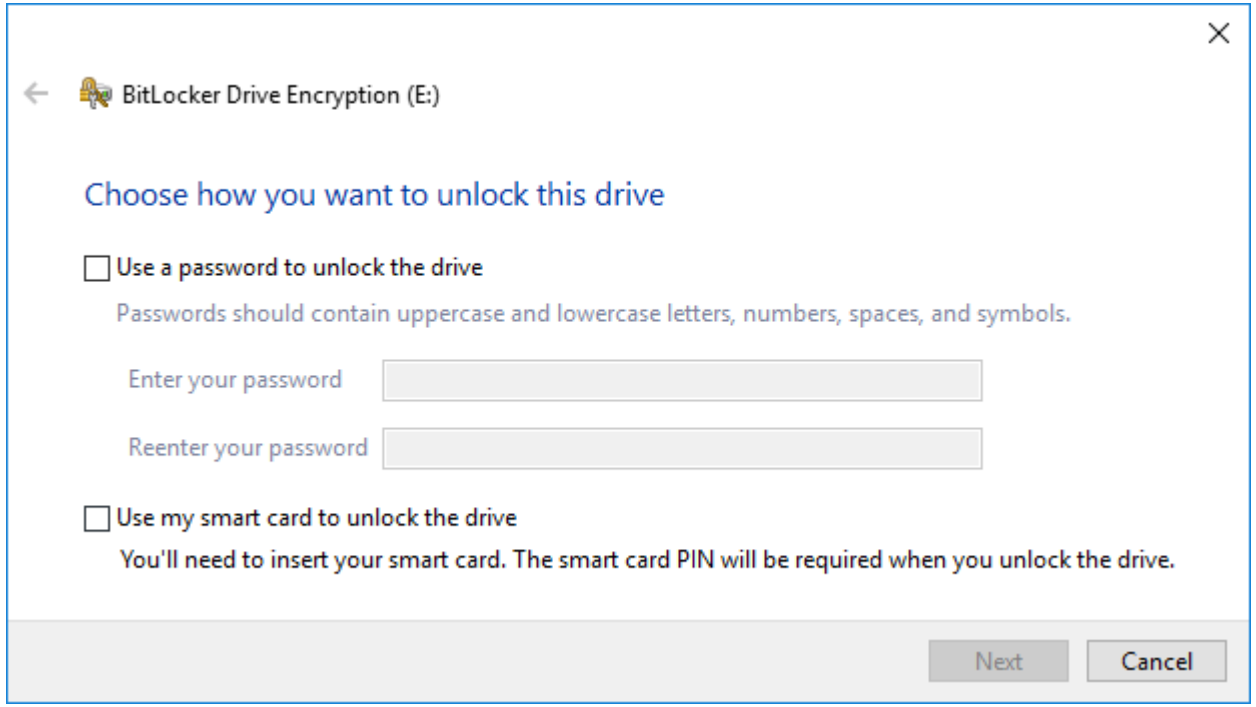


7-Zip



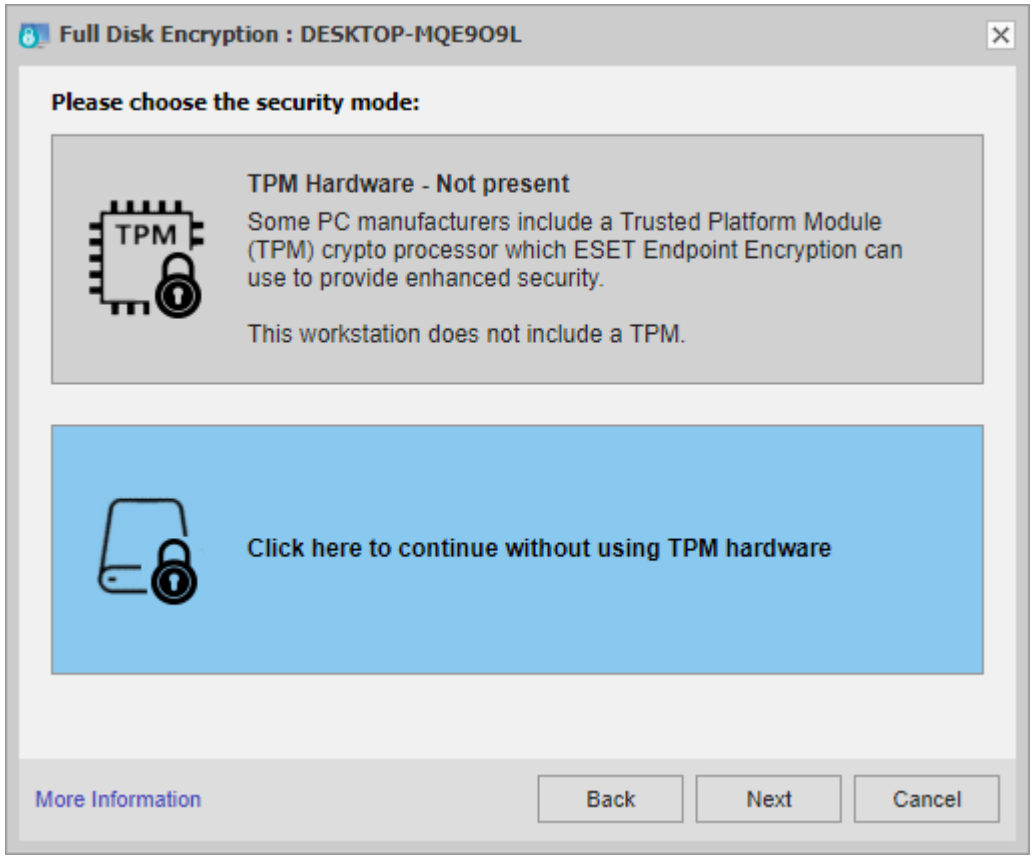
WinRAR

USB encryption



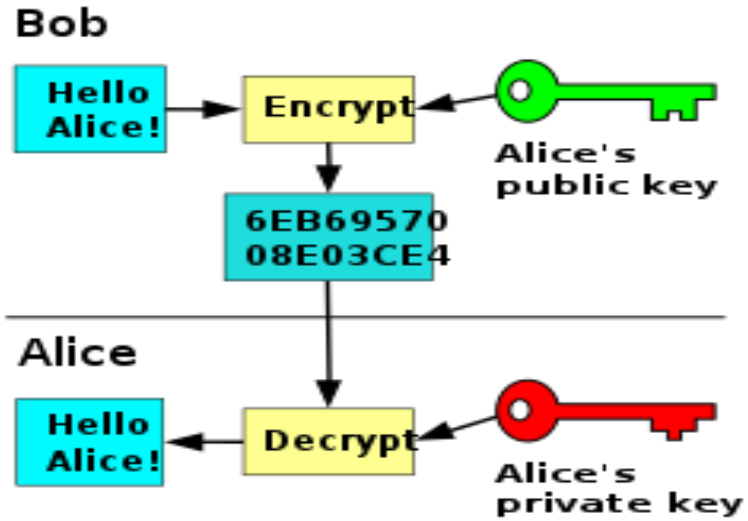
Disk encryption

ESET Endpoint Encryption Server (managed)

