แนวปฏิบัติในการใช้เทคโนโลยีสารสนเทศในสถานพยาบาล

9 กันยายน 2565

วิทยากร

ทรงพล เพียเพ็งต้น
เจ้าพนักงานสาธารณสุขอาวุโส

จิระเดช ช่างสาย
นักวิชาคอมพิวเตอร์ปฏิบัติการ

สำนักงานสาธารณสุขจังหวัดสระแก้ว

- Security & Privacy
- แนวปฏิบัติด้าน Security ของระบบ
- แนวปฏิบัติด้าน Privacy ของข้อมูล
- PDPA พรบ.คุ้มครองข้อมูลส่วนบุคคล

ความหมายของ Security และ Privacy

- **Security** : หมายถึง การปกป้องข้อมูลของผู้ใช้
- **Privacy** : หมายถึง อำนาจในการควบคุมข้อมูลส่วนตัวของผู้ใช้ และข้อมูลส่วนตัวจะถูกนำไปทำอะไรได้บ้าง ในโลกออนไลน์ ข้อมูลส่วนตัวจะหมายถึงข้อมูลใด ๆ ก็ตามที่สามารถใช้ระบุตัวตนของผู้ใช้งานได้

แหล่งที่มาของการโจมตี

- Hackers
- Viruses & Malware
- ระบบที่มีปัญหาข้อผิดพลาด/ช่องโหว่
- Insiders (บุคลากรที่มีเจตนาร้าย)
- การขาดความตระหนักของบุคลากร
- ภัยพิบัติ

ผลกระทบ/ความเสียหาย

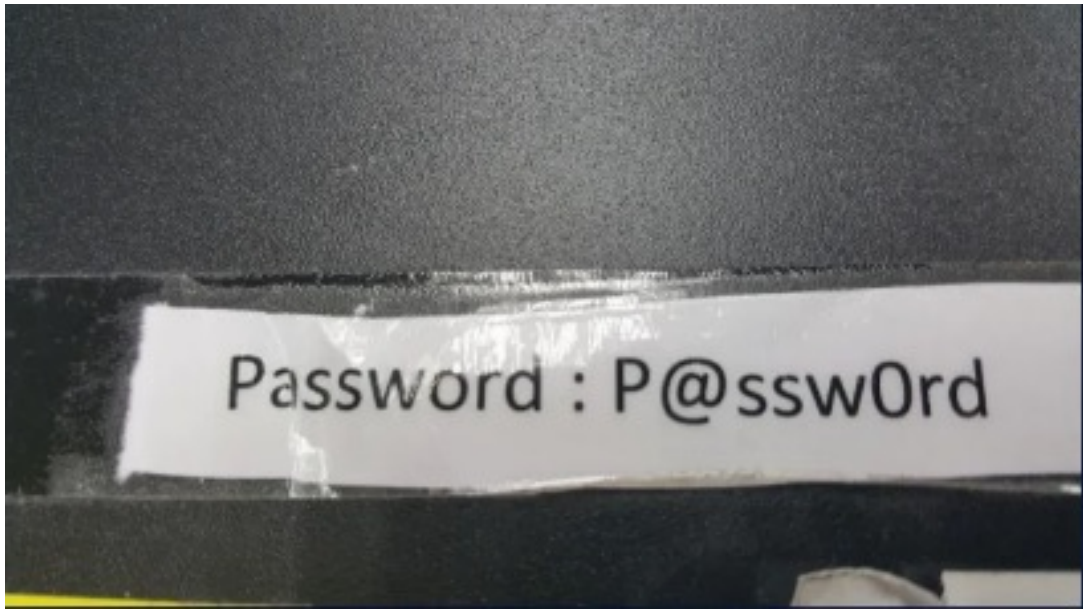
- ความลับถูกเปิดเผย
- ความเสี่ยงต่อชีวิต สุขภาพ จิตใจ การเงิน และการงานของบุคคล
- ระบบล่ม การให้บริการมีปัญหา
- ภาพลักษณ์ขององค์กรเสียหาย

แนวปฏิบัติด้าน Security ของระบบสารสนเทศ

Password

- ความยาว 8 ตัวอักษรขึ้นไป
- ความซับซ้อน: 3 ใน 4 กลุ่มตัวอักษร
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Symbols
- ไม่มีความหมาย (ป้องกัน "Dictionary Attacks")
- ไม่ใช่ simple patterns (12345678, 11111111)
- ไม่เกี่ยวกับข้อมูลส่วนตัวที่คนสนิทอาจรู้ (เช่น วันเกิด ชื่อคนในครอบครัว ชื่อสัตว์เลี้ยง)

Password


Password : P@ssw0rd


SER CONTROLLED AREA
VISITORS
LEASE PRESS BELL
FOR ADMITTANCE

แล้วจะจำ Password ได้ยังไง?

