การสัมมนาเพื่อพัฒนานวัตกรรมการอำนวยความยุติธรรม
เรื่อง “การทำเอกสารและลงลายมือชื่ออิเล็กทรอนิกส์ : โอกาสและความท้าทายของศาลบนเส้นทางของความเปลี่ยนแปลง”
ผ่านระบบถ่ายทอดสัญญาณภาพและเสียง (Streaming) และ Facebook Live เพจสื่อศาล
วันพฤหัสบดีที่ 28 พฤษภาคม 2563 ณ ศูนย์วิทยบริการศาลยุติธรรมเฉลิมพระเกียรติ ชั้น 6 อาคารศาลอาญา

หลักการและเหตุผล

ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) เป็นลายเซ็นที่อยู่ในรูปแบบของอิเล็กทรอนิกส์เป็นข้อความที่ส่งไปเพื่อเป็นการแสดงตัวตนในการพิสูจน์ว่าใครเป็นคนเซ็นเอกสารและสามารถตรวจสอบได้ว่าข้อมูลที่ได้รับมาไม่ได้มีการดัดแปลงหรือแก้ไข ทำให้เกิดความสบายใจ ความเชื่อถือในการปกป้องข้อมูล และปกป้องสิทธิจากบุคคลที่จงใจจะทำผิดสัญญา ในกรณีที่มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ทำธุรกรรมทางอิเล็กทรอนิกส์ แล้วมีการทำผิดสัญญาสามารถใช้ลายมือชื่ออิเล็กทรอนิกส์เป็นหลักฐานในการเอาผิดทางกฎหมายได้ ในปัจจุบันการทำธุรกรรมทางอิเล็กทรอนิกส์ได้เข้ามีบทบาทสำคัญทั้งในภาครัฐ และภาคเอกชน ซึ่งได้มีมติคณะรัฐมนตรีในวันที่ 2 เมษายน 2562 เรื่อง “การออกเอกสารหลักฐานของทางราชการผ่านระบบดิจิทัล” เพื่อให้การพัฒนางานบริการภาครัฐให้เป็นระบบการให้บริการอิเล็กทรอนิกส์ รวมทั้งการออกเอกสารของทางราชการผ่านระบบอิเล็กทรอนิกส์ให้มีมาตรฐานในการดำเนินงานในแนวทางเดียวกัน และเกิดผลอย่างเป็นรูปธรรมต่อไป อย่างไรก็ตามจากรายงานผลการสำรวจความคิดเห็นโครงการ เรื่อง “การนำ Digital Signature มาใช้เพื่อสนับสนุนการบริหารงานธุรการศาลยุติธรรม” ของสถาบันวิจัยและพัฒนารพีพัฒนศักดิ์ โดยรวบรวมข้อมูลจากหน่วยงานศาลยุติธรรมทั่วประเทศ พบว่า ผู้ตอบแบบสำรวจส่วนใหญ่เห็นด้วยในการนำลายเซ็นอิเล็กทรอนิกส์มาใช้ในงานธุรการศาลยุติธรรม ร้อยละ 87.8 ส่วนที่เหลือไม่เห็นด้วยในการนำลายเซ็นอิเล็กทรอนิกส์มาใช้ในงานธุรการศาลยุติธรรม ร้อยละ 12.2 เนื่องจากเห็นว่าไม่มีความปลอดภัย

ดังนั้น สถาบันวิจัยและพัฒนารพีพัฒนศักดิ์ในฐานะมีบทบาทหน้าที่สำคัญในการจัดทำการวิจัยและพัฒนาระบบงานของศาลยุติธรรมเพื่อสร้างองค์ความรู้ในงานธุรการของศาลยุติธรรม งานส่งเสริมงานตุลาการและงานวิชาการ สนับสนุนและอำนวยความสะดวกในการปฏิบัติภารกิจของศาลยุติธรรมให้สอดคล้องกับนโยบายประธานศาลฎีกา ในข้อ 3 นำเทคโนโลยีมาสนับสนุนการอำนวยความยุติธรรมการพิจารณาพิพากษาคดี และการมีส่วนร่วมของประชาชน โดยคำนึงถึงช่องทางอื่นที่สะดวกและประหยัดสำหรับประชาชนที่ยังไม่สามารถเข้าถึงเทคโนโลยีได้ รวมทั้งแผนยุทธศาสตร์ศาลยุติธรรม พ.ศ. 2561 – 2564 ยุทธศาสตร์ E Excellence Organization เพิ่มศักยภาพองค์กรสู่ความเป็นเลิศ โดยศาลยุติธรรมวางเป้าหมายการพัฒนาให้เป็น D-Court (ดิจิทัลคอร์ท) ในปี พ.ศ.2563 จึงเห็นความสำคัญในการจัดสัมมนา เรื่อง “การทำเอกสารและลงลายมืออิเล็กทรอนิกส์ : โอกาสและความท้าทายของศาลบนเส้นทางของความเปลี่ยนแปลง” เพื่อให้ข้าราชการฝ่ายตุลาการศาลยุติธรรม และบุคลากรในสังกัดสำนักงานศาลยุติธรรมได้รับความรู้ ความเข้าใจเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์และเพื่อให้มีความรู้ ความเข้าใจเกี่ยวกับความน่าเชื่อถือในการใช้ลายมือชื่ออิเล็กทรอนิกส์ในการทำธุรกรรมทางอิเล็กทรอนิกส์และการทำเอกสารของทางราชการผ่านระบบอิเล็กทรอนิกส์ รวมถึงหากเกิดข้อพิพาทเกี่ยวกับการใช้ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) จะสามารถนำมาใช้เป็นพยานหลักฐานหรือไม่เพียงใด

วัตถุประสงค์

1. เพื่อให้ข้าราชการฝ่ายตุลาการศาลยุติธรรม และบุคลากรในสังกัดสำนักงานศาลยุติธรรมได้รับความรู้ ความเข้าใจเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์

2. เพื่อให้มีความรู้ ความเข้าใจเกี่ยวกับความน่าเชื่อถือในการใช้ลายมือชื่ออิเล็กทรอนิกส์ในการทำธุรกรรมทางอิเล็กทรอนิกส์และการทำเอกสารของทางราชการผ่านระบบอิเล็กทรอนิกส์ รวมถึงหากเกิดข้อพิพาทเกี่ยวกับการใช้ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) จะสามารถนำมาใช้เป็นพยานหลักฐานหรือไม่เพียงใด

ประโยชน์ที่คาดว่าจะได้รับ

ข้าราชการฝ่ายตุลาการศาลยุติธรรม บุคลากรในสังกัดสำนักงานศาลยุติธรรม และผู้สนใจได้รับความรู้ ความเข้าใจเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ และได้รับความรู้ ความเข้าใจเกี่ยวกับความน่าเชื่อถือในการใช้ลายมือชื่ออิเล็กทรอนิกส์ในการทำธุรกรรมทางอิเล็กทรอนิกส์ และการทำเอกสารของทางราชการผ่านระบบอิเล็กทรอนิกส์ รวมถึงหากเกิดข้อพิพาทเกี่ยวกับการใช้ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) จะสามารถนำมาใช้เป็นพยานหลักฐานหรือไม่เพียงใด

สรุปผลการสัมมนา

การสัมมนาเพื่อพัฒนานวัตกรรมการอำนวยความยุติธรรม เรื่อง “การทำเอกสารและลงลายมือชื่ออิเล็กทรอนิกส์ : โอกาสและความท้าทายของ ศาลบนเส้นทางของความเปลี่ยนแปลง” มีวัตถุประสงค์เพื่อให้ข้าราชการฝ่ายตุลาการศาลยุติธรรมและบุคลากรในสังกัดสำนักงานศาลยุติธรรมได้รับความรู้ ความเข้าใจเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ ความน่าเชื่อถือในการใช้ลายมือชื่ออิเล็กทรอนิกส์ในการทำธุรกรรมทางอิเล็กทรอนิกส์ และการทำเอกสารของทางราชการผ่านระบบอิเล็กทรอนิกส์ รวมถึงหากเกิดข้อพิพาทเกี่ยวกับการใช้ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) จะสามารถนำมาใช้เป็นพยานหลักฐานหรือไม่เพียงใด โดยมี ดร. ไกรพล อรัญรัตน์ ผู้พิพากษาศาลจังหวัดนครราชสีมา ช่วยทำงานชั่วคราวในตำแหน่งผู้พิพากษาศาลแพ่ง นายโอวาท โอวาทตระกูล CTO บริษัท ครีเดนเอเชีย จำกัด และนายธีรวุฒิ จันทดิษฐ์ กรรมการผู้จัดการ บริษัท 9 ดิจิตอล จำกัด เป็นวิทยากร ซึ่งสามารถสรุปผลการสัมมนาได้ดังนี้

1. ความตื่นตัวของหน่วยงานภาครัฐและภาคเอกชนเกี่ยวกับการจัดทำเอกสารอิเล็กทรอนิกส์

ดร. ไกรพล อรัญรัตน์ ความตื่นตัวของหน่วยงานภาครัฐเกี่ยวกับการจัดทำเอกสารอิเล็กทรอนิกส์มีมากขึ้น เช่น ในโรงพยาบาลหลายๆ ที่ และกรมสรรพากรมีการนำระบบเอกสารอิเล็กทรอนิกส์มาใช้มากขึ้น

นายโอวาท โอวาทตระกูล ในช่วงสถานการณ์โควิด 19 หน่วยงานภาครัฐมีความตื่นตัวมากขึ้น เช่น กรมพัฒนาที่ดินเริ่มให้พนักงานทำงานที่บ้าน (Work From Home) บางโรงพยาบาลก่อนช่วงสถานการณ์โควิด 19 ยังไม่มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) แต่ช่วงเกิดสถานการณ์โควิด 19 ได้มีการผลักดันให้ใช้มากขึ้น

ดร. ไกรพล อรัญรัตน์ ในสำนักงานศาลยุติธรรมมีการนำระบบการลงลายมือชื่ออิเล็กทรอนิกส์และเอกสารอิเล็กทรอนิกส์มาใช้ในหน่วยงาน ซึ่งเห็นได้จากระบบการยื่นและส่งคำคู่ความและเอกสาร (e-Filing) ทั้งนี้ ระบบการลงลายมือชื่ออิเล็กทรอนิกส์และเอกสารอิเล็กทรอนิกส์จะไม่หยุดนิ่งแค่การนำไปใช้ในระบบ e-Filing ในอนาคตอาจจะมีการนำไปใช้ในระบบงานธุรการ และระบบงานศาลต่าง ๆ เทคโนโลยีไม่มีทางที่จะใช้น้อยลง มีแต่จะพัฒนาเทคโนโลยีต่อไปเรื่อย ๆ

2. ความเสี่ยงและข้อท้าทายในการนำเทคโนโลยีและเอกสารอิเล็กทรอนิกส์มาใช้

ดร. ไกรพล อรัญรัตน์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ได้รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเตอร์เน็ตในประเทศไทย พบว่า สัดส่วนผู้ใช้อินเทอร์เน็ตร้อยละ 70 จากประชากร 70 ล้านคน ซึ่งหากเปรียบเทียบเทียบเมื่อ 10 ปีที่แล้วมีสัดส่วนผู้ใช้อินเทอร์เน็ตแค่ร้อยละ 20 เพิ่มขึ้นมากกว่าร้อยละ 50 รวมทั้งประชากรในประเทศใช้อินเทอร์เน็ตเฉลี่ยวันละ 10 ชั่วโมง 22 นาที และช่วงวัยของประชากรที่ใช้อินเทอร์เน็ตมากที่สุดจะเป็นช่วงวัย Generation Y อายุประมาณ 20 - 40 ปี ใช้อินเทอร์เน็ตประมาณ 10 ชั่วโมง 36 นาที ส่วน Generation X อายุประมาณ 40 - 50 ปี ใช้อินเทอร์เน็ตประมาณ 9 ชั่วโมง และวัยหลังเกษียณ Baby Boomer อายุประมาณ 55 - 73 ปี ใช้อินเทอร์เน็ตประมาณ 10 ชั่วโมง สิ่งนี้แสดงให้เห็นว่าวัยทำงานจะใช้อินเทอร์เน็ตมากกว่าวัยอื่น และทำให้เห็นว่าอินเทอร์เน็ตเข้ามามีบทบาทที่สำคัญในการใช้ชีวิตในปัจจุบันนี้ เช่น การทำธุรกรรมทางการเงินผ่านระบบอิเล็กทรอนิกส์ เพราะฉะนั้นหน่วยงานของรัฐที่ทำหน้าที่การจัดทำบริการสาธารณะต้องเข้าสู่โลกอินเทอร์เน็ตโดยเฉพาะอย่างยิ่งช่วงเกิดสถานการณ์โควิด 19 เป็นสิ่งที่ทำให้รัฐต้องหาทางดำเนินการขับเคลื่อนกลไกของรัฐให้ดำเนินต่อไปได้โดยที่ต้องทำงานที่บ้าน (Work From Home) ซึ่งในหลายหน่วยงานได้ประชุมผ่านระบบการประชุมทางไกล (Teleconference) และการประชุมทางวีดิโอผ่านจอภาพ (Video conference) เช่น การประชุมออนไลน์ Zoom หรือการประชุมออนไลน์ผ่าน Google Hangouts มาใช้ในการประชุมของหน่วยงาน เป็นต้น อย่างไรก็ตามการประชุมออนไลน์ยังไม่เพียงพอที่จะขับเคลื่อนกลไกต่าง ๆ

เนื่องจากต้องมีการลงนามสั่งการเพื่อที่จะขับเคลื่อนองค์กรให้ดำเนินต่อไป จึงทำให้การจัดทำเอกสารอิเล็กทรอนิกส์และลงลายมือชื่ออิเล็กทรอนิกส์เข้ามามีบทบาทสำคัญซึ่งการลงลายมือชื่ออิเล็กทรอนิกส์มีหลายรูปแบบ เช่น ลงลายมือชื่อรับสินค้าจากบริษัทขนส่งเคอรี่ เอ็กซ์เพรสถือว่าเป็นรูปแบบหนึ่งการลงลายมือชื่ออิเล็กทรอนิกส์ เซ็นลายเซ็นของตนเองลงในกระดาษแล้วถ่ายรูปเก็บเป็นไฟล์ไว้ในคอมพิวเตอร์ และนำไฟล์ลายเซ็นนั้นไปวางไว้ในเอกสาร และการคลิกส่งคำรับฟ้องในระบบ e-Filing หลังจากที่ตรวจคำคู่ความเรียบร้อยแล้ว ก็ไม่ได้เซ็นด้วยปากกาแต่การคลิกก็เป็นการลงลายมือชื่ออิเล็กทรอนิกส์ได้ ซึ่งจะเห็นได้ว่ารูปแบบการลงลายมือชื่ออิเล็กทรอนิกส์มีหลากหลาย

นายธีรวุฒิ จันทดิษฐ์ ได้อภิปรายในประเด็นเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) ซึ่งมีรายละเอียด ดังนี้

1) กฎหมายที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ของประเทศไทย

- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 ประกอบด้วยประกาศคณะกรรมการทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. 2562 ประกาศคณะกรรมการทางอิเล็กทรอนิกส์ เรื่อง การรับรองสิ่งพิมพ์ออก พ.ศ. 2555 ประกาศคณะกรรมการทางอิเล็กทรอนิกส์ เรื่อง หน่วยงานรับรองสิ่งพิมพ์ออก พ.ศ. 2555 ประกาศคณะกรรมการทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553 และประกาศคณะกรรมการทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. 2552
- พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรม
- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐพ.ศ. 2549 ประกอบด้วยประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ (ฉบับที่ 2) พ.ศ. 2556 ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 และประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ. 2553
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 ประกอบด้วยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

2) หลักการของลายเซ็นอิเล็กทรอนิกส์

คำนิยามเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 ได้นิยามไว้ว่า เป็นอักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์ ที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ถือได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์เหมือนกัน รวมทั้งต้องดูคำนิยามตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 3 พ.ศ. 2563 มาตรา 9 ประกอบด้วยว่าลายมือชื่ออิเล็กทรอนิกส์ต้องสามารถระบุตัวเจ้าของลายมือชือได้ว่าใครเป็นคนลงลายมือชือ ต้องมีวิธีการน่าเชื่อถือ มีความปลอดภัยโดยต้องมีศักยภาพเพียงพอ มีความน่าเชื่อถือ มีความเหมาะสมต่อธุรกรรมนั้น ๆ และสามารถแสดงเจตนาของเจ้าของลายมือชือ เช่น ถ้าเอารูปไปวางสแกนส่งไปทีจดหมายอิเล็กทรอนิกส์ (electronic mail) อาจจะไม่มีความน่าเชื่อถือเพียงพอ ซึ่งลายมือชื่อถืออิเล็กทรอนิกส์ที่เชื่อถือได้ต้องพิจารณาตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 26 ลายมือชื่ออิเล็กทรอนิกส์สามารถเชื่อมโยงกับเจ้าของลายมือชื่อได้ และสามารถจะบอกการเปลี่ยนแปลงของข้อมูลได้ ซึ่งในส่วนนี้จะประกอบมาตรา 28 และมีการใช้กระบวนการเข้ารหัสข้อมูลอิเล็กทรอนิกส์ซึ่งจะเรียกว่าลายมือชื่อดิจิทัล (Digital Signature)

ในทางกฎหมายลายมือชื่ออิเล็กทรอนิกส์ ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ และลายมือชื่อดิจิทัลไม่มีความแตกต่างกัน แต่จะมีความแตกต่างในทางวิธีการใช้งานซึ่งในทั่วไปจะเรียกลายมือชื่ออิเล็กทรอนิกส์ ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ และลายมือชื่อดิจิทัลว่า “ลายมือชื่ออิเล็กทรอนิกส์” ทั้งนี้ ลายมือชื่อดิจิทัลจะยากที่สุดของการลงลายมือชื่อดิจิทัลเนื่องจากลายมือชื่อดิจิทัลต้องมีการเข้ารหัส รหัสถูกสร้างจากบุคคลอื่น

ดร. ไกรพล อรัญรัตน์ เมื่อพิจารณานิยามตามกฎหมายลายมือชื่ออิเล็กทรอนิกส์จะมีความหมายที่กว้างมาก แต่ไม่ใช่ลายมือชื่ออิเล็กทรอนิกส์ทุกประเภทที่จะเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หากจะเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้จะต้องสามารถจะบ่งบอกได้ว่าใครเป็นเจ้าของ และระบบนั้นต้องบอกการเปลี่ยนแปลงของข้อมูลได้

นายโอวาท โอวาทตระกูล ตัวอย่างของรูปแบบลายมือชื่ออิเล็กทรอนิกส์ เมื่อเข้าสู่ระบบของผู้ใช้งานจะมีปุ่มยอมรับหรือตกลงหรือทำเครื่องหมาย เช่น การโอนเงินในแอพพลิเคชั่นของธนาคารจะมีการใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP) และนำรหัสที่ได้รับกรอกใส่ในแอพพลิเคชั่นของธนาคารบนโทรศัพท์มือถือ หลังจากนั้นจะมีปุ่มให้กดยอมรับการทำธุรกรรมซึ่งถือได้ว่าเป็นการลงลายมืออิเล็กทรอนิกส์อีกรูปแบบหนึ่ง

3) การพิสูจน์และยืนยันตัวตน

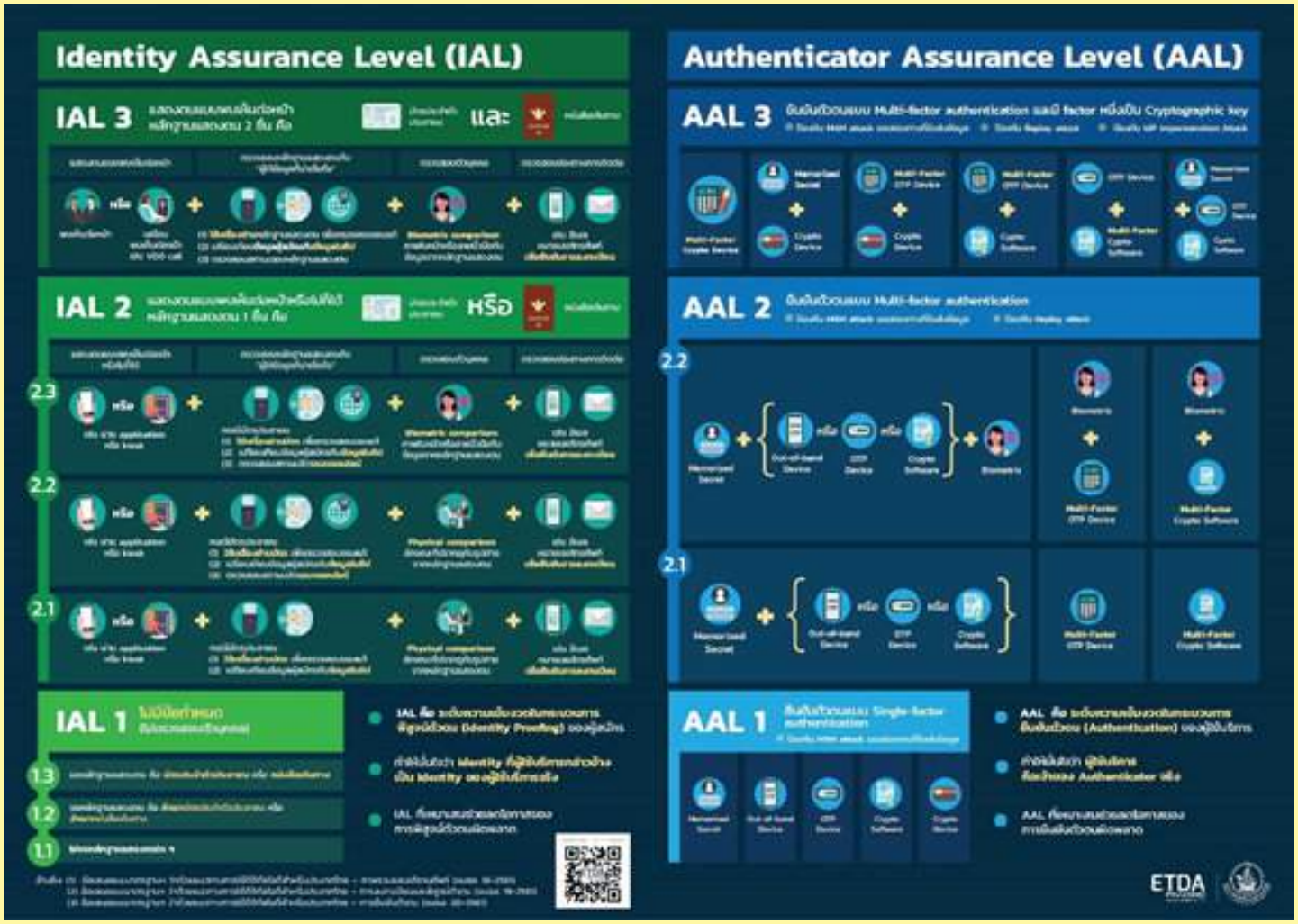
นายธีรวุฒิ จันทดิษฐ์ การพิสูจน์และยืนยันตัวตนจะประกอบได้สองส่วน คือ

- การใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) จะประกอบด้วยลายมือชื่ออิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 26 และมาตรา 28 และ
- การพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)

นายโอวาท โอวาทตระกูล ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เป็นการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public Key Infrastructure : PKI) ผู้ที่เซ็นเอกสารหรือทำเอกสารจะทำได้เมื่อมีเลขส่วนบุคคลของตัวเอง เช่น การทำธุรกรรมทางระบบอิเล็กทรอนิกส์ ต้องมีการยืนยันตัวตนก่อนในวิธีที่มีความเชื่อถือได้ อาจจะใช้ระบบยืนยันตัวตนจากการเสียบบัตรประชาชนจะได้ข้อมูลของแต่ละบุคคลเก็บไว้ เป็นการลงลายมือชื่อในเอกสารที่เชื่อถือได้ ข้อมูลต่าง ๆ ที่ได้รับมีความถูกต้องครบถ้วน ไม่ถูกเปลี่ยนแปลงแก้ไข สามารถพิสูจน์ และยืนยันตัวบุคคลได้ว่าเป็นบุคคลผู้ที่เราติดต่อด้วยจริง

