หลักสูตร

กฎหมายดิจิทัลมาตรฐาน และหลักปฏิบัติที่ดีด้านดิจิทัล สำหรับบุคลากรภาครัฐ

ผู้เข้าร่วมการฝึกอบรม

1. นายชยารพ บุญมัติ ศทส.
2. นายกษิดิศ จุฑาภูวดล ศทส.
3. นางสาวสรัณรัตน์ อุษณกรกุล ศทส.
4. นางวิไล ฉวาง สทข. 4

วันที่เข้ารับการฝึกอบรม

วันที่ 16-17, 23-24 มกราคม 2568

การฝึกอบรมประกอบด้วย 7 หัวข้อ

1) กฎหมายการบริการงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
2) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
3) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
5) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
6) กฎหมายทรัพย์สินทางปัญญา
7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

1) กฎหมายการบริการงานและการให้บริการภาครัฐผ่านระบบดิจิทัล

1) กฎหมายการบริการงานและการให้บริการภาครัฐผ่านระบบดิจิทัล

- กฎหมายฉบับนี้ถูกประกาศในราชกิจจานุเบกษาเมื่อวันที่ 22 พฤษภาคม 2562 และมีผลบังคับใช้ ตั้งแต่วันที่ 23 พฤษภาคม 2562 เป็นต้นไป
- กฎหมายนี้ใช้บังคับกับหน่วยงานของรัฐทุกองค์กร ได้แก่ ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน รัฐสภา ศาล องค์กรอิสระตามรัฐธรรมนูญ องค์กรอัยการ สถาบันอุดมศึกษาของรัฐ และหน่วยงานอิสระของรัฐ

1) กฎหมายการบริการงานและการให้บริการภาครัฐผ่านระบบดิจิทัล

วัตถุประสงค์เพื่อนำเทคโนโลยีดิจิทัลมาใช้ในการบริหารงานภาครัฐและการบริการประชาชน เพื่อให้เกิดความสะดวก รวดเร็ว โปร่งใส และมีประสิทธิภาพ โดยกฎหมายนี้กำหนดให้มีการบูรณาการฐานข้อมูลภาครัฐ การรักษาความมั่นคงปลอดภัยของข้อมูล และการเปิดเผยข้อมูลเพื่อให้ประชาชนสามารถเข้าถึงบริการได้ง่ายขึ้น

สิ่งที่กฎหมาย/พรบ. ดังกล่าวทำให้เกิดขึ้น :

1. การบูรณาการ เชื่อมโยงการทำงานระหว่างหน่วยงานภาครัฐ
2. ประสิทธิภาพ ลดขั้นตอน แก้ไขการทำงานซ้ำ
3. ธรรมาภิบาลข้อมูล มีมาตรการควบคุม จัดการข้อมูลอย่างปลอดภัย
4. พัฒนาบุคลากร ยกระดับทักษะด้านดิจิทัลของเจ้าหน้าที่
5. บริการประชาชน ให้มีความสะดวก ไม่ต้องสำเนาเอกสาร มีระบบชำระเงินอิเล็กทรอนิกส์

2) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หลักการ

- มุ่งเน้นที่จะป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ อาชญากรคอมพิวเตอร์ ที่ทำให้ระบบคอมพิวเตอร์หรือโครงข่ายของหน่วยงานโครงสร้างพื้นฐานที่สำคัญไม่สามารถทำงานได้เป็นปกติกระทบต่อการให้บริการแก่ประชาชน หรือความสงบเรียบร้อยภายในประเทศ

2) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

<u>จุดมุ่งหมาย</u>

- เพื่อสร้างกรอบกฎหมายด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุม โครงสร้างพื้นฐานสำคัญของประเทศ (CRITICAL INFORMATION INFRASTRUCTURE – CII) มีด้วยกัน 8 ด้าน ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสารณูปโภค ด้านสาธารณสุข และด้านอื่นๆ
- ให้หน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และประมวลแนวทางปฏิบัติขั้นต่ำ

3) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

3) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เป็นกฎหมายที่รองรับ "สิทธิได้รู้" ของประชาชนที่เกี่ยวกับการดำเนินการของรัฐ โดยประชาชนไม่จำเป็นต้องมีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูลข่าวสารนั้น เมื่อประชาชนได้รู้ข้อมูลข่าวสารแล้วจะไปใช้ประโยชน์ เพื่อปกป้องประโยชน์ของตนเอง ปกป้องประโยชน์สาธารณะ และเพื่อการมีส่วนร่วมในการปกครองตามระบอบประชาธิปไตย

<u>โดยมีหลักแนวคิด ดังนี้</u>

- ให้ประชาชนมีโอกาศรับรู้ข้อมูลข่าวสารเกี่ยวกับการดำเนินงานต่างๆ ของรัฐ
- รับรองสิทธิของประชาชนในการเข้าถึงข้อมูลข่าวสารของราชการ
- เปิดเผยเป็นหลัก ปกปิดเป็นการยกเว้น โดยรัฐไม่ต้องเปิดเผยข้อมูลเฉพาะที่มีกฎหมายกำหนดเท่านั้น

3) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

หน้าที่ของหน่วยงานรัฐ

หน่วยงานของรัฐมีหน้าที่เปิดเผยข้อมูลข่าวสารบางประเภทตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เพื่อให้ประชาชนสามารถเข้าถึงข้อมูลของราชการอย่างโปร่งใส และตรวจสอบได้ โดยข้อมูลข่าวสารที่หน่วยงานของรัฐต้องเปิดเผยมี 4 ประเภทหลัก ๆ ดังนี้

3.1 ข้อมูลข่าวสารที่ต้องจัดไว้ให้ประชาชนตรวจดูได้ (มาตรา 7)

- โครงสร้างและการจัดองค์กร
- อำนาจหน้าที่และวิธีการดำเนินงาน
- สถานที่ติดต่อเพื่อขอรับข้อมูล
- กฎ ระเบียบ คำสั่ง มติคณะรัฐมนตรี หรือคำวินิจฉัยของศาลที่ใช้บังคับกับประชาชน
- นโยบายหรือการตีความของหน่วยงาน
- แผนงาน โครงการ งบประมาณ
- คู่มือหรือคำแนะนำในการปฏิบัติงาน

3) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

3.2 ข้อมูลข่าวสารที่ต้องจัดพิมพ์ในราชกิจจานุเบกษา (มาตรา 9)ข้อมูลที่มีผลกระทบกับสิทธิและหน้าที่ของประชาชน หน่วยงานของรัฐต้องเผยแพร่ใน ราชกิจจานุเบกษา เช่น

- กฎหมาย กฎ ระเบียบ คำสั่ง
- มติคณะรัฐมนตรี
- ข้อบังคับ ประกาศต่าง ๆ
- หลักเกณฑ์ในการพิจารณาอนุมัติ อนุญาต
- มาตรฐานการให้บริการ
- สิทธิในการร้องเรียน หรืออุทธรณ์

3.3 ข้อมูลข่าวสารที่ต้องให้เมื่อมีผู้ขอ (มาตรา 11) หากประชาชนต้องการข้อมูลอื่น ๆ ที่ไม่ได้อยู่ในมาตรา 7 หรือ 9 สามารถยื่นคำขอได้ โดยหน่วยงานมีหน้าที่ให้ข้อมูล ยกเว้นในกรณีที่ :

- เป็นข้อมูลลับ
- กระทบต่อความมั่นคงของประเทศ
- กระทบสิทธิของบุคคลอื่น
- อยู่ในระหว่างพิจารณาของหน่วยงาน

3) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

3.4 ข้อมูลข่าวสารที่ไม่ต้องเปิดเผย (มาตรา 14 – 18) โดยหน่วยงานของรัฐสามารถปฏิเสธการเปิดเผยข้อมูลได้ หากเป็นข้อมูลที่

- กระทบต่อความมั่นคงของชาติ ความสัมพันธ์ระหว่างประเทศ หรือความปลอดภัยของประชาชน
- กระทบต่อการปฏิบัติหน้าที่ของรัฐ
- เป็นข้อมูลส่วนบุคคลที่ละเมิดสิทธิของผู้อื่น
- เกี่ยวกับการพิจารณาคดี หรืองานสอบสวนที่ยังไม่สิ้นสุด