- คิดประโยคภาษาอังกฤษสัก 1 ประโยค
- ประโยคนี้ควรมีคำ 8 คำขึ้นไป และควรมีตัวเลข
- หรือสัญลักษณ์พิเศษด้วย
- ใช้ตัวอักษรตัวแรกของแต่ละคำ เป็น Password
- หรือพิมพ์เป็นคำภาษาไทยด้วยแป้นพิมพ์ภาษาอังกฤษ

- ประโยค:

I love reading all 7 Harry Potter books!

- Password: Ilra7HPb!
- Password: อากาศโคตรดี -> vkdkLF89ifu

Password

- อย่าแชร์ Password กับคนอื่น
- เปลี่ยน Password ทุกๆ 6 เดือน

Logout After Use

- อย่าลืม Logout หลังใช้งานเสมอ โดยเฉพาะเครื่องสาธารณะ (หากไม่อยู่หน้าจอ แม้เพียงชั่วครู่ ให้ Lock Screen เสมอ)
- หรือเพียงแค่ตั้งเวลา Logout โดยอัตโนมัติ

Mobile Security

- ตั้ง PIN สำหรับ Lock Screen เอาไว้
- ไม่เก็บข้อมูลสำคัญเอาไว้
- ระวังไม่ให้สูญหาย หากสูญหายรีบแจ้งระงับ

แค่มือถือหาย อาจจะร้ายกว่าที่คิด!

- เมื่อมือถือสูญหายหรือถูกขโมยข้อมูลที่ไม่อยากเปิดเผย หรือข้อมูลองค์กรที่เก็บไว้ในโทรศัพท์อาจจะหลุดออกไป และมีความเสี่ยงที่ข้อมูลไม่สามารถกู้คืนได้
- ถูกนำข้อมูลไปเผยแพร่ เพื่อข่มขู่ เรียกค่าไถ่
- ถูกสะกดรอยการใช้งานจากบริการต่าง ๆ
- ถูกแอบอ้างสวมรอยใช้งานเพื่อกระทำความผิด

คำแนะนำในการใช้มือถือ

- ต้องรู้ก่อนว่าเราเก็บข้อมูล หรือมีโปรแกรมอะไรในมือถือบ้างเพื่อป้องกันข้อมูลอื่น ๆ ของเราที่เชื่อมกับอุปกรณ์อื่น เพื่อหยุดการเชื่อมต่อกับมือถือได้ เช่น ข้อมูลการเงินผ่านการใช้แอปของธนาคาร หรือโปรแกรมกล้องวงจรปิดที่เชื่อมต่อกับมือถือ
- ตั้งรหัสล็อกหน้าจอมือถือ และใส่พาสเวิร์ดในการเข้าโปรแกรมต่าง ๆ ในมือถือ เช่น Line ที่สามารถตั้งค่าก่อนเข้าใช้งานได้ เหมือนใส่ล็อก 2 ชั้น
- เมื่อใช้งานโปรแกรม หรือแอปแล้ว ควร Logout เสมอ
- ไม่บันทึกข้อมูล Username และพาสเวิร์ด ไว้ในมือถือ
- ข้อมูลสำคัญ ๆ หรือข้อมูลส่วนตัว เมื่อใช้งานเสร็จแล้วควรลบทิ้ง

