แนวทางปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ บริษัท วิริยะประกันภัย จำกัด (มหาชน)

บริษัท วิริยะประกันภัย จำกัด (มหาชน) ได้จัดทำแนวทางปฏิบัตินี้ขึ้นมา เพื่อให้ผู้ใช้งานที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ ทราบถึงนโยบาย แนวทาง และขั้นตอนที่ถูกต้องครบถ้วนในทางปฏิบัติ อันจะส่งผลให้เกิดประสิทธิภาพในการปฏิบัติงาน และการพัฒนาระบบงานยิ่งขึ้น อีกทั้งต้องการให้ผู้ใช้งานได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ ณ ปัจจุบัน

แนวทางปฏิบัติ

1. **การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)**

ผู้ดูแลทรัพย์สินหรือผู้ได้รับมอบหมายจากผู้บริหาร มีหน้าที่ปฏิบัติดังนี้

1.1 ผู้บริหารมอบอำนาจ หรือกำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน

1.2 กำหนดมาตรการความปลอดภัยและผู้รับผิดชอบเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน

1.3 ควบคุมดูแลให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน และต้องได้รับอนุญาตจากผู้มีอำนาจเท่านั้น

1.4 กำหนดระยะเวลาของการนำทรัพย์สินออกไปใช้งานนอกหน่วยงาน

1.5 บันทึกข้อมูลการนำทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำทรัพย์สินส่งคืน พร้อมทั้งมีการบันทึกผู้รับผิดชอบในการดูแลรักษาทรัพย์สินหรืออุปกรณ์นอกพื้นที่

1.6 เมื่อมีการนำทรัพย์สินส่งคืน ให้ตรวจสอบจำนวนทรัพย์สินกับเอกสาร การชำรุดเสียหายของทรัพย์สินด้วยทุกครั้ง

1.7 บุคลากรที่มีส่วนเกี่ยวข้องทุกคนต้องไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะโดยไม่มีผู้รับผิดชอบ

1.8 เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

2. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

ผู้ดูแลทรัพย์สินมีหน้าที่ปฏิบัติดังนี้

2.1 ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

2.2 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

2.3 เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล (Procedure for Media Disposal) ดังนี้

ก. คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับ และไม่แน่ใจว่าลับหรือไม่ ให้อยู่ในกลุ่มเอกสารลับ

ข. ทำลายข้อมูลในสื่อบันทึกข้อมูล เพื่อป้องกันการกู้คืน โดยใช้วิธีการ ดังนี้

- ประเภท Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
- ประเภทกระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
- ประเภทแผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายแผ่น CD/DVD
- ประเภทเทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
- ประเภทฮาร์ดดิสก์	ใช้วิธีการทุบ บดให้เสียหาย หรือทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) หรือการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ

3. การบริหารจัดการข้อมูล

3.1 บริษัท วิริยะประกันภัย จำกัด (มหาชน) ถือเป็นเจ้าของข้อมูล หรือผู้มีสิทธิอนุญาตให้ใช้ข้อมูลที่เจ้าหน้าที่หรือผู้บันทึกข้อมูลของแต่ละหน่วยงานจัดทำขึ้น ห้ามมิให้บุคคลใดทำซ้ำ ดัดแปลง เปิดเผย แปล แก้ไขชื่อ เลข รหัสหรือเรียบเรียงใหม่ เว้นแต่ได้รับความยินยอมจากบริษัท วิริยะประกันภัย จำกัด (มหาชน) เป็นลายลักษณ์อักษร

3.2 ผู้ใช้งานทุกคนมีหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลของบริษัท ห้ามมิให้ผู้ใดเปิดเผยข้อมูลใดๆ ของบริษัท ให้แก่บุคคลภายนอกหรือบุคคลนอกหน่วยงาน ในกรณีที่จำเป็นให้ทำบันทึกเป็นลายลักษณ์อักษร และให้ผู้บังคับบัญชาลงลายมือชื่อพร้อมวันที่กำกับในบันทึก

3.3 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลและสอดคล้องกับกฎหมายหรือข้อกำหนดตามสัญญาต่างๆ เช่น การใช้ SSL การใช้ VPN การทำ Digital Signature ฯลฯ