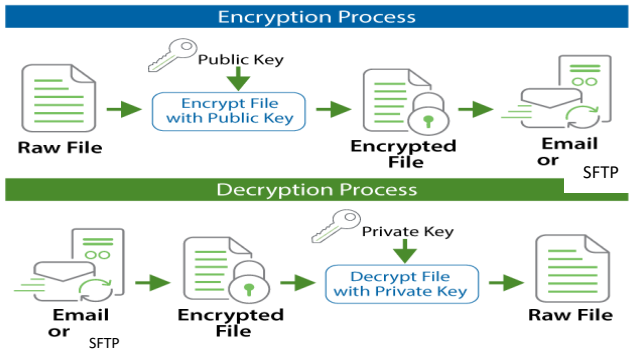


Trend Micro Endpoint Encryption

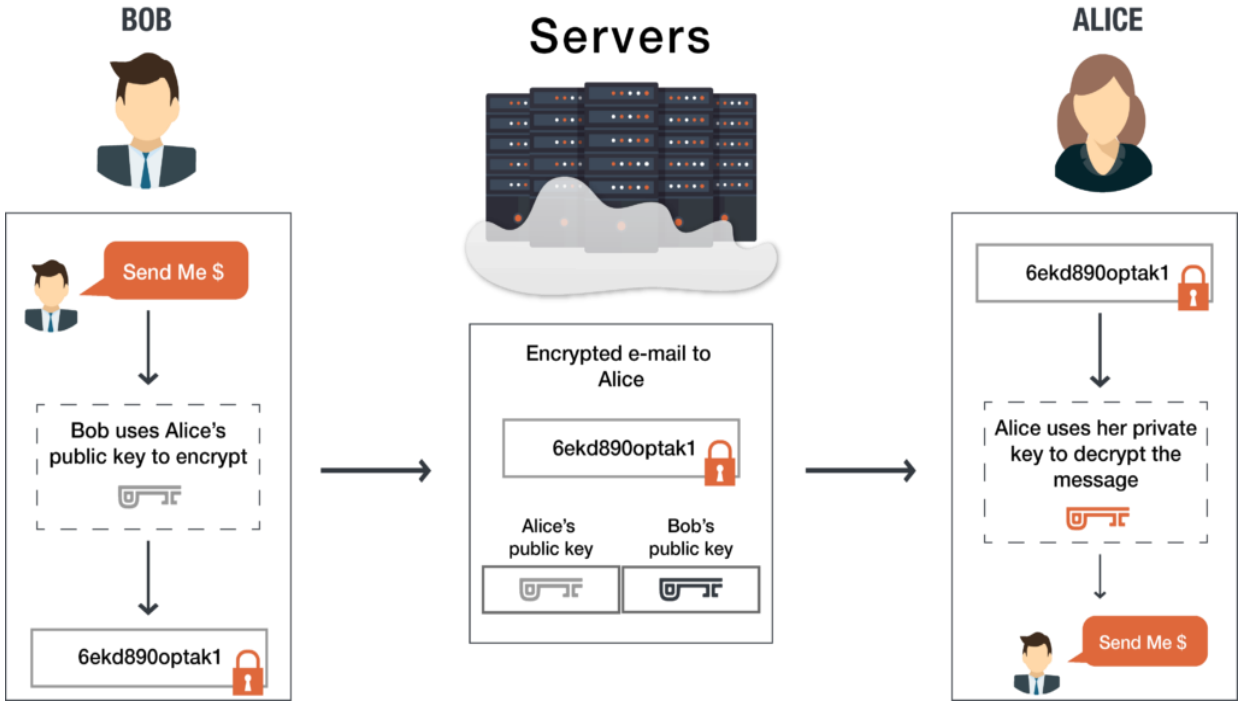
Asymmetric system



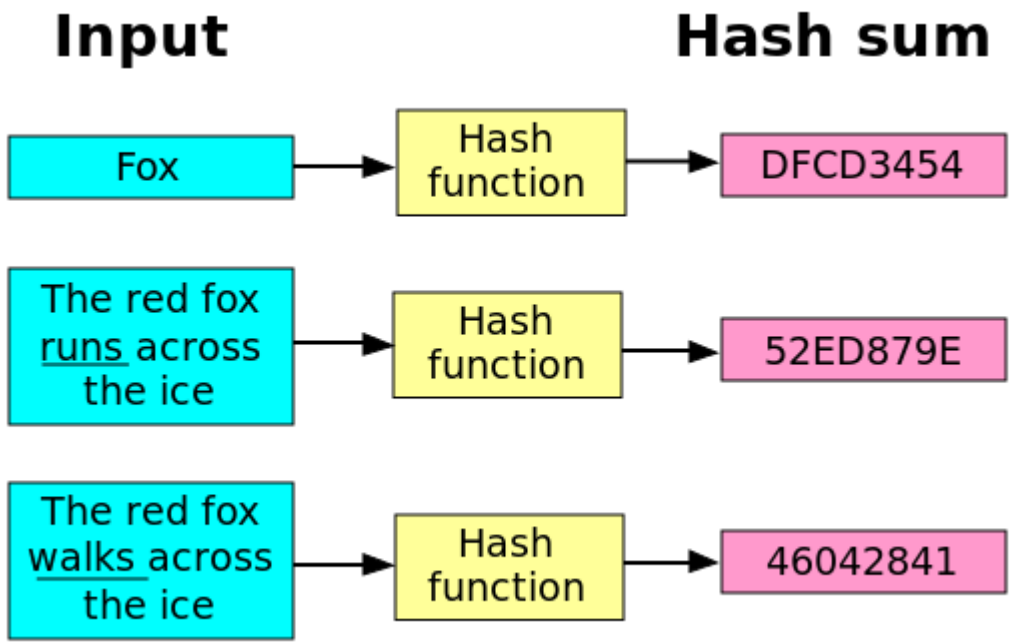
อ้างอิง https://en.wikipedia.org/wiki/Public-key_cryptography

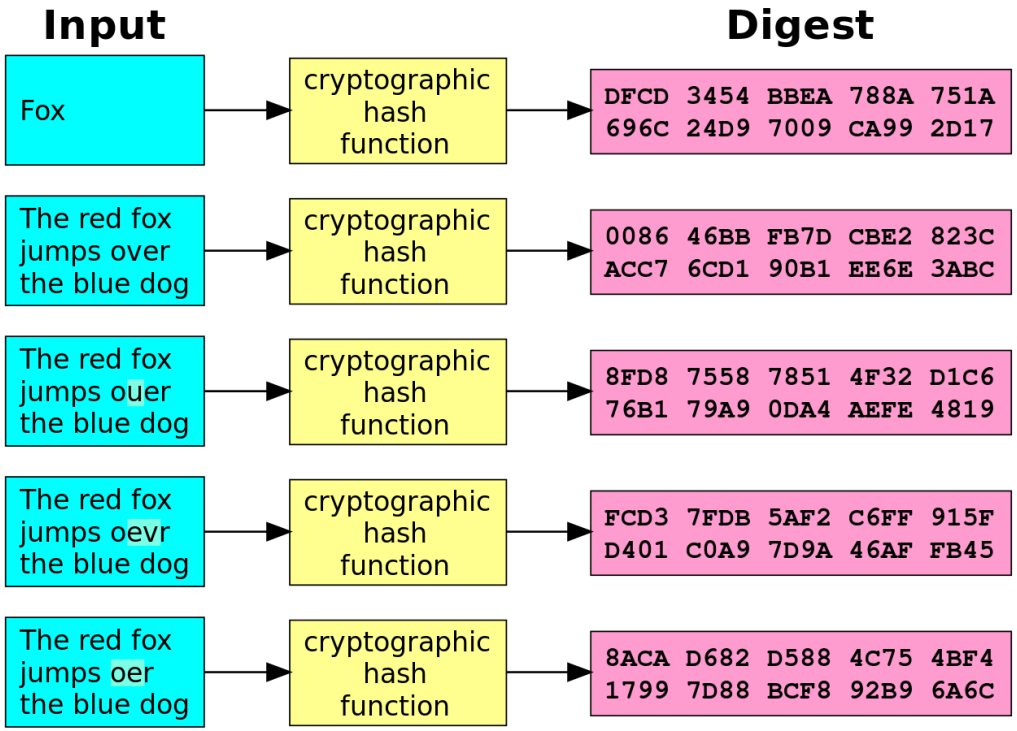


Trend Micro Endpoint Encryption



Hashing





Algorithm	Operation	Status	Alternative
DES	Encryption	Avoid	AES
3DES	Encryption	Legacy	AES
RC4	Encryption	Avoid	AES
MD5	Integrity	Avoid	SHA-256
SHA-1	Integrity	Legacy	SHA-256