นายธีรวุฒิ จันทดิษฐ์ การพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) เป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 รวมทั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ได้มีมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย จึงได้มีการกำหนดข้อแนะนำระดับการกำหนดการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยแบ่งออกเป็นระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน (IAL) และระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) เป็นกระบวนการเข้าสู่ระบบก่อนไปเซ็นเอกสาร เช่น User และPassword ในการ Login เข้าระบบถือได้ว่าเป็นสิ่งใช้ยืนยันตัวตนรูปแบบหนึ่ง

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ได้มีการกำหนดมาตรฐานแนวทางและข้อแนะนำควรที่จะใช้ความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน (IAL) อยู่ในระดับ 2 และความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) อยู่ในระดับ 2 เช่นกัน ซึ่งจะให้แต่ละหน่วยงานนำไปปรับใช้ในหน่วยงานเอง ซึ่งธนาคารจะนำไปปรับใช้ในการทำธุรกรรมซึ่งส่วนใหญ่จะใช้ IAL 2.2 และ 2.3 ซึ่งขึ้นอยู่กับระดับธุรกรรม ส่วนบริษัทหลักทรัพย์จะใช้ IAL 2.2 การตรวจสอบบัตรประชาชนเป็นเอกสารของจริงหรือของปลอม มีความน่าเชื่อถือขนาดไหน และนำข้อมูลที่ได้มาตรวจสอบความถูกต้องอีกรอบ ส่วน AAL 2 เป็นการเข้าสู่ระบบซึ่ง User และ Password ในการ Login เข้าระบบยังไม่มีความน่าเชื่อถือเท่าที่ควร จึงต้องมีการใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP) มายืนยันการเข้าระบบให้มีความน่าเชื่อถือยิ่งขึ้น



ดร. ไกรพล อรัญรัตน์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ได้มีการเก็บสถิติเกี่ยวกับรูปแบบการยืนยันตัวบุคคลว่ารูปแบบไหนที่ประชาชนคุ้นเคยที่สุด ซึ่งผลการสำรวจพบว่ารูปแบบการยืนยันตัวบุคคลที่ประชาชนคุ้นเคยมีหลายรูปแบบ เช่น การใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP) รหัสลับ กรอกเลขบัตรเครดิต หรือเลขหลังบัตรเครดิต กรอกเลขบัตรประชาชน การตั้งรหัส การให้ข้อมูลส่วนบุคคลต่าง ๆ สำหรับรูปแบบที่ประชาชนคุ้นเคยมากที่สุด คือ การใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP) ซึ่งเมื่อส่งข้อความไปแล้ว ก็จะได้รับข้อความจากทางโทรศัพท์เคลื่อนที่มาให้กรอกตัวเลขที่ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งส่วนใหญ่ผู้ใช้อินเทอร์เน็ตร้อยละ 91.6 เคยผ่านประสบการณ์การใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP)

4) องค์ประกอบการลงลายมือชื่ออิเล็กทรอนิกส์

นายธีรวุฒิ จันทดิษฐ์ องค์ประกอบการลงลายมือชื่ออิเล็กทรอนิกส์ตามหลักมาตรฐานสากลทางฝั่งอเมริกาและยุโรปที่ใช้เป็นหลักในการตรวจพิสูจน์ว่าลายมือชื่อนี้มีความน่าเชื่อถือตามกฎหมายและตามมาตรฐาน มีดังนี้

- รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ (Electronic Form of Signature) รูปแบบลายมือชื่ออิเล็กทรอนิกส์ เช่น การใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP) และกดปุ่มยอมรับ หรือการกรอกรหัสต่าง ๆ รูปแบบนี้มีความเหมาะสมที่จะลงลายมือชื่อในการทำธุรกรรมประเภทนั้นหรือไม่ การที่จะพิจารณาการลงลายมือชื่อที่เหมาะสม อาจจะใส่ชื่อในท้ายจดหมายอิเล็กทรอนิกส์ หรือใช้รหัสผ่านหรือรหัสลับ(PIN) และกดปุ่มยอมรับ

- การพิสูจน์และยืนยันตัวตน (Identification & Authentication) ต้องพิสูจน์ได้ว่าใครเป็นบุคคลลงลายมือชื่อนั้น ซึ่งเป็นไปตามกฎหมายที่มีการระบุไว้ และสามารถเชื่อมโยงเจ้าของลายมือชื่อได้ รวมทั้งพิสูจน์ได้ว่า "ใคร" เป็นผู้ลงลายมือชื่อนั้น

- การเชื่อมโยงข้อมูลกับลายมือชื่อ (Association of Signature to the Record) เจ้าของลายมือชื่อต้องเข้าใจว่ากำลังลงลายมือชื่อ เพื่อรับรองข้อความใด และมีโอกาสทบทวนข้อความที่กำลังลงลายมือชื่อได้ ซึ่งเกี่ยวข้องกับรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ และการพิสูจน์และยืนยันตัวตน หลังจากนั้นการเชื่อมโยงต้องไม่ทำให้ผู้ใช้สับสนในการลงลายมือชื่อและต้องให้ผู้ใช้ทบทวนลายมือชื่อได้ กล่าวได้ว่าไม่ว่าจะเป็นการกดหรือการวาดรูป หรือลงลายมือชื่อ ต้องสามารถกลับมาทบทวนได้อีกครั้งก่อนเสร็จสิ้น

- การแสดงเจตนาในการลงลายมือชื่อ (Intent to Sign) ต้องไม่มีการหลอกให้ผู้ใช้กดยอมรับด้วยการวาดรูปหรือลงลายมือชื่อ ต้องแสดงให้เห็นถึงเจตนาในการรับรองข้อมูลนั้นจริง เช่น การคลิกยอมรับข้อตกลงการใช้วัตถุประสงค์หรือมีบริบทในการลงลายมือชื่อที่ชัดเจน เช่น การลงลายมือชื่อรับรองสัญญา

- การรักษาความครบถ้วนของข้อมูล (Integrity of the Signed Record) ข้อมูลที่ลงลายมือชื่อต้องไม่มีการแก้ไขข้อความใด ๆ หลังจากที่ลงลายมือชื่อ มีการรับรองความครบถ้วนแล้ว และมีการประทับรับรองเวลา (Time Stamp)

ดร. ไกรพล อรัญรัตน์ องค์ประกอบการลงลายมือชื่ออิเล็กทรอนิกส์ที่เป็นตามหลักสากล สามารถสรุปได้ ดังนี้ 1) ระบบต้องอยู่ในรูปแบบที่น่าเชื่อถือมิใช่ว่าจะเป็นระบบอะไรก็ได้ 2) ต้องสามารถพิสูจน์และยืนยันตัวตนของผู้ใช้งานในระบบได้ 3) ต้องสามารถเชื่อมโยงได้ว่าใครเป็นคนลงลายมือชื่อ 4) แสดงให้เห็นเจตนา และ 5) สามารถรักษาความครบถ้วนของข้อมูลได้ ซึ่งเป็นองค์ประกอบที่ต้องพิจารณา

นายโอวาท โอวาทตระกูล ตัวอย่างลักษณะหนึ่งของการพิสูจน์ตัวตนของลายมือชื่ออิเล็กทรอนิกส์ มีขั้นตอนดังนี้ 1) การยืนยันตัวตนโดยการใช้ระบบการเสียบบัตรประชาชน อ่านข้อมูลจากบัตรประชาชนเพื่อดูว่าเป็นของจริง 2) ส่งข้อมูลไปตรวจสอบกับกรมการปกครองจะประมวลผลข้อมูลได้ทันทีเพื่อให้แน่ใจว่าบัตรยังมีสถานะการใช้งานได้อยู่ไม่ได้โดนเก็บมาหรือมีการแจ้งหาย 3) หลังจากนั้นต้องเทียบใบหน้าที่อ่านมาจากในบัตร กับบุคคลที่กำลังจะเซ็นจริง ๆ ว่าใบหน้าที่อ่านในบัตรเป็นหน้าตาอย่างไรเป็นบุคคลเดียวกันกับบุคคลที่อ้างอิงหรือไม่ คือการพิสูจน์และยืนยันตัวตน

นายธีรวุฒิ จันทดิษฐ์ รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ (Electronic Form of Signature) จะเป็นรูปแบบไหนก็ได้ แต่ต้องมีความเหมาะสม การที่ใส่ลายมือชื่อจริง ข้อมูลจริงไปในท้ายจดหมายอิเล็กทรอนิกส์ถือว่าเป็นการลงลายมือชื่อเหมือนกัน แต่ต้องดูว่ามีความเหมาะสมกับการทำธุรกรรมนั้นหรือไม่ และอีกแบบหนึ่งคือการยืนยันตัวตน การพิสูจน์และยืนยันตัวตนในการเชื่อมโยงข้อมูลกับลายมือชื่อ (Association of Signature to the Record) วิธีที่ง่ายที่สุด คือ การออกเป็นใบรับรองให้ที่หน้าสุดท้ายในเอกสารที่มีการเซ็นหรือที่มีการลงลายมือชื่อทางอิเล็กทรอนิกส์ โดยแสดงรายละเอียดว่าใครเป็นผู้ที่มีส่วนที่เกี่ยวข้องกับเอกสาร

อิเล็กทรอนิกส์ฉบับนี้บ้าง มีเลข IP อะไร จดหมายอิเล็กทรอนิกส์อะไร วันและเวลาไหน และเจตนาในการลงลายมือชื่อ (Intent to Sign) ต้องทำให้ชัดเจนว่า ผู้ที่เซ็นมีเจตนาที่จะลงลายมือชื่อในข้อความในเอกสารตรงนี้ในเนื้อหาตรงนี้ ไม่ใช่ว่าลายมือชื่อไปอยู่อีกหน้าหนึ่งแล้วเอกสารไปอยู่อีกหน้าหนึ่ง

กรณีการลงลายมือชื่อเอกสารราชการที่อยู่ในหน้าสุดท้ายของเอกสารราชการ และจะมีคำต่อท้ายของหน้าต่อไปว่าขึ้นต้นด้วยอะไรบ้าง กล่าวได้ว่าต้องมีการแสดงเจตนาที่ชัดเจน ตัวถัดมาต้องบอกว่า ต้องไม่มีการแก้ไขข้อความได้ แล้ววิธีที่จะรู้ได้ว่ามีการแก้ไขหรือไม่แก้ไขเอกสาร คือ การเปิดโปรแกรม Adobe Acrobat เพราะว่าการลงลายมือชื่ออิเล็กทรอนิกส์ ส่วนใหญ่ใช้ไฟล์ PDF เป็นนามสกุล สามารถเปิดโปรแกรมแล้วดูได้เลย จะมีด้านข้างที่บอกว่า Panel Signature ที่มีการใช้จะเป็นตัวสีเขียว แต่ถ้ามีการแก้ไขจะขึ้นเป็นตัวสีแดง หรือว่าในปัจจุบันนี้ต้องเป็น Blockchain ซึ่งสามารถใช้ในการตรวจสอบได้ อีกตัวอย่างหนึ่ง คือ การลงประทับเวลาเอกสารทางอิเล็กทรอนิกส์ (e-Timestamp) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ซึ่งกรมสรรพากรก็นำมาใช้ สามารถนำเอกสารที่มีการใช้ระบบนี้มาตรวจสอบในระบบของ ETDA ได้

5) การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์

นายธีรวุฒิ จันทดิษฐ์ การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์เป็นส่วนสำคัญ เนื่องจากลายมือชื่ออิเล็กทรอนิกส์ต้องมีความน่าเชื่อถือ มีความเหมาะสมกับขนาดของการทำธุรกรรม โดยต้องพิจารณาจากองค์ประกอบอย่างน้อย 5 ข้อได้กล่าวมาข้างต้น ส่วนที่เหลือเป็นเรื่องของมั่นคงความปลอดภัยของระบบ เรื่องประเภท ขนาดของธุรกรรม และมูลค่าของธุรกรรม บางครั้งถ้ามูลค่าของธุรกรรมสูงๆ อาจก็จะต้องมีระบบในการลงลายมือชื่อที่มีความรัดกุมมากกว่าระบบปกติ เช่น การลงลายมือชื่อทั่ว ๆ ไปจะมีความเสี่ยงสูง แต่ด้วยกระบวนการจะมีความปลอดภัยมาก ตัวอย่างเช่น การทำธุรกรรมที่เกี่ยวกับการเงิน โดยการกดรหัสลับเพียงแค่ 9 ตัว อาจจะมีความเสี่ยงสูง เพราะไม่มีการยืนยัน หรือไม่มีการแสดงเจตนาที่ต้องการทำธุรกรรมจริง ๆ แต่การที่จะได้เลขรหัสลับ 9 ตัว ไม่ได้มาได้ง่าย ต้องไปทำธุรกรรมที่ตู้ ATM หรือทำที่ธนาคาร โดยการใช้บัตร ATM เพื่อยืนยันอีกรอบหนึ่ง โดยทั่วไปอาจมองว่าเป็นความเสี่ยง แต่มีความปลอดภัยสูง

นายโอวาท โอวาทตระกูล ลายมือชื่ออิเล็กทรอนิกส์มีข้อสันนิษฐานทางกฎหมายน้อยกว่าประเภทที่ 2 และ 3 จะได้เปรียบในการทำธุรกรรม เพียงแต่ว่าจะต้องรับความเสี่ยงมากกว่า แต่ถ้าระบบของธนาคารทำระบบไว้ดีแล้ว ทำให้การใช้ตัวเลขเพียงนั้นก็ถือว่ามีความปลอดภัยสูง

6) วิธีในการตรวจสอบเอกสาร

นายธีรวุฒิ จันทดิษฐ์ ลายมือชื่ออิเล็กทรอนิกส์มีความเหมาะสมหรือมีความปลอดภัยขนาดไหน ขึ้นอยู่กับผู้ให้บริการด้วยว่ามีการให้บริการอย่างไร ซึ่งจะสอดคล้องกับวิธีในการตรวจเอกสารว่าจะตรวจสอบอย่างไรบ้าง เช่น วิธีในการตรวจสอบเอกสารแบบ Extensible Markup Language (XML) ซึ่งเป็นระบบแบบเก่า

นายโอวาท โอวาทตระกูล วิธีในการตรวจสอบเอกสารแบบ Extensible Markup Language (XML) เป็น format ที่จะบอกแหล่งที่มา และรายละเอียดข้อมูลได้ ซึ่งเป็นระบบเก่าที่เป็นการสื่อสารทางเว็บเซอร์วิส (Web service) machine-to-machine ทำอย่างไรถึงจะเชื่อถือได้ว่าอีกฝั่งหนึ่งเป็นตัวตนจริง ๆ ก็จะใช้ Digital Certificate ซึ่งเป็นเทคโนโลยีแบบเก่า

นายธีรวุฒิ จันทดิษฐ์ วิธีนี้เป็นการสร้างความยุ่งยากให้กับผู้ใช้เหมือนกัน เนื่องจากต้องมีใบรับรอง (Certificate) ประกอบ ต้องเสียค่าใช้จ่ายสูงทำให้ไม่เป็นนิยม ถึงแม้ว่ากฎหมายจะยอมรับตั้งแต่ปี 2544 แล้ว ต่อมาในปีพ.ศ. 2561 - 2562 มีเรื่องของการพิสูจน์ตัวตนในระบบดิจิทัลขึ้นมา ไม่ต้องใช้ใบรับรอง (Certificate) แบบที่ต้องไปซื้อแล้ว เนื่องจากมีการสร้างใบรับรอง (Certificate) ที่ระบุตัวตนได้เอง ที่เรียกว่าเป็นกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) เป็นการปรับเปลี่ยนวิธีในการพิสูจน์และยืนยันตัวตน และอีกวิธีหนึ่งที่ง่ายที่สุดโดยวิธีในการตรวจสอบเอกสารด้วยโปรแกรม Adobe Acrobat ซึ่งทุกคนก็สามารถเข้าไปตรวจสอบได้ ว่ามีการใช้ลายมือชื่อ ในการลงลายมือชื่อ สามารถตรวจสอบได้เลยว่าเป็นตัวสีแดงหรือตัวสีเขียว ซึ่งเป็นวิธีที่ไม่ซับซ้อนในการพิสูจน์ ส่วนวิธีอื่นนั้นต้องดูลักษณะของรายละเอียดโปรแกรมที่ใช้อีกทีหนึ่งว่าเป็นการใช้ในลักษณะวิธีใดในการตรวจพิสูจน์

7) การรักษาความมั่นคงปลอดภัยทางสารสนเทศ

การรักษาความมั่นคงปลอดภัยทางสารสนเทศถ้าอ้างอิงตามกฎหมาย ได้ดังนี้

- กฎหมายการรักษาความมั่นคงปลอดภัยทางสารสนเทศ
- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และ ฉบับที่ 2 พ.ศ. 2553
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ 2555
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

8) เตรียมพร้อมเพื่อความมั่นคงปลอดภัยของข้อมูล

นายธีรวุฒิ จันทดิษฐ์ สิ่งสำคัญขององค์กรไม่ว่าหน่วยงานรัฐหรือเอกชนที่ต้องมี คือ 1) จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูล 2) กำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแล 3) กำหนดระดับของภัยคุกคามทางไซเบอร์ 4) วิเคราะห์สถานการณ์ และประเมินความเสี่ยงผลกระทบ ว่ามีความเสี่ยงใดที่จะเกิดขึ้นบ้างกับระบบนั้น

ดร. ไกรพล อรัญรัตน์ ปัจจัยอะไรเป็นสิ่งที่บอกว่าควรใช้ลายมือชื่ออิเล็กทรอนิกส์มากกว่าลายมือชื่อธรรมดา หากมองความเสี่ยงของเอกสารธรรมดาทั่วไปที่ใช้กันอยู่แล้ว ความเสี่ยงที่อาจจะเจอคือ 1) การแก้ไขข้อความในเอกสารที่ใครลงลายมือชื่อเอาไว้ ซึ่งอาจทำให้เข้าใจว่าคนที่ลงลายมือชื่อเป็นคนแก้ไขเอง หรือว่าทำข้อความนั้นขึ้นมาจริง ๆ 2) การปลอมลายมือชื่อ 3) เอกสารธรรมดาอาจจะถูกทำลาย ถูกฉีก หรือเสื่อมสภาพไปตามกาลเวลา หรือถูกแก้ไขได้โดยง่ายถ้าเปรียบเทียบกับการแก้ไขเอกสารอิเล็กทรอนิกส์

นายธีรวุฒิ จันทดิษฐ์ เอกสารอิเล็กทรอนิกส์นั้นสามารถแก้ไขได้ และทำได้โดยง่ายซึ่งสามารถใช้โปรแกรมอะไรก็ได้ในการแก้ไข แต่ว่าถ้ามีการแก้ไขแล้วสามารถตรวจพิสูจน์ได้ทันทีว่ามีการแก้ไข เนื่องจากพอแก้ไขแล้วจะรู้ได้เลยว่าไม่ครบองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ทำให้ไม่สามารถใช้ได้

ส่วนเรื่องของการปลอมเอกสารอิเล็กทรอนิกส์สามารถทำได้แต่ต้องมีกระบวนการในการแสดงเจตนาอีกครั้งหนึ่งว่าบุคคลนั้นมีเจตนาจริง ๆ เช่น การโอนเงินผ่านธนาคารต้องมีการ กด OTP หรือกด PIN อีกครั้งหนึ่ง เวลาลงลายมือชื่อนอกจากใส่ User และPassword และการวาดรูป ก็ควรจะมีการยืนยันตัวตนอีกขั้นหนึ่ง คือ สิ่งที่ใช้ยืนยันตัวตน (AAL) ระดับ 2 กล่าวได้ว่าอย่างน้อย 2 สิ่งในการยืนยัน เรียกว่า Double Modify เพื่อป้องกันการปลอม ถ้าในทางกฎหมายก็เสมือนคนนั้นเป็นคนทำธุรกรรมเอง ซึ่งไม่ควรให้ User และPassword กับใคร แต่คนไทยก็อาจจะมีการเขียนไว้ที่เครื่องคอมพิวเตอร์เลย

สำหรับเอกสารธรรมดาอาจจะหายได้ อาจถูกทำลาย ถูกฉีก หรือเสื่อมสภาพไปตามกาลเวลา และในส่วนของเอกสารไฟล์อิเล็กทรอนิกส์ โอกาสสูญหายนั้น ความจริงมันอาจจะไม่หายไปไหน แต่เป็นกรณีที่หาไม่เจอมากกว่าว่าเราเอาไปไว้ที่ไหน ซึ่งอาจจะเก็บไว้ในหลายที่ เช่น ใส่ในจดหมายอิเล็กทรอนิกส์ ใส่ในอุปกรณ์บันทึกข้อมูล (Hard disk) เป็นต้น ซึ่งในเรื่องนี้หากนำลายมือชื่ออิเล็กทรอนิกส์ไปไว้ในระบบออนไลน์ เช่น บริษัท ครีเดนเอเชีย จำกัด หรือของต่างประเทศ ก็จะมีระบบของการจัดเก็บไว้ใน Cloud Computing แต่ก็มีการลบได้ และก็สามารถมาดาวน์โหลดในเครื่องของเราได้

ดร. ไกรพล อรัญรัตน์ ปกติการลงลายมือชื่อแบบปกติ กับการจัดทำเอกสารอิเล็กทรอนิกส์ ต่างก็มีความเสี่ยงทั้งคู่

นายธีรวุฒิ จันทดิษฐ์ การที่เป็นดิจิทัลทุกอย่างเลยง่าย ไม่ว่าจะอยู่ที่ไหนก็สามารถลงลายมือชื่อดิจิทัลได้ ไม่จำกัดสถานที่ ไม่จำกัดเวลา และสามารถตรวจเช็คได้ง่ายกว่า พอรู้ว่ามีการแก้ไข หรือปลอมแปลง เมื่อเปิดจะรู้ได้เลยว่ามีการแก้ไข ทุกคนสามารถพิสูจน์ได้ ไม่จำเป็นต้องใช้ผู้เชี่ยวชาญหรือต้องใช้นิติวิทยาศาสตร์ในการพิสูจน์ว่าลายมือชื่อนี้เป็นของจริงหรือของปลอม เราสามารถรู้ได้ว่าใครเป็นคนทำธุรกรรม เป็นคนลงลายมือชื่อหรือเป็นเจ้าของได้ รวมทั้งช่วยในการลดการเก็บเอกสาร และช่วยในเรื่องการเก็บเอกสารนั้นไว้ได้นาน อย่างธุรกรรมบางประเภทต้องเก็บเอกสารไว้ 10 ปี หรือ 20 ปี หรือสัญญามีอายุ 15 ปี ก็ต้องเก็บ

9) การบริหารและจัดการความเสี่ยง

ดร. ไกรพล อรัญรัตน์ ข้อดีอีกประการ คือ การปลอมลายมือชื่อ การแก้ไขข้อความ การฉีกเอกสาร ใครก็สามารถทำได้ แต่การที่จะทำอะไรต่อเอกสารหรือการลงลายมือชื่ออิเล็กทรอนิกส์ ไม่ใช่ว่าใครสามารถทำได้ ต้องเป็นบุคคลที่เรียนมาด้านนี้โดยเฉพาะ ดังนั้น จะลดจำนวนผู้กระทำความผิด กล่าวได้ว่าอาชญากรพัฒนารูปแบบตามมา แต่ด้วยระบบอิเล็กทรอนิกส์นี้ จะติดตามตัวได้