เมื่อมือถือหายให้ตั้งสติ และดำเนินการตามขั้นตอน ดังนี้

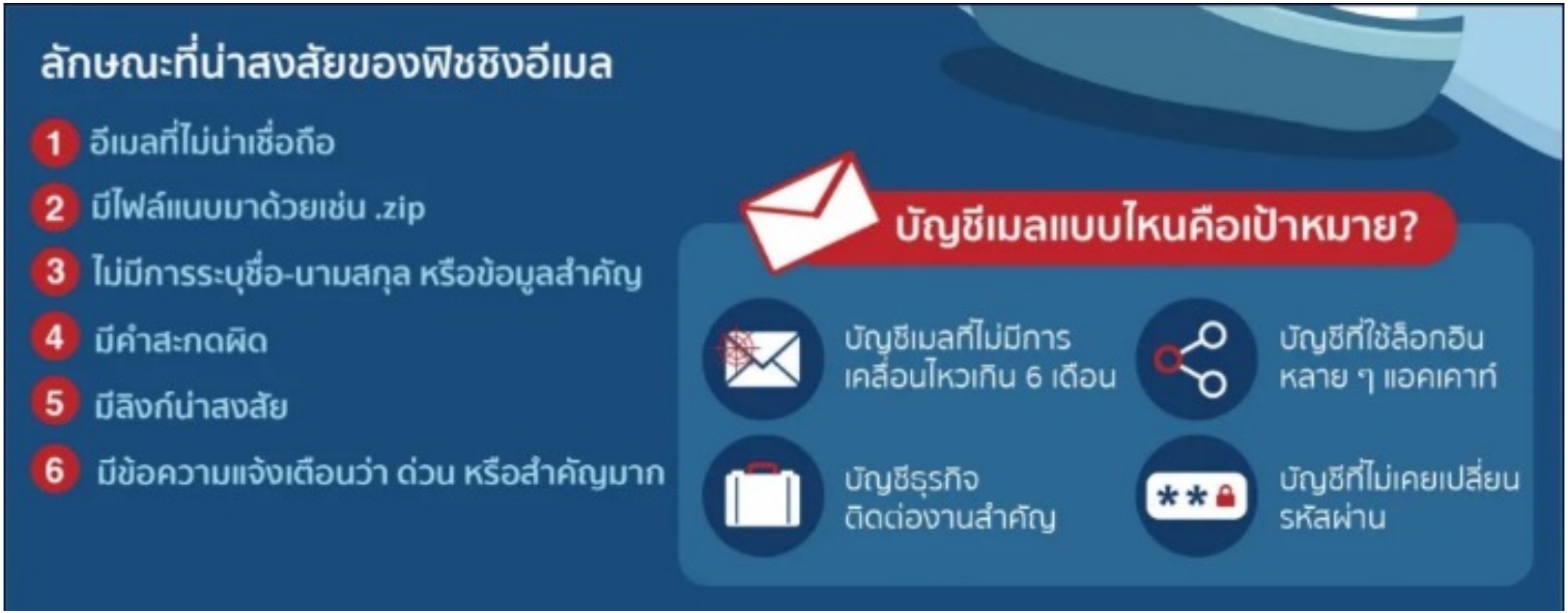
- แจ้งผู้ให้บริการแอปพลิเคชัน เพื่อระงับการให้บริการ เช่น e-Banking
- เปลี่ยน Username และพาสเวิร์ดในการเข้าใช้บริการต่าง ๆ ที่มีในมือถือ
- แจ้งความกับตำรวจเพื่อหาตัวผู้ร้าย และเพื่อเป็นหลักฐานกรณีผู้ร้ายอาจนำมือถือกระทำความผิดต่อภายหลัง
- เข้าโปรแกรมของมือถือ เช่น Find My iPhone หรือ Find My Device เพื่อค้นหา บล็อกการเข้าถึง หรือลบข้อมูลในมือถือจากระยะไกล

อีเมลถือเป็นทรัพย์สินสำคัญที่ต้องมีมาตรการรักษาความมั่นคงปลอดภัย

เพราะถ้าถูกผู้ไม่หวังดีเข้าถึงหรือยึดอีเมลได้ ก็จะใช้แอบอ้างเพื่อทำธุรกรรมต่าง ๆ แทนเรา สร้างความเสียหายทั้งเงินและชื่อเสียงอีกด้วย ดังนั้น เราควร