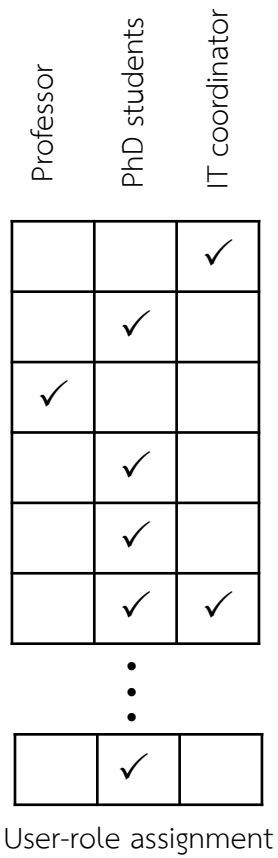
PDPA Security Checklist

มาตรการในการควบคุมการเข้าถึง

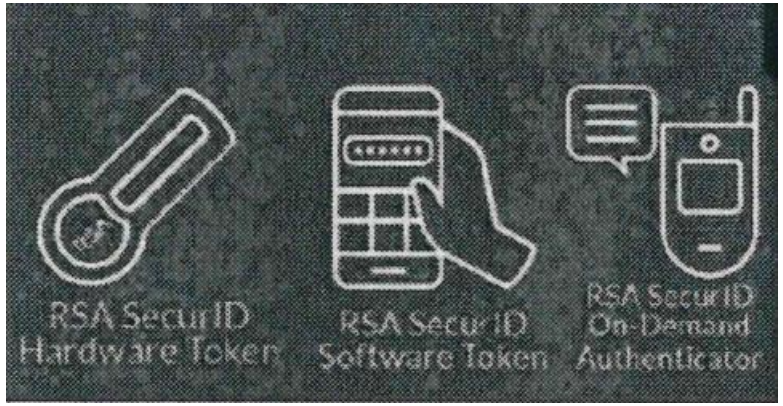
- ท่านมีนโยบาย Password (Password Policy) ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่
- ท่านกำหนดให้ สถานที่จัดเก็บข้อมูลส่วนบุคคล ทั้งเอกสารและ File electronic มีความปลอดภัย อนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงได้เท่านั้น
- ท่านมีนโยบายบริหารจัดการสิทธิ์ (Account management) ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่
- ท่านกำหนดให้ พนักงานที่ลาออก จะถูกลบสิทธิ์ออกจากระบบที่เกี่ยวข้องอย่างทันเวลาหรือไม่
- ท่านให้สิทธิ์การเข้าถึงระบบตามหลักการ Need to know basis หรือไม่
- ท่านไม่อนุญาตให้มีการใช้ User ร่วมกัน (Shared account) หรือไม่
- ท่านให้สิทธิ์การเข้าถึง Shared folder ตามหลักการ Need to know basis หรือไม่
- ท่านได้ใช้งาน Computer screen lockout หรือไม่ หากมีการใช้งานตั้งไว้กี่นาที (Session timeout)

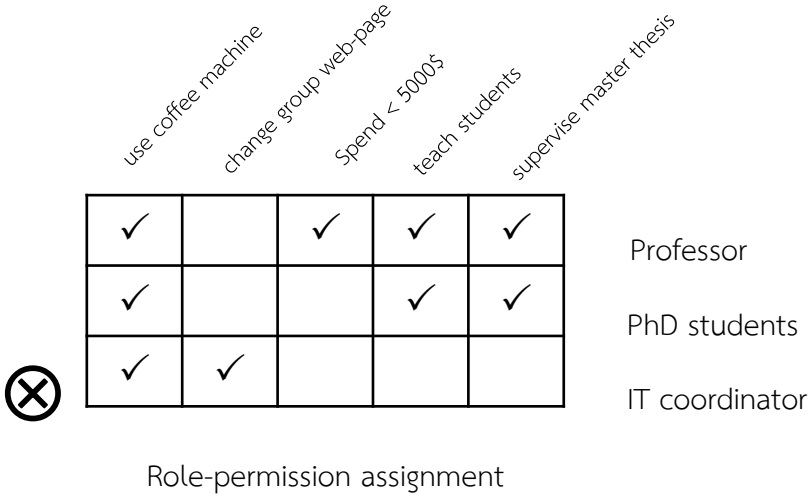
Access control (logical access control)

- AAA
  - Authentication
    - Something you know
    - Something you have
    - Something you are
    - Something you authen
  - Authorization
  - Audit
    - Nonrepudiation



User-role assignment





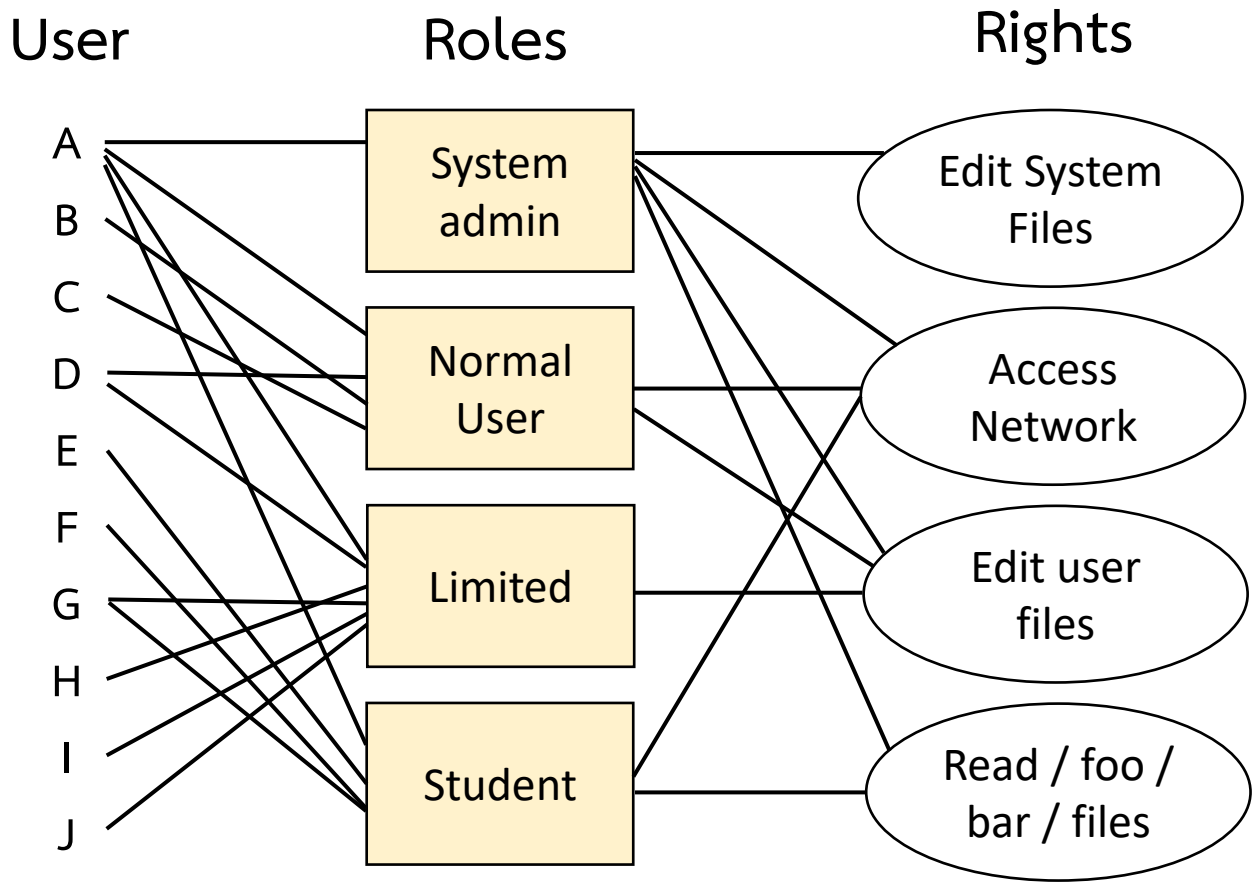
Role-permission assignment

อ้างอิง เอกสาร พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล สำหรับผู้ตรวจสอบ (PDPA for Auditors)