4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

แบ่งออกเป็น 7 หมวด ได้แก่

หมวด 1 – คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 8–18)
หมวด 2 – การคุ้มครองข้อมูลส่วนบุคคล (มาตรา 19–21)
หมวด 3 – สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา 30–42)
หมวด 4 – สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 43–70)
หมวด 5 – การร้องเรียน (มาตรา 71–76)
หมวด 6 – ความรับผิดทางแพ่ง (มาตรา 77–78)
หมวด 7 – บทกำหนดโทษ (มาตรา 79–90) รวมทั้งบทเฉพาะกาล (มาตรา 91–96)

4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประเด็นสำคัญในแต่ละหมวด

- นิยาม “ข้อมูลส่วนบุคคล”: ข้อมูลที่สามารถระบุตัวบุคคลทางตรงหรือทางอ้อม เช่น ชื่อ, รหัสบัตรประชาชน, รูปถ่าย ฯลฯ
- หลักการเก็บและใช้ข้อมูล: ต้องดำเนินตามวัตถุประสงค์ที่ชัดเจน และจำเป็นต้องได้รับ ความยินยอมที่ชัดแจ้ง จากเจ้าของข้อมูล เว้นแต่มีข้อยกเว้นตามกฎหมาย เช่น จำเป็นตามสัญญา หรือในกรณีเฉพาะที่เกี่ยวข้องกับผลประโยชน์ของรัฐหรือสาธารณะ
- สิทธิของเจ้าของข้อมูล: เช่น สิทธิในการเข้าถึงข้อมูล (access), แก้ไข, ลบ (right to erasure/"สิทธิที่จะถูกลืม"), คัดค้านการใช้ข้อมูล, และโอนย้ายข้อมูล (data portability)
- ความปลอดภัยของข้อมูล: ผู้ควบคุมและผู้ประมวลผลข้อมูลต้องดูแลให้ข้อมูลปลอดภัย ไม่ให้รั่วไหล และต้องมีมาตรการป้องกันอย่างเหมาะสม
- การโอนข้อมูลข้ามประเทศ: ต้องเกิดในประเทศที่มีมาตรการคุ้มครองข้อมูลในระดับเทียบเท่า หรือได้รับความยินยอมจากเจ้าของข้อมูล
- การบังคับใช้นอกประเทศไทย: กฎหมายนี้มีผลบังคับย้อนหลังไปยังผู้ควบคุมหรือผู้ประมวลผลที่อยู่ต่างประเทศ หากเกี่ยวข้องกับการนำเสนอสินค้า/บริการ หรือมีการติดตามพฤติกรรมของบุคคลในประเทศไทย
- บทลงโทษ: มีทั้งโทษทางแพ่ง, ปรับทางปกครองสูงสุดถึง 5 ล้านบาท, และโทษทางอาญา (จำคุก)

5) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

5) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

<u>แบ่งเนื้อหาออกเป็น 2 หมวด ได้แก่ ความผิดเกี่ยวกับคอมพิวเตอร์ กับพนักงานหน้าที่</u>

หมวด ความผิดเกี่ยวกับคอมพิวเตอร์ ประกอบด้วย กำหนดฐานความผิด องค์ประกอบความผิด และโทษ ประกอบด้วย การเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์, การดักรับข้อมูลระหว่างส่ง การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือปลอมแปลงแหล่งที่มาเพื่อรบกวนระบบคอมพิวเตอร์ของบุคคลอื่น หรือก่อความรำคาญด้วยการส่งข้อมูล (สแปมอีเมล), จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อไปใช้เป็นเครื่องมือกระทำผิด, การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลต้องห้าม หรือเผยแพร่ข้อมูลต้องห้าม หรือเผยแพร่ภาพบุคคลอื่น, หน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

หมวด พนักงานเจ้าหน้าที่ ประกอบด้วย คุณสมบัติ อำนาจหน้าที่ และความรับผิดชอบ, คณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์