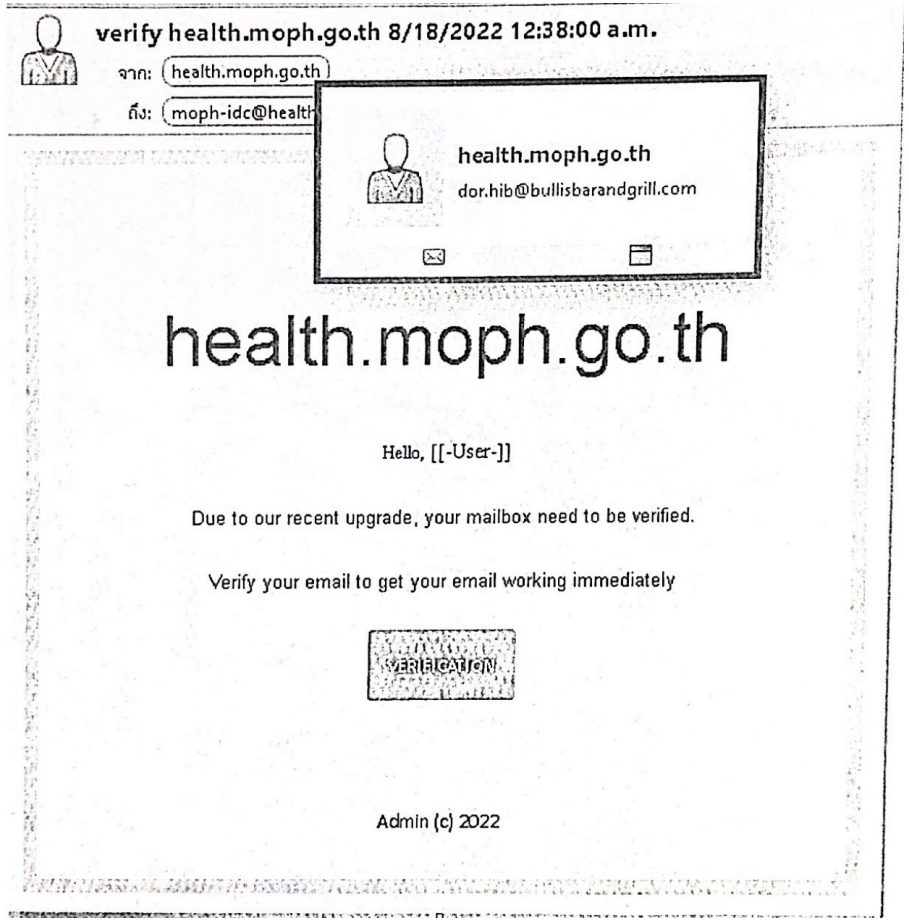
1. ตั้งพาสเวิร์ด ที่ไม่ซ้ำ ไม่ง่าย และไม่บอกใคร
2. ตั้งคำหรือปรับปรุงข้อมูลระตัวตนให้ทันสมัย และตรงกับความเป็นจริง เช่น อีเมลสำรองสำหรับกู้คืนบัญชี
3. ตรวจสอบประวัติการใช้งานที่น่าสงสัย รวมถึงช่องทางในการนนตัวตนอย่างสม่ำเสมอ
4. ติดตั้งโปรแกรมแอนด์โวรัส อัปเดตระบบปฏิบัติการ เบราว์เซอร์
5. ไม่ติดตั้งโปรแกรมจากแหล่งที่ไม่รู้จัก ไม่ใช้โปรแกรมเถื่อน
6. ระมัดระวังอิเมลที่มีไฟล์แนน หรือลิงก์ที่พาไปเว็บไซด์อื่น
7. ยืนยันการเปลี่ยนเลขบัณผ่านช่องทางอื่นที่ไม่ใช่อึเมล
8. เปิดการใช้งานยืนยันตัวตนแบบ Multi-Factor Authentication
9. เช็กรายชื่อผู้จะได้รับอีเมล ก่อนกดปุ่ม Reply หรือ Reply All ทุกครั้ง
10. อย่าหลงเชื่ออีเมลที่หลอกใปลี่ยนพาสเวิร์ดหรือให้อัปเดตข้อมูลส่วนบุคคล หากไม่แน่ใจว่าเป็นอิเผลที่มาจากใคร ให้บปรึกษาผู้เชี่ยวชาญด้านไอที่ หรือสอบถามกับผู้ที่ส่งข้อมูลมาในช่องทางอื่น ๆ กลับไปอีกครั้ง เพื่อยืนนว่ความถูกต้องก่อนดำเนินการใด