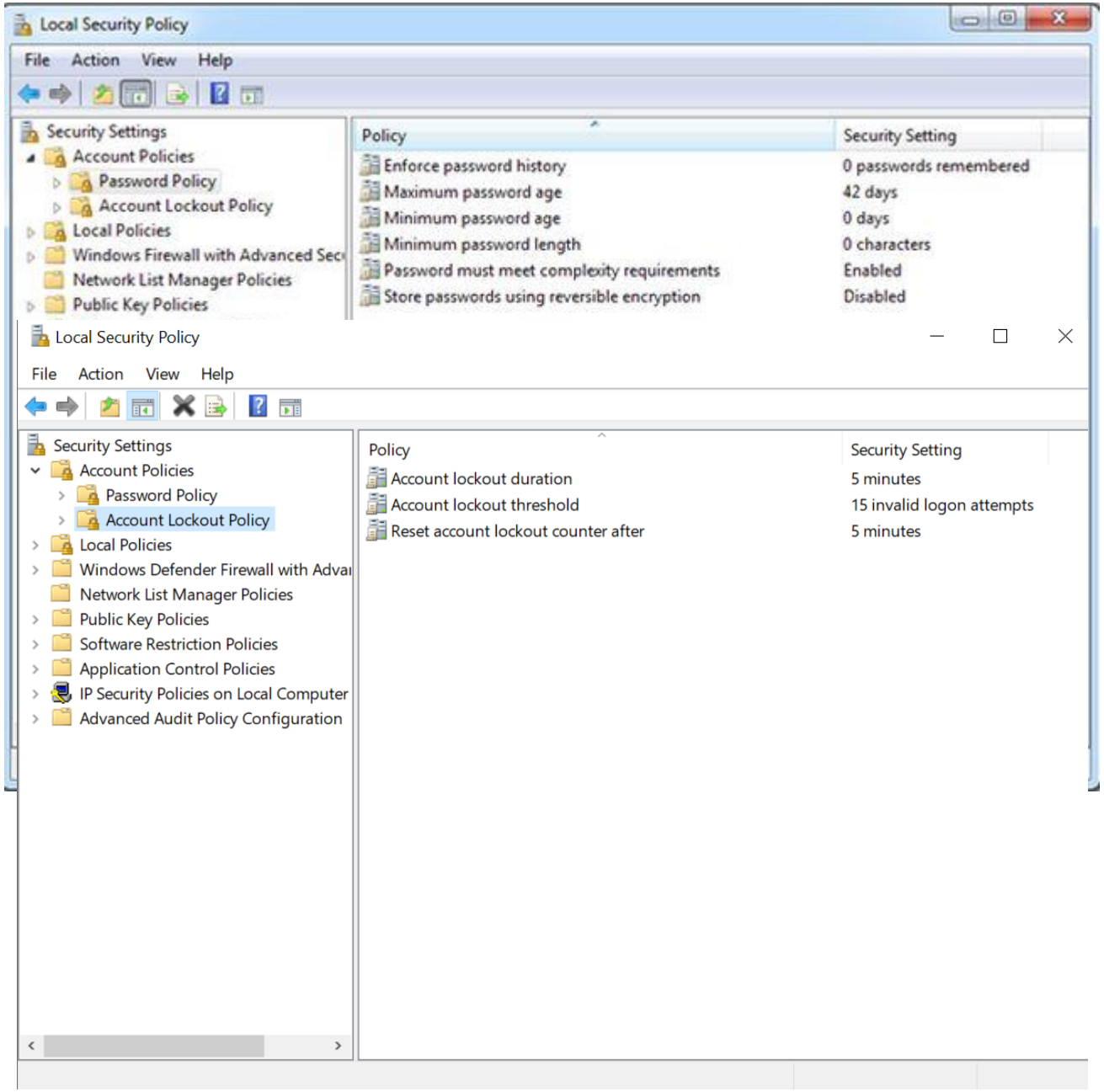
User Management

- พนักงานใหม่ ลาออก ย้ายแผนก
- User review process
- Role base access control

Roles and Permissions Matrix	Role Group 1			Role Group 2		
		Administrator	Manager		Sales	Customer
Activity						
Create new account		X	X			X
Modify account		X	X			X
Create order		X	X		X	X
View reports		X	X		X	
Create reports		X	X		X	

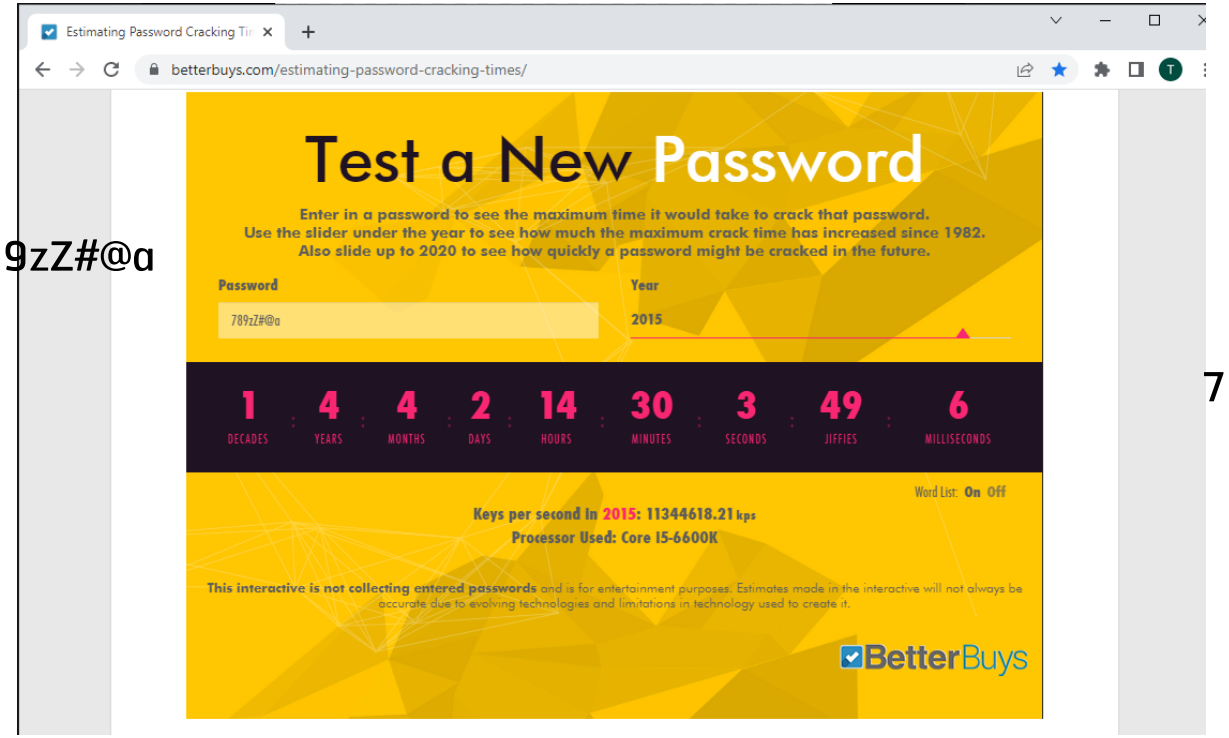


อ้างอิง เอกสาร พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล สำหรับผู้ตรวจสอบ (PDPA for Auditors)