6) กฎหมายทรัพย์สินทางปัญญา

6) กฎหมายทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญา (Intellectual Property) หมายถึง ผลงานอันเกิดจากการประดิษฐ์ คิดค้น หรือการสร้างสรรค์ของมนุษย์ ซึ่งเน้นที่ผลผลิตของสติปัญญาและความชำนาญ โดยไม่จำกัดชนิดของการสร้างสรรค์หรือวิธีการแสดงออกในรูปแบบของสิ่งที่จับต้องได้ เช่น สินค้าต่างๆ หรือในรูปแบบของสิ่งของที่จับต้องไม่ได้ เช่น บริการ แนวคิดในการดำเนินธุรกิจ กรรมวิธีการผลิตในอุตสาหกรรม เป็นต้น

ทรัพย์สินทางปัญญา แบ่งออกเป็น 2 ประเภท ได้แก่ ลิขสิทธิ์ (COPYRIGHT) และทรัพย์สินทางอุตสาหกรรม (INDUSTRIAL PROPERTY) ดังนี้

1. ลิขสิทธิ์ (COPYRIGHT)

หมายถึง สิทธิแต่เพียงผู้เดียวของเจ้าของลิขสิทธิ์ที่จะกระทำการใดๆ กับงานที่ผู้สร้างสรรค์ได้ทำขึ้น ไม่ว่างานดังกล่าวจะแสดงออกในรูปแบบอย่างใด โดยประเภทของงานอันมีลิขสิทธิ์ที่กฎหมายกำหนดไว้ ได้แก่

- งานวรรณกรรม
- งานนาฎกรรม
- งานศิลปกรรม
- งานดนตรีกรรม
- งานโสตทัศนวัสดุ
- งานภาพยนต์
- งานบันทึกเสียง
- งานแพร่เสียงแพร่ภาพ

6) กฎหมายทรัพย์สินทางปัญญา

2. ทรัพย์สินทางอุตสาหกรรม (INDUSTRIAL PROPERTY)

หมายถึง ความคิดสร้างสรรค์ของมนุษย์ที่เกี่ยวกับสินค้าอุตสาหกรรมต่างๆ ความคิดสร้างสรรค์นี้อาจ เป็นความคิดในการประดิษฐ์คิดค้น ซึ่งอาจจะเป็นกระบวนการหรือเทคนิคในการผลิต ที่ได้ปรับปรุงหรือคิดค้นขึ้นใหม่ หรือการออกแบบผลิตภัณฑ์อุตสาหกรรมที่เป็นองค์ประกอบและรูปร่างของตัวผลิตภัณฑ์ นอกจากนี้ยังรวมถึง 2 เครื่องหมายการค้า ความลับทางการค้า การคุ้มครองพันธุ์พืช แบบผังภูมิของวงจรรวม และสิ่งบ่งชี้ทางภูมิศาสตร์

ทรัพย์สินทางอุตสาหกรรมมีวัตถุประสงค์หลักเพื่อมอบสิทธิแต่เพียงผู้เดียวให้แก่เจ้าของในการแสวงหาผลประโยชน์จากการสร้างสรรค์ของตนเอง เช่น การผลิต การขาย การใช้ หรือการอนุญาตให้ผู้อื่นใช้ ภายในระยะเวลาที่กฎหมายกำหนด

การละเมิดทรัพย์สินทางปัญญา

การละเมิดอาจเกิดได้หลายรูปแบบ เช่น

- คัดลอกเพลง หนัง โปรแกรม โดยไม่ได้รับอนุญาต
- ใช้โลโก้ หรือชื่อที่จดทะเบียนแล้ว
- ผลิตสินค้าปลอมแปลง
- ขโมยสูตรลับของบริษัทไปใช

โทษมีทั้ง ทางแพ่ง (เรียกค่าเสียหาย) และ ทางอาญา (จำคุก ปรับ)