3.4 ต้องมีมาตรการรักษาความปลอดภัยข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน ฯลฯ

3.5 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

3.6 ไม่ควรวางไฟล์ข้อมูลไว้บนหน้าจอ Desktop โดยให้มีเฉพาะทางลัดโปรแกรมที่จำเป็นเท่านั้น

3.7 หน่วยงานผู้รับผิดชอบจะต้องจัดหาสถานที่ที่ใช้ในการจัดเก็บเอกสาร สื่อบันทึกข้อมูล เครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ ที่เกี่ยวข้องให้มีความเหมาะสม ไม่ให้ได้รับความเสี่ยง

3.8 ภายหลังการใช้งานเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

3.9 ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกิน 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

3.10 ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่มีการดูแลชั่วคราว

3.11 เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4. การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

4.1 การเข้าถึงแฟ้มข้อมูล

ก. ผู้ใช้งานมีสิทธิในการเข้าถึงไฟล์ (File) หรือแฟ้มข้อมูล (Folder) ที่ผู้ใช้งานรับผิดชอบหรือได้รับมอบหมายเท่านั้น

ข. หากตรวจสอบได้ว่ามีการเข้าถึง หรือมีความพยายามที่จะเข้าถึงข้อมูลหรือแฟ้มข้อมูลที่ไม่ได้รับอนุญาต บริษัท จะถือว่าเป็นความผิด และเจ้าของรหัสผู้ใช้งาน (User ID) ที่ถูกใช้ในการเข้าถึงที่ไม่ได้รับอนุญาตดังกล่าว จะต้องรับผิดชอบในทุกกรณี และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้อง (เอกสารแนบท้าย)

4.2 การเข้าถึงโปรแกรมคอมพิวเตอร์

ก. ผู้ใช้งานหรือผู้ที่ได้รับมอบหมายมีสิทธิในการใช้งานโปรแกรมคอมพิวเตอร์ ตามความเหมาะสมกับหน้าที่ความรับผิดชอบ หรือตามที่ได้รับมอบหมายเท่านั้น เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) สิทธิการใช้งานอินเทอร์เน็ต สิทธิการใช้งานไปรษณีย์อิเล็กทรอนิกส์

ข. กรณีผู้ใช้งานขอเปลี่ยนชื่อ-นามสกุล ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาก่อน รวมทั้งระบุข้อมูลต่างๆ ที่ต้องการแก้ไข จากนั้นเจ้าหน้าที่ฝ่ายสารสนเทศหรือเจ้าหน้าที่สารสนเทศที่ได้รับมอบหมายที่มีหน้าที่รับผิดชอบดำเนินการแก้ไข แล้วทำการแจ้งกลับผู้ร้องขอต่อไป

ค. กรณีผู้ใช้งานขอโอนย้ายหน่วยงานหรือสถานที่ปฏิบัติงาน ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาต้นสังกัดและสถานที่ปฏิบัติงานใหม่ก่อน รวมทั้งระบุข้อมูลต่างๆ ให้ชัดเจนก่อนมีผลอย่างน้อย 7 วันทำการ จากนั้นเจ้าหน้าที่ฝ่ายสารสนเทศหรือเจ้าหน้าที่สารสนเทศที่ได้รับมอบหมายที่มีหน้าที่รับผิดชอบ ดำเนินการแก้ไขสิทธิโดยให้มีผลตามประกาศคำสั่งของฝ่ายบุคคล หลังจากนั้นจึงทำการแจ้งกลับผู้ร้องขอหรือผู้บังคับบัญชาของผู้ร้องขอต่อไป

ง. กรณีผู้ใช้งานขอยกเลิกสิทธิการใช้ระบบงาน สิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน ให้ยกเลิกสถานะของผู้ใช้ระบบงาน และทำการลบข้อมูลออกจากรายชื่อผู้มีสิทธิตามระยะเวลาที่กำหนด

4.3 การใช้งานอินเทอร์เน็ตขององค์กร

ก. ผู้ใช้งานที่ได้รับอนุญาตให้ใช้งานระบบอินเทอร์เน็ต ต้องได้รับความเห็นชอบ และอนุมัติเป็นลายลักษณ์อักษรจากผู้จัดการฝ่าย ผู้จัดการภาค หรือ ผู้บริหารระดับสูง เท่านั้น