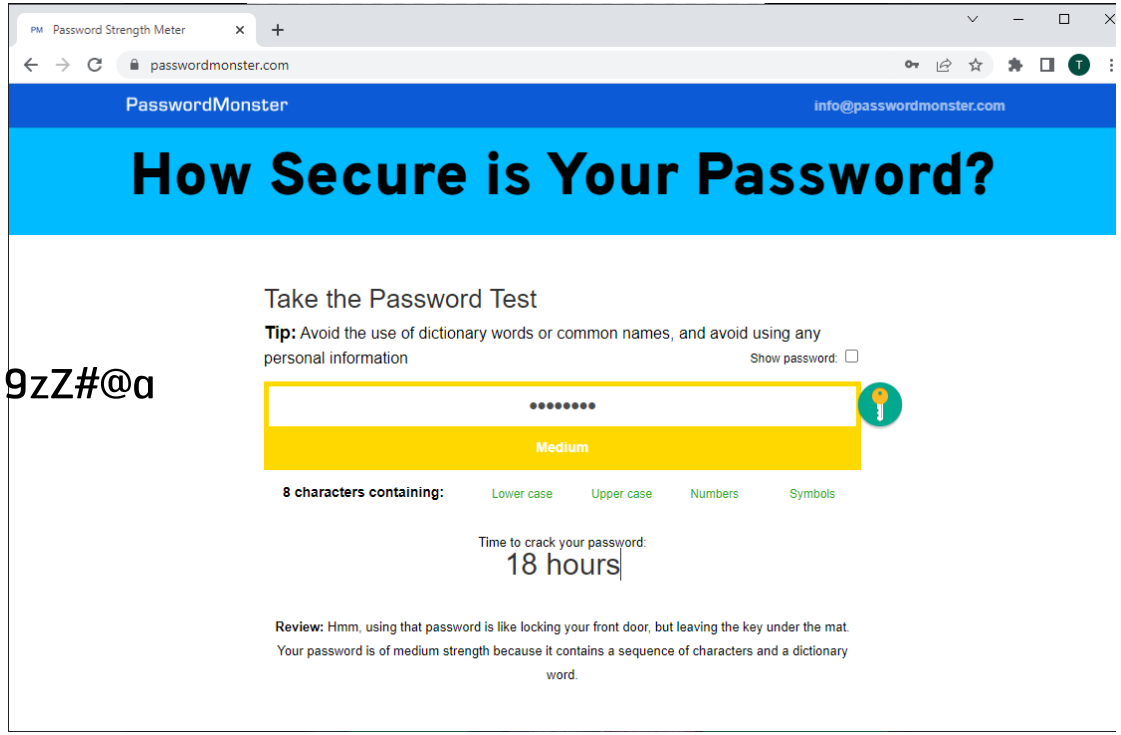
https://www.betterbuys.com/estimating-password-cracking-times/

789zZ#@a



https://www.passwordmonster.com/

789zZ#@a



PDPA Security Checklist

ท่านมีนโยบายการทำลายข้อมูลส่วนบุคคลอย่างปลอดภัย (Data sanitization) ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่

มาตรการในเรื่องความพร้อมใช้

ท่านมีนโยบายการจัดเก็บข้อมูล (Data retention policy) ที่กำหนดระยะเวลาสำหรับการจัดเก็บข้อมูลส่วนบุคคล และการควบคุมที่จำเป็น ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่

ท่านมีนโยบายการสำรองข้อมูล (Backup policy) และการจัดเก็บ และการทดสอบฟื้นฟูข้อมูล (Storage and restoration policy) ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่

PDPA Security Checklist

มาตรการในการสร้างความตระหนัก

- ท่านมีนโยบายอบรมการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ที่ประกาศใช้ทั่วทั้งองค์กร หรือไม่
- ท่านทำการสอบทาน การปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยหน่วยงานท่านเอง หรือ ร่วมมือกับหน่วยงานตรวจสอบภายในอย่างน้อยปีละ 1 ครั้ง หรือไม่
- ท่านมั่นใจว่า เจ้าของข้อมูล/ผู้ควบคุมข้อมูล รับทราบหน้าที่และบทลงโทษ อันเกิดจากการละเมิดของข้อมูลส่วนบุคคล หรือไม่
- ท่านได้ใช้งาน Banner เพื่อย้ำเตือนหน้าที่และความรับผิดชอบ ของ User ก่อนเข้าใช้งานคอมพิวเตอร์หรือไม่
- ท่านมีนโยบาย กฎระเบียบ ที่เกี่ยวข้องกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ที่ครบถ้วนและเป็นปัจจุบัน หรือไม่
- ท่านได้รับการอบรมเรื่อง Data protection policy & practice เพื่อให้ทราบถึงหน้าที่และความรับผิดชอบ ก่อนที่จะเริ่มปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่
- ท่านมีบทลงโทษ ที่ชัดเจนเกี่ยวกับการไม่ปฏิบัติตาม นโยบาย หรือ ระเบียบ ที่เกี่ยวข้องกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่
- ท่านมีหลักฐานการอบรมของมันนักงานทุกคน หรือการยอมรับของพนักงาน ว่าได้รับอบรม หรือ รับทราบหน้าที่ความรับผิดชอบ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือไม่
- ท่านได้รับการย้ำเตือนเรื่องการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เป็นระยะ เช่น ผ่าน email, training, poster

Workflow Privacy Guideline

การเก็บรวบรวมข้อมูลส่วนบุคคล

- การจัดทำและปรับปรุงบันทึกกิจกรรม การประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities)
- การกำหนดวัตถุประสงค์ การประมวลผลข้อมูลส่วนบุคคล
- การกำหนดฐาน การประมวลผลข้อมูลส่วนบุคคล
- การบริหารจัดการความยินยอม
- การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ เกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล
- การประเมินผลกระทบ ด้านการคุ้มครองข้อมูลส่วนบุคคล

การใช้ข้อมูลส่วนบุคคล

- การใช้ข้อมูลส่วนบุคคล
- มาตรการรักษาความมั่นคง ปลอดภัยสารสนเทศ
- การจัดทำข้อตกลง การประมวลผลข้อมูลส่วนบุคคล
- การบริหารจัดการสิทธิ ของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management)
- การรายงานเหตุละเมิด ข้อมูลส่วนบุคคล