นายธีรวุฒิ จันทดิษฐ์ เห็นว่าจะเป็นเหมือนกับการเปลี่ยนรูปแบบความเสี่ยงให้เป็นไปในลักษณะอื่น เช่น จากการ skimmer ตู้เอทีเอ็ม เป็นการปลอมแปลงชื่อคนรับเงินในบัญชี แต่หากจะกล่าวว่าระบบอิเล็กทรอนิกส์ไม่มีความเสี่ยงเลย ไม่สามารถพูดได้ แต่เราต้องพิจารณาความเสี่ยงนั้นด้วยว่าคุ้มค่า มีความเหมาะสมหรือไม่ มีมาตรฐานจัดการความปลอดภัยในระดับใด เช่น อย่างองค์กรของรัฐจะมีเกี่ยวกับสารสนเทศ อาจเป็น server ภายใน มีมาตรฐาน ISO คอมพิวเตอร์นั้นต้องไม่ต่อ internet ภายนอก เป็นต้น ส่วนความเสี่ยงที่ระบบจะล่มขึ้นอยู่กับปัจจัยหลายอย่าง และทรัพยากรของเครื่องนั้น เหมือนกับคอมพิวเตอร์ที่เราใช้งานบางครั้งก็มีความหน่วง และช้า ดังนั้น ขึ้นอยู่กับสภาพการใช้งาน

ดร. ไกรพล อรัญรัตน์ หลายคนมีความกังวลในเรื่องการดำเนินคดี เพราะบางรายมีทุนทรัพย์การดำเนินคดีที่สูงมาก หากมาใช้ระบบอิเล็กทรอนิกส์นี้จะไว้ใจ เชื่อถือได้หรือไม่ เมื่อเทียบกับการยื่นเอกสารเอง เห็นลายมือชื่อด้วยตัวเอง จะดีกว่าหรือไม่

นายธีรวุฒิ จันทดิษฐ์ จากประสบการณ์ทำงานกับองค์กรต่างประเทศ ซึ่งจะมีการส่งเอกสารให้ลงนาม เช่น การควบรวมบริษัทลงทุน มูลค่าหลักสิบล้าน โดยการลงนามออนไลน์นี้ไม่ได้มีกฎหมายไทยรองรับ เป็นเรื่องของทัศนคติและความน่าเชื่อถือของระบบ เพราะกฎหมายต้องให้สามารถระบุแล้วก็พิสูจน์ตัวตนได้ มีความหมายกว้าง การใช้จดหมายอิเล็กทรอนิกส์ก็อาจจะเป็นการพิสูจน์ได้เหมือนกัน ถ้าสองฝ่ายมีความเชื่อถือซึ่งกันและกัน

ดร. ไกรพล อรัญรัตน์ ปัจจัยระบบไม่น่าเป็นปัญหา ถ้ามีมาตรฐาน มีความปลอดภัย และตัวบุคคลด้วย ประกอบกับที่ทำให้ระบบนั้นมีความเสี่ยงมากน้อยเพียงใด

นายธีรวุฒิ จันทดิษฐ์ สำหรับเรื่องระบบล่มนั้น เช่น ทำธุรกรรมแล้วหาข้ออ้างว่าทำไม่สำเร็จ จะมีการประทับรับรองเวลา (Time Stamp) ถ้าการทำธุรกรรมไม่สำเร็จ ระบบ time stamp จะไม่ปรากฏ เพราะระบบ time stamp จะส่งตัวเลขไปไว้ที่อื่น ถ้าศาลยุติธรรมจะใช้ระบบนี้ ไม่ควรทำเอง แต่ให้หน่วยงานอื่นดำเนินการให้ ซึ่ง ETDA ให้บริการนี้อยู่ โดยสรรพากรใช้บริการของ ETDA เช่นเดียวกัน การออกใบกำกับภาษีอิเล็กทรอนิกส์

ดร. ไกรพล อรัญรัตน์ เรื่องนี้เป็นประเด็นตอนที่ปฏิบัติงานที่จังหวัดนครราชสีมา มีทนายท่านหนึ่งมีประเด็นถามมา มีกรณีที่ยื่นคำร้องเกินกำหนดระยะเวลาที่ศาลกำหนดไว้ โดยมายื่นเองที่ศาล โดยอ้างว่าเคยยื่นผ่านระบบอิเล็กทรอนิกส์แล้ว แต่ระบบไม่รับ เลยต้องมายื่นวันนี้ ซึ่งช่วงเวลาที่ยื่นในระบบเล็กทรอนิกส์ยังอยู่ในระยะเวลาตามกฎหมายแต่ระบบไม่รับ จึงทำให้ต้องมายื่นที่ศาลวันนี้ที่เลยกำหนดระยะเวลาตามกฎหมาย ในเชิงเทคนิคแล้วเป็นไปได้หรือไม่

นายธีรวุฒิ จันทดิษฐ์ เป็นไปได้แต่จะมีระบบการพิสูจน์ คือ การบันทึกเส้นทางการทำธุรกรรม สามารถบอกได้ว่าใครเข้ามาทำอะไร เวลาใด มีกิจกรรมอะไร โดยจะบันทึกไว้ แต่โดยปกติบริการภาครัฐจะขึ้นคำแนะนำไว้ว่าควรกระทำก่อนหมดเวลา (ตามที่ศาลกำหนด) ซึ่งอาจต้องกำหนดว่ากระบวนการทั้งหมดต้องเสร็จสิ้นภายใน 15.00 นาฬิกา ไม่ใช่ว่าเริ่มเข้าระบบช่วงเวลา 14.59 นาฬิกา จะทำให้เกินระยะเวลาที่กำหนด แล้วระบบก็ตัดการทำธุรกรรมบางครั้งบอกไม่ได้ว่าคอมพิวเตอร์ของผู้ใช้บริการหรือของภาครัฐมีความช้า

ดร. ไกรพล อรัญรัตน์ หากสมมุติว่าเกิดกรณีนั้น เป็นไปตามที่ทนายอ้าง จะสามารถ capture หน้าจอไว้เมื่อทำธุรกรรมนั้น ๆ แล้วนำมาประกอบการยื่นคำร้องได้หรือไม่

นายธีรวุฒิ จันทดิษฐ์ แท้จริงควรมีกระบวนการตรวจสอบได้ทั้งผู้ยื่นและเจ้าของระบบ คล้ายกับธุรกรรมการโอนเงิน สามารถตรวจสอบได้ว่ารายการใดสำเร็จ หรือรายใดรอการอนุมัติ

ดร. ไกรพล อรัญรัตน์ ถ้าระบบไม่มีการ time stamp ก็จะหมายความว่าเขายังทำกระบวนการไม่เสร็จสิ้น ถ้าเสร็จสิ้นแล้วก็จะมีกระบวนการ time stamp ที่ตรวจสอบได้

มีประเด็นการจัดทำเอกสารอิเล็กทรอนิกส์ หากมีการแก้ไขเปลี่ยนแปลงข้อมูล หากเป็นเอกสารธรรมดา เมื่อมีการปลอมลายมือชื่อจะต้องมีการส่งตรวจพิสูจน์โดยผู้เชี่ยวชาญแล้วนำมาประกอบการพิจารณาว่าเป็นการปลอมจริงหรือไม่ แต่ในการลงลายมือชื่ออิเล็กทรอนิกส์ หากมีการปลอมแปลงขึ้นมา จะมีวิธีการพิสูจน์ได้อย่างไร

นายธีรวุฒิ จันทดิษฐ์ ต้องย้อนไปดูระบบมีการให้เขาพิสูจน์ยืนยันตัวตนหรือไม่

นายโอวาท โอวาทตระกูล ก่อนทำธุรกรรม หากมีมาตรฐานอยู่แล้ว เช่น บางระบบให้ทางเลือกว่าจะยืนยันตัวตนหรือไม่ยืนยันตัวตน เมื่อตรวจสอบหลักฐานด้วยบัตรประชาชนและกรมการปกครอง ก็จะได้ใบรับรอง (certificate) มาเพื่อใช้ระบุแทนบุคคลรายนี้เลย ไม่สามารถระบุเป็นบุคคลอื่นได้แล้ว เมื่อตรวจสอบได้ว่าบุคคลนี้เป็นใคร เพราะใบรับรอง (certificate) จะจำแนกเป็นรายบุคคล ในประเด็นเรื่องการแก้ไขจะมี time stamp ไม่มีทางแก้ไขได้อยู่แล้ว โดยที่สามารถตรวจดูได้จากโปรแกรมว่าใครเป็นผู้ลงลายมือชื่อและมีการแก้ไขหรือไม่ หากเจ้าตัวปฏิเสธว่าไม่ได้ทำจะยาก เพราะกว่าจะได้ลายเซ็นอิเล็กทรอนิกส์นี้มาเป็นไปไม่ได้ที่คนอื่นจะสวมรอย หากพลาดจริง ๆ คือตอน log in ที่ให้คนอื่นทราบหรือมาใช้งานแทน

นายธีรวุฒิ จันทดิษฐ์ ในทางกฎหมายไม่ได้เขียนไว้ว่าวิธีการจัดเก็บควรเป็นอย่างไร จะเป็นในเชิงเทคนิค

ดร. ไกรพล อรัญรัตน์ มีวิธีการพิสูจน์อย่างไร หากระบบน่าเชื่อถือ ก็จะตามรอยได้เองอยู่ด้วย ไม่ต้องอาศัยผู้เชี่ยวชาญ

นายธีรวุฒิ จันทดิษฐ์ บางโปรแกรมไม่ต้องอาศัยผู้เชี่ยวชาญ เช่น PDF สามารถเปิดดูได้ว่าใครแก้ไขอะไร หากไม่มั่นใจก็ผู้ให้บริการแพลตฟอร์มในการลงนามอิเล็กทรอนิกส์ตรวจสอบข้อมูลเพิ่มเติม

นายโอวาท โอวาทตระกูล เครื่องมือนี้จะมีความเป็นสากล คือ การทำรายการแบบนี้ก็จะใช้เทคโนโลยีเดียวกัน

10) การกำกับดูแลข้อมูล

ดร. ไกรพล อรัญรัตน์ การที่นำระบบเอกสารอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์มาใช้อาจมีความเสี่ยง โดยเฉพาะการเป็นองค์กรของรัฐ จะมีวิธีการเตรียมพร้อม รับมือ หรือประเมินความเสี่ยงที่จะเกิดขึ้นกับการใช้ e-signature อย่างไร

นายธีรวุฒิ จันทดิษฐ์ การใช้ e-signature จะแนะนำว่าองค์กรที่มีระบบสารสนเทศขนาดใหญ่ เช่น ศาลควรขอมาตรฐาน ISO 27001 (2013) คือเป็นระบบในการจัดการความมั่นคงปลอดภัยของสารสนเทศ รัฐวิสาหกิจขนาดใหญ่ในประเทศไทยใช้ระบบนี้ ส่วนภาครัฐคือ DGA สำนักงานพัฒนารัฐบาลดิจิทัล สรรพากร กรมพัฒนาธุรกิจการค้า มาตรฐานนี้จะเป็นเรื่องของการจัดการข้อมูลความปลอดภัยขององค์กร โดยหลักคือ การที่ต้องมีการวางแผนจัดทำนโยบาย วิธีการรับมือความเสี่ยงที่จะเกิดขึ้นและการจัดการข้อมูลรั่วไหล

ถัดมาคือแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ มีฉบับปี พ.ศ. 2553 และ พ.ศ. 2556 เป็นเรื่องเกี่ยวกับการจัดทำนโยบาย ในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ การจัดให้มีระบบสำรองของสารสนเทศในกรณีฉุกเฉิน การตรวจสอบและการประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 จะมี 3 รูปแบบ คือ แบบปลอดภัย แบบปกติ และแบบเคร่งครัด โดยกำหนดรายละเอียดไว้ โดยหลักเน้นที่บุคลากร อุปกรณ์คอมพิวเตอร์ และวิธีการการเข้าถึงอุปกรณ์คอมพิวเตอร์ เช่น การตั้งรหัสผ่าน การเข้าถึงอินเทอร์เน็ตภายนอก เนื่องจากเกรงกลัวการถูกเจาะระบบข้อมูล

การกำกับดูแลข้อมูล หรือ Data Governance หรือที่เรียกว่าธรรมาภิบาลข้อมูล ซึ่งสำนักงานพัฒนารัฐบาลดิจิทัล ได้ประกาศในราชกิจจานุเบกษาแล้วเมื่อเดือนมีนาคมที่ผ่านมาโดยให้หน่วยงานภาครัฐปฏิบัติตาม แต่ในส่วนที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ในส่วนโครงสร้างนั้นจะเน้น 3 อย่าง คือ

1) การปฏิบัติตามกฎเกณฑ์ คือ กำหนดขอบเขตวิธี การติดตามผล ต้องกำหนดนโยบายตัวชี้วัดว่าต้องจัดการอย่างไรถ้าเกิดความเสี่ยงขึ้นมา ใครเป็นผู้มีหน้าที่ในการจัดการ

2) การบริหารและจัดการความเสี่ยง

3) การบริหารจัดการผลกระทบ องค์กรต้องมีนโยบายและบริหารจัดการความเสี่ยงขององค์กร รวมทั้งการสื่อสารทำความเข้าใจเมื่อเกิดความเสี่ยงขึ้น สามารถที่จะระบุความเสี่ยงที่เกิดขึ้นได้ประเมินความเสี่ยงล่วงหน้า กำหนดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เช่น หากเอกสารหลุดไปสู่สาธารณะ เอกสารดังกล่าวอยู่ในชั้นความลับระดับใด หากเอกสารดังกล่าวเป็นเอกสารทั่วไป ความเสี่ยงนั้นยอมรับได้ เพราะผลกระทบไม่ร้ายแรง แต่หากเป็นเอกสารในระดับชั้นความลับมาก ไม่ควรจะหลุดไปสู่ภายนอก ต้องบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงที่จะเกิดขึ้น อาจต้องกำหนดตัวชี้วัดและรายงานผล กำหนดหน้าที่ความรับผิดชอบให้ชัดเจน บริหารจัดการผลกระทบที่จะเกิดขึ้นทั้งทางตรงและทางอ้อม องค์กรต้องกำหนดชัดเจนเพื่อตอบสนองให้ได้อย่างเหมาะสมที่สุด

แนวทางพัฒนาสมรรถนะด้านการกำกับข้อมูลขององค์กร ประการแรก คือ การกำหนดแนวทางและกลยุทธ์ต้องกำหนดชัดเจนและเป็นไปตามกฎหมายเพื่อลดความเสี่ยง ซึ่งควรกำหนดให้สามารถตรวจสอบได้ มีการคุ้มครองข้อมูลส่วนบุคคลระดับใด มีความเชื่อมั่นและพร้อมใช้ ถ้ามีการเปิดเผยข้อมูลและข้อมูลสามารถเปิดเผยต่อสาธารณะได้ และต้องกำหนดให้ทบทวนวิสัยทัศน์ ทิศทางการดำเนินงานขององค์กร

ประการต่อมาคือผู้ดูแลข้อมูลหรือบริการข้อมูล ทำหน้าที่ในการร่างนโยบายข้อมูล ระบุมาตรฐานที่ควรใช้ว่าข้อมูลแต่ละประเภทควรมีมาตรฐานจัดการอย่างไร รวมถึงการตรวจสอบการปฏิบัติตามนโยบายของผู้ที่เกี่ยวข้องในองค์กร การตรวจสอบคุณภาพและการวิเคราะห์ความมั่นคงปลอดภัยของข้อมูล ต้องมีระบบและแนวทางหน่วยงานกำหนดไว้ หน่วยงานรัฐที่กำหนดไว้ เช่น การควบคุมการเข้าถึง การควบคุมซอฟต์แวร์ การควบคุมการออกแบบระบบ การควบคุมอุปกรณ์ ควบคุมการเข้าถึงเว็บไซต์ เป็นต้น การมีนโยบายการควบคุมเป็นไปเพื่อป้องกันความเสี่ยงที่จะเกิดขึ้น

ดร. ไกรพล อรัญรัตน์ อาจกล่าวได้ว่าการจัดการความเสี่ยงเป็นกระบวนการตั้งแต่ก่อนที่จะความเสี่ยงจะเกิดขึ้น ซึ่งอยู่ในเรื่องของมาตรฐาน เมื่อมีความเสี่ยงเกิดขึ้นก็มีแนวทางจะจัดการอย่างไร เราควรจัดลำดับว่าใครสามารถเข้าถึงข้อมูลได้ เพื่อป้องกันการรั่วไหลของข้อมูล

มีประเด็นสอบถามว่าถ้าหน่วยงานราชการนำระบบเอกสารอิเล็กทรอนิกส์มาใช้ในงานธุรการ บรรดาเจ้าหน้าที่ธุรการหลายท่านต้องมีรอบโยกย้ายตามปกติในแต่ละปี หากว่าปีนี้ปฏิบัติงานที่ศาลหนึ่ง เช่น สมมุติว่าเป็นศาลแพ่ง ก็จะมีอำนาจหน้าที่เข้าถึงข้อมูลและอนุมัติข้อมูล แต่ได้แอบเก็บรหัสเข้าใช้งานไว้ แล้วเมื่อได้โยกย้ายแล้วก็เข้ามาดูข้อมูลในระบบ กรณีเช่นนี้จะจัดการอย่างไร

นายธีรวุฒิ จันทดิษฐ์ ในทางหลักการคือ privacy by design ต้องเริ่มตั้งแต่การจัดการข้อมูลตั้งแต่การออกแบบระบบของโปรแกรม เมื่อมีเรื่องการโยกย้ายเข้ามา ตำแหน่งจะต้องมีผลต่อการเข้าถึงข้อมูล ตำแหน่งที่สามารถเข้าถึงข้อมูลได้เฉพาะส่วน หากออกแบบไว้แต่แรกจะไม่มีปัญหา หรือถ้าเป็นระบบธุรการภายใน ระบบสารบรรณ แนะนำว่าควรจะใช้ของสำนักงานพัฒนารัฐบาลดิจิทัลจะมีระบบสารบรรณของหน่วยงานภาครัฐให้ใช้ได้ เข้าใจว่าศาลก็น่าจะใช้ได้เหมือนกัน แต่เป็นระบบกลางอาจจะไม่ได้ตอบโจทย์กับทุกหน่วยงานของรัฐ อาจใช้เป็นไกด์ไลน์ได้ ซึ่งมีมาตรฐานของระบบสารบรรณของหน่วยงานภาครัฐอยู่ว่าถ้าจะออกแบบ ควรจะต้องทำอย่างไร

ส่วนประเด็นการเปลี่ยนรหัสผู้ใช้งาน ไม่มั่นใจว่าเป็นการละเมิดสิทธิความเป็นส่วนตัวหรือไม่ ยกตัวอย่างภาครัฐที่ใช้ลายมือชื่ออิเล็กทรอนิกส์ในการให้บริการประชาชน ซึ่งมีการใช้กันอย่างมาก ดังนี้ การจดทะเบียนนิติบุคคลทางอิเล็กทรอนิกส์ของกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ซึ่งได้จัดทำระบบออนไลน์ขึ้นมา ซึ่งทำการจดทะเบียนออนไลน์ผ่าน internet โดยประสบการณ์ส่วนตัวใช้งานผ่านระบบออนไลน์มีความรวดเร็วกว่าการติดต่อที่สำนักงานโดยตรง และสามารถทำได้มากกว่าการจดทะเบียนออนไลน์ ซึ่งสามารถแก้ไขได้หลายอย่าง เช่น แก้ไขผู้ถือหุ้น เลิกบริษัท ชำระบัญชี แก้ไขวัตถุประสงค์บริษัท การควบรวมบริษัท แก้ไขกรรมการบริษัท เป็นต้น โดยให้ผู้ใช้งานลงลายมือชื่อรวมถึงตราประทับ โดยให้ผู้ใช้งานกรอกรหัสผ่านแล้วจะมีรหัส OTP มายืนยันธุรกรรมอีกครั้งเพื่อแสดงเจตนารมณ์ของผู้ใช้งาน

ในระบบนิติบุคคลที่ยื่นของบการเงินออนไลน์ โดยต้องสมัครอีกรหัสผู้ใช้ เพื่อให้ได้ public key โดยของแต่ละคนจะไม่ซ้ำกัน โดยจะถูกนำไปใส่ในเอกสาร ซึ่งไม่ต้องอาศัยตราประทับ เพราะ public key ทำหน้าที่แทนตราประทับแล้ว และมีความน่าเชื่อถือสูง แต่ต้องกรอกรหัสผ่านอีกรอบและรหัส OTP เพื่อยืนยันอีกครั้ง

การประทับตราบริษัทด้านหน้าบริษัทที่ต้องใส่รหัสผ่านของระบบเพื่อยื่นงบการเงินนี้ ที่ต้องให้ใช้รหัสผ่านอีกชุดที่เป็นเฉพาะการยื่นงบการเงินก็เพื่อเป็นการยืนยันอย่างแท้จริงว่าเราจะยื่นงบการเงินและประทับตรารับรองธุรกรรมนั้น ซึ่งจัดว่ามีความปลอดภัยมาก

สรุปลายมือชื่ออิเล็กทรอนิกส์ มี 3 ประการ ได้แก่ 1) ต้องมีองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ 5 ข้อ ได้แก่ 1.1) รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ มีความเหมาะสมหรือไม่ 1.2) การพิสูจน์และยืนยันตัวตน ได้มาตรฐานหรือไม่ ต้องมีความน่าเชื่อถือเพียงพอ เช่น ทราบได้ว่า User Password นี้เป็นของใคร ก็สามารถพิสูจน์และยืนยันตัวตนได้ 1.3) การเชื่อมโยงข้อมูลกับลายมือชื่อ 1.4) เจตนาการลงลายมือชื่อ และ 1.5) การรักษาความครบถ้วนของข้อมูล 2) ความมั่นคงปลอดภัยและรัดกุมของระบบและอุปกรณ์ และ 3) ลักษณะ ประเภท ขนาดหรือมูลค่าของธุรกรรมมีความเหมาะสมเพียงใด

ถ้ามีองค์ประกอบ 5 ข้อนี้ ก็สามารถที่จะเชื่อได้ว่ายืนยันและทำธุรกรรมทางอิเล็กทรอนิกส์ได้

ดร. ไกรพล อรัญรัตน์ ต้องพิสูจน์ความเชื่อถือในหลาย ๆ อย่าง ระบบสร้างความเชื่อถือด้วยการ double verified คือ ยืนยันธุรกรรมสองชั้น และมีหลายปัจจัยประกอบกันให้เชื่อถือว่าได้ว่าการทำธุรกรรมนั้นเกิดจากเจตนาของบุคคลนั้นจริง ๆ ซึ่งเป็นไปโดยการออกแบบของระบบได้ดีเพียงใด

นายโอวาท โอวาทตระกูล จากประสบการณ์ที่มีส่วนร่วมพัฒนาเอกสารอิเล็กทรอนิกส์และระบบการลงลายมือชื่ออิเล็กทรอนิกส์ ขอแบ่งเป็นบุคคลและระบบ ดังนี้

ตัวบุคคล (human error) เช่น เอา password ให้คนอื่น จดทิ้งไว้ หรือลืมโทรศัพท์ไว้ในห้องน้ำ

ระบบ (system error) แยกออกเป็นสองประการ คือ 1) ระบบเสียหาย ไม่ปลอดภัย กับ 2) ระบบมีความยุ่งยากต่อการใช้ โดยหลักคือตัวบุคคลผู้ใช้งาน

นายธีรวุฒิ จันทดิษฐ์ หากพิจารณาเรื่องการประเมินความเสี่ยง จะพบเรื่องตัวบุคคลมากกว่าระบบ เพราะตัวระบบมีความซับซ้อนและยุ่งยากกว่า แต่การหลอกคนจะง่ายกว่าการหลอกระบบ เช่น หลอกแจกโทรศัพท์ฟรีให้ลงทะเบียนแล้วถูกดึงข้อมูลไป เป็นต้น ซึ่งอาชญากรจะมุ่งไปที่ตัวคนมากกว่า