6) กฎหมายทรัพย์สินทางปัญญา

อายุความคุ้มครอง (โดยทั่วไปในไทย) ของทรัพย์สินทางปัญญา

ประเภท	รายละเอียด	อายุความคุ้มครอง (โดยทั่วไปในไทย)
ลิขสิทธิ์ (Copyright)	งานเขียน หนัง เพลง งานศิลป์ โปรแกรมคอมพิวเตอร์ ฯลฯ	ตลอดอายุผู้สร้าง + 50 ปีหลังเสียชีวิต
สิทธิบัตร (Patent)	การประดิษฐ์ใหม่ เช่น อุปกรณ์ เทคโนโลยี	สิทธิบัตรการประดิษฐ์: 20 ปี, อนุสิทธิบัตร: 10 ปี
เครื่องหมายการค้า (Trademark)	โลโก้ ชื่อแบรนด์ สัญลักษณ์ที่ใช้ในการค้า	10 ปี ต่ออายุได้เรื่อย ๆ
แบบผลิตภัณฑ์ (Design)		
แบบผลิตภัณฑ์ (Design	รูปแบบภายนอกของผลิตภัณฑ์ เช่น ขวดน้ำ รองเท้า	10 ปี
ความลับทางการค้า (Trade Secret)	ข้อมูลที่มีมูลค่าในเชิงพาณิชย์ เช่น สูตรอาหาร สูตรเคมี	ไม่มีจำกัดเวลา (ตราบที่ยังเป็นความลับอยู่)
สิ่งบ่งชี้ทางภูมิศาสตร์ (GI)	สินค้าที่มีแหล่งกำเนิดเฉพาะ เช่น กาแฟดอยตุง ผ้าไหมแพรวา	คุ้มครองตราบที่ยังใช้ชื่อภูมิศาสตร์นั้นอย่างถูกต้อง

7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

กฎหมายธุรกรรมทางอิเล็กทรอนิกส์หลักคือ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม โดยปัจจุบันมีฉบับที่ 2 ปี 2551 ฉบับที่ 3 ปี 2562 และฉบับที่ 4 ปี 2562

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

เพิ่มคำนิยาม

- “การพิสูจน์และยืนยันตัวตน”
- “ระบบการพิสูจน์และยืนยันตัวตนทาง ดิจิทัล”

รองรับกำรพิสูจน์และยืนยันตัวตนทำงดิจิทัล (เพิ่ม ม.34/3)

- กำหนดเงื่อนไขเกี่ยวกับความน่าเชื่อถือ

ให้มีการตรา พ.ร.ฎ. (เพิ่ม ม.34/4)

- กำหนดประเภทธุรกิจบริการที่กำกับดูแล โดยกำหนดหลักเกณฑ์ที่ผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะต้องปฏิบัติ

กำหนดโทษ (เพิ่ม ม.45/1)

- กรณีไม่ได้รับอนุญาต หรือฝ่าฝืนคำสั่ง พักใช้หรือเพิกถอนใบอนุญาต
- จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ

บทเฉพาะกาล (ม.7)

- เมื่อมีพระราชกฤษฎีกาแล้ว ให้ยื่นขออนุญาตภายใน 90 วันนับแต่วันที่ พ.ร.ฎ. มีผลใช้บังคับ

7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

Digital ID สำคัญอย่างไร

ใช้ระบุตัวบุคคล ผู้ทำธุรกรรม

ไม่ต้องสร้าง Digital ID ใหม่ทุกครั้ง
สามารถใช้เข้าถึงบริการต่าง ๆ ได้ จาก Digital ID เดิมที่ผ่านการพิสูจน์ตัวตนที่น่าเชื่อถือ

ลดกระบวนการ ระยะเวลา
และค่าใช้จ่าย ในการพิสูจน์ตัวตน

ผู้ใช้บริการสามารถเข้าถึงบริการดิจิทัล
ของทั้งภาครัฐ และภาคเอกชนได้ง่ายขึ้น

7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

Digital Identity (ดิจิทัลไอดี) คือ อัตลักษณ์ (identity) ที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งใช้บ่งบอกหรือจำแนกบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ โดยอัตลักษณ์ (identity) จะหมายถึง ลักษณะเฉพาะของบุคคลซึ่งสามารถบ่งบอกหรือจำแนกได้โดยคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคลนั้น

