

ข้อมูลความรู้ที่ 1 (ไม่มีการประเมินผลหลังเรียนรู้)


การเคหะแห่งชาติ
 National Housing Authority

รหัสผ่าน

รหัสผ่าน คือ สายอักขระหรือคำที่เป็นความลับ ที่ใช้สำหรับยืนยันตัว พิสูจน์ความเป็นเจ้าของ หรือเข้าถึงแหล่งข้อมูล รหัสผ่านควรจะเก็บเป็นความลับ เพื่อไม่ให้คนอื่นเข้าถึงได้

ทำไมต้องตั้งรหัสผ่าน

- 

ป้องกันบุคคลที่ไม่พึงประสงค์ มาแอบใช้คอมพิวเตอร์
- 

ช่วยลดปัญหาเกี่ยวกับไวรัสหรือ Hacker ที่พยายามเข้าถึงคอมพิวเตอร์
- 

ลดปัญหาการแอบใช้คอมพิวเตอร์ จากเด็ก ๆ ที่บ้าน

ข้อปฏิบัติการใช้งานให้ปลอดภัย

- 

ไม่เปิดเผยรหัสผ่าน ของตนเองให้ผู้อื่นทราบ
- 

Log Off ออกจากคอมพิวเตอร์ทุกครั้ง หลังจากไม่ได้ใช้งาน

การตั้งรหัสผ่านให้ปลอดภัย

- 

ความยาวไม่น้อยกว่า 8 ตัวอักษร และยากต่อการคาดเดา
- 

ไม่ใช้คำที่ปรากฏในพจนานุกรม และอักขระไม่เรียงกัน เช่น 123
- 

ไม่ใช้รหัสผ่านที่เคยตั้งมาแล้ว
- 

ไม่ตั้งรหัสผ่าน โดยมีช่องว่างหรือตัวอักษรที่ไม่ใช่ภาษาอังกฤษ
- 

เปลี่ยนรหัสผ่าน ทุก ๆ 90 วัน
- 

ไม่จดรหัสผ่าน ลงกระดาษหรือในไฟล์เอกสารที่ไม่มีการป้องกันการเข้าถึง

ฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลความรู้ที่ 2 (ไม่มีการประเมินผลหลังเรียนรู้)

ทำความรู้จัก “ Malware ”

Malware ย่อมาจาก Malicious Software หมายถึงโปรแกรม
ประสงค์ร้ายที่ถูกสร้างขึ้นมา เพื่อโจมตีระบบโดยเฉพาะ ทำให้
ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล



ช่องทางการแพร่ระบาดของ Malware



วิธีป้องกัน Malware



วิธีใช้

เครือข่ายสังคมออนไลน์ให้ปลอดภัย



Item 1

แชร์ข้อมูลส่วนบุคคลเท่าที่จำเป็น และ
จำกัดคนที่สามารถเข้าถึงข้อมูลส่วนบุคคล



Item 2

ตั้งค่าความปลอดภัย



Item 3

คิดก่อนโพสต์



Item 4

ระมัดระวังข่าวปลอม

ข้อมูลความรู้ที่ 4 (ไม่มีการประเมินผลหลังเรียนรู้)

วิธีป้องกันภัยคุกคาม ที่เกิดขึ้นบนโทรศัพท์มือถือ



ติดตั้งซอฟต์แวร์ Anti-malware

หลีกเลี่ยงการ Root (Android)
หรือ Jailbreak (ios)



ติดตั้ง Application จาก Store เท่านั้น และ
ให้สังเกตรายละเอียดของ Application ที่จะ
ติดตั้ง เช่น จำนวนผู้โหลด รีวิว เป็นต้น

ควรตั้งค่าเพื่อป้องกันการโหลด
ซอฟต์แวร์จากแหล่งที่ไม่รู้จัก



ล็อคหน้าจอโทรศัพท์มือถือ
ด้วยวิธีที่ปลอดภัย

ข้อมูลความรู้ที่ 5 (ไม่มีการประเมินผลหลังเรียนรู้)

สิทธิของเจ้าของ ข้อมูลส่วนบุคคล



Personal
Information



สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (มาตรา 30)