3. ข้อคำถามจากผู้เข้าร่วมรับชมการสัมมนา

- คำถาม เกี่ยวกับเรื่องการใช้ลายเซ็นสำเร็จรูปให้คนอื่นทำให้ ไม่สามารถอ้างอิงได้ มีผลทางกฎหมายอย่างไร เข้าใจว่าเป็นระบบ offline ไม่ได้สร้างขึ้นมาโดยระบบ แต่หากเป็นระบบออนไลน์ เป็นระบบในการเซ็นลายเซ็นมาให้เราพิมพ์ชื่อลงไป ก็จะปรากฏเป็นลายเซ็นของเรา แต่ต้องมีการแสดงเจตนาว่าต้องการลงลายมือชื่อด้วยรูปแบบนี้ จากประสบการณ์เคยพบใบแต่งทนายความ ในแผ่นหลังโดยปกติจะเซ็นชื่อ แต่ทนายความท่านนั้นใช้การพิมพ์ชื่อแทน โดยเริ่มจาก offline แล้วนำเข้าสู่ระบบ online ซึ่งสามารถใช้ได้แต่ไม่ได้ถูกสร้างโดยระบบ แต่จะพิสูจน์ได้ยากกว่าเป็นเจ้าของตัวจริงหรือไม่ ต้องดูเจตนา เพราะไม่มีระบบเข้ามารับรอง และต้องพิสูจน์ให้ได้ว่าบุคคลนั้นจริง ตัวอย่างเช่น ในจดหมายอิเล็กทรอนิกส์ของเรามีการพิมพ์ชื่อนามสกุลต่อท้ายจดหมายอิเล็กทรอนิกส์ ก็คือการยืนยันในระดับหนึ่งว่าข้อความในจดหมายอิเล็กทรอนิกส์ฉบับนี้ เราเป็นคนอนุมัติ ไม่ว่าเราจะให้คนอื่นกดใช้ส่งแทนให้ก็ตาม

- คำถาม เกี่ยวกับการทำเอกสารและลงลายมือชื่ออิเล็กทรอนิกส์ อยากจะนำมาใช้ในการทำสัญญาประนีประนอมยอมความและจะให้ศาลพิพากษาตามยอม โดยที่เขาไม่ต้องเดินทางมาที่ศาล ถ้าเป็นการทำสัญญาประนีประนอมยอมความนอกศาล เข้าใจว่าไม่มีข้อห้ามในการทำ แต่ถ้าจะให้ศาลพิพากษาตามยอม จากการที่ค้นหาข้อมูลวิจัยของต่างประเทศ การพิพากษายังไม่สามารถใช้การลงลายมือชื่ออิเล็กทรอนิกส์ได้ ในบางรัฐของประเทศสหรัฐอเมริกาได้กำหนดข้อยกเว้นไว้ ในมาตรฐานว่าเอกสารใดไม่ให้ใช้วิธีการลงลายมือชื่ออิเล็กทรอนิกส์ แล้วมีเรื่องคำพิพากษาให้ใช้วิธีการลงลายมือชื่อปกติ

การทำสัญญายอมความกันภายนอกศาล ไม่ติดข้อกฎหมายใด แต่หากให้ศาลทำคำพิพากษาตามยอมด้วย ยังมีข้อกังวลหลายประการ โดยในทางสากลยังไม่ยอมรับให้มาใช้กับการทำคำพิพากษาตามยอม ทั้งนี้ การลงลายมือชื่ออิเล็กทรอนิกส์จะสามารถทำได้ในบางเฉพาะประเภทคดีประเทศในโซนยุโรปและสาธารณรัฐประชาชนจีน ส่วนของประเทศไทยในราชกิจจานุเบกษาตั้งแต่ปี 2560 ไม่มีลายเซ็นอยู่ในราชกิจจานุเบกษาที่ปรากฏ online (ที่เผยแพร่) แต่ในทาง offline ยังมีลายเซ็นอยู่

- คำถาม เกี่ยวกับการลงลายมือชื่อดิจิทัลเพื่อออกคำสั่งทางปกครองได้หรือไม่ ต้องพิจารณาระเบียบภายในหน่วยงานแต่ละหน่วยว่ามีระเบียบกฎเกณฑ์อย่างไร ให้ลงลายมือชื่อดิจิทัลได้หรือไม่ ประเทศไทยได้กำหนดไว้อยู่ในพระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์มาบังคับใช้ เป็นเรื่องเกี่ยวกับครอบครัว มรดก ประเทศอื่นไม่ได้มีข้อห้ามไว้ แต่ไม่ได้บังคับ เปิดกว้างให้แต่ละหน่วยงานพิจารณาเอง หน่วยงานรัฐของไทยหลายแห่งก็มีการใช้ลายมือชื่อดิจิทัลปรับใช้ แต่ส่วนใหญ่ยังเป็นระดับผู้บริหารเพราะว่าลายมือชื่อดิจิทัลมีค่าใช้จ่ายสูง

- คำถาม เกี่ยวกับกรณีเอกสารคำขอท้ายฟ้องทางแพ่งและอาญาสามารถพิมพ์ชื่อแทน การลงลายมือชื่อได้หรือไม่ เห็นว่าเป็นกรณีคล้ายกับใบแต่งทนายที่ได้อธิบายไปข้างต้น คือ ถ้าพิมพ์ลงในคอมพิวเตอร์ชื่อส่วนตัวแล้วพิมพ์ลงในช่องลายมือชื่อ upload เข้าระบบโดยที่ไม่ได้เซ็น ซึ่งระบบไม่ได้ generate ให้ เช่นนี้ก็จะเป็นคำตอบเดิมเดียวกับกรณีใบแต่งทนายความ หากไม่อ้างว่าระเบียบทำได้หรือไม่ ต้องดูว่าธุรกรรมนั้นมีผลอย่างไร มีลักษณะอย่างไร เหมาะสมหรือไม่ มีการสวมรอยแทนได้หรือไม่ มีความผิดหรือไม่ เช่น การร้องเรียนหน่วยงาน ซึ่งมีแบบฟอร์มให้เราพิมพ์ชื่อ ก็ไม่ถึงกับจำเป็นขนาดให้เราต้องทำการระบุตัวพร้อมภาพถ่ายบัตรประชาชนและให้ได้ใบรับรองมาประกอบการร้องเรียน จะต้องพิจารณาลักษณะประเภทธุรกรรมประกอบกัน

กรณีถ้าเป็นการลงลายมือชื่อท้ายฟ้องแพ่งที่ทำในระบบ E-filing หรือระบบอื่น ไม่น่ามีปัญหา แต่ต้องแยกให้ได้ว่าพิมพ์ชื่อนั้น การพิมพ์ชื่อทำโดยระบบ หรือเราสร้างไฟล์นั้นเอง ถ้าเราพิมพ์สร้างไปเอง ก็จะติดตามได้ยาก ตามหาว่าใครเป็นผู้พิมพ์ชื่อนั้นได้ยาก แต่ถ้าระบบจัดการให้ก็จะไม่มีปัญหาในการตามรอย

- คำถาม เกี่ยวกับหากเกิดข้อพิพาทเกี่ยวกับระบบ ตามระบบกฎหมายแล้วจะถือว่ามูลคดีเกิดที่ใด เข้าใจคำถามนี้ว่าถ้ามีการทำสัญญากันโดยใช้ระบบเอกสารอิเล็กทรอนิกส์ จะถือว่ามูลคดีเกิดขึ้นที่ใด ในประเด็นนี้ต้องตรวจสอบจากพระราชบัญญัติธุรกรรมอิเล็กทรอนิกส์ว่าถ้าไม่มี คงต้องรอคำพิพากษาศาลฎีกาต่อไป

กรณียืมเงินออนไลน์จะใช้เป็นพยานหลักฐานได้หรือไม่ แต่ถ้ามูลคดีเกิดขึ้นที่ใด เช่น คนยืมอยู่กรุงเทพ คนให้ยืมอยู่เชียงใหม่ จะมีประเด็นว่าฟ้องที่ศาลใด ซึ่งคำถามนี้ไม่ได้ระบุว่าคดีแพ่งหรืออาญา แต่ถ้าเป็นคดีแพ่งจะมีหลักเกณฑ์แตกต่างกันออกไปโดยต้องตรวจสอบจากคำพิพากษาศาลฎีกาอีกครั้งหนึ่ง

- คำถาม เกี่ยวกับในเรื่องคดีความอิเล็กทรอนิกส์ว่าเคยเกิดขึ้นแล้วหรือไม่ จากที่สืบค้นเคยมีคำพิพากษาของศาลฎีกาเกี่ยวกับเรื่องการรับฟังข้อมูลอิเล็กทรอนิกส์ว่าเป็นพยานหลักฐานได้ (ฎ.8089/2556) มีเรื่องฟ้องร้องเกี่ยวกับการกดเงินผ่านตู้เอทีเอ็ม ศาลก็อธิบายว่าการกดเงินเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 9 พระราชบัญญัติธุรกรรมฯ สามารถนำไปใช้เป็นหลักฐานการกู้ยืมเงินได้ และมีคำพิพากษาการยืมเงินหรือการยกหนี้ผ่าน Facebook ซึ่งศาลให้เหตุผลว่าเป็นข้อมูลอิเล็กทรอนิกส์ตามมาตรา 7 เป็นพยานหลักฐานตามมาตรา 8 และเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 9 (ฎ. 6757/2560) จะเห็นว่าทั้งสองคดี จะเป็นเรื่องของมาตรา 9 คือ การที่ลงลายมือชื่อแบบอิเล็กทรอนิกส์และสามารถระบุตัวตนได้แต่ยังไม่มีเรื่องของมาตรา 26 กับมาตรา 28 เพราะฉะนั้นเป็นประเด็นที่เข้มข้น และทำได้ยาก จึงไม่พบปัญหาเรื่องคดีความ

- คำถาม เกี่ยวกับกรณีฝ่ายหนึ่งเป็นสมาชิกของ electronic sign แต่คู่สัญญาไม่ได้เป็นสมาชิกด้วย ฝ่ายที่เป็นสมาชิกสามารถให้อีกฝ่ายลงลายมือชื่ออิเล็กทรอนิกส์ได้หรือไม่ ถ้าได้ คู่สัญญาที่ไม่ได้เป็นสมาชิกลงลายมือชื่อไป มาตรฐานป้องกันต่าง ๆ จะเทียบเท่าเช่นเดียวกับฝ่ายที่เป็นสมาชิกด้วยหรือไม่ ด้วยระบบคงไม่ยินยอม เพราะระบบต้องมีการตรวจพิสูจน์ยืนยันตัวตนของผู้ที่ต้องลงลายมือชื่ออิเล็กทรอนิกส์ก่อน โดยต้องสมัครเป็นสมาชิกของระบบนั้น แม้แต่ระบบ electronic signature ต่างบริษัทกัน ก็ยังไม่อนุญาตให้ใช้ร่วมกัน เพราะเจ้าของทั้งสองระบบไม่เชื่อมต่อกันในทางเทคนิคเป็นไปได้ แต่ว่าในทางปฏิบัติอาจเป็นไปได้ยาก เพราะเจ้าของระบบอาจสร้างขึ้นมาโดยอ้างอิง อาจใช้ไม่ได้ตามกฎหมายไทยซึ่งปัจจุบันยังต้องสมัครสมาชิก

- คำถาม เกี่ยวกับการพิสูจน์ตัวตนของผู้ใช้บริการแอพพลิเคชั่น LINE และ Facebook ว่าใครเป็นผู้ลงทะเบียนเป็นผู้ใช้เพื่อยืนยันข้อความที่ได้พูดคุยกันมีวิธีการอย่างไรและมีหน่วยงานใดในประเทศไทยที่สามารถตรวจสอบได้ ประการแรกคือไม่น่าจะตรวจสอบได้ ถ้าไม่ขออำนาจศาล แต่สามารถที่จะทราบอยู่แล้วว่าบุคคลนั้นเป็นใคร กรณีการเข้าถึงข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติคอมพิวเตอร์ให้อำนาจเจ้าพนักงานในกรณีที่เจ้าพนักงานต้องการเข้าถึงข้อมูลสามารถร้องขอให้ศาลทำการตรวจสอบเงื่อนไขต่าง ๆ ตามที่กฎหมายกำหนดไว้ แล้วศาลจะพิจารณาควรให้มีการเข้าถึงข้อมูลคอมพิวเตอร์หรือไม่ จึงจะสามารถให้เจ้าของระบบเปิดเผยข้อมูลส่วนนั้นได้ เคยมีประเด็นคดีของ FBI ขอให้ทางบริษัท Apple เปิดเผยข้อมูลโทรศัพท์ไอโฟนของลูกค้า

แต่บริษัท Apple แถลงการณ์ว่าต้องการรักษาความเป็นส่วนตัวของลูกค้าไว้ แต่ถ้าถามถึงประเด็นดังกล่าวนี้ ต้องอาศัยแนวทางตามพระราชบัญญัติคอมพิวเตอร์ อย่างไรก็ตามสรุปได้ว่าไม่มีหน่วยงานใดสามารถตรวจสอบได้ ยกเว้นขออำนาจศาล ซึ่งโดยปกติเวลาลงทะเบียนยืนยันก็จะใช้เบอร์โทรศัพท์และรหัส OTP เพื่อใช้ยืนยันตัว ก็จะสอดคล้องกับข้อมูลส่วนบุคคล คือ ขอเท่าที่ใช้และเท่าที่จำเป็น

การพิสูจน์ตัวตนของผู้ใช้บริการ Facebook และ Line ว่าใครเป็นผู้ใช้ มีวิธีการอย่างไรและมีหน่วยงานใดตรวจสอบได้ กรณีนี้ไม่น่าจะตรวจสอบได้ ถ้าไม่ได้ขออำนาจศาล การเข้าถึงข้อมูลคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จะมีการให้อำนาจเจ้าพนักงานในกรณีที่เจ้าพนักงานต้องการจะเข้าถึงข้อมูล สามารถร้องขอให้ศาลตรวจสอบเงื่อนไขต่าง ๆ ตามที่กฎหมายกำหนดไว้ ลักษณะเหมือนการออกหมายจับ ศาลจะเป็นคนพิจารณาทั้งหมดว่าควรจะให้เข้าถึงข้อมูลคอมพิวเตอร์ในกรณีนั้นหรือไม่ เมื่อได้การอนุญาตจากศาลแล้ว จึงจะให้เจ้าของระบบสามารถเข้าถึงข้อมูลได้ ก่อนหน้านี้เคยมีกรณีที่ FBI ขอให้ Apple ที่ประเทศสหรัฐอเมริกาเปิดเผยข้อมูลในโทรศัพท์ไอโฟน หลังจากนั้น Apple ออกแถลงการณ์ว่าบริษัทต้องรักษา Privacy ของลูกค้าไว้ไม่สามารถเปิดเผยได้ ประเด็นที่ว่าถ้าอยากรู้ข้อมูลของผู้ใช้งาน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตามที่กล่าวไปแล้วอาจจะทำได้ ส่วนวิธีการทำอย่างไร อาจจะต้องขอศาล โดยปกติการลงทะเบียนยืนยันเรื่องเหล่านี้ ส่วนใหญ่จะใช้เบอร์โทรศัพท์ และ OTP ในการยืนยัน จะไปสอดคล้องกับข้อมูลส่วนบุคคลที่ให้ขอเท่าที่ใช้เท่านั้น

- คำถาม เกี่ยวกับความแตกต่างของโลกแบบเก่า คือ โลกที่เราใช้ระบบเอกสารดั้งเดิมโดยใช้ปากกาเซ็น กับโลกดิจิทัลลักษณะโดยทั่วไปมีความแตกต่างอย่างไร ลายมือชื่อธรรมดามีรูปร่างสามารถจับต้องได้ ต้องปรากฏตัวเพื่อลงลายมือชื่อ มีต้นทุนระบบต่ำ ต้นทุนทรัพยากรสูง และคนมีความคุ้นเคยสูง ในขณะที่ลายมืออิเล็กทรอนิกส์ไม่มีรูปร่างทางกายภาพ ลงลายมือชื่อจากที่ใดก็ได้ ต้นทุนระบบสูง ต้นทุนทรัพยากรต่ำ และคนมีความคุ้นเคยต่ำ เมื่อเปรียบเทียบความเสี่ยงจากการใช้งานลายมือชื่อธรรมดาจะปลอมลายมือชื่อได้ง่าย แก้ไขข้อความในเอกสารได้ง่าย ถูกทำลายทางกายภาพ เสื่อมสภาพได้ตามกาลเวลา และต้องใช้ผู้เชี่ยวชาญด้านลายมือชื่อในการตรวจสอบ ในขณะที่ลายมือชื่ออิเล็กทรอนิกส์ ปลอมแปลงตัวบุคคลผู้มีอำนาจลงชื่อยาก แก้ไขข้อความในเอกสารได้ยาก ไม่ถูกทำลายทางกายภาพ ไม่เสื่อมสภาพตามกาลเวลา และระบบสามารถตรวจสอบลายมือเองได้

- คำถาม เรื่อง Facebook และ Line ใครก็ตั้งชื่อใครก็ได้ หรือเอารูปใครมาเป็นรูป โปรไฟล์ก็ได้ ทางผู้คุมกฎมีวิธีควบคุมเรื่องนี้หรือไม่ และมีการคุ้มครองอย่างไร ในทางกฎหมาย ETDA มีหน้าที่ในการควบคุมดูแลให้เป็นไปตามมาตรฐาน แต่ไม่ได้มีหน้าที่ในการให้บริการ ตามคำพิพากษาศาลฎีกา การให้บริการ Facebook และ Line เป็นการลงลายมืออย่างหนึ่งซึ่งสามารถบังคับได้ตามมาตรา 9 เช่น กรณีมีคนเสนอขายของทาง Line และเราพิมพ์ตอบกลับไปว่ายินยอมซื้อ ก็ถือว่าเป็นการลงลายมือชื่อทางอิเล็กทรอนิกส์แล้ว เพราะเป็นการตกลงโดยการลงลายมือชื่อทางอิเล็กทรอนิกส์แล้ว ระบบไหนจะสามารถเชื่อถือได้ตามกฎหมายหรือไม่ ต้องพิจารณาเป็นระบบไป การพิจารณาความน่าเชื่อถือของระบบ ต้องพิจารณาจากความเสี่ยงและความปลอดภัย บางระบบมีความเสี่ยงต่ำมาก แต่มีความปลอดภัยสูงมาก อาจจะสามารถนำมาทดแทนกันได้ขึ้นอยู่กับความรัดกุมและการให้บริการ ปัจจุบันหลายหน่วยงานเปลี่ยนมาให้บริการโดยการเสียบบัตรประชาชนแทนการเซ็น เพราะเมื่อเสียบบัตรประชาชนจะปรากฏ Private Key เฉพาะของบุคคลในนั้นอยู่แล้ว เป็นการบอกว่าคนคนนั้นยินยอมในการลงลายมือชื่อในภาคเอกชนมักจะตั้งคำถามบ่อย ๆ ว่ามีผลทางกฎหมายหรือไม่ ต้องพิจารณาถึงองค์ประกอบของลายเซ็น โดยดูว่าระบบที่เราจะใช้มีการพิสูจน์ตัวตนหรือไม่ อย่างน้อยต้องรู้ว่าใครเป็นผู้ทำธุรกรรม และจะสืบกลับอย่างไร มีตั้งแต่ขั้นพื้นฐาน ซึ่งมีความเสี่ยงจะสูง แต่ถ้าต้องการจะทำธุรกรรมเกี่ยวกับเงินจำนวนมาก ต้องพิจารณาระบบที่รองรับความเสี่ยงตามมาตรฐานของ ETDA นอกจากนี้ต้องพิจารณาด้วยว่าระบบที่จะใช้สามารถป้องกันการแก้ไขได้หรือไม่ และพิจารณาความน่าเชื่อถือของตัวระบบเอง โดยหลักแล้วจะเน้นไปที่ผู้ใช้บริการต้องพิจารณาว่าการลงลายมือชื่อหรือการทำธุรกรรมมีความเหมาะสมหรือไม่ เพราะว่าผู้ให้บริการ Platform ไม่มีทางรู้เลยว่าเอกสารที่เราจะเซ็นมีรูปแบบอย่างไร

- คำถาม เกี่ยวกับแนวโน้มการใช้ลายเซ็นอิเล็กทรอนิกส์ในไทยจะเป็นอย่างไร ตั้งแต่ช่วงการระบาดของ Covid-19 เป็นต้นมามียอดการใช้งานมากกว่า 500 % นั่นหมายถึงมีความต้องการสูงมาก เพราะไม่สามารถออกจากบ้านได้ เช่น กรณีการลงนามข้อตกลง (MOU) ของบางองค์กร เมื่อมีผู้ใช้บริการใช้ไปแล้ว จะไม่อยากกลับไปใช้ระบบเดิมอีก เพราะมีความสะดวกและประหยัดค่าใช้จ่าย นอกจากนี้ ปัจจุบันมีกฎหมายการรองรับเกี่ยวกับลายเซ็นอิเล็กทรอนิกส์ซึ่งเป็นทิศทางที่ดีที่หน่วยงานภาครัฐจะหันมาใช้การลงลายมือชื่อทางอิเล็กทรอนิกส์ ส่วนภาคเอกชน ก็จะคลายกังวลมากขึ้นเกี่ยวกับการรับรองทางกฎหมาย

4. แนวทางการนำลายมือชื่ออิเล็กทรอนิกส์และเทคโนโลยีมาใช้ในหน่วยงาน

การลงลายมือชื่อทางอิเล็กทรอนิกส์ต้องอย่ากังวล และอย่ากลัวในการใช้ ต้องเริ่มจากการใช้ในการทำธุรกรรมเล็ก ๆ น้อย ๆ ก่อน การทำสัญญามูลค่าน้อย ๆ จะสามารถทำได้เลย หรือกรณีทำ MOU หรือข้อตกลงกันที่ไม่มีผลทางกฎหมายก็สามารถทำได้ ในหน่วยงานภาครัฐงานคดีและงานธุรการคงจะหลีกหนีไม่ได้ เพราะจำเป็นต้องใช้ เราต้องเข้าใจและเตรียมความพร้อมในการใช้งาน ซึ่งเป็นหน้าที่ของคนรุ่นใหม่ในการก้าวไปสู่การใช้เทคโนโลยีใหม่ๆ โดยไม่ทิ้งคนรุ่นเก่าที่ใช้ระบบแอนะล็อก (analog) ไว้ข้างหลัง ระยะหลังมีการพิจารณาว่า ระบบปัญญาประดิษฐ์ (artificial intelligence) อาจจะสามารถนำมาใช้แทนผู้พิพากษาในการพิจารณาคดีได้ แต่ความจริงแล้วระบบปัญญาประดิษฐ์ (artificial intelligence) อาจจะไม่มีอคติ มีมาตรฐานและเป็นกลาง แต่ระบบปัญญาประดิษฐ์ (artificial intelligence) อาจจะมีอคติในตัวมันเอง เนื่องจากผู้พัฒนาระบบปัญญาประดิษฐ์ (artificial intelligence) เช่น กรณีในสหรัฐอเมริกามีผลการสำรวจออกมาว่า ผู้หญิงมีแนวโน้มกลับมากระทำความผิดมากกว่าผู้ชาย ที่เป็นเช่นนี้เพราะผู้พัฒนาระบบปัญญาประดิษฐ์ (artificial intelligence) เป็นผู้ชาย นอกจากนี้ปัจจัยเรื่องผลการสำรวจที่ผ่านมาอาจจะมีการใส่ไว้ในระบบปัญญาประดิษฐ์ (artificial intelligence) เพื่อพิจารณาด้วย ทุกคนกลัวว่าระบบปัญญาประดิษฐ์ (artificial intelligence) จะมาแทนที่ แต่ความจริงแล้วระบบปัญญาประดิษฐ์ (artificial intelligence) จะมาแทนที่ได้เพียงงานที่เป็นลักษณะ Routine เช่น งานโรงงาน โดยหลักแล้วจะเป็นการช่วยมากกว่าการแทนที่