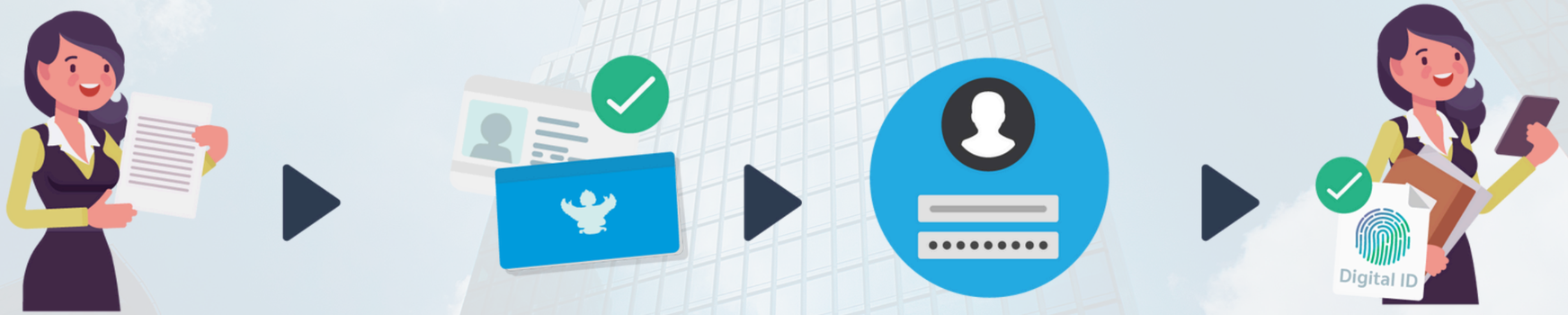
ตัวอย่างคุณลักษณะที่เกี่ยวข้องกับบุคคลธรรมดา เช่น เลขประจำตัว ชื่อ ที่อยู่ วันเดือนปีเกิด เบอร์โทรศัพท์ ภาพใบหน้า อีเมล หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน เป็นต้น ส่วนตัวอย่างคุณลักษณะที่เกี่ยวข้องกับนิติบุคคล เช่น เลขทะเบียนนิติบุคคล ชื่อนิติบุคคล ที่ตั้งสำนักงานใหญ่ ชื่อกรรมการของนิติบุคคล เป็นต้น

7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

การพิสูจน์และยืนยันตัวตนทางดิจิทัล

การพิสูจน์ตัวตน

เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP) รวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริง



1. บุคคลมาแสดงตนกับ IdP
2. IdP พิสูจน์ตัวตนของบุคคล
3. IdP ออกหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตน (Authenticator)
4. บุคคลเปลี่ยนสถานะเป็นผู้ใช้บริการ

หมายเหตุ IDP (IDENTITY PROVIDER) คือ หน่วยงานหรือระบบที่ทำหน้าที่ พิสูจน์และยืนยันตัวตน ของผู้ขอใช้บริการ

7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

การพิสูจน์และยืนยันตัวตนทางดิจิทัล

การยืนยันตัวตน

เป็นกระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนนั้นจริง

1. ผู้ใช้บริการขอทำธุรกรรมกับ RP
2. RP ให้ผู้ใช้บริการไปยืนยันตัวตนกับ IdP
3. IdP ตรวจสอบสิ่งที่ใช้ยืนยันตัวตน และส่งผลให้กับ RP
4. ผู้ใช้บริการเข้าใช้งานที่ RP

หมายเหตุ RP (RELYING PARTY) หมายถึง บุคคลหรือหน่วยงานซึ่งให้บริการทำธุรกรรม

7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

ลายมือชื่ออิเล็กทรอนิกส์ หรือ E-SIGNATURE

คือ อักษร ตัวเลข เสียง หรือสัญลักษณ์อื่นใดที่ใช้ประกอบข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคล ผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่า บุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น โดยต้องสามารถระบุตัวบุคคลที่ลงนามและแสดงเจตนาว่ายอมรับข้อความในเอกสารได้ ซึ่งมีกฎหมายไทยรองรับให้มีผลทางกฎหมายเช่นเดียวกับการเซ็นบนเอกสารกระดาษ และยังสามารถแบ่งเป็นประเภทต่างๆ ได้ตามระดับความน่าเชื่อถือและความปลอดภัย

รูปแบบลายมือชื่อที่มีผลทางกฎหมาย ในมาตราที่ 9 ได้อธิบายถึงผลทางกฎหมายเมื่อทำการลงลายมือชื่อ ดังนี้