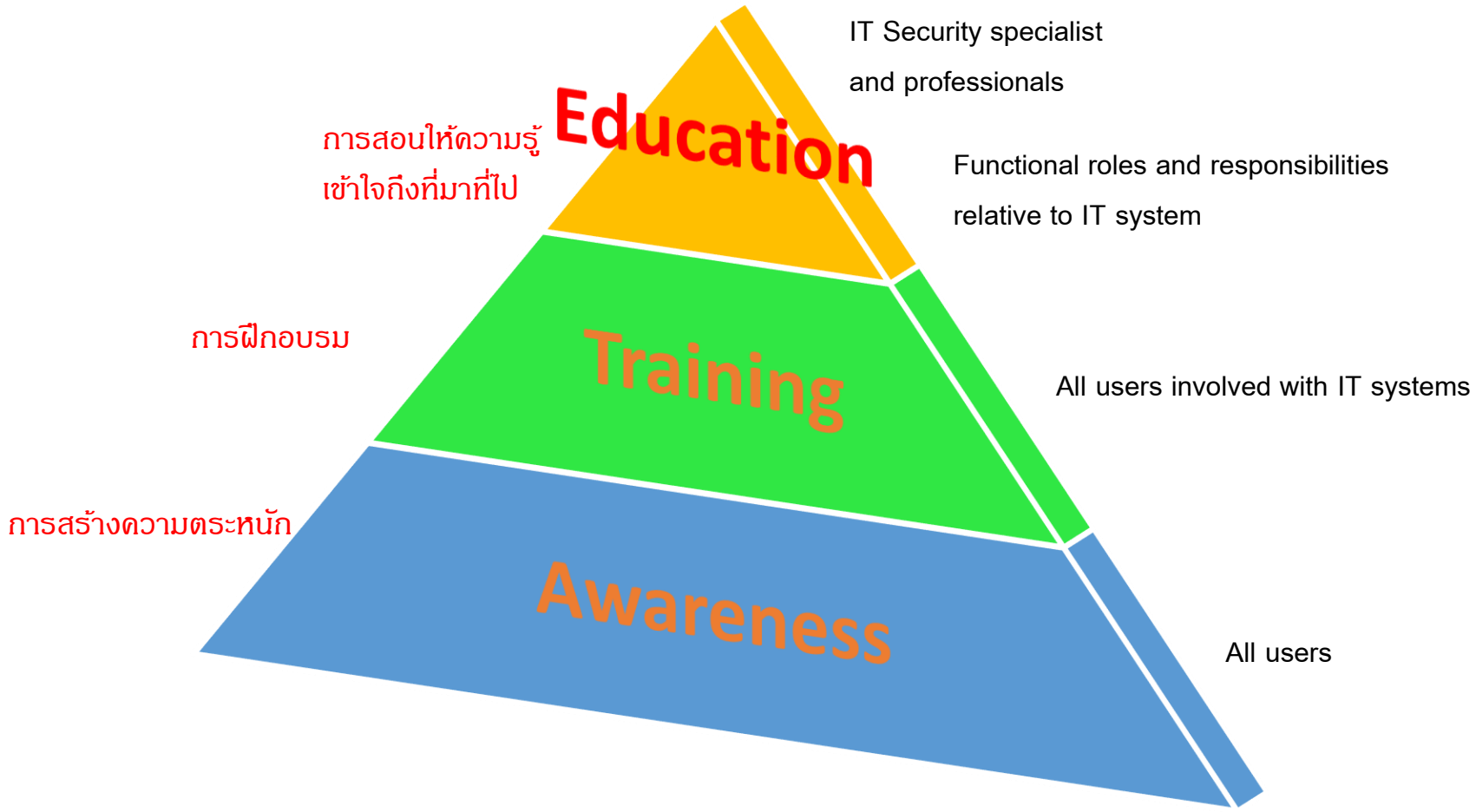
การเผยแพร่ หรือ ส่งต่อข้อมูลส่วนบุคคล

- หลักเกณฑ์การโอนข้อมูลส่วนบุคคล ไปยังต่างประเทศหรือองค์กรระหว่างประเทศ
- การได้รับการยกเว้น ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและ สามารถโอนย้ายข้อมูลไปยังต่างประเทศได้
- ขั้นตอนปฏิบัติสำหรับการจัดส่ง ข้อมูลส่วนบุคคลไปยังต่างประเทศ
- ขั้นตอนปฏิบัติสำหรับการร้องขอ ข้อมูลส่วนบุคคลจากหน่วยงานภายนอก

การเก็บรักษา และ การทำลายข้อมูลส่วนบุคคล

- มาตรการเชิงเทคนิค เพื่อแปลงข้อมูลที่จัดเก็บไว้เป็นข้อมูล อย่างอื่นเพื่อรักษาความปลอดภัยของข้อมูล
- ขั้นตอนปฏิบัติสำหรับการลบ หรือทำลายข้อมูลส่วนบุคคล

ความแตกต่างระหว่าง Education, Training, Awareness



Popular topics from security awareness training programs and Privacy Awareness Course Outline

- เจ้าของข้อมูลส่วนบุคคล Data Subject
- ผู้ควบคุมข้อมูลส่วนบุคคล Data Controller
- ผู้ประมวลผลข้อมูลส่วนบุคคล Data Processor
- หน่วยงานกำกับดูแล (Supervisory Authority)
- ข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลอ่อนไหว (Personal Data, Sensitive Data)
- ข้อมูลแฝง (Pseudonymous Data)

- Responsibilities of Data Controllers and Processors
- Data Protection Officer
- Training
- Security
- Data Protection by Design and Default
- Records of Data Processing Activities
- Data Breach Notification
- Data Transfer to Processors
- International Data Transfer
- Enforcement
- Conclusion

Lawful Processing
Consent
Contract
Legal Compliance
Vital Interests
Public Interests
Legitimate Interests

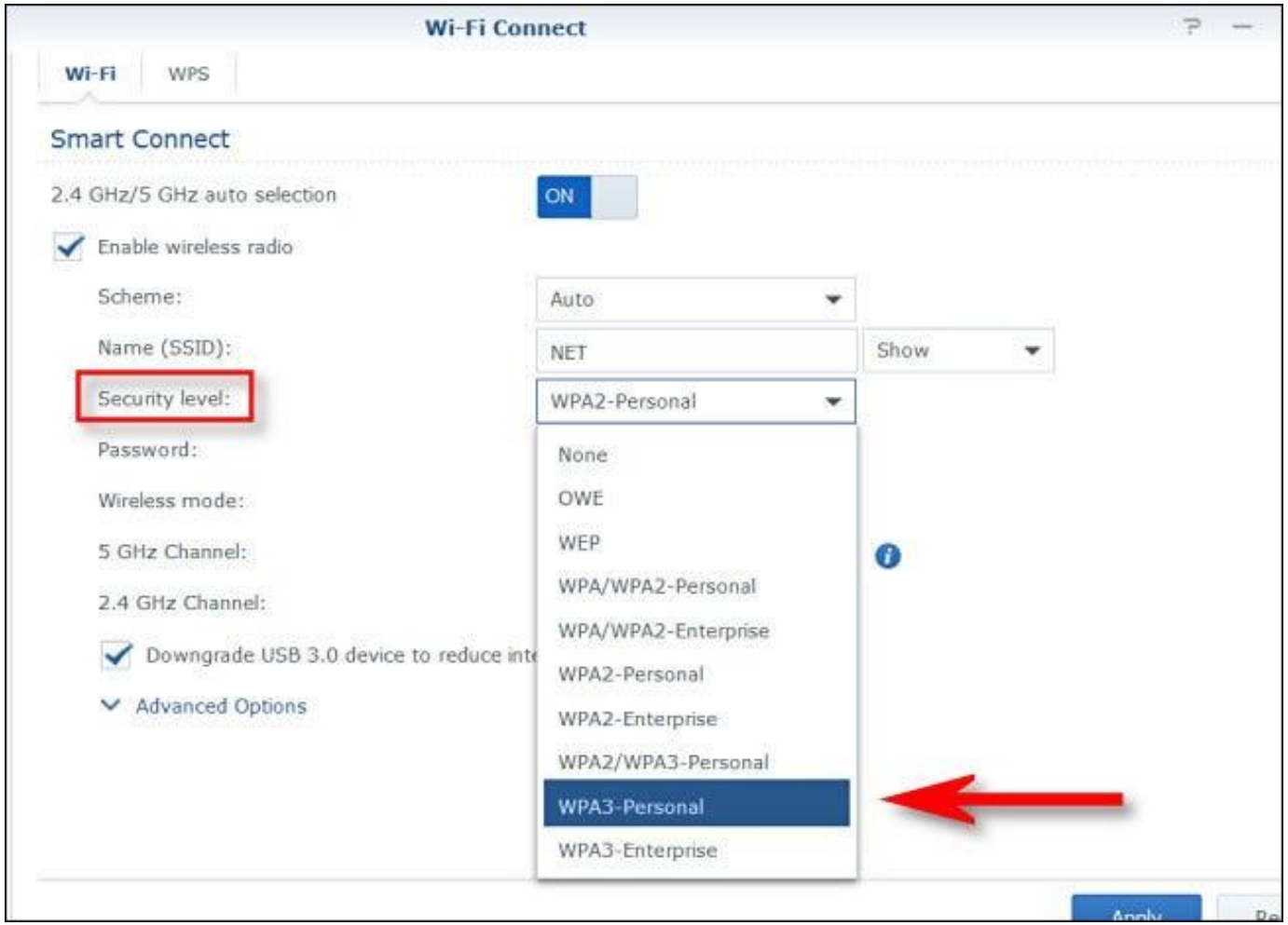
CONSENT
Individual Rights
Right to be informed
Right to Access
Right to Rectification
Right to Erasure
Right to Withdrawn consent
Right to Restriction of Processing
Right to Data Portability
Right to Object

PDPA Security Checklist

มาตรการด้านความปลอดภัยเครือข่ายและระบบงาน

- ท่านมีนโยบายปกป้องภัยคุกคามผ่านเครือข่าย (Firewall, IDS/IPS, Network segmentation) ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่
- ท่านมีนโยบายการควบคุมการเข้าถึงระบบและข้อมูลจากทางไกล (Remote access) ทั้งจากพนักงานและผู้ให้บริการภายนอก ที่ประกาศใช้ทั่วทั้งองค์กรหรือไม่
- ท่านมีการจะทำ Standard software ที่ใช้งานองค์กร และมีการเฝ้าติดตามการใช้งาน Software ที่ไม่เป็นมาตรฐาน หรือไม่
- ท่านได้ยกเลิกการใช้งาน Software/Protocol ที่เก่าล้าสมัย ซึ่งมีความเสี่ยงที่จะถูกดักจับข้อมูลหรือไม่ เช่น FTP, TELNET, SSH, Https
- ท่านได้ติดตั้ง Patch ระบบงาน/ระบบปฏิบัติการที่สำคัญอย่างทันเวลาตามนโยบายการจัดการช่องโหว่ของระบบหรือไม่
- ท่านได้ติดตั้งโปรแกรม Antivirus บนเครื่องคอมพิวเตอร์ของพนักงาน Mobile device และติดตาม Update signature ให้เป็นปัจจุบันหรือไม่
- ท่านได้ยกเลิกการใช้ระบบปฏิบัติการที่ล่าสมัย แช่น Windows XP, Windows ME, Windows Vista หรือไม่
- ท่านอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตทำการติดตั้ง หรือแก้ไขโปรแกรมระบบปฏิบัติการ หรือไม่