Phishing E-mail



ผลกระทบ - ข้อมูลส่วนบุคคล/ข้อมูลการเงิน /แฝงมัลแวร์ (Malware) ไว้ที่ Device

Phishing E-mail



แจ้งเตือนอีเมลหลอกลวง (Phishing Mail)

หากพบอีเมลหลอกลวงให้ดำเนินการลบอีเมลทิ้งทันที ห้ามคลิกลิงก์หรือไอคอน หลอกลวง ดาวน์โหลด หรือติดตั้งโปรแกรมที่ส่งมาพร้อมอีเมลหลอกหลวง

Ransomware


รูปแบบการโจมตีของ Ransomware
เพื่อยึดข้อมูลในเครื่องคอมพิวเตอร์ของเหยื่อ
MALICIOUS
MALICIOUS
1
2
3
4
5
6
100%


ข้อแนะนำในการป้องกันความเสียหายจากภัย Ransomware
ดำเนินการทันทีเพื่อรักษาความพร้อมใช้งานของข้อมูล
สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอ
ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ
มีความตระหนักในการใช้อีเมลและเปิดเว็บไซต์
ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย
ดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น
ในกรณีที่ตกเป็นเหยื่อ
ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อและอุปกรณ์เก็บข้อมูลเคลื่อนที่
ให้ติดต่อผู้เชี่ยวชาญหรือ ไทยเซิร์ต ทันที
GO DIGITAL
ETDA

เทคนิคดูแลคอมพิวเตอร์ส่วนตัว ให้ใช้งานปลอดภัย ไม่ถูกขโมยข้อมูล

มาดูกันว่า **หากจะยืดอายุคอมพิวเตอร์ ให้ใช้งานได้อย่างปลอดภัยนาน ๆ** ควรทำอย่างไรบ้าง?

ควรทำ ทุกวัน

- ใช้รหัสผ่านหรือ Pin เพื่อ Log in เข้าใช้งาน
- เริ่มโปรแกรมสแกนไวรัส ก่อนเริ่มต้นใช้งานโปรแกรมอื่น
- ล้างคำค้นหาในเว็บเบราว์เซอร์ ที่ใช้งานในแต่ละวัน
- Log Out บัญชีออนไลน์ ทุกบัญชี หลังการใช้งาน

ควรทำ เป็นประจำ

- อัปเดตซอฟต์แวร์ ให้อยู่ในเวอร์ชันล่าสุด
- ลบโปรแกรม หรือ ซอฟต์แวร์ ที่ไม่จำเป็นต้องใช้งาน
- สำรองข้อมูลสำคัญไว้กับ อุปกรณ์ที่มีความปลอดภัย
- ตั้งค่าบัญชีโซเชียล โดยจำกัดสิทธิ์ การเข้าถึง เพื่อความปลอดภัย


พฤติกรรมเสี่ยงใช้งาน LINE
ที่ง่ายต่อการสวมรอยบัญชี
การโดนสวมรอยบัญชี LINE ไม่ใช่เรื่องไกลตัวอีกต่อไป
หากคุณมีพฤติกรรมการใช้งานส่วนใหญ่ เข้าข่ายกรณีเหล่านี้
1 อีเมลที่ใช้ลงทะเบียน ไม่ใช่อีเมล์ที่ล็อกอินทุกวัน
2 ใช้รหัสผ่านที่คาดเดาง่าย
LINE
E-mail
Password
Login
Accounts
Facebook
Link
Allow Login
Version 2.3.0
3 เพิ่มคนที่ไม่รู้จักมาไว้ในรายชื่อ
4 เชื่อมต่อกับ Facebook ด้วยอีเมล และรหัสผ่านชุดเดียวกัน
5 อนุญาตให้ล็อกอินหลาย ๆ อุปกรณ์ได้
ON
6 ละเลยการอัปเดตซอฟต์แวร์
สัญญาณเตือนว่า กำลังมีใครใช้งานบัญชีคุณอยู่
E-mail
Password
ล็อกอินไม่ได้ แจ้งว่ารหัสผ่านผิด
LINE
1
พบข้อความแจ้งเตือน ว่ามีคนอื่นล็อกอิน
เจอข้อความ ที่เราไม่ได้พิมพ์
LOGIN
ใช้งานอยู่ แล้วบัญชี เด้งกลับไปหน้าล็อกอิน