สิทธิในการขอให้โอนข้อมูลส่วนบุคคล
(มาตรา 31)



สิทธิคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผย
ข้อมูลส่วนบุคคล (มาตรา 32)



สิทธิขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วน
บุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (มาตรา
33)



สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล
(มาตรา 34)



สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล
(มาตรา 35)



สิทธิในการร้องขอให้ดำเนินการ (มาตรา 36)



เจ้าของข้อมูลส่วนบุคคล มีสิทธิร้องเรียนในกรณีที่คุณควบคุม
ข้อมูลส่วนบุคคล หรือผู้ที่เกี่ยวข้อง ผ่าฝืนหรือไม่ปฏิบัติตาม
พ.ร.บ. หรือประกาศที่ออกตาม พ.ร.บ. นี้ (มาตรา 73)

ข้อมูลความรู้ที่ 6 (มีการประเมินผลหลังเรียนรู้)



พ.ร.บ.

คุ้มครองข้อมูลส่วนบุคคล

ทำไม

ต้องคุ้มครองข้อมูลส่วนบุคคล



ความก้าวหน้าของเทคโนโลยี ทำให้การเก็บรวบรวมข้อมูล การใช้ การเปิดเผยข้อมูลส่วนบุคคล ซึ่งกระทำได้ง่ายและรวดเร็ว ทำให้มีการละเมิดสิทธิข้อมูลส่วนบุคคล และก่อให้เกิดความเสียหายต่อตัวบุคคล

สาระสำคัญ



1. **บุคคลเจ้าของข้อมูล** ต้องให้ความยินยอม การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล



2. **ผู้เก็บรวบรวมข้อมูลส่วนบุคคล** ต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลง แก้ไข หรือมีใครเข้าถึงได้โดยมิชอบ



3. **บุคคลเจ้าของข้อมูล** มีสิทธิถอนความยินยอม หรือขอให้ลบ หรือทำลายข้อมูลได้ เมื่อถูกนำไปใช้ในทางไม่ชอบด้วยกฎหมาย

หน่วยงานที่เกี่ยวข้อง



สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- กำหนดมาตรฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ให้ความรู้และการฝึกอบรมแก่หน่วยงานรัฐ เอกชน และบุคคลทั่วไป ในการคุ้มครองข้อมูลส่วนบุคคล



คณะกรรมการผู้เชี่ยวชาญ

- พิจารณาเรื่องร้องเรียนเมื่อมีการละเมิด
- ตรวจสอบผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล
- โกล่เกลี่ยข้อพิพาท

คนไทยได้อะไรจาก พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

1. ป้องกันการล่วงละเมิดความเป็นส่วนตัวของข้อมูลส่วนบุคคล
2. ปกป้องความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล และความเดือดร้อนรำคาญ
3. สร้างกลไก หรือมาตรฐานการกำกับดูแลในการคุ้มครองข้อมูลส่วนบุคคล
4. สามารถฟ้องเรียกค่าสินไหมทดแทนกรณีถูกละเมิดข้อมูลส่วนบุคคล



ผู้เรียนรู้สามารถประเมินผลหลังเรียนรู้ได้ โดย Scan QR Code

ฝ่ายเทคโนโลยีสารสนเทศ



พ.ร.บ.

ความมั่นคงปลอดภัยไซเบอร์

สาระสำคัญ

- 1.กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐ มีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
- 2.มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ
- 3.มีการร่วมมือและประสานกันและกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้จนทำให้ประชาชนเดือดร้อน

ประชาชนได้ะไรจาก พ.ร.บ. ไซเบอร์

- 1.ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญมีความปลอดภัยสามารถให้บริการได้ต่อเนื่อง
- 2.มีแนวทางในการรับมือภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบเป็นวงกว้างและกลับมาทำงานได้อย่างรวดเร็ว
- 3.มีการจัดทัพหน่วยงานขึ้นมาดูแลและให้ความช่วยเหลือแก่หน่วยงานโครงสร้างพื้นฐานที่สำคัญ
- 4.เมื่อเกิดภัยคุกคามร้ายแรงการเข้าไปแก้ไขปัญหาคือต้องเข้าตั้งกรณียุติสินจะคือจะใช้คำสั่งศาลเพื่อคุ้มครองสิทธิ์