การพัฒนากรอบการกำกับดูแลข้อมูล กรณีลายมือชื่ออิเล็กทรอนิกส์

ธีรวุฒิ จันทดิษฐ์

บทคัดย่อ

ลายมือชื่ออิเล็กทรอนิกส์ซึ่งเป็นธุรกรรมทางอิเล็กทรอนิกส์ที่มีแนวโน้มอันจะสร้างผลกระทบต่อการดำเนินธุรกิจในระบบเศรษฐกิจดิจทัล จะส่งผลให้เกิดการปรับเปลี่ยนวิธีการติดต่อสื่อสารโดยอาศัยเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ มีความสะดวก รวดเร็ว ประหยัดต้นทุน และเอื้ออำนวยต่อการประกอบธุรกิจภาคเอกชนหรือการให้บริการประชาชนของภาครัฐในรูปแบบของธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจะเป็นกลไกสำคัญในการขับเคลื่อนเศรษฐกิจดิจิทัลและยกระดับคุณภาพชีวิตของประชาชน รวมถึงสอดคล้องกับนโยบายอำนวยความสะดวกในการประกอบธุรกิจ (Ease of Doing Business) แม้ว่า ลายมือชื่ออิเล็กทรอนิกส์ จะสามารถใช้ได้ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551 โดยอาศัยองค์ประกอบของลายชื่ออิเล็กทรอนิกส์ในการทำรับรองข้อความ แต่พบว่า องค์กรภาครัฐและผู้ประกอบการภาคเอกชน ยังขาดความเชื่อมั่นและความมั่นใจในการใช้ลายมือชื่ออิเล็กทรอนิกส์ ซึ่งเป็นปัญหาและอุปสรรคในเชิงนโยบายและการปฏิบัติ ทั้งในเรื่องการบริหารและจัดการความเสี่ยง การบริหารจัดการผลกระทบ และการรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งปัญหาและอุปสรรคส่วนใหญ่มักเป็นผลมาจากการบริหารที่ไม่ชัดเจนขององค์กร

ธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล (Data Governance) จะเป็นหัวใจสำคัญในการบริหารจัดการข้อมูล จะช่วยส่งเสริมให้องค์กรมีกลไกในการกำหนดทิศทาง นโยบาย ควบคุม และบริหารจัดการข้อมูล เพื่อให้องค์กรสามารถดำเนินการให้เป็นไปตามนโยบาย กฎ ระเบียบ สามารถจัดการความเสี่ยงและผลกระทบที่ก่อให้เกิดขึ้นอย่างมีประสิทธิภาพและมั่นคงปลอดภัย องค์กรต้องกำหนดแนวทางและกลยุทธ์การดูแลข้อมูล การรักษาความมั่นคงปลอดภัย และความรับผิดชอบของผู้มีส่วนได้ส่วนเสีย ที่สำคัญจะต้องสามารถวัดผลการดำเนินการได้ ก่อให้เกิดการบริหารจัดการข้อมูลที่ดี ส่งผลให้ข้อความมีความมั่นคงปลอดภัย มีคุณภาพ มีคุณค่าทางเศรษฐกิจและสังคม

การพัฒนากรอบการกำกับดูแลข้อมูล กรณีลายมือชื่ออิเล็กทรอนิกส์นี้ มุ่งหวังให้สามารถบริหารจัดการความเสี่ยง ความมั่นคงปลอดภัย รักษาความเป็นส่วนบุคคล และมีประสิทธิภาพ ซึ่งจะเป็นแนวทางให้องค์กรสามารถปรับใช้ตามลักษณะ สภาพแวดล้อม และวัฒนธรรมองค์กร เพื่อให้สามารถปรับตัวตามบริบทที่เปลี่ยนแปลงอย่างต่อเนื่อง

คำสำคัญ: ลายมือชื่ออิเล็กทรอนิกส์ , การกำกับดูแลข้อมูล , ธุรกรรมทางอิเล็กทรอนิกส์

บทนำ

ปัจจุบันการทำธุรกรรมทางอิเล็กทรอนิกส์มีบทบาทสำคัญในชีวิตประจำวันเป็นอย่างมาก ส่งผลให้เกิดการปรับเปลี่ยนวิธีการติดต่อสื่อสารโดยอาศัยเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ มีความสะดวก รวดเร็ว ประหยัดต้นทุน และเอื้ออำนวยต่อการประกอบธุรกิจภาคเอกชนหรือการให้บริการประชาชนของภาครัฐในรูปแบบของธุรกรรมทางอิเล็กทรอนิกส์ จนกลายเป็นยุคของการสื่อสารบนโลกดิจิทัล ซึ่งจะเป็นกลไกสำคัญในการขับเคลื่อนเศรษฐกิจดิจิทัลและยกระดับคุณภาพชีวิตของประชาชน รวมถึงสอดคล้องกับนโยบายอำนวยความสะดวกในการประกอบธุรกิจ (Ease of Doing Business) สำหรับประเทศไทยนั้น รัฐบาลได้เล็งเห็นถึงแนวโน้มของการพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ ที่เกี่ยวข้องหรือสนับสนุนการประกอบธุรกิจต่างๆ เพื่ออำนวยความสะดวก และการสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ จึงตราเป็นกฎหมายกำหนดหลักเกณฑ์เกี่ยวกับการกำกับดูแลธุรกิจบริการด้านธุรกรรมอิเล็กทรอนิกส์ เพื่อป้องกันความเสี่ยงที่อาจก่อให้เกิดขึ้นหรืออาจส่งผลกระทบในวงกว้าง

ในวันที่ 2 ตุลาคม 2561 คณะรัฐมนตรีมีมติ เรื่อง มาตรการอำนวยความสะดวกและลดภาระแก่ประชาชน (การไม่เรียกสำเนาเอกสารที่ทางราชการออกให้ จากประชาชน) ให้หน่วยงานของรัฐที่มีกฎหมาย กฎ ระเบียบ ข้อบังคับให้ประชาชนต้องยื่นหรือส่งสำเนาเอกสารที่ทางราชการออกให้ ดำเนินการเชื่อมโยงข้อมูลกับหน่วยงานที่เกี่ยวข้อง โดยไม่ต้องทำบันทึกข้อตกลง (MoU) หากประชาชนมาติดต่อขอรับบริการ ให้เจ้าหน้าที่เป็นผู้สั่งพิมพ์เอกสารหรือหลักฐานที่ต้องใช้จากระบบที่เชื่อมโยงไว้และลงนามรับรอง โดยประชาชนผู้มาติดต่อไม่ต้องเป็นผู้นำสำเนามาและไม่ต้องลงนามรับรอง รวมถึงเร่งรัดการดำเนินการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานราชการ ตามนัยมติคณะรัฐมนตรีเมื่อวันที่ 10 ตุลาคม 2560 [เรื่อง นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ พ.ศ. 2560-2564] ที่กำหนดให้หน่วยงานของรัฐบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงาน และพัฒนาขีดความสามารถองค์กรทุกภาคส่วนบุคลากรที่เกี่ยวข้องให้มีความรู้ความชำนาญด้านไซเบอร์อย่างต่อเนื่องต่อไป

ต่อมาในวันที่ 2 เมษายน 2562 คณะรัฐมนตรีมีมติ เรื่อง “การอออกเอกสารหลักฐานของทางราชการผ่านระบบดิจิทัล” เป็นนโยบายปรับปรุงประสิทธิภาพการปฏิบัติราชการให้กับประชาชน ซึ่งเป็นไปตามหลักการพัฒนาระบบราชการเพื่อชีวิตที่ดีขึ้นของประชาชน (Good Governance for Better life) ซึ่งเห็นชอบในหลักการการออกเอกสารหลักฐานของทางราชการผ่านระบบดิจิทัล โดยให้มีการนำร่องดำเนินการในภารกิจของหน่วยงานที่มีผลกระทบต่อประชาชน ผู้ประกอบการ และนักลงทุนเป็นสำคัญก่อน ตามความเห็นของกระทรวงอุตสาหกรรม หากหน่วยงานที่เกี่ยวข้องมีความจำเป็นต้องแก้ไขกฎหมายเพื่อรองรับการดำเนินการดังกล่าว ให้ดำเนินการให้สอดคล้องกับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ตามความเห็นของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หากหน่วยงานใดไม่สามารถปรับปรุงแก้ไขกฎระเบียบเพื่อรองรับการดำเนินการผ่านระบบดิจิทัลได้ภายในปี พ.ศ. 2562 หรือไม่

สามารถพัฒนางานบริการให้เป็นระบบการให้บริการอิเล็กทรอนิกส์ (e-Service) หรือยกเลิกการใช้กระดาษได้ภายในปี พ.ศ. 2563 ตลอดจนในกรณีที่มีปัญหาในทางปฏิบัติ ให้หน่วยงานดังกล่าวเร่งประสานงานกับสำนักงาน ก.พ.ร. เพื่อพิจารณาขยายระยะเวลาการดำเนินการเป็นรายกรณี

โดยมีเป้าหมายเพื่ออำนวยความสะดวกแก่ประชาชน ลดต้นทุนของประชาชนและเพิ่มประสิทธิภาพในการให้บริการของภาครัฐ ซึ่งเป็นไปตามหลักการของพระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. 2558 กรณีที่มีกฎหมายกำหนดให้การกระทำใดจะต้องได้รับอนุญาต ผู้อนุญาตจะต้องจัดทำคู่มือสำหรับประชาชน ซึ่งอย่างน้อยต้องประกอบด้วย หลักเกณฑ์ วิธีการ และเงื่อนไข (ถ้ามี) ในการยื่นคำขอ ขั้นตอนและระยะเวลาในการพิจารณาอนุญาตและรายการเอกสารหรือหลักฐานที่ผู้ขออนุญาตจะต้องยื่นมาพร้อมกับคำขอ และจะกำหนดให้ยื่นคำขอผ่านทางอิเล็กทรอนิกสแทนการมายื่นคำขอด้วยตนเองก็ได้ การสร้างให้เกิดความโปรงใสในการปฏิบัติราชการ โดยการลดการใช้ดุลยพินิจของเจ้าหน้าที่ เปิดเผย ขั้นตอน ระยะเวลาให้ประชาชนทราบ เพื่อเป้าหมายอันเปนหัวใจสำคัญในการอำนวยความสะดวกประชาชน

กฎหมายและประกาศที่เกี่ยวข้องกับการลงลายมือชื่ออิเล็กทรอนิกส์

การใช้ลายมือชื่ออิเล็กทรอนิกส์ เป็นการลงลายมือชื่อเพื่อรับรองข้อความ หรือข้อมูลที่อยู่ในรูปแบบของข้อมูลทางอิเล็กทรอนิกส์ ซึ่งต้องสามารถระบุและยืนยันเจ้าของผู้ลงลายมือชื่อ และสามารถตรวจสอบได้ว่าข้อมูลจะไม่มีการดัดแปลงแก้ไข การยืนยันตัวตนในรูปแบบดิจิทัลเป็นผลไม่ต่างจากการยืนยันตัวตนโดยการจับปากกาในกระดาษ หากผู้ใช้งานหรือองค์กรสามารถลงลายชื่ออิเล็กทรอนิกส์ได้อย่างถูกต้องตามกฎหมาย อย่างไรก็ตามประเด็นเรื่องความน่าเชื่อถือ อาจเป็นปัญหาสำคัญในทางปฏิบัติมากกว่า ดังนั้นควรทำความเข้าใจกฎหมายและประกาศที่เกี่ยวข้องกับการลงลายมือชื่ออิเล็กทรอนิกส์ ประกอบด้วย

- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551
    - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. 2562
    - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง การรับรองสิ่งพิมพ์ออก พ.ศ. 2555
    - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หน่วยงานรับรองสิ่งพิมพ์ออก พ.ศ. 2555
    - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553
    - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. 2552

- พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรม
- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

นิยาม หลักเกณฑ์ และวิธีการลงลายมือชื่ออิเล็กทรอนิกส์

ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 รวมถึงแก้ไขเพิ่มเติม ฉบับที่ 2 พ.ศ. 2551 และฉบับที่ 3 พ.ศ. 2563 ซึ่งกำหนดนิยาม หลักเกณฑ์ และวิธีการลงลายมือชื่ออิเล็กทรอนิกส์ไว้ ดังนี้

1. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 “ลายมือชื่ออิเล็กทรอนิกส์” หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่น ใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดง ความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็น เจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคล ดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น”
2. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ฉบับที่ 3 พ.ศ. 2563 มาตรา 7 ยกเลิกความในมาตรา ๙ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ และให้ใช้ความต่อไปนี้แทน “มาตรา 9 ในกรณีที่กฎหมายกำหนดให้มีการลงลายมือชื่อ หรือกำหนดผลทางกฎหมายกรณีที่ไม่มีการลงลายมือชื่อไว้ ให้ถือว่าได้มีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงเจตนาของเจ้าของลายมือชื่อ เกี่ยวกับข้อความในข้อมูลอิเล็กทรอนิกส์ และ

(๒) ใช้วิธีการในลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(ก) วิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมทั้งปวง รวมถึงข้อตกลงใด ๆ ที่เกี่ยวข้อง หรือ

(ข) วิธีการอื่นใดที่สามารถยืนยันตัวเจ้าของลายมือชื่อและสามารถแสดงเจตนาของเจ้าของลายมือชื่อตาม (๑) ได้ด้วยวิธีการนั้นเองหรือประกอบกับพยานหลักฐานอื่น

วิธีการที่เชื่อถือได้ตามวรรคหนึ่ง (๒) (ก) ให้คำนึงถึง

๑) ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้งาน ของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมาย ระดับความมั่นคง ปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

(๒) ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำจำนวนครั้งหรือความสม่ำเสมอใน การทำธุรกรรม ประเพณีทางการค้าหรือทางปฏิบัติ ความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

(๓) ความรัดกุมของระบบการติดต่อสื่อสาร ให้นำความในวรรคหนึ่งมาใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ด้วย โดยอนุโลม”

3. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 26 ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อ โดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใดๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้และ

(๔) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความ ครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบ ได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๘ ในกรณีมีการให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มี ผลทางกฎหมายเสมือนหนึ่งลงลายมือชื่อผู้ให้บริการออกใบรับรองต้องดำเนินการ ดังต่อไปนี้

(๑) ปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ตนได้แสดงไว้

(๒) ใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและความสมบูรณ์ของการแสดงสาระสำคัญทั้งหมดที่ตนได้กระทำเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

(๓) จัดให้มีวิธีการในการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบ ข้อเท็จจริงในการแสดงสาระสำคัญทั้งหมดจากใบรับรองได้ในเรื่องดังต่อไปนี้

(ก) การระบุผู้ให้บริการออกใบรับรอง

(ข) เจ้าของลายมือชื่อซึ่งระบุในใบรับรองได้ควบคุมข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ในขณะมีการออกใบรับรอง

(ค) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผล ใช้ได้ในขณะหรือก่อนที่มีการออกใบรับรอง

(๔) จัดให้มีวิธีการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบกรณีดังต่อไปนี้จากใบรับรองหรือจากวิธีอื่น

(ก) วิธีการที่ใช้ในการระบุตัวเจ้าของลายมือชื่อ

(ข) ข้อจำกัดเกี่ยวกับวัตถุประสงค์และคุณค่าที่มีการนำข้อมูลสำหรับใชสร้างลายมือชื่ออิเล็กทรอนิกส์หรือใบรับรอง

(ค) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผลสมบูรณ์ใช้ได้และไม่สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(ง) ข้อจำกัดเกี่ยวกับขอบเขตความรับผิดที่ผู้ให้บริการออกใบรับรองได้ระบุไว้

(จ) การมีวิธีการให้เจ้าของลายมือชื่อส่งคำบอกกล่าวเมื่อมีเหตุตามมาตรา ๒๗ (๒)

(ฉ) การมีบริการเกี่ยวกับการเพิกถอนใบรับรองที่ทันการ

(๕) ในกรณีที่มีบริการตาม (๔) (จ) บริการนั้นต้องมีวิธีการที่ให้เจ้าของลายมือชื่อสามารถ แจ้งได้ตามหลักเกณฑ์ที่กำหนดตามมาตรา ๒๗ (๒) และในกรณีที่มีบริการตาม (๔) (ฉ) บริการนั้น ต้องสามารถเพิกถอนใบรับรองได้ทันการ

(๖) ใช้ระบบ วิธีการ และบุคลากรที่เชื่อถือได้ในการให้บริการ

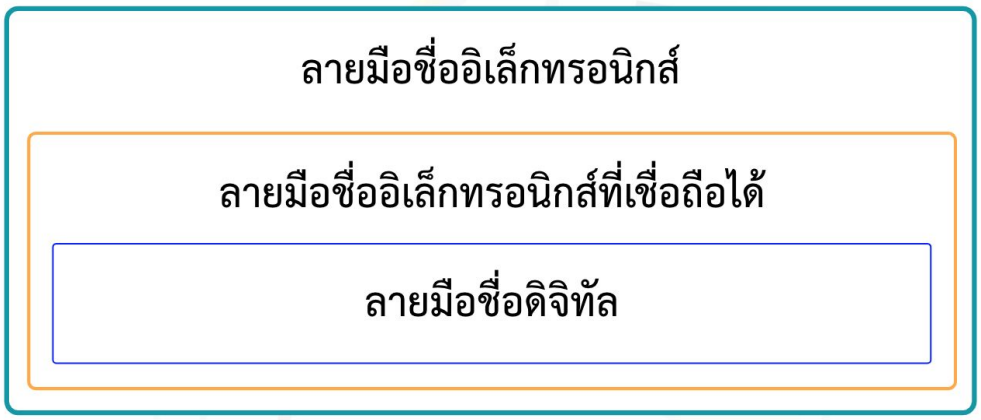
หลักการของลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ = **ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้** = **ลายมือชื่อดิจิทัล**

เมื่อพิจารณาจากนิยาม หลักเกณฑ์ และวิธีการลงลายมือชื่ออิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์แล้วนั้น สามารถสรุปเป็นรูปข้างต้นนี้ โดยแบ่งลายมือชื่ออิเล็กทรอนิกส์เป็น 3 รูปแบบ ในทางเทคโนโลยีสารสนเทศจะมีความแตกต่างกัน แต่ในทางกฎหมายแล้วการลงลายมือชื่ออิเล็กทรอนิกส์ใน 3 รูปแบบนั้นมีผลทางกฎหมายเท่ากัน

ลายมือชื่ออิเล็กทรอนิกส์*	**มาตรา 4** แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กำหนดนิยามไว้ว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์ ที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ *เป็นเพียงนิยามของกฎหมาย*
ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป	ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป เป็นลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบใด ๆ ที่มีลักษณะตามที่กำหนดใน**มาตรา 9**แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ○ สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงเจตนาของเจ้าของลายมือชื่อ ○ วิธีการที่น่าเชื่อถือ กล่าวคือ มีความปลอดภัย มีศัพยภาพเพียงพอ ความน่าเชื่อถือและความน่าเหมาะสมของธุรกรรม
ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้	ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดใน**มาตรา 26** แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และ**มาตรา 28** (**ลายมือชื่อดิจิทัล**) อาศัยใบรับรองที่ออกโดยผู้ให้บริการออก ใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์

แต่หากพิจารณาโดยอาศัยหลักการทางเทคโนโลยีสารสนเทศ ซึ่งเทียบเคียงตามหลักการทางกฎหมาย สามารถแบ่งลายมือชื่ออิเล็กทรอนิกส์เป็นดังภาพด้านล่างนี้

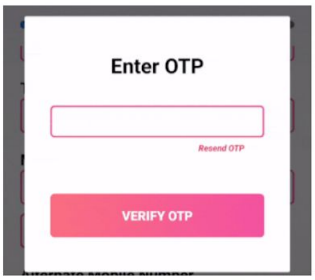


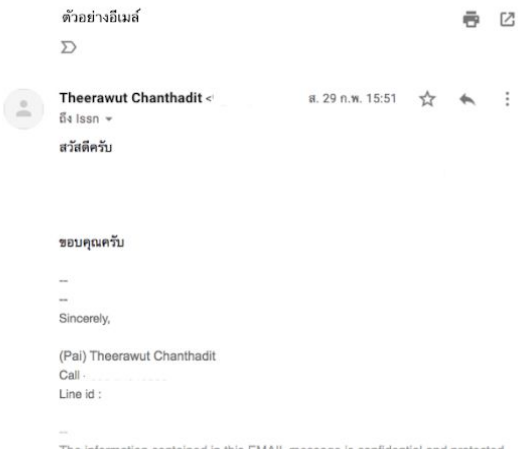
ลายมือชื่ออิเล็กทรอนิกส์ เป็นคำที่กว้างมากไม่ได้เฉพาะเจาะจงหรือกำหนดหลักการไว้ เพียงว่าเป็นการกระทำการบางอย่าง เพื่อรับรองข้อความหรือตกลงเพื่อใช้งาน

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ เป็นการเชื่อมโยงข้อมูล และแสดงเจตนาอย่างชัดแจ้งของเจ้าของลายมือชื่อ โดยต้องมีพยานหลักฐานรองรับ

ลายมือชื่อดิจิทัล เป็นการนำกุญแจสาธารณะ (Public Key - Infrastructure - PKI) หรือเทคโนโลยีอื่นใด เข้าเป็นมีส่วนประกอบในการลงลายมือชื่อ เพื่อสร้างความน่าเชื่อถือและความปลอดภัยมากยิ่งขึ้น

ตัวอย่างของรูปแบบลายมือชื่ออิเล็กทรอนิกส์





- การเข้าสู่ระบบของผู้ใช้งาน จากนั้นให้คลิกปุ่มยอมรับหรือตกลงหรือทำเครื่องหมาย
- การเขียนลายมือชื่อด้วยมือโดยอุปกรณ์ใดๆลงบนหน้าจอและบันทึกไว้ในรูปแบบอิเล็กทรอนิกส์
- การพิมพ์ชื่อไว้ในอีเมล
- รูปภาพลายมือชื่อ
- การใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP)
- การใช้รหัสผ่านหรือรหัสลับส่วนบุคคล (PIN)
- การใช้ลายมือชื่อดิจิทัล
- การใช้ข้อมูลชีวมิติ เช่น ลายนิ้วมือ ม่านตา

การพิสูจน์และยืนยันตัวตน

เป็นการระบุตัวตน การแสดงตน การพิสูจน์ตัวตน การแสดงหลักฐานใดๆ และการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับผู้ขอใช้บริการและการยืนยันตัวตนของผู้ขอใช้บริการ ช่วยในการตรวจสอบข้อมูลและยืนยันตัวบุคคล ทำให้อุปสรรคต่าง ๆ กลายเป็นเรื่อง ง่าย ตอบโจทย์ทุกความต้องการใช้งานง่าย สะดวกรวดเร็ว มีความปลอดภัยสูง

1. ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)

ข้อมูลอิเล็กทรอนิกส์ หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้ สร้างลายมือชื่ออิเล็กทรอนิกส์ ซึ่งออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority : CA) ที่มีความน่าเชื่อถือ อาศัยเทคโนโลยีที่เรียกว่า กุญแจสาธารณะ (Public Key Infrastructure : PKI) สามารถนำมาใช้ในการลงลายมือชื่อดิจิตอล (Digital Signature) หรือ การเข้า-ถอดรหัส (Encryption) ได้