แนวทาง และข้อปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ

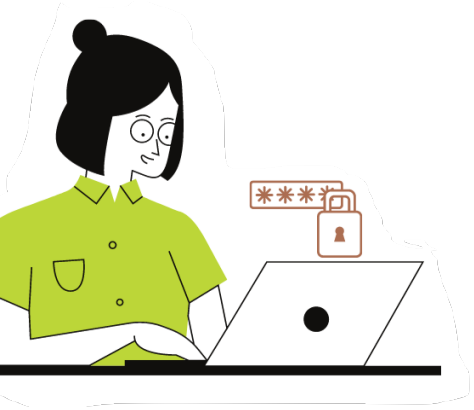
ลงทะเบียนบุคลากรการใช้งาน
คอมพิวเตอร์ ระบบเครือข่าย
อินเตอร์เน็ต และการยกเลิกการใช้งาน
เช่น ลาออก ย้าย ในหน่วยงาน

กำหนดรหัสผ่าน เข้าใช้งาน
คอมพิวเตอร์ และระบบเครือข่าย
อินเตอร์เน็ต และบันทึกเก็บข้อมูล Log

ตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ
(Screen saver) เพื่อทำการล็อก
หน้าจอภาพเมื่อไม่มีการใช้งาน
หลังจากนั้นเมื่อต้องการใช้งานต้องใส่
รหัสผ่านเพื่อเข้าใช้งาน

การสำรองข้อมูล

แนวทาง และข้อปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ



- ต้องใช้รหัสผ่านของตนเอง และรักษารหัสผ่านไว้เป็นความลับ
- ต้องออกจากระบบทุกครั้ง เมื่อเลิกใช้งาน
- ต้องเก็บข้อมูลไว้ในที่ปลอดภัย
- หลีกเลี่ยงอุปกรณ์โอนถ่ายข้อมูล
- ไม่ติดตั้งโปรแกรมอื่นใดที่ไม่เกี่ยวข้องกับการปฏิบัติงาน
- ไม่เข้าใช้งานเว็บไซต์ที่ขาดความน่าเชื่อถือ

OneDrive

Google Drive

ทำความรู้จัก PDPA พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

Personal Data Protection Act.

PDPA คืออะไร ?

RMUTT
www.rmutt.ac.th ราชมงคลธัญบุรี

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ ย่อมาจาก Personal Data Protection Act
บทบัญญัติที่ให้ความคุ้มครองข้อมูลส่วนบุคคลของ “บุคคลธรรมดา”
ให้สิทธิ์ในการแก้ไข, เข้าถึง หรือ แจ้งลบข้อมูลที่ให้ไว้กับองค์กรเป็นต้น
และกำหนดบทบาทหน้าที่และบทลงโทษหากองค์กรไม่ปฏิบัติตาม

ข้อมูลแบบไหนเป็น “ข้อมูลส่วนบุคคล”

ข้อมูลส่วนบุคคลคือ ข้อมูลเกี่ยวกับบุคคล
ที่ทำให้ระบุตัวบุคคลได้ ทั้งทางตรงและทางอ้อม

- เลขบัตรประจำตัวประชาชน
- ชื่อ - นามสกุล
- ที่อยู่
- เบอร์โทรศัพท์
- อีเมล
- ข้อมูลทางการเงิน
- เชื้อชาติ
- ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ

www.rmutt.ac.th มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)

เจ้าของข้อมูลส่วนบุคคล คือคนที่ข้อมูลส่วนบุคคลชุดนั้นๆ จะชี้มาที่ตัวตนของบุคคลนั้นได้

2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ควบคุมข้อมูลส่วนบุคคลคือคน บริษัทหรือองค์กรต่าง ๆ ที่เป็นคนตัดสินใจว่า จะมีการประมวลผลข้อมูลส่วนบุคคลอะไร เพื่ออะไร อย่างไร ภายใต้ PDPA ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีหน้าที่และความรับผิดหลักที่ต้องปฏิบัติตาม PDPA ให้ครบถ้วน บริษัททุกบริษัททันทีที่มีพนักงานคนแรก ที่ต้องใช้ข้อมูลเพื่อจ่ายเงินเดือนก็เป็น Data Controller แล้วทั้งสิ้น