ข. ผู้จัดการฝ่ายสารสนเทศมีอำนาจเต็มในการพิจารณา หรืออนุมัติการใช้งานอินเทอร์เน็ตของพนักงานทุกคน และฝ่ายสารสนเทศขอสงวนสิทธิในการพิจารณา หรืออนุมัติการใช้งานระบบอินเทอร์เน็ตของพนักงานแต่ละคนเป็นรายๆ ไป

4.4 การติดต่อสื่อสารทางอิเล็กทรอนิกส์

ก. ผู้ที่ต้องการใช้ระบบไปรษณีย์อิเล็กทรอนิกส์ ต้องแจ้งความจำนงต่อฝ่ายสารสนเทศ โดยเขียนใบคำร้อง และต้องได้รับการรับรองเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาระดับแผนกขึ้นไป

ข. ผู้จัดการฝ่ายสารสนเทศมีอำนาจเต็มในการพิจารณา หรืออนุมัติการใช้งานระบบไปรษณีย์อิเล็กทรอนิกส์ของพนักงานทุกคน และฝ่ายสารสนเทศขอสงวนสิทธิในการพิจารณา หรือการอนุมัติใช้งานระบบไปรษณีย์อิเล็กทรอนิกส์ของพนักงานแต่ละคนเป็นรายๆ ไป

5. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

5.1 การใช้งานเครือข่ายไร้สาย (Wireless Policy)

ก. ไม่อนุญาตให้ผู้ใช้งานเปิด Ad-hoc หรือ Peer-to-Peer Network

ข. การเข้าใช้ “Wireless จะต้องเข้าใช้ผ่าน Username และ Password ที่หน่วยงานกำหนด

ค. เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

ง. ห้ามมิให้ผู้ใดนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็นอุปกรณ์กระจายสัญญาณ (Access Point), Wireless Routers, Wireless USB Client หรือ Wireless Card ภายในหน่วยงาน ยกเว้นจะได้รับอนุญาตจากฝ่ายสารสนเทศ

จ. การเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) จะต้องได้รับอนุญาตจากผู้ดูแลระบบ และมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้นๆ ก่อนเข้าใช้งานเครือข่ายของหน่วยงาน

5.2 การเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆ กับเครือข่าย

ก. ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆ กับเครือข่ายอื่น

ข. นอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

ค. ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้ดูแลระบบ

6. การควบคุมคอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

6.1 การใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile devices) ต้องกำหนดวิธีการป้องกันข้อมูลและทรัพย์สินสารสนเทศที่อยู่ในอุปกรณ์คอมพิวเตอร์แบบพกพาหรืออุปกรณ์สื่อสารอื่นๆ

6.2 การปฏิบัติงานภายนอกหน่วยงาน (Teleworking) อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานโดยต้องใช้งานผ่านช่องทางที่จัดเตรียมไว้ให้ และต้องตรวจสอบตัวตนก่อนการใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน รวมทั้งต้องไม่นำข้อมูลลับของบริษัทไปไว้บนอุปกรณ์ส่วนตัว หรือหากมีความจำเป็นต้องใช้งาน เมื่อใช้งานเสร็จแล้วควรลบทิ้งไป

7. การใช้ระบบสารสนเทศในการดำเนินงาน

7.1 การส่งข้อมูลใดๆ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้อง (เอกสารแนบท้าย)

7.2 ผู้ใช้งานต้องใช้ข้อมูลในระบบสารสนเทศในการดำเนินงานอย่างระมัดระวัง

7.3 ผู้ใช้งานต้องพิจารณาถึงความเหมาะสมและความสำคัญของข้อมูลก่อนการนำข้อมูลเข้าสู่ระบบสารสนเทศ

7.4 ข้อมูล ข้อความ และเอกสารใดๆ ที่จัดเก็บไว้ในระบบสารสนเทศขององค์กรให้ถือเป็นสินทรัพย์ขององค์กร

7.5 การใช้งานจะต้องไม่เป็นการขัดขวางประสิทธิภาพในการปฏิบัติงานภายในองค