- สามารถระบุตัวคนได้ว่าใครเป็นใคร
- สามารถระบุเจตนาของการเซ็นเอกสารได้ เช่นการลงลายมือชื่อเพื่อเปิดบัญชีธนาคาร หรือการลงลายมือชื่อเพื่อยอมรับข้อตกลง เป็นต้น
- จะต้องเป็นการลงลายมือชื่อด้วยวิธีการที่น่าเชื่อถือ

ลายมือชื่ออิเล็กทรอนิกส์สามารถเป็นได้หลายรูปแบบ เช่น

- การพิมพ์ชื่อ : การใส่ชื่อตัวเองไว้ในส่วนท้ายของเนื้อหาอีเมล
- รูปภาพลายเซ็น : การสแกนลายเซ็นที่เขียนด้วยมือและนำไปแนบกับเอกสารอิเล็กทรอนิกส์
- การคลิกยอมรับ : การกดปุ่มเพื่อตกลงหรือยอมรับในแบบฟอร์มต่างๆ
- การใช้สไตลัส : การใช้ปากกา (stylus) เขียนลายเซ็นด้วยมือลงบนหน้าจอและบันทึกเป็นรูปแบบอิเล็กทรอนิกส์
- ลายมือชื่อดิจิทัล (Digital Signature) : เป็นลายมือชื่ออิเล็กทรอนิกส์ขั้นสูงที่ใช้กระบวนการเข้ารหัสเพื่อยืนยันตัวตนและตรวจจับการเปลี่ยนแปลงของข้อมูล

7) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานว่าด้วยดิจิทัลไอดี

ประเภทของลายมือชื่ออิเล็กทรอนิกส์แบ่งออกเป็น 3 ประเภทตามระดับความเชื่อถือ

- ประเภทที่ 1: ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป คือ รูปแบบอิเล็กทรอนิกส์ของอักษร อักขระ ตัวเลข เสียง หรือสัญลักษณ์อื่น ๆ ที่ใช้เพื่อระบุตัวตนและแสดงความสัมพันธ์กับข้อมูลอิเล็กทรอนิกส์ โดยกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ไทยรองรับให้มีผลทางกฎหมายเช่นเดียวกับลายมือชื่อบนกระดาษ ตัวอย่างเช่น การพิมพ์ชื่อท้ายอีเมล การสแกนลายมือชื่อจริง การใช้ปากกา stylus เขียนลงบนหน้าจอ หรือการคลิกปุ่ม "ยอมรับ" ในแบบฟอร์มออนไลน์
- ประเภทที่ 2: ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ คือ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะที่กำหนดตามมาตรา 26 ของ พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งหมายถึง ข้อมูลที่ใช้สร้างลายมือชื่อที่เชื่อมโยงกับเจ้าของลายมือชื่อ ควบคุมโดยเจ้าของ และสามารถตรวจจับการเปลี่ยนแปลงได้ทั้งตัวลายมือชื่อและเนื้อหา. ประเภทที่พบได้ทั่วไปคือ ลายมือชื่อดิจิทัล (Digital Signature) ซึ่งใช้เทคโนโลยี PKI เพื่อรักษาความปลอดภัยของเอกสารและยืนยันตัวตน
- ประเภทที่ 3: ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง (CA) เป็นรูปแบบที่ใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง (CA) คือ ลายมือชื่อดิจิทัล (Digital Signature) ซึ่งเป็นประเภทที่มีความปลอดภัยสูงสุด ถูกสร้างขึ้นจากการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์โดยอาศัย ใบรับรองอิเล็กทรอนิกส์ ที่ออกโดยผู้ให้บริการออกใบรับรอง (CA) เพื่อยืนยันตัวตนของผู้ลงนาม และรักษาความครบถ้วนสมบูรณ์ของข้อมูล ทำให้สามารถตรวจสอบได้ว่าใครเป็นผู้ลงนาม และข้อมูลถูกเปลี่ยนแปลงหรือไม่ ถือเป็นลายมือชื่อที่มั่นคงปลอดภัยและได้รับการยอมรับตามกฎหมายธุรกรรมทางอิเล็กทรอนิกส์


Thank You!