3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคลคือ คน บริษัทหรือองค์กรต่าง ๆ ที่ประมวลผลข้อมูลส่วนบุคคล โดยจะทำภายใต้คำสั่ง หรือในนามของ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) เท่านั้น ไม่ได้เป็นคนตัดสินใจทำการประมวลผลข้อมูลด้วยตัวเอง

RMUTT
www.rmutt.ac.th ราชมงคลธัญบุรี

เจ้าของข้อมูลส่วนบุคคล มีสิทธิอะไรบ้าง ?

- สิทธิได้รับการแจ้งให้ทราบ
- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล
- สิทธิขอให้โอนข้อมูลส่วนบุคคล
- สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล
- สิทธิคัดค้านการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- สิทธิขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
- สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล

✖✖ ข้อมูลคนตาย ข้อมูลนิติบุคคล ไม่เป็นข้อมูลส่วนบุคคลตามกฎหมายนี้ ✖✖

www.rmutt.ac.th มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

RMUTT
www.rmutt.ac.th ราชมงคลธัญบุรี

ผู้ควบคุมข้อมูลส่วนบุคคล จะสามารถรวบรวม ใช้ หรือ เปิดเผย ข้อมูลส่วนบุคคลก็ต่อเมื่อ ?

บุคคลธรรมดา หรือนิติบุคคล (บริษัท ห้างร้าน มูลนิธิ สมาคม หน่วยงาน องค์กร ร้านค้า หรืออื่นใดก็ตาม) หากมีการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ หรือมีการนำข้อมูลส่วนบุคคลไปใช้ หรือนำไปเปิดเผยไม่ว่าจะวัตถุประสงค์ใด ก็ตาม จำเป็นต้องได้รับ คำยินยอม (Consent) จากเจ้าของข้อมูลด้วย เว้นแต่จะเป็นไปตามข้อยกเว้นที่ พรบ. กำหนดไว้

ข้อยกเว้นที่สามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องขอความยินยอม

Scientific or Historical Research
เป็นการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ การศึกษาวิจัย หรือสถิติ

Vital Interest
เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล เช่น การเข้ารับบริการทางการแพทย์ ณ โรงพยาบาล

Contract
เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาเช่น เจ้าของข้อมูลส่วนบุคคลทำสัญญากู้ยืมเงินจากธนาคาร ธนาคารสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ตามวัตถุประสงค์ของสัญญา

Public Task
เป็นการจำเป็นเพื่อปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

Vital Interest
เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือนิติบุคคลอื่น

Contract
เป็นการปฏิบัติตามกฎหมาย

เมื่อ PDPA บังคับใช้แล้วแต่ไม่ได้ปฏิบัติตามจะมีบทลงโทษอะไรบ้าง ?

โทษทางแพ่ง

โทษทางแพ่งกำหนดให้ชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจจะต้องจ่ายบวกเพิ่มอีกเป็นค่าค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดได้อีก 2 เท่าของค่าเสียหายจริง

โทษทางอาญา

โทษทางอาญาจะมีทั้งโทษจำคุกและโทษปรับ โดยมี โทษจำคุกสูงสุดไม่เกิน 1 ปี หรือ ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ กรณีหากผู้กระทำความผิดคือ บริษัท(นิติบุคคล) ก็อาจจะสงสัยว่าใครจะเป็นผู้ถูกจำคุก เพราะบริษัทติดคุกไม่ได้ ในส่วนตรงนี้ก็อาจจะตกมาที่ ผู้บริหาร, กรรมการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทนั้น ๆ ที่จะต้องได้รับการลงโทษจำคุกแทน

โทษทางปกครอง

โทษปรับ มี ตั้งแต่ 1 ล้านบาทจนถึงสูงสุดไม่เกิน 5 ล้านบาท ซึ่งโทษปรับสูงสุด 5 ล้านบาท จะเป็นกรณีของการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศของประเภทข้อมูลที่มีความละเอียดอ่อน(Sensitive Personal Data) ซึ่งโทษทางปกครองนี้จะแยกต่างหากกับการชดใช้ค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญาด้วย

- Thank you