อุปกรณ์สำหรับเข้ารหัส

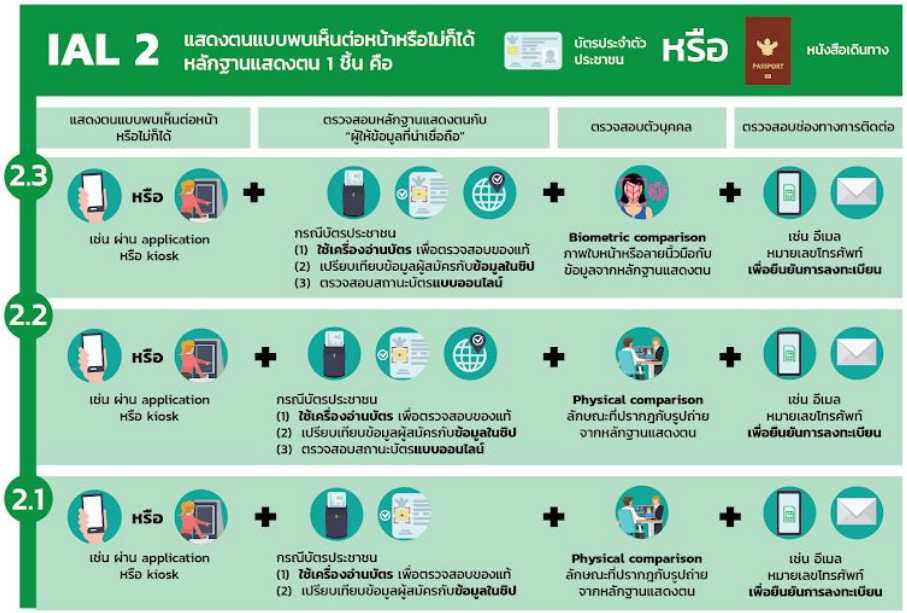
การใช้ใบรับรองอิเล็กทรอนิกส์ ผู้ใช้จะสามารถมั่นใจได้ว่า

- ข้อมูลต่างๆ ที่ได้รับมีความถูกต้อง ครบถ้วน ไม่ถูกเปลี่ยนแปลงแก้ไข
- สามารถพิสูจน์ และยืนยันตัวบุคคลได้ ว่าเป็นบุคคลผู้ที่เราติดต่อด้วยจริง
- สามารถรักษาความลับของข้อมูลได้ หากเป็นข้อมูลที่ต้องการให้ผู้รับเท่านั้นที่สามารถอ่านอีเมล์ฉบับนั้นๆได้ ซึ่งกรณีนี้จะต้องมีการใช้ใบรับรองอิเล็กทรอนิกส์ในการเข้ารหัสก่อนทำการส่งอีเมล์ไปยังผู้รับ

2. การพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)

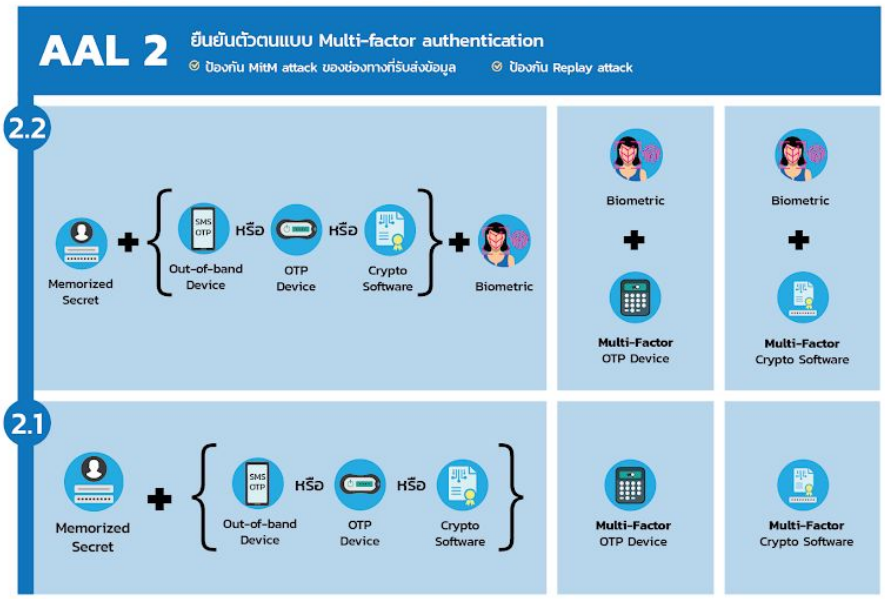
การพิสูจน์และยืนยันตัวตน เป็นไปตามประกาศของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย (Digital Identity Guideline for Thailand)

- ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL)



ตามหลักการทำธุรกรรมพิสูจน์และยืนยันตัวตนให้ได้มาตรฐานนั้น ควรจะใช้ความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนระดับ 2 หรือ Identity Assurance Level 2 (IAL2)

- ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL)



เป็นกระบวนการที่ใช้ยืนยันในการเข้าถึงข้อมูลซึ่งควรเป็นการยืนยันตัวตนแบบหลายปัจจัย อย่างไรก็ตามขึ้นอยู่กับความสามารถด้านความปลอดภัยของระบบด้วย โดยทั่วไปควรใช้ความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนระดับ 2 หรือ Authenticator Assurance Level2 (AAL2

3. วิธีการอื่น ๆ

เช่น การให้ผู้ใช้บริการหรือผู้ที่ลงลายมือชื่ออิเล็กทรอนิกส์ ต้องมาลงทะเบียนพิสูจน์ตัวตน ณ สถานที่แห่งใดแห่งหนึ่งด้วยวิธีการที่น่าเชื่อถือและยอมรับได้

องค์ประกอบลายมือชื่ออิเล็กทรอนิกส์

เป็นปัจจัยในการพิจารณาความน่าเชื่อถือ ความเหมาะสมของการลงลายมือชื่ออิเล็กทรอนิกส์ เพื่อให้ข้อมูลอิเล็กทรอนิกส์ที่เจ้าของลายมือชื่อต้องการรับรองนั้น สามารถเป็นพยานหลักฐานที่ใช้ในกระบวนการพิจารณาตามกฎหมายได้ อย่างไรก็ดีองค์ประกอบลายมือชื่ออิเล็กทรอนิกส์นี้ไม่ได้กำหนดขึ้นตามบทบัญญัติของตามกฎหมาย แต่เป็นการเทียบเคียงกับมาตรฐานของต่างประเทศ ดังนี้

- **รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ (Electronic Form of Signature)**

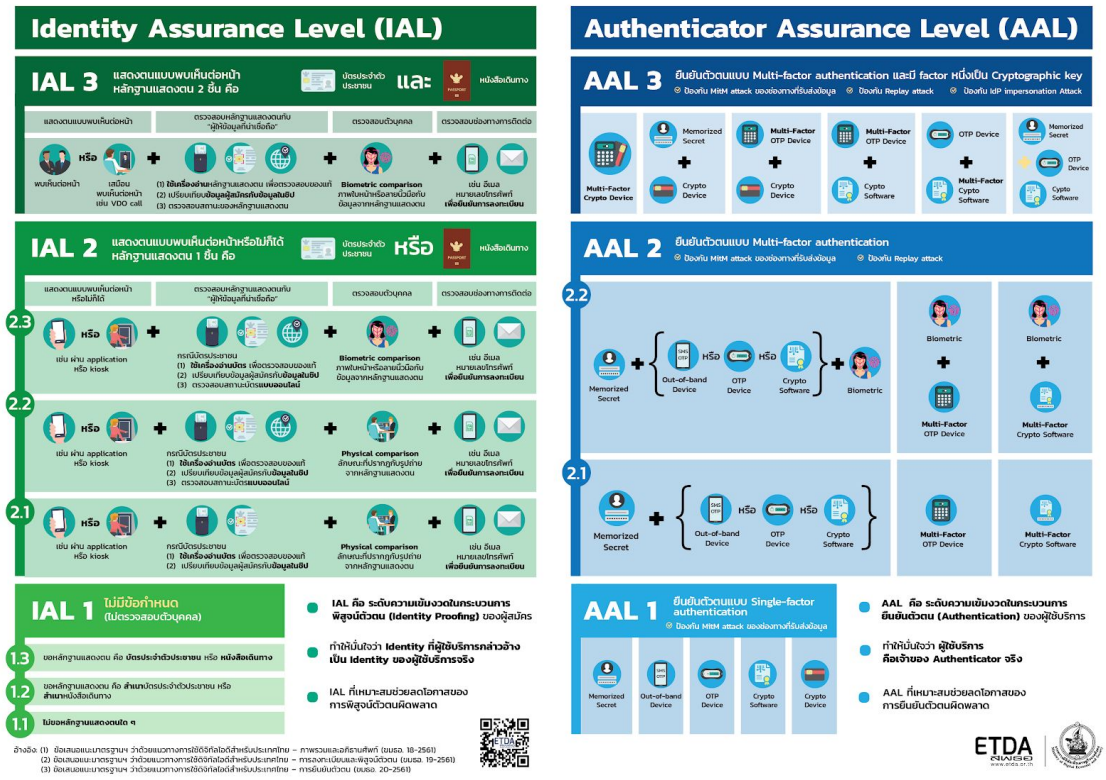
รูปแบบของลายมือชื่อที่เคยใช้อยู่ จะเป็นการเขียนชื่อ สัญลักษณ์ การพิมพ์ลายนิ้วมือ การทำเครื่องหมาย รวมถึงวิธีการอื่นๆ ลงในกระดาษ แต่การลงลายมือชื่ออิเล็กทรอนิกส์ตามนิยามมาตรา 4 ไม่ได้เฉพาะเจาะจงรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ไว้ แต่กำหนดลักษณะที่ควรจะเป็น ดังนั้นการจะเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบใดก็ได้ แต่ควรจะพิจารณาความเหมาะสม ความน่าเชื่อ ลักษณะ ประเภท หรือมูลค่าในการทำธุรกรรมนั้นด้วย เช่น

- การคลิกปุ่มยอมรับเงื่อนไขข้อตกลง
- การบันทึกเสียง
- การใส่รูปลายมือชื่อ
- การใช้รหัสผ่านหรือรหัสลับ (PIN)

- ลายมือชื่อดิจิทัล
- ข้อมูลชีวิตภาพ เช่น ม่านตา ลายนิ้วมือ
- การใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP)
- การพิมพ์ในท้ายเอกสาร หรือท้ายอีเมล์

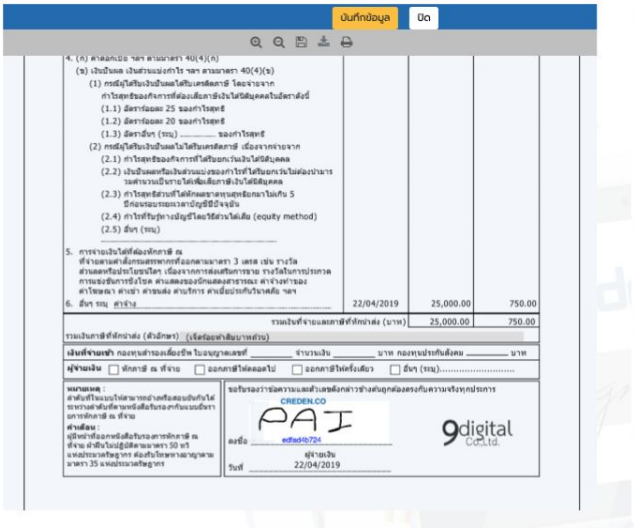
หมายเหตุ รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ ไม่เป็นองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (ขมธอ. 23-2563) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

- **การพิสูจน์และยืนยันตัวตน (Identification & Authentication)**



เดิมการพิสูจน์และยืนยันตัวตนของผู้ลงลายมือชื่อ จะต้องพิสูจน์และยืนยันตัวตนด้วยนิติวิทยาศาสตร์หรือพยานบุคคล พยานแวดล้อม เป็นต้น แต่ลายมือชื่ออิเล็กทรอนิกส์จะเป็นที่ยอมรับได้ต้องสามารถพิสูจน์ต่อศาลได้ว่า ผู้ใด เป็นเจ้าของลายมือชื่อนั้น ซึ่งถือว่าเป็นปัจจัยที่สำคัญมาก แต่รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ที่ใช้ ไม่จำเป็นต้องสามารถระบุตัวเจ้าของลายมือชื่อ เช่น การคลิกปุ่มหรือทำเครื่องยอมรับ ดังนั้นต้องอาศัยวิธีการอื่น เพื่อให้สามารถระบุและยืนยันตัวเจ้าของลายมือชื่อได้ โดยอาจจะใช้ ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) หรือ การพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) เป็นต้น

- **การเชื่อมโยงข้อมูลกับลายมือชื่อ (Association of Signature to the Record)**



Certificate Of Completion/ใบรับรองการสำเร็จ	
Envelope Id/หมายเลขเอกสาร: 1590139505	Status: Completed/สถานะ:สมบูรณ์
Subject: Please DocuSign/เรื่องเอกสาร: t	.pdf
Document Pages/จำนวนหน้า: 1	Signatures/ลายเซ็น: 1
Certificate Pages/จำนวนหน้าใบรับรอง: 1	
Envelopeld Stamping: Enabled/เวลาเปิดใช้งาน	IP Address: 184.22.86.21
Time Zone: (GMT+07:00) Bangkok	

Record Tracking/การติดตามบันทึก		
Status/สถานะ: 22/05/2020 16:26:48	Holder/เจ้าของ: t	Location/สถานะ: Creden.co

Signer Events/ลำดับการเซ็น	Timestamp/เวลา
1)	Sent/ส่งเมื่อ: 22/05/2020 16:26:48
	Signed/เซ็นครบเมื่อ: 22/05/2020 16:30:05
Security Level/ระดับความปลอดภัย : Email/อีเมล์,OTP/รหัสยืนยัน	Using IP Address/ใช้หมายเลข IP Address: 184.22.86.21

Envelope Summary Events/สรุปกิจกรรมการเซ็น	Timestamp/เวลา
Envelope sent/ส่งเมื่อ	22/05/2020 16:26:48
Signing complete/เซ็นครบเมื่อตอนไหน	22/05/2020 16:30:05
completed/เซ็นสมบูรณ์	22/05/2020 16:30:09

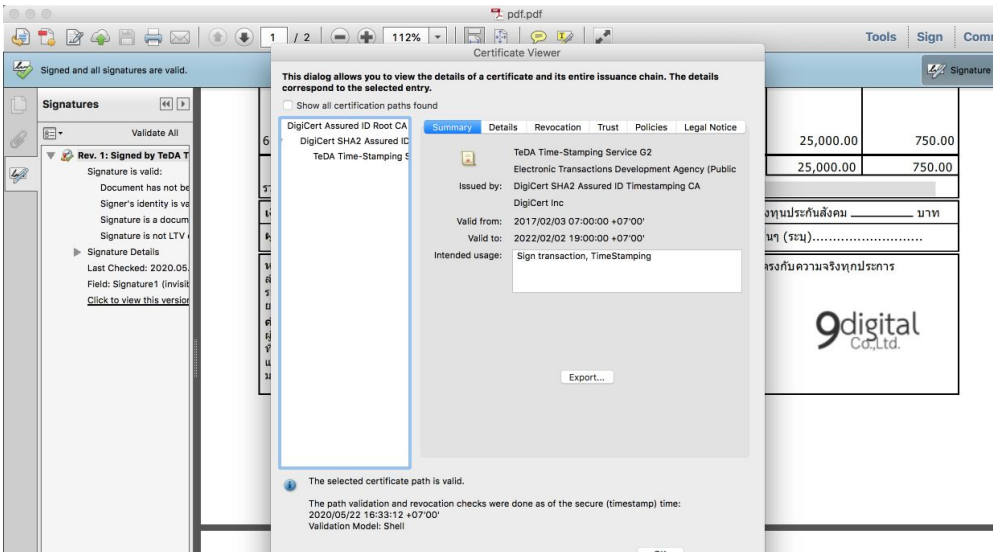
การใช้กระดาษจะปรากฏข้อความต่อหน้าผู้ที่จะลงลายมือชื่ออย่างชัดเจนว่า ต้องการจะรับรองข้อความใด โดยมีโอกาสใยการทวบทวนและทำความเข้าใจได้ว่า ตนกำลังจะลงลายมือชื่อ แต่ในทางธุรกรรมอิเล็กทรอนิกส์นั้น จะต้องออกแบบวิธีการลงลายมือชื่อให้ชัดเจน และให้มั่นใจว่าเจ้าของลายมือชื่ออิเล็กทรอนิกส์กับข้อความเท่าที่ปรากฏเท่านั้น และมีโอกาสทบทวนข้อความที่กำลังลงลายมือชื่อได้ กล่าวคือ เมื่อลายมือชื่ออิเล็กทรอนิกส์แล้ว จะต้องมีแสดงเจตนาในการลงลายมือชื่ออีกครั้งเป็นการยืนยัน และจะต้องมีการเชื่อมโยงข้อมูลลายมือชื่ออิเล็กทรอนิกส์กับเจ้าของลายมือชื่ออย่างถาวร ไม่สามารถลบหรือแก้ไขภายหลังได้ ในระบบควรจะสามารถบ่งบอกความสมบูรณ์ของการลงลายมือชื่อหรือบันทึกข้อความของการลงลายมือชื่อ เช่น การจัดเก็บ Log ควบคู่กับข้อมูลส่วนประกอบอื่นอันจะเป็นพยานหลักฐานทางอิเล็กทรอนิกส์ที่สำคัญ

หมายเหตุ การเชื่อมโยงข้อมูลกับลายมือชื่อ ไม่เป็นองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (ขมธอ. 23-2563) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

- **เจตนาในการลงลายมือชื่อ (Intent to Sign)**

การออกแบบวิธีการลงลายมือชื่ออิเล็กทรอนิกส์ จะต้องออกแบบให้ลดความเสี่ยงที่เจ้าของลายมือชื่อจะสามารถอ้างได้ว่า ไม่ทราบรูปแบบของลายมือชื่ออิเล็กทอรนิกส์ ซึ่งทำให้ไม่เข้าใจวัตถุประสงค์หรือเจตนาในการลงลายมือชื่อ โดยทั่วไปแล้ว สามารถอนุมานหรือเข้าใจได้ว่า การแสดงออก หรือ การตอบสนองบางอย่างของเจ้าของลายมือชื่อต่อข้อความที่แสดงวัตถุประสงค์ในการลงลายมือ เช่น การคลิกปุ่ม “ยอมรับข้อตกลง” หรือ “หน้าถัดไป” ถือว่าข้าพเจ้าได้รับทราบและยอมรับเงื่อนไขการใช้งาน ซึ่งประโยคนี้แสดงให้เห็นวัตถุประสงค์ในการลงลายมือชื่อ และวิธีการที่บุคคลจะใช้แสดงเจตนาในการลงลายมือชื่อ ซึ่งการคลิกปุ่มของผู้ใช้ เป็นการแสดงให้เห็นเจตนาในการลงลายมือชื่ออย่างชัดเจน

- **การรักษาความครบถ้วนของข้อมูล (Integrity of the Signed Record)**



เป็นปัจจัยที่สำคัญอย่างมากในการลงลายมือชื่อทางอิเล็กทรอนิกส์ เพราะหากว่าเอกสารหรือข้อมูลอิเล็กทรอนิกส์ที่เจ้าของลายมือชื่อได้ให้การรับรองได้แล้ว มีการแก้ไขเปลี่ยนแปลง จะไม่สามารถนำมาใช้บังคับได้ ดังนั้นการออกแบบควรจะต้องมีวิธีการรักษาความครบถ้วนของข้อมูล มีมาตรการป้องกันการแก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลอิเล็กทรอนิกส์ตลอกเวลาของการจัดเก็บ จะต้องมีความน่าเชื่อถือเพียงพอที่จะใช้เป็นพยานหลักฐานต่อศาลได้ โดยมักใช้การประทับรับรองเวลา (Time stamp) ซึ่งสามารถตรวจพบการแก้ไขเปลี่ยนแปลงข้อมูลอิเล็กทรอนิกส์นั้นได้

การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์

ผู้ที่ต้องการลงลายมือชื่ออิเล็กทรอนิกส์ ต้องตระหนักถึงความจำเป็นและต้องคำนึงถึงความน่าเชื่อถือความเหมาะสมกับวัตถุประสงค์ที่กำหนด และรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ เพื่อทำให้ลายชื่ออิเล็กทรอนิกส์สามารถนำมาใช้บังคับได้ โดยพิจารณาจาก

- องค์ประกอบของลายมือชื่ออเล็กทรอนิกส์ (5ข้อ)
    - รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ (Electronic Form of Signature)
    - การพิสูจน์และยืนยันตัวตน (Identification & Authentication)
    - การเชื่อมโยงข้อมูลกับลายมือชื่อ (Association of Signature to the Record)
    - เจตนาในการลงลายมือชื่อ (Intent to Sign)
    - การรักษาความครบถ้วนของข้อมูล (Integrity of the Signed Record)
- มีความมั่นคงปลอดภัยและ รัดกุมของระบบและอุปกรณ์
- ลักษณะ ประเภท ขนาดหรือมูลค่าของธุรกรรม

ทั้งนี้ ควรมีการประเมินความเสี่ยงในการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ เพื่อป้องกันการกล่าวปฏิเสธว่า ไม่มีเจตนาในการลงลายมือชื่อ หรือการกล่าวอ้างว่าข้อมูลไม่มีความครบถ้วน

การรักษาความมั่นคงปลอดภัยทางสารสนเทศ

มาตรการที่ใช้สำหรับป้องกันข้อมูลสารสนเทศที่เกี่ยวข้องกับซอฟต์แวร์และฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนข้อมูลสารสนเทศนั้นเพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตในการเข้าถึง ลบ แก้ไข หรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตเข้าใช้งาน ให้อยู่ในสถานะที่มีความปลอดภัยไร้ความกังวลและความกลัว มุ่งเน้นให้

- การรักษาความลับ (Confidentiality) คุณสมบัติว่าข้อมูลจะไม่ถูกเผยแพร่หรือเปิดเผยให้บุคคล กิจการ หรือกระบวนการที่ไม่ได้รับอนุญาต
- ความครบถ้วนถูกต้อง (Integrity) คุณสมบัติของการปกป้องความถูกต้องและครบถ้วนของทรัพย์สิน

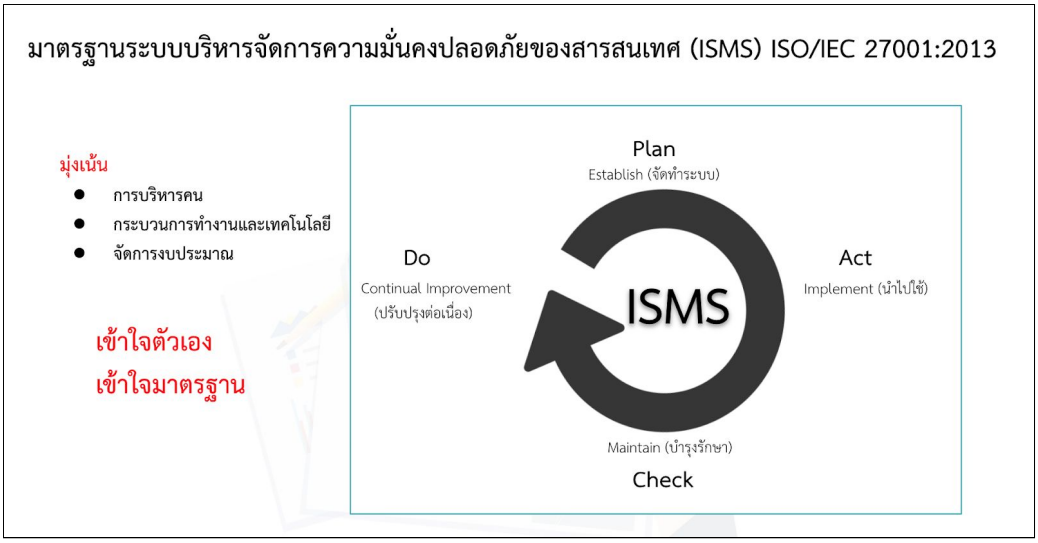
- ความพร้อมใช้ (Availability) คุณสมบัติของการเป็นที่สามารถเข้าถึงและใช้งานได้ตามความต้องการโดยกิจการที่ได้รับอนุญาต

รวมทั้งคุณสมบัติอื่นๆ ประกอบด้วย คือ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางสารสนเทศ

- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และ ฉบับที่ 2 พ.ศ. 2553
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555
  - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
  - ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
  - ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ พ.ศ. 2560
  - ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่ง ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ พ.ศ. 2560

องค์กรควรต้องตระหนักถึง ความมั่นคงปลอดภัยทางสารสนเทศอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง ป้องกันปัญหาหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ องค์กรต้องกำหนดให้มีนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ ให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ กำหนดหน้าที่ บทบาท วิเคราะห์สถานการณ์ ประเมินความเสี่ยง จัดระดับความเสี่ยง ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ โดยควรจะมีดังนี้

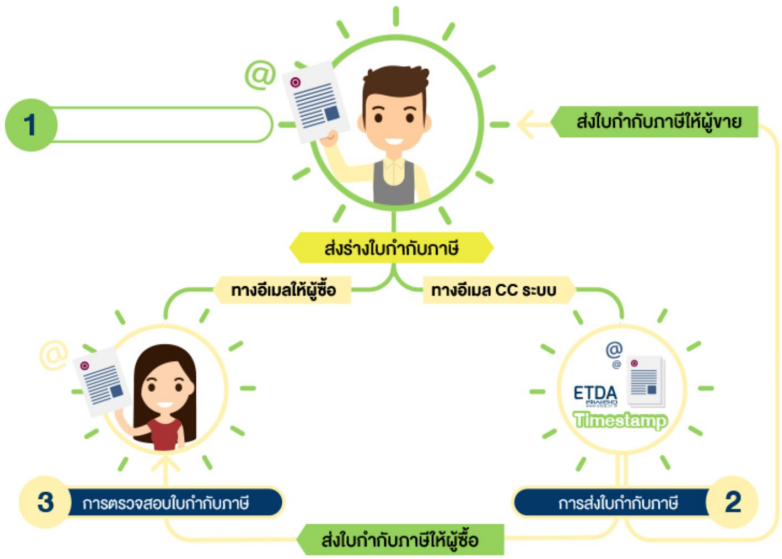


- นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งาน
- แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และ 2556
- มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
- กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ ให้เป็นไปตามมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS) ISO/IEC 27001:2013
- อื่นๆ ตามกฎหมายที่เกี่ยวข้อง

อย่างไรก็ตาม เบื้องต้นองค์กร ควรมี มาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใชงาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือขาย และระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพยสินที่มีค่าและอาจจำเปนตองรักษาความลับ จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบสารสนเทศ

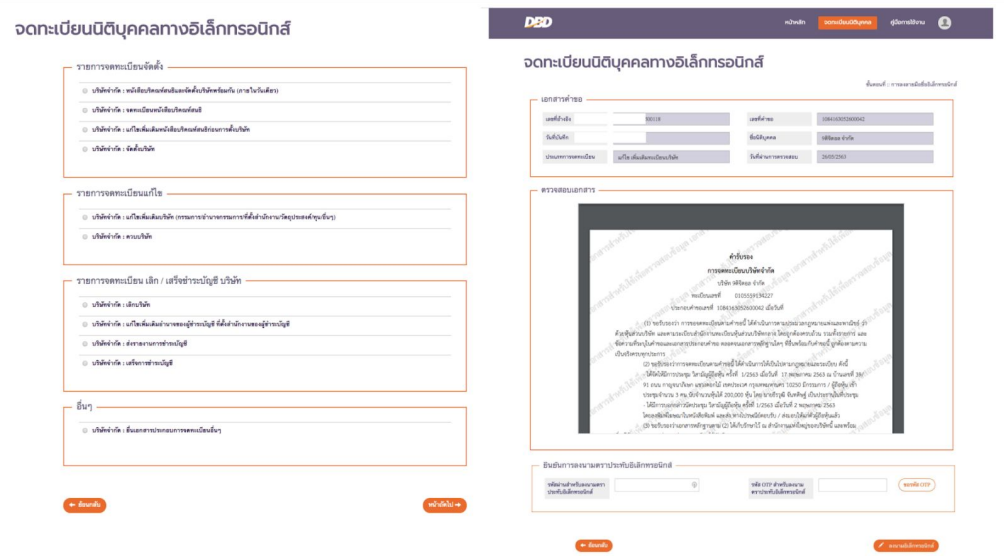
ตัวอย่างการใช้ลายมือชื่ออิเล็กทรอนิกส์

กรมสรรพากร



กรมสรรพากร มีนโยบายในการส่งเสริมและสนับสนุนให้ผู้ประกอบการจัดทำและนำส่งใบกำกับภาษีอิเล็กทรอนิกส์และใบรับรองอิเล็กทรอนิกส์ (e-Tax invoice & e-Receipt) เพื่อสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาคเอกชน และเพิ่มประสิทธิภาพการให้บริการอิเล็กทรอนิกส์ของภาครัฐ ซึ่งสอดคล้องตามมาตรฐานสากล รวมทั้งข้อเสนอแนะของสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อนเศรษฐกิจและสังคม โดยการจัดทำใบกำกับภาษีอิเล็กทรอนิกส์ (e-Tax invoice) และใบรับรองอิเล็กทรอนิกส์ (e-Receipt) เป็นรูปแบบข้อมูลอิเล็กทรอนิกส์ที่มีการลงลายมือชื่อดิจิทัล (Digital Signature) และประทับรับรองเวลา (e-Time Stamp) ผู้ประกอบจะใช้ผ่านระบบบัญชี หรือสามารถพัฒนาระบบงานของตนเอง หรือจัดหาซอฟต์แวร์ สำหรับการจัดทำใบกำกับภาษีอิเล็กทรอนิกส์ (e-Tax invoice) รวมถึงใบรับรองอิเล็กทรอนิกส์ (e-Receipt) อาจจะเป็นรูปแบบ เช่น PDF , PDF/A-3 , XML File ที่มีการลงลายมือดิจิทัล หรือ อื่นๆ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และต้องนำส่งข้อมูลรูปแบบ XML File ที่มีการลงลายมือชื่อดิจิทัล ผ่านระบบอิเล็กทรอนิกส์ของกรมสรรพากร และหากผู้ประกอบการที่มีรายได้ไม่เกิน 30 ล้านบาท สามารถจัดทำเฉพาะใบกำกับภาษี ใบเพิ่มหนี้ ใบลดหนี้ให้อยู่ในรูปแบบของไฟล์ที่กำหนดและแนบไฟล์ทางอีเมล์ส่งถึงผู้ซื้อหรือผู้รับบริการ พร้อมสำเนา (CC) ถึงระบบ e-Tax invoice By Email เพื่อประทับรับรองเวลา และระบบจะส่งกลับไปยังอีเมล์ผู้ออกใบกำกับภาษีและผู้ซื้อหรือผู้รับบริการ

กรมพัฒนาธุรกิจการค้า



กรมพัฒนาธุรกิจการค้า ให้บริการจดทะเบียนนิติบุคคลทางอิเล็กทรอนิกส์ (e-Registration) ช่วยอำนวยความสะดวกการบริการประชาชน พัฒนาการบริการของภาครัฐด้วยเทคโนโลยีสมัยใหม่ เพื่อผลักดันการบริหารจัดการสู่การเป็นรัฐบาลดิจิทัล จึงได้มีการให้บริการจดทะเบียนนิติบุคคลทางอิเล็กทรอนิกส์ แก้ไขเปลี่ยนแปลงข้อมูลรายการจดทะเบียนนิติบุคคล ขอหนังสือรับรองนิติบุคคลและรับรองสำเนา รวมถึงการลงลายมือชื่อของนายทะเบียน ด้วยการนำเทคโนโลยี Public Key Infrastructure (PKI) ซึ่งเป็นลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) มาใช้อย่างเต็มรูปแบบ โดยเป็นไปตามหลักเกณฑ์และข้อกำหนดของพระราชบัญญัติว่าด้วยธุรกรรมทาง อิเล็กทรอนิกส์พ.ศ. 2544 มีระบบรักษาความปลอดภัยขั้นสูง เพื่อให้ผู้ประกอบธุรกิจได้รับความสะดวกรวดเร็ว ลดขั้นตอนการยื่นขอจดทะเบียน ลดการใช้เอกสาร และระยะเวลาการติดต่อกับเจ้าหน้าที่ สามารถจดทะเบียนเริ่มต้นธุรกิจได้ทุกที่ ทุกเวลา

แนวคำพิพาษาข้อมูลอิเล็กทรอนิกส์

คำพิพากษาฎีกาที่ 8089/2556

การที่จำเลยนำบัตรกดเงินสดควิกแคชไปถอนเงินและใส่รหัสส่วนตัวเปรียบได้กับการลงลายมือชื่อตนเอง ทำรายการเบิกถอนเงินตามที่จำเลยประสงค์ และกดยืนยันทำรายการพร้อมรับเงินสดและสลิป

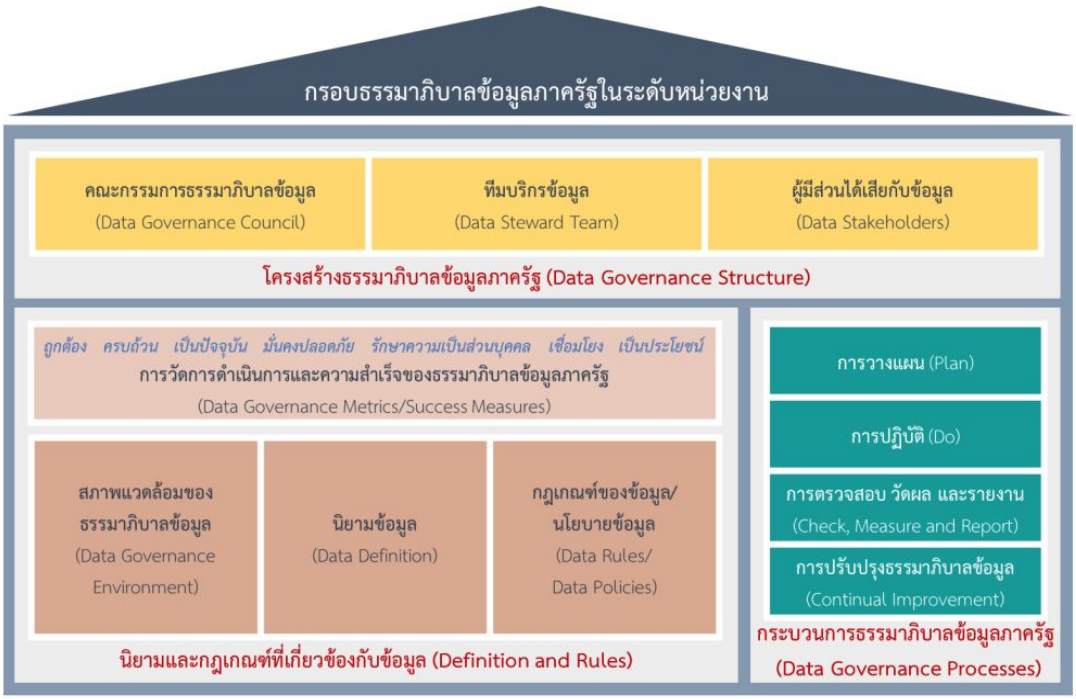
- การเบิกถอนเงินสดจากบัญชีสินเชื่อเงินสด ผ่านตู้ ATM เป็นธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 4 มีผลใช้บังคับตามมาตรา 7 ซึ่งบัญญัติว่า ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
- การนำบัตรกดเงินสดไปถอนเงินและใส่รหัสส่วนตัว เป็นเสมือนการลงลายมือชื่อตนเองและถือเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 9 บัญญัติว่า ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า (1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อและสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน
- เมื่อจำเลยนำบัตรกดเงินสดไปถอนเงิน ใส่รหัสเพื่อทำรายการถอนเงิน และกดยนยันทำรายการพร้อมรับเงินสดและสลิป การกระทำดังกล่าวจึงถือเป็นหลักฐานการกู้ยืมเงินตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 8 วรรคหนึ่งบัญญัติว่า ภายใต้บังคับบทบัญญัติแห่งมาตรา 9 ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

คำพิพากษาฎีกาที่ 6757/2560

ข้อความที่โจทก์ส่งถึงจำเลยทาง Facebook มีใจความว่า “เงินทั้งหมดจำนวน 670,000 บาทนั้น จำเลยไม่ต้องส่งคืนให้แก่โจทก์แล้ว และไม่ต้องส่งดอกเบี้ยอะไรมาให้อีก โจทก์ยกให้ทั้งหมด จะได้ไม่ต้องมีภาระหนี้สินติดตัว”

- การส่งข้อความผ่าน Facebook เพื่อยกหนี้ให้ เป็นการส่งข้อมูลทางอิเล็กทรอนิกส์ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 7 บัญญัติว่า ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
- การส่งข้อมูลทางอิเล็กทรอนิกส์ ถือว่าเป็นการทำหนังสือหรือมีหลักฐานเป็นหนังสือแล้ว ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 8 บัญญัติว่า ภายใต้บังคับบทบัญญัติแห่งมาตรา 9 ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดงแล้ว ดังนั้น ข้อความดังกล่าวที่โจทก์ส่งถึงจำเลยทางเฟสบุ๊ค แม้จะไม่มีการลงลายมือชื่อโจทก์ก็ตามแต่การส่งข้อความของโจทก์ทางเฟสบุ๊คจะปรากฏชื่อผู้ส่งด้วยและโจทก์ก็ยอมรับว่าได้ส่งข้อความดังกล่าวทางเฟสบุ๊คถึงจำเลยจริง

การกำกับดูแลข้อมูล (Data Governance)



ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) เป็นการกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูล โดยประกอบด้วย สภาพแวดล้อมของธรรมาภิบาลข้อมูล กฎเกณฑ์หรือนโยบายที่เกี่ยวข้องกับการดำเนินงานกับข้อมูล บทบาทและความรับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ กระบวนการธรรมาภิบาลข้อมูลภาครัฐ และการวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ กล่าวคือ บุคคลที่ได้รับบทบาทในธรรมาภิบาลข้อมูลภาครัฐ จะมีหน้าที่ในการกำหนดขอบเขต กฎเกณฑ์ และนโยบายข้อมูลที่ใช้ในกระบวนการธรรมาภิบาลข้อมูลภาครัฐ เพื่อควบคุมและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย โดยกฎเกณฑ์และนโยบายข้อมูลต้องสอดคล้องกับสภาพแวดล้อมและวัฒนธรรมองค์กรของแต่ละหน่วยงาน การวัดผลการดำเนินการช่วยให้เห็นระดับการดำเนินการของธรรมาภิบาลข้อมูลภาครัฐ ซึ่งส่งผลต่อความสำเร็จของการดำเนินการหรือคุณภาพของข้อมูล

อ้างอิงข้อมูล จาก ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ 12 มีนาคม 2563

เพื่อให้การกำกับดูแลและบริหารจัดการการใช้ลายมือชื่ออิเล็กทรอนิกส์ มีความสอดคล้องกับวัตถุประสงค์ มีประสิทธิภาพ มีความโปร่งใส่ และเป็นไปตามกฎหมาย กฎ ระเบียบ และนโยบายขององค์กร ผู้บริหารองค์กร ควรวิเคราะห์และระบุถึงปัจจัยสภาพแวดล้อมภายในและภายนอก ภาระผูกพันต่างๆ แนวโน้ม บทบาทต่อที่จะส่งผลต่อการเปลี่ยนแปลงในอนาคต พิจารณาระดับความสำคัญของการนำเทคโนโลยีมาใช้และประเมินผลกระทบ รวมทั้งทำความเข้าใจเกี่ยวกับวัฒนธรรมองค์กร เพื่อให้นโยบายการกำกับดูแลการจัดการการใช้ลายมือชื่ออิเล็กทรอนิกส์ระดับองค์กรที่ดี ควรกำหนดบทบาทของบุคคลกรที่เกี่ยวข้อง

แนวทางการพัฒนาโครงสร้างด้านการกำกับดูแลข้อมูลขององค์กร (Data Governance Framework Structuring Options)

- **การปฏิบัติตามกฎเกณฑ์ (Compliance Management)**

การปฏิบัติงานขององค์กร ต้องยึดถือและปฏิบัติตามนโยบาย แผนงาน วิธีการปฏิบัติงาน กฎหมาย ระเบียบ ข้อบังคับ สัญญา ตลอดจนข้อกำหนดต่างๆ ทั้งภายในและภายนอกองค์กร จะต้องมีกระบวนการในการตรวจสอบเพื่อติดตาม การกำกับปฏิบัติงานให้เป็นไปตามข้อกำหนดของกฎหมายที่เกี่ยวข้อง เพื่อไม่ให้การดำเนินงานขององค์กรมีความเสียหายอันเกิดจากการฝ่าฝืน

การกำกับการปฏิบัติตามกฎเกณฑ์ คือ การกำหนดขอบเขต วิธีการปฏิบัติ และติดตามให้ปฏิบัติได้ถูกต้องตามกฎเกณฑ์ โดยใช้หลักการการปฏิบัติตามกฎเกณฑ์

- ❏ เป็นศูนย์กลางในการให้คำแนะนำ และปรึกษาด้านกฎหมาย กฎเกณฑ์ต่างๆ แก่ผู้เกี่ยวข้อง
- ❏ ระบุความเสี่ยงด้านการปฏิบัติการ รวมถึงแนวทางการปฏิบัติทางธุรกิจ
- ❏ พิจารณาวิธีการวัดความเสี่ยง ด้านการปฏิบัติตามกฎเกณฑ์
- ❏ ประเมินความเหมาะสมของขั้นตอนและแนวทางตามกฎเกณฑ์เพื่อติดตามผลและเสนอแนะ
- ❏ ประสานหน่วยงานบริหารความเสี่ยง และหน่วยงานที่เกียวข้อง เพื่อดำเนินการตามแผนงาน
- ❏ ตรวจสอบ ประเมินผล รายงานการปฏิบัติตามกฎเกณฑ์

กระบวนการกำกับการปฏิบัติตามกฎเกณฑ์ มี 2 ระดับ คือ

1. ระดับองค์กร กำหนดโดยผู้บริหารองค์กร หรือผู้มีอำนาจสูงสุดในองค์กร จัดให้มีฝ่ายกำกับดูแลหรือระบบการกำกับดูแลให้การดำเนินงานควบถ้วนและเป็นไปตามวัตถุประสงค์
2. ระดับปฏิบัติการ กำหนดโดยฝ่ายกำกับดูแล จัดให้มีระบบการควบคุมภายใน เพื่อให้การติดตามการปฏิบัติหน้าที่สามารถบรรลุวัตถุประสงค์

- **การบริหารและจัดการความเสี่ยง (Risk Management)**

เพื่อให้การบริหารและจัดการความเสี่ยงสำหรับการใช้ลายมือชื่ออิเล็กทรอนิกส์ เป็นไปอย่างถูกต้องเหมาะสมและมีประสิทธิภาพ ผู้บริหารองค์กร หรือผู้มีอำนาจสูงสุดในองค์กรต้องจัดให้มีนโยบายการบริหารและจัดการความเสี่ยงขึ้น รวมทั้งสื่อสารทำความเข้าใจกับผู้ที่เกี่ยวข้อง และทบทวนการหรือปรับปรุงนโยบายอย่างสม่ำเสอม โดยควรกำหนดขั้นตอนและวิธีการปฏิบัติในระดับที่องค์กรยอมรับได้ (Risk Appetite) และลดความผิดพลาดที่อาจจะเกิดขึ้น อย่างมีประสิทธิภาพ เป็นไปในแนวทางเดียวกัน ดังนั้นองค์กรควรมีกระบวนการในการบริหารและจัดการความเสี่ยงที่มีการดำเนินอย่างต่อเนื่อง ดังนี้

❑ การจัดทำนโยบายบริหารและจัดการความเสี่ยง (Enterprise Risk Management)

ผู้บริหารองค์กร หรือผู้มีอำนาจสูงสุดในองค์กร จะต้องพิจารณาหรือมอบหมายให้ผู้ที่เกี่ยวข้องในการจัดทำนโยบายบริหารและจัดการความเสี่ยง รวมถึงแนวระเบียบวิธีการปฏิบัติ ให้สอดคล้องถูกต้องตามกฎหมาย อีกทั้งต้องทบทวนและปรับปรุงอย่างสม่ำเสมอ

❑ การระบุความเสี่ยงที่เกี่ยวข้อง (Risk Identification)

การบริหารและจัดการความเสี่ยงสำหรับการใช้ลายมือชื่ออิเล็กทรอนิกส์ ผู้ที่เกี่ยวข้องจะต้องสำรวจ วิเคราะห์ กระบวนการ และรวบรวมข้อมูลความเสี่ยงที่เป็นไปได้ที่จะเกิดขึ้น มีการประเมินสภาพแวดล้อมทั้งภายในและภายนอก ผลกระทบในอดีตและอนาคตที่คาดว่าจะก่อให้เกิดขึ้น ทั้งนี้อาจจะรวมถึงข้อจำกัด ประเด็นปัญหา ภัยคุกคาม ความปลอดภัยทางอินเตอร์เน็ต และการแก้ไขปัญหา โดยอาจแบ่งกลุ่มหมวดหมู่ ประเภทของความเสี่ยง จะช่วยในการกำหนดขอบเขตการบริหารและจัดการความเสี่ยง และเป็นเครื่องมือที่ให้ผู้บริหารความเสี่ยงเห็นภาพรวมทั้งหมด ควรมีการพิจารณาและปรับปรุงความเสี่ยงที่เป็นไปได้ให้เป็นปัจจุบันเสมอตามสภาพแวดล้อมที่เปลี่ยนแปลงไป

❑ การกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite)

เป็นการรวบรวมความเสี่ยงที่เกิดจากการระบุความเสี่ยงที่เกี่ยวข้อง โดยกำหนดระดับความเสี่ยงที่สามารถยอมรับได้ ซึ่งอาจจะพิจารณาจากนโยบายบริหารและจัดการความเสี่ยง

- ระดับความสูญเสียขององค์กรที่ยอมรับได้
- วัฒนธรรมองค์กร หรือ ระดับการยอมรับความเสี่ยงของผู้บริหาร

❑ การประเมินความเสี่ยง (Risk Assessment)

จากการระบุความเสี่ยง กำหนดความเสี่ยง รวมถึงความเสี่ยงที่ยอมรับได้ ซึ่งผู้ที่เกี่ยวข้องต้องประเมินโอกาสและผลกระทบที่อาจจะเกิดจากความเสี่ยงที่เกิดขึ้นในการใช้ลายมือชื่ออิเล็กทรอนิกส์ โดยอาจจะทำแผนประเมินความเสี่ยงที่เกี่ยวข้องทั้งหมด และใช้ในการจัดลำดับและความสำคัญ โดยทั่วไปการประเมินความเสี่ยงประกอบด้วย 2 ด้าน ได้แก่ 1) โอกาสที่อาจเกิดขึ้น ณ เหตุการณ์ที่มีโอกาสจะเกิดขึ้นมากน้อยเพียงใด 2) ผลกระทบ ณ เหตุการณ์ที่เกิดขึ้นจะได้รับผลกระทบมากน้อยเพียงใด

การประเมินความเสี่ยง สามารถทำได้ทั้งเชิงคุณภาพและเชิงปริมาณ โดยพิจารณาจากเหตุการณ์ที่เกิดขึ้นจากภายนอกและภายในองค์กร นอกจากนี้ การประเมินความเสี่ยงควรพิจารณาปัจจัยต่อไปนี้

- การปฏิบัติงานของผู้บริหารและพนักงาน
- กระบวนการปฏิบัติงาน
- การควบคุมภายใน
- การวัดผลและติดตามผลการปฏิบัติงาน
- การบริหารจัดการเพื่อตอบสนองความเสี่ยง (Risk Response)

สำหรับผู้ที่เกี่ยวข้องกับการบริหารและจัดการความเสี่ยงขององค์กรนั้น จะต้องกำหนดวิธีการเพื่อตอบสนองความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งพิจารณาจากระดับความสำคัญของความเสี่ยง สามารถดำเนินการได้ 4 ลักษณะ ได้แก่

- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)
- การยอมรับความเสี่ยง (Risk Acceptance)
- การร่วมรับความเสี่ยง (Risk Sharing)
- การลดความเสี่ยง (Risk Reduction)

ผู้บริหารองค์กร หรือผู้มีอำนาจสูงสุดในองค์กร จะต้องมีกระบวนการบริหารจัดการความเสี่ยงจากการใช้ลายมือชื่ออิเล็กทรอนิกส์ นอกจากการประเมินความมั่นคงปลอดภัยของระบบแล้ว หากผู้ใช้งานบางส่วนไม่สามารถใช้ลายมือชื่ออิเล็กทรอนิกส์ได้เนื่องด้วยปัญหาจากสัญญาณอินเตอร์เน็ต ผู้บริหารองค์กร หรือผู้มีอำนาจสูงสุดในองค์กร อาจจะต้องพิจารณายอมรับความเสี่ยงนี้จากปัญหาดังกล่าว หรือลดความเสี่ยงด้วยการเพิ่มทางเลือกปกติให้เป็นอีกทางเลือกหนึ่งในการลงลายมือชื่อ

❑ การกำหนดตัวชี้วัดและรายงานผล (Risk Indicator)

จะต้องประเมินความเสี่ยงที่มีผลต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง เพื่อนำไปประกอบการตัดสินใจในการกำหนดตัวชี้วัดของผลกระทบจากความเสี่ยงทั้งหมด โดยตัวชี้วัดสามารถสะท้อนการเปลี่ยนแปลงของความเสี่ยงเมื่อความเสี่ยงมีการเปลี่ยนแปลงเกิดขึ้น ดังนั้นควรจะต้องหาสาเหตุที่แท้จริงและผลกระทบอย่างเหมาะสม รวมถึงรายงานผลการบริหารและจัดการความเสี่ยงในรูปแบบที่สามาถนำไปประกอบการตัดสินใจได้ มีประสิทธิภาพและประสิทธิผลของการควบคุม ข้อตรวจพบ หรือข้อปรับปรุงสามารถตรวจสอบโดยผู้ตรวจสอบภายนอกและภายใน เพื่อวัดคุณภาพได้

❑ การกำหนดหน้าที่และความรับผิดชอบ

ผู้บริหารองค์กร หรือผู้มีอำนาจสูงสุดในองค์กร ควรเป็นผู้พิจารณาและรับผิดชอบ ในการให้แนวทางและเห็นชอบนโยบายบริหารและจัดการความเสี่ยง รวมถึงติดตามผลการปฏิบัติงาน ที่สำคัญผู้บริหารหรือสายงานที่ได้รับมอบหมาย ต้องการกำหนดกรอบและกระบวนการบริหารจัดการความเสี่ยง รวมถึงรับผิดชอบและปรับปรุงในกิจกรรมความเสี่ยงต่างๆที่อาจจะเกิดขึ้น ซึ่งมอบหมายบทบาทหน้าที่ที่เกี่ยวข้องในการบริหารและจัดการความเสี่ยง โดยคำนึงถึงหลักการถ่วงดุล และการแบ่งแยกหน้าที่ความรับผิดชอบ เป็น 3 ระดับ ได้แก่ ผู้ปฏิบัติงาน ผู้บริหารความเสี่ยง และผู้ตรวจสอบ

เมื่อผู้บริหารองค์กร หรือผู้มีอำนาจสูงสุดในองค์กร ตัดสินใจการใช้ลายมือชื่ออิเล็กทรอนิกส์ควรต้องรีบดำเนินการตามกรอบจัดการความเสี่ยงนี้ โดยมีการกำหนดแผนและจัดการความเสี่ยง ซึ่งต้องชี้แจงให้ผู้เกี่ยวข้องทราบ พร้อมมาตรการที่จะรองรับความเสี่ยงที่อาจจะเกิดขึ้น โดยผู้บริหารองค์กรต้องสร้างกระบวนการเพื่อสนับสนุนให้เกิดนโยบาย การจัดการ การประเมิน และการรายงานความเสี่ยงอย่างต่อเนื่องและเป็นส่วนหนึ่งของการปฏิบัติงานตามปกติ

- **การบริหารจัดการผลกระทบ (Impact Management)**

จากการดำเนินงานขององค์กร ทั้งที่เป็นผลกระทบโดยตรง ผลกระทบภายนอก และผลกระทบต่างๆ เหล่านี้ พิจารณาจากผลกระทบที่ตกต่อผู้มีส่วนเกี่ยวข้องทั้งหมด โดยองค์กรจะต้องกำกับดูแลให้มั่นใจว่าองค์กรมีความสามารถที่จะจัดการดูแลผลกระทบทุกประเภทได้อย่างเหมาะสม และสร้างผลกระทบต่อการดำเนินงานให้น้อยที่สุด ต้องติดตาม วิเคราะห์ และประเมินผลจากความเสี่ยงที่เกิดขึ้นจากการใช้ลายมือชื่ออิเล็กทรอนิกส์อยู่ตลอด และต้องมีมาตรการรองรับสำหรับการแก้ไข ลด และรับมือผลกระทบที่จะเกิดขึ้นอย่างเป็นรูปธรรมและทันท่วงที

แนวทางการพัฒนาสมรรถนะด้านการกำกับดูแลข้อมูลขององค์กร (Data Governance Framework Capabilities Model)

- **การกำหนดแนวทางและกลยุทธ์ (Data Strategy)**

กระบวนการและระบบที่จะทำให้องค์กรสามารถดำเนินการตามกฎหมาย ระเบียบ และมาตรฐาน เพื่อป้องกันชื่อเสียงขององค์กร เพื่อลดความเสี่ยงจากการดำเนินงาน สนับสนุนการบริหารจัดการให้ถูกต้อง หลีกเลี่ยงการลงโทษที่เกิดจากการฝ่าฝืนหรือละเมิดกฎระเบียบ ป้องกันชื่อเสียงเสียหาย ป้องกันการทุจริต สร้างกระบวนการบริหารงานที่โปร่งใส่

เพื่อให้การใช้ลายมือชื่ออิเล็กทรอนิกส์ เป็นไปอย่างมีเหมาะสม มีประสิทธิภาพและประสิทธิผล โดยที่องค์กรจะต้องคำนึงถึงความเปลี่ยนแปลงของเทคโนโลยีและการนำไปใช้ รวมถึงจัดการและควบคุมการใช้ทรัพยากรและงบประมาณด้วย แผนด้านยุทธศาสตร์นี้จะต้องสอดคล้องกับนโยบาย หรือแผนงานขององค์กร มุ่งเน้นที่ความต้องการของผู้มีส่วนได้ส่วนเสีย ความโปร่งใส่ ความน่าเชื่อถือ ความปลอดภัย ความคุ้มค่าของการใช้ทรัพยากร และประโยชน์ของทุกคน

องค์กรต้องจัดทำแผนด้านยุทธศาสตร์ ที่มุ่งเน้นความโปร่งใส่ ตรวจสอบได้ มีการคุ้มครองข้อมูลส่วนบุคคล ความเชื่อมั่น ความพร้อมใช้งาน ประเมินประโยชน์หรือโอกาสที่ได้รับ การเปิดเผยข้อมูลและความรับผิดชอบ รวมทั้งความท้าทายที่อาจเกิดขึ้นจากการนำเทคโนโลยีไปใช้ เพื่อให้การทำงานเป็นไปในทิศทางเดียวกัน ข้อมูลต่างๆ ที่สำคัญจะต้องมีผู้รับผิดชอบที่ชัดเจนในการรวบรวมและวิเคราะห์ ให้ผู้ที่เกี่ยวข้องเพื่อรวบรวมและนำมาเป็นปัจจัยให้ผู้บริหารองค์กร ใช้ประกอบการกำหนด ทบทวน วิสัยทัศน์ ภารกิจ ค่านิยม ทิศทางการดำเนินงานขององค์กรอย่างครบถ้วน

แต่หนึ่งที่สิ่งสำคัญคือ การประเมินต้นทุนทางตรงและต้นทุนทางอ้อมของการใช้เทคโนโลยี ต้องสามารถสื่อสารถึงเป้าหมายชัดเจน รวมถึงวิธีการติดตามผลการดำเนินการ เพื่อให้มั่นใจว่า ทรัพยากรที่จะใช้สามารถจัดการความเสี่ยงที่จะเกิดขึ้นได้ คำนึงถึงการกำหนดหลักเกณฑ์เพื่อใช้เป็นแนวทางในการจัดสรรและบริหารทรัพยากรสารสนเทศ รวมถึงขีดความสามารถด้วย

- **การดูแลข้อมูล (Data Stewardship)**

ผู้ดูแลข้อมูล หรือ ทีมบริกรข้อมูล จะทำหน้าที่ร่างนโยบายข้อมูล ระบุมาตรฐานที่จะใช้ และอาจให้คำแนะนำต่อเกี่ยวกับการกำกับดูแลข้อมูล รวมถึงการตรวจสอบการปฏิบัติตามนโยบาย ข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัย ของข้อมูล วิเคราะห์ผลจากการ ตรวจสอบ ซึ่งสามารถมีได้หลายคนมีหลายระดับทั้งนี้ขึ้นอยู่กับความซับซ้อนของการจัดการ หรือการจัดให้มีคณะกรรมการบริกรข้อมูล (Data Stewardship Council) ขององค์กรก็ได้

ทำหน้าที่มุ่งเน้นการดำเนินงาน และกำหนดมาตรฐานในการบริหารจัดการตามองค์ประกอบของการบริหารจัดการข้อมูลอย่างน้อยหนึ่งองค์ประกอบ ผู้ที่เกี่ยวข้องประกอบไปด้วยหัวหน้าบริกรข้อมูล (Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคง ปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุนให้เกิดการ กำกับดูแลข้อมูลที่ดีภายในหน่วยงาน ทีมบริกรข้อมูลรับคำสั่งโดยตรงจากผู้บริหารองค์กร หรือผู้ที่ทำหน้าที่กำกับดูแล ในขณะเดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจด้วย โดยบริกรข้อมูลด้านธุรกิจเป็นผู้ให้การสนับสนุนด้านธุรกิจ ขณะที่บริกรข้อมูลด้านเทคนิคเป็นผู้ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตามบริกรข้อมูลด้านธุรกิจและบริกรข้อมูลด้านเทคนิคอาจจะเป็นบุคคลเดียวกัน ซึ่งขึ้นอยู่กับคุณสมบัติของบุคคลหรือความเหมาะสมขององค์กร

- **การรักษาความมั่นคงปลอดภัย (Data Protection)**

การถูกโจมตีทางไซเบอร์กลายเป็นปัญหาลุกลามที่สร้างความเสียหายแก่องค์กรต่างๆทั่วโลก และมีแนวโน้มที่จะซับซ้อนและส่งผลกระทบรุนแรงต่อระบบสังคมและเศรษฐกิจอย่างต่อเนื่อง ยิ่งเทคโนโลยีมีการเจริญเติบโตมากเท่าไหร่ ยิ่งทำให้การโจมตีของอาชญากรคอมพิวเตอร์เปลี่ยนไปและคาดเดายากยิ่งขึ้น แม้ว่า

ปัจจุบันจะมีเครื่องมือที่ช่วยในการตรวจสอบที่มีความซับซ้อนมากขึ้น เช่น ปัญญาประดิษฐ์ (AI) การเรียนรู้ของเครื่อง (Machine Learing) ในการตรวจสอบพฤติกรรมต้องสงสัย แต่นั้นเป็นเพียงการเรียนรู้จากรูปแบบ ที่เกิดขึ้น (Pattern) ในอดีต อาจทำให้ไม่สามารถป้องกันการภัยคุกคามรูปแบบใหม่ๆได้ ดังนั้นการรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน รวมถึงข้อมูลจึงมีความสำคัญอย่างยิ่งยวด

หลักการพื้นฐานที่ต้ององค์กร ต้องมีในการควบคุมและการรักษาความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ มีดังนี้

- การควบคุมการรักษาความปลอดภัยของซอฟต์แวร์ (Software Control)
    - การควบคุมจากระบบภายใน (Internal Progran Control) คือ การควบคุมสิทธิการเข้าถึงและสิทธิในการใช้ข้อมูลภายในระบบ ซึ่งถูกจัดเก็บไว้ในภายในระบบ
    - การควบคุมโดยระบบปฏิบัติการ (Operating System Control) คือ การควบคุมสิทธิการเข้าถึงและการใช้ข้อมูลในส่วนต่างๆภายในคอมพิวเตอร์ของผู้ใช้และจำแนกแตกต่างจากผู้ใช้คนอื่นๆ
    - การควบคุมและการออกแบบซฮฟต์แวร์ (Development Control) คือ การควบคุมตั้งแต่การออกแบบ การทดสอบการใช้งานจริง
- การควบคุมความมั่นคงปลอดภัยของอุปกรณ์ (Hardware Control) โดยเลือกใช้เทคโนโลยีของอุปกรณ์ที่สามารถควบคุมการเข้าถึง และป้องกันการทำงานที่ผิดพลาด ด้วยอุปกรณ์ภายในตัวเอง
- การใช้นโยบายการควบคุม (Policies) มีการประกาศใช้นโยบาย และปรับปรุงนโยบายให้มีการทำงานที่สอดคล้องกับธุรกิจ และสภาพแวดล้อมที่เปลี่ยนแปลง โดยมีผลทั้งองค์กร
- การป้องกันทางกายภาพ (Physical Control) การมีมาตรการการเข้าถึงคอมพิวเตอร์ อุปกรณ์ หรือสื่อบันทึกข้อมูลต่างๆ รวมถึงมีระบบสำรองข้อมูลอย่างสม่ำเสมอ

การประเมินความมั่นคงปลอดภัยของข้อมูล เป็นวิธีการในการตรวจสอบและรักษาความปลอดภัยของข้อมูล โดยใช้หลักเกณฑ์ในด้านต่าง ๆ ดังนี้

- จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลที่รวมถึงการป้องกันข้อมูล การรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล
- การจัดชั้นความลับของข้อมูล ให้สอดคล้องกับกฎหมาย เงื่อนไข และข้อกำหนดต่าง ๆ
- กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล คำนึงถึงชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงข้อมูล หรือเปิดเผยข้อมูลที่อ่อนไหวนั้น รวมถึงเพื่อป้องกันการดัดแปลง แก้ไข แต่งเติมข้อมูลโดยไม่ได้รับอนุญาต
- ข้อมูลถูกใช้งานอย่างเหมาะสม การนำข้อมูลไปใช้ควรดำเนินการให้สอดคล้องกับสัญญาอนุญาต และไม่ขัดต่อกฎหมาย

- ข้อมูลต้องมีความพร้อมใช้อยู่เสมอ ต้องมีการดำเนินการเตรียมความพร้อมไม่ว่าข้อมูลจะเป็นแบบใดประเภทใดก็ตาม และสามารถเข้าถึงโดยผู้มีสิทธิได้อย่างสม่ำเสมอ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ต้องมีการเตรียมความพร้อมเรื่องระบบงาน การสำรองข้อมูล การเข้าถึงข้อมูล รวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินใด ๆ ที่อาจมีผลต่อการใช้ข้อมูลด้วย

เพื่อให้มั่นใจว่า ข้อมูลที่องค์กรจัดเก็บไว้ มีความมั่นคงปลอดภัย ได้รับการจัดการอย่างถูกต้อง จึงมีการโดยความมั่นคงปลอดภัยของข้อมูลต้องดำเนินการตั้งแต่การวางแผน การจัดทำ การปฏิบัติตาม และการบังคับใช้นโยบายและขั้นตอนด้านการรักษาความปลอดภัย เพื่อสนับสนุนในด้านที่เกี่ยวข้องกับการพิสูจน์ตัวตน การกำหนดสิทธิ์ การเข้าถึงข้อมูล การตรวจสอบ และความพร้อมใช้ของข้อมูลอย่างเหมาะสม ทั้งนี้อาจศึกาเพิ่มเติมจากหัวข้อ การรักษาความมั่นคงปลอดภัยทางสารสนเทศ

นอกจากนี้ ต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยควรจะมีกระบวนการออกแบบที่คำนึงถึงความเป็นส่วนตัว (Privacy by Design) ตั้งแต่แรกของการเริ่มต้นกำหนดขอบเขตและพัฒนาระบบ และต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับ ความยินยอมจากเจ้าของข้อมูลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

บทสรุป

การพัฒนากรอบการกำกับดูแลข้อมูล กรณีลายมือชื่ออิเล็กทรอนิกส์ เนื่องจากการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) เป็นตัวเร่งให้องค์กรทั้งภาครัฐและภาคเอกชนต้องปรับตัววิธีการติดต่อสื่อสารโดยอาศัยเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ มีความสะดวก รวดเร็ว ประหยัดต้นทุน และเอื้ออำนวยต่อการประกอบธุรกิจหรือการให้บริการประชาชนของภาครัฐในรูปแบบของธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจะเป็นกลไกสำคัญในการขับเคลื่อนเศรษฐกิจดิจิทัลและยกระดับคุณภาพชีวิตของประชาชน

องค์กรที่จะมีการใช้ลายมือชื่ออิเล็กทรอนิกส์นั้น จะเป็นการช่วยสนับสนุนการประกอบธุรกิจต่างๆ เพื่ออำนวยความสะดวก และการสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งองค์กรควรจะต้องคำนึงถึง องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ 5 ประการ คือ รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ การพิสูจน์และยืนยันตัวตน การเชื่อมโยงข้อมูลกับลายมือชื่ออิเล็กทรอนิกส์ เจตนาในการลงลายมือชื่ออิเล็กทรอนิกส์ และการรักษาความครบถ้วนของข้อมูล เพื่อให้สามารถใช้ลายมือชื่ออิเล็กทรอนิกส์ได้อย่างถูกต้องตามกฎหมาย แต่องค์กรต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบ รวมถึงลักษณะ ประเภท และขนาดของธุรกรรมด้วย ให้มีความเหมาะสม มีความน่าเชื่อถือ อย่างไรก็ตามองค์กรต้องมีความมุ่งมั่นที่จะกำกับดูแลการบริหารงาน ให้เป็นไปตามหลักการและนโยบายการกำกับกิจการที่ดี มีธรรมาภิบาล เพื่อให้มั่นใจว่า การดำเนินงานหรือการปฏิบัติงานใดๆขององค์กรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล คำนึงถึงผลประโยชน์ของทุกฝ่ายเป็นสำคัญ จากสภาวะตอนนี้การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์นั้น จะต้องดำเนินการอย่างรอบคอบและให้การดำเนินงานให้เป็นไปตามการปฏิบัติตามกฎเกณฑ์ การบริหารและจัดการความเสี่ยง การบริหารจัดการผลกระทบ การกำหนดแนวทางและกลยุทธ์ด้านทรัพยากร การดูแลข้อมูล และการรักษาความมั่นคงปลอดภัย มีความโปร่งใสในการดำเนินงานที่สามารถตรวจสอบได้ และมีการเปิดเผยข้อมูลสารสนเทศบางประการแก่ผู้ที่เกี่ยวข้องอย่างโปร่งใส่ ครบถ้วนและถูกต้อง เป็นการส่งเสริมให้เกิดการมีส่วนร่วมของผู้มีส่วนได้เสีย

ดังนั้นสิ่งที่ องค์กรควรริเริ่ม คือ การวางแผนในการกำกับดูแลจัดการข้อมูล ซึ่งถือเป็นหัวใจสำคัญ จะเป็นกลไกในการดำเนินนโยบาย กลยุทธ์ กำหนดทิศทาง ควบคุม และจัดการข้อมูล เพื่อให้มั่นใจได้ว่า จะดำเนินการได้อย่างถูกต้องตามนโยบาย กฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ องค์กรควรต้องจัดให้มีการถ่วงดุลในองค์กร กล่าวคือ มีระบบควบคุมภายในซึ่งสามารถตรวจสอบ ประเมิน และทบทวนการปฏิบัติงานของผู้ที่เกี่ยวข้องได้ ซึ่งไม่ใช่การจับผิดแต่เป็นการป้องกันและหาแนวทางในการลดความเสี่ยงที่จะเกิดขึ้น ถือปฏิบัติอย่างเคร่งครัด

รายละเอียดเกี่ยวกับผู้เขียน

ธีรวุฒิ จันทดิษฐ์ กรรมการผู้จัดการ บริษัท 9ดิจิตอล จำกัด

Theerawut <PAI> Chanthadit

He is currently CEO of 9Digital.co, a custom software development, e-commerce platforms, CRM and ERP class systems development. He is also ex-COO of Creden.co, a fintech Startup to provide eKYC , eSignature and Credit scoring in Thailand. He is also ex-COO of SHIPPOP, an online logistic booking platform in Thailand. When he was in high school, he had a chance to join 2nd JWC (Junior Webmaster Camp), This was starting point in his life to studying Com-Sci and IT. And when he studied in the University, he had the opportunity to join 11th YWC (Young Webmaster Camp). The nationwide computer camp of Thai Webmaster Association. After that he started working as a Web Development Freelancer and Content Blogger. Before graduated from University, he joined to 4th AUCC . He earned the Excellent Paper Award in 2016.

Personal Info

Name : Theerawut <PAI> Chanthadit
E-mail : theispie@gmail.com
Web : www.theerawut.com

Education

M.S. Digital Innovation and Technology Management | 2019 - Now
The University of the Thai Chamber of Commerce

Digital and Transformative Leaders #1
The University of the Thai Chamber of Commerce

Digital Network Advantage #4 | 2019
School of Business Administration Sripatum University

B.Sc Computer Science | 2012 - 2016
King Mongkut's Institute of Technology Ladkrabang

Experiences

2016 - Now 9Digital Co.,Ltd.
Co-Founder and CEO

2018 - 2019 Creden Co.,Ltd.
Chief Operating Officer

2016 - 2018 SHIPPOP Co.,Ltd.
Chief Operating Officer

2015 - Now Wanchart Co.,Ltd.
Co-Founder and CEO

2014 Menlonbox Co.,Ltd.
Content Marketing

Activities

2009 Founder of ICT Academy Club (ICTA) Darunaratchaburi School

2010 National Gold Award of Region Excellent fair for students

2011 The 1st Prize Winner Trueplookpanya 1st By True Corporation Plc.

2013 Young Webmaster Camp#11 By Thai Webmaster Association

2016 "Excellent Paper Award" The 4th ASEAN Undergraduate Conference in Computing (AUCC) University Sakaeo Campus.

2017 "AIS: Executive Leadership Program" By COO of Workpoint

2017 "AIS: Personality for Public Speaking" By RISE Academy

2017 Pitching Challenge 2017 [Songkhla] 1st Prize Winner Startup Thailand

2018 "How Thai Tech Startups can expand into the UK Market" By AIS The StartUp

2018 Brain Storming Bachelor of Science (IT) By Rajabhat Maha Sarakham University.

เอกสารอ้างอิง

1. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551 , (ฉบับที่ 3) พ.ศ. 2562 และ (ฉบับที่ 4) พ.ศ. 2562
2. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ 12 มีนาคม 2563
3. กรอบการกำกับดูแลข้อมูลของ ดร.ชัยยุทธ์ ชำนาญเลิศกิจ
4. Use of Electronic Signatures in Federal Organization Transactions 25 January 2013.
5. Electronic Signature Platforms: Key Contractual Issues in the January/February 2017 issue of PLC Magazine
6. U.S. Guide to Electronic Signatures White Paper by Adobe Sign ,Septmber 2017
7. Federal Information Processing Standards Publications Digital Signature Standard (DSS) July 2013.
8. The Electronic Signature and Records Association (ESRA)
9. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
10. ISO 14533-4:2019(en) Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes)
11. แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ เลขที่ ขมธอ. 18-2561
12. แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน เลขที่ ขมธอ. 19-2561
13. แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน เลขที่ ขมธอ. 20-2561
14. ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (ขมธอ. 23-2563) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์