The Best Wi-Fi Encryption is WPA3



https://www.howtogeek.com/782993/whats-the-best-wi-fi-encryption-to-use-in-2022/

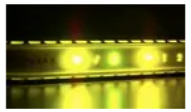
The Best Wi-Fi Encryption is WPA3

As of February 2022, the best Wi-Fi security standard is called Wi-Fi Protected Access Version 3, or WPA3 for short. Introduced in 2018 by the Wi-Fi Alliance, there are several variations of the WPA3 standard:

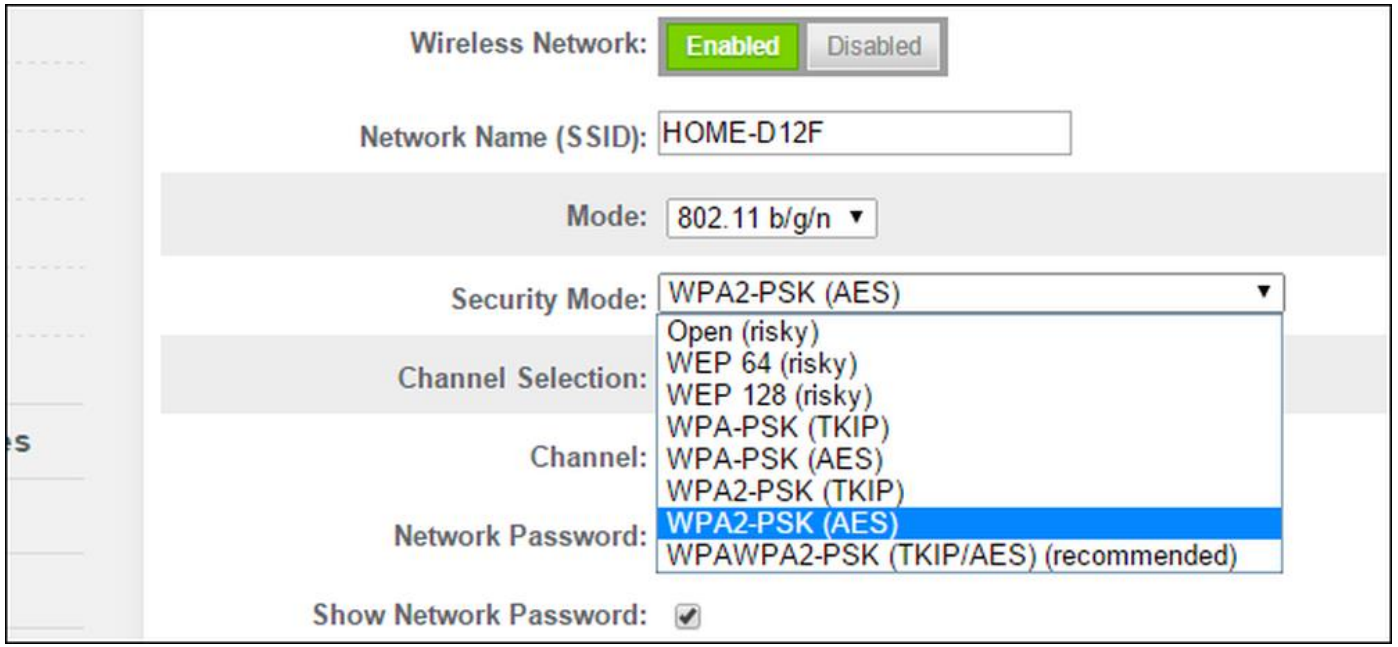
- **WPA3-Personal:** This is designed for individual and home Wi-Fi users. For ease-of-use, it allows you to pick your own arbitrary password, including one that might not be optimally secure.
- **WPA3-Enterprise:** This standard enforces minimum 128-bit authentication encryption, 256-bit key derivation encryption, and the use of an authentication server instead of a password. It also utilizes Protected Management Frames for greater hack protection, and imposes other authentication requirements to secure the network.
- **WPA3-Enterprise with 192-bit Mode:** This is similar to WPA3-Enterprise but with the option for minimum 192-bit encryption instead of 128-bit. It also ups the authentication encryption to 256-bit and the key encryption to 384-bit.

For home Wi-Fi users, the best choice is WPA3-Personal, since it won't require a deep knowledge of wireless security to configure properly. If you're running a business or organization with high data security needs, consult IT experts that can help you set up WPA3-Enterprise wherever possible.

The Wi-Fi Alliance also promotes a standard called "Wi-Fi Enhanced Open" that seamlessly applies a low-level of encryption (called OWE) to open Wi-Fi access spots (those that don't require a password). However, OWE has already been compromised by researchers. Even if it had not been compromised, we do not recommend running an open Wi-Fi access point.



RELATED
Why You Shouldn't Host an Open Wi-Fi Network Without a Password



Main features of WEP, WPA and WPA-2

	WEP	WPA	WPA-2
Authentication	N/A	IEEE 802.1X/EAP/PSK	IEEE 802.1X/EAP/PSK
Cryptographic algorithm	RC4	RC4	AES
Key size	40 or 104 bits	128 bits	128 bits
Encryption method	WEP	TKIP	CCMP
Data integrity	CRC32	MIC	CCM
Keys for packets	No	Yes	Yes
IV length	24 bits	48 bits	48 bits

PDPA Security Checklist

ท่านมีนโยบายการใช้บริการจากผู้ให้บริการภายนอก (IT outsourcing policy) ที่ครอบคลุมถึงการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ที่ประกาศใช้ทั่วทั้งองค์กรก่อนหรือไม่

มาตรการควบคุมการใช้บริการจากผู้ให้บริการภายนอก

ท่านได้ทราบอย่างดีว่า การใช้บริการจากผู้ให้บริการภายนอก ไม่ทำให้องค์กรปราศจากการรับผิด กรณีเกิดข้อมูลรั่วไหลจากผู้ให้บริการภายนอก

ท่านมีมาตรการที่เหมาะสมในการติดตาม หรือได้รับความเชื่อมั่นในการปฏิบัติตาม SOP ของผู้ให้บริการภายนอก

Logs

Access Logs

Filters

Time	Auth User	Source IP	HTTP Method	Request URL Path
Aug 24, 2017, 3:21:25 PM	-	10.157.128.146	GET	/jcsadmin/api/v1.1/webui/metrics
Aug 24, 2017, 3:27:35 PM	-	10.157.128.146	GET	/jcsadmin/api/v1.1/library/
Aug 24, 2017, 3:31:17 PM	-	10.157.128.146	GET	/jcsadmin/api/v1.1/library/
Aug 24, 2017, 3:31:26 PM	-	10.157.128.146	GET	/jcsadmin/api/v1.1/webui/metrics
Aug 24, 2017, 3:31:26 PM	-	10.157.128.146	GET	/jcsadmin/api/v1.1/application/
Aug 24, 2017, 3:33:43 PM	-	10.157.128.146	G	
Aug 24, 2017, 3:33:55 PM	-	10.157.128.146	G	
Aug 24, 2017, 3:34:03 PM	-	10.157.128.146	G	
Aug 24, 2017, 3:34:08 PM	-	10.157.128.146	G	
Aug 24, 2017, 3:34:08 PM	-	10.157.128.146	G	

Page 1 of 10 (1-10 of 100 items) 1 2 3 4 5

Importance of transaction log in SQL Server

Results | Messages

	Current LSN	Operation	Transaction Name	Transaction ID	UserAccount
1	00000032:0000032b:0001	LOP_BEGIN_XACT	DROPOBJ	0000:0000187f	HQNT\CCOV648
2	0000006b:00003639:0001	LOP_BEGIN_XACT	DROPOBJ	0000:000870d0	HQNT\CCOV648
3	0000006b:00003639:0004	LOP_BEGIN_XACT	DROPOBJ	0000:000870d1	HQNT\CCOV648
4	0000006b:00005485:0001	LOP_BEGIN_XACT	DROPOBJ	0000:000871f5	HQNT\CCOV648
5	0000006b:0000548f:0001	LOP_BEGIN_XACT	DROPOBJ	0000:000871f6	HQNT\CCOV648
6	0000006b:00005496:0001	LOP_BEGIN_XACT	DROPOBJ	0000:000871f7	HQNT\CCOV648
7	0000006b:0000549c:0001	LOP_BEGIN_XACT	DROPOBJ	0000:000871f8	HQNT\CCOV648
8	0000006b:00005505:0001	LOP_BEGIN_XACT	DROPOBJ	0000:000871fa	HQNT\CCOV648

Current LSN	Operation	Transaction Name	Transaction ID	Log Record Fixed Length	Transaction SID	SPID	Begin Time
00000274:000015b0:0002	LOP_HK	NULL	0000:00000000	28	152	NULL	NULL
00000274:000015b1:0001	LOP_BEGIN_CKPT	NULL	0000:00000000	96	96	NULL	NULL
00000274:000015b2:0001	LOP_XACT_CKPT	NULL	0000:00000000	24	28	NULL	NULL
00000274:000015b3:0001	LOP_END_CKPT	NULL	0000:00000000	136	136	NULL	NULL
00000274:000015b4:0001	LOP_HK	NULL	0000:00000000	28	88	NULL	NULL
00000274:000015b4:0002	LOP_HK	NULL	0000:00000000	28	152	NULL	NULL
00000274:000015b5:0001	LOP_BEGIN_XACT	QDS nested transaction	0000:007952a8	76	128	48	2018/08/10 11:02:29:77(
00000274:000015b5:0002	LOP_BEGIN_XACT	QDS base transaction	0000:007952a9	76	124	48	2018/08/10 11:02:29:77(

วงจรชีวิตข้อมูลส่วนบุคคล+Security Measures

1 Data Collection
(Lawful basis, Notice requirement purpose limitation, data minimization)

- ระบบ PDPA (Consent, Privacy Notice, ROPA)
- Data Discovery

2 Data Storage
(รูปแบบการจัดเก็บ แหล่งที่จัดเก็บ)

- DB Encryption
- Endpoint Encryption
- DLP
- Network and Infrastructure Security

3 Data Use Access to Personal Data
(ภายในองค์กร: ใครบ้าง ที่ใช้และเข้าถึงข้อมูล)

- AAA: Authorization, Authentication, Accountability
- MFA
- Data Masking
- AD Policy, Data Sharing Storage Policy
- User Management
- Application Security: Role based access control, Secure Logon, Log, VA, Pen-test, Malware Protection
- SIEM

4 Data Disclosure
(องค์กรภายนอกที่มีการเปิดเผยข้อมูล)

- Secure File Transfer
- Encrypted Protocol; HTTPS
- E-mail Encryption
- DLP

5 Data Transfer
(Rules for international transfer)
(มีการโอนข้อมูลฯไปต่างประเทศหรือไม่ รูปแบบ, วิธีการโอน)

- Secure File Transfer
- Encrypted Protocol
- E-mail Encryption
- DLP

6 Data Archival
(มีการสำรองข้อมูลไว้ที่ไหนหรือไม่)

- Data backup and archival Tool
- Test and Restoration

7 Data Disposal
(การลบและทำลายข้อมูล)

- Media Sanitization Tool
- Anonymization Technique

- Physical Security
- Clear Desk Clear Screen Policy
- Information classification Procedure, DLP
- NDA, AUP

Physical/Electronic | (Handling of Data Subject Request/Response of Request) | Retention Period

ระบบ PDPA; DSR

Automatic Deletion Tool

(มีการสำรองข้อมูลไว้ที่ไหนหรือไม่)

Incident Response Process Flow

หมายเหตุ เป็นการวิเคราะห์ส่วนบุคคล เวลานำไปใช้ต้องวิเคราะห์และประเมินความเสี่ยงของแต่ละองค์กร ขึ้นอยู่กับความเสี่ยงและความจำเป็นในการปกป้องข้อมูลขององค์กร

Ensure Security Measures

คำแนะนำเบื้องต้นสำหรับการประเมินมาตรการด้านความมั่นคงปลอดภัย

1. ทำ Gap Analysis ก่อน โดยนำ Checklist ที่ได้นำเสนอไว้ไปประเมินเพื่อให้ทราบจุดอ่อนจุดแข็งของตนเอง
2. ประเมิน DPIA, Risk Assessment + Prioritize ข้อมูลที่ต้องปกป้องมากสุดและรองลงมา + Budget + Risk Option
3. วางแผนการดำเนินงานเพื่อปิด Gap ตามลำดับความสำคัญ ถ้าท่านเป็นหน่วยงานที่มีการจัดเก็บข้อมูลส่วนบุคคลเป็นจำนวนมาก ควรหาเครื่องมือเข้ามาช่วยสนับสนุนกระบวนการ PDPA ก่อน และอันไหนที่เป็น Organizational Measures เช่น การกำกับกระบวนการ นโยบาย ขั้นตอนปฏิบัติควรเริ่มดำเนินการก่อนเลย
4. ดำเนินการตามแผนที่กำหนด
5. ให้ DPO เข้ามาตรวจสอบเพื่อเช็คว่าได้ปฏิบัติและมีความสอดคล้องกับกฎหมายหรือไม่

Ensure Security Measures

PDPA ตรวจสอบความพร้อม 11 หลักการ 7 ขั้นตอน เตรียมองค์กรทำตามกรอบ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

หลักการ 11 ประการ
นำทางองค์กรปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ข้อกำหนดตามกฎหมาย

1 แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

2 จัดทำประกาศความเป็นส่วนตัว (Privacy Notice)

3 จัดทำบันทึกรายการประมวลผล (Record of Processing Activities: ROPA)

4 จัดทำเอกสารขอความยินยอมในกรณีที่มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคล (Consent Form)

5. จัดทำข้อตกลงการประมวลผล (Data Processing Agreement) ในกรณีที่มีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล

แนวปฏิบัติที่ดี (Best Practices)

1 จัดตั้งคณะทำงาน PDPA ภายในหน่วยงาน (PDPA Working Team)

2 สำรวจข้อมูลภายในหน่วยงานและจัดทำผังวงจรชีวิตข้อมูลส่วนบุคคล (Data Inventory)

3 จัดทำนโยบายและแนวปฏิบัติของหน่วยงาน (Privacy Policy and Codes of Practice)

4 จัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement) ในกรณีที่มีการแลกเปลี่ยนและแบ่งปันข้อมูลระหว่างองค์กร

5 สร้างความตระหนักรู้และฝึกอบรม (Capacity Building and Awareness Raising)

6 กำกับดูแลและตรวจสอบอย่างสม่ำเสมอ (Audit and Compliance)

7 ขั้นตอนภาคปฏิบัติ
"รู้-ทำ นำสู่ความสำเร็จ"

1 การจัดทำแผนผังข้อมูลส่วนบุคคล (Data Flow)

2 การกำหนดหน้าที่ของบุคคลและฐานกฎหมายที่ใช้

3 การจัดทำเอกสารสำคัญตามที่กฎหมายกำหนด

4 การบริหารจัดการข้อมูล ตลอดวงจรชีวิตของข้อมูล

5 การปรับระบบไอทีให้รองรับ

6 การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล(DPO)

7 การสร้างความตระหนักรู้

อ้างอิงจากนายกำพล ศรธนะรัตน์ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officer (DPO) และที่ปรึกษาด้าน Digital Transformation สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และประธานชมรม DPO
https://www.jrit-ichi.com/cutting/2022/04/20/1050/

บริษัท ที-เน็ต จำกัด
121 หมู่ 9 อาคาร Garden of Innovation ห้องเลขที่ 1-11 อุทยานวิทยาศาสตร์ประเทศไทย
ถนนพหลโยธิน คลองหนึ่ง คลองหลวง ปทุมธานี 12120
โทรศัพท์: 0818663297
e-mail: doungkamol@tnetsecurity.com