ทำไมต้องมี พ.ร.บ. ไซเบอร์

เพื่อปกป้องระบบคอมพิวเตอร์และโครงข่าย IT ของโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ หรือ บริการที่สำคัญของประเทศมีความมั่นคงปลอดภัยสามารถให้บริการได้เป็นปกติและหน่วยงานสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

หน่วยงานหลัก ๆ

- หน่วยงานควบคุมหรือกำกับดูแล** ดูแลการดำเนินงานของหน่วยงานรัฐหรือโครงสร้างพื้นฐานสำคัญให้มีมาตรฐาน
- สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ** เป็นศูนย์กลางเฝ้าระวังความปลอดภัยไซเบอร์ของประเทศและให้การช่วยเหลือในการป้องกันและรับมือเมื่อเกิดภัยคุกคามในระดับร้ายแรง
- ภัยคุกคามทางไซเบอร์ระดับร้ายแรง** ระบบในการให้บริการที่สำคัญของหน่วยงานโครงสร้างพื้นฐานถูกโจมตี จนไม่สามารถให้บริการได้
- ภัยคุกคามทางไซเบอร์ระดับวิกฤติ** ระบบบริการพื้นฐานที่สำคัญถูกโจมตี ไม่สามารถให้บริการได้เป็นวงกว้าง กระทบกับชีวิตและความปลอดภัยของประชาชนจำนวนมาก และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ



ผู้เรียนรู้สามารถประเมินผลหลังเรียนรู้ได้ โดย Scan QR Code

พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562



ที่มา

การพิสูจน์ตัวตนผู้ใช้บริการต้องไป
แสดงตนต่อผู้ให้บริการ เช่น มีการ
พิสูจน์ตัวตน การให้ความยินยอม
การลงลายมือชื่อ หรือการแสดง
เจตนาของผู้ทำธุรกรรม

หลักการ

1.ให้มีการพิสูจน์และยืนยัน
ตัวตนผ่านระบบการพิสูจน์
และยืนยันตัวตนทางดิจิทัล
ได้โดยให้แจ้งเวียนไขกับ
ความน่าเชื่อถือให้
ผู้ใช้บริการทราบล่วงหน้า

พระราชกฤษฎีกากำหนดให้ผู้ให้บริการ ระบบฯ ต้องขออนุญาต (ถ้ามี)

กำหนดหลักเกณฑ์เพื่อกำกับดูแลผู้ใช้บริการระบบฯ
เพื่อให้กระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัล
เป็นไปอย่างถูกต้องครบถ้วน

ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Platform)

ผู้ให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลขอ
ใบอนุญาตจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ระบบทำการแทน (Proxy Server)

ให้บริการระบบทำการแทนแก่ผู้ที่ประสงค์จะเข้าสู่ Platform
แต่ไม่มีมาตรฐานทางเทคโนโลยีเพียงพอ เพื่อให้สามารถ
เชื่อมต่อกับ Platform ผ่านระบบทำการแทน

การคุ้มครองข้อมูลส่วนบุคคล

มาตรฐานการเข้ารหัสข้อมูล หลักเกณฑ์การส่งผ่านข้อมูล
ระหว่าง Platform และ Proxy Server รวมถึงอำนาจใน
การเรียกผู้ที่เกี่ยวข้องมาให้ข้อมูลหรือพิจารณาคำอุทธรณ์
ของผู้ที่ได้รับความเสียหาย

2.ให้มีการตราพระราช
กฤษฎีกากำหนดให้ผู้
ให้บริการระบบการพิสูจน์
และยืนยันตัวตนทางดิจิทัล
เป็นธุรกิจที่ต้องขออนุญาต
และกำหนดให้มี
คณะกรรมการกำกับดูแล
เป็นการเฉพาะก็ได้

3.ผู้ประกอบการธุรกิจระบบ
การพิสูจน์และยืนยันตัวตน
ทางดิจิทัลที่ไม่ได้รับ
อนุญาตตามพระราช
กฤษฎีกา (ถ้ามี) มีโทษทาง
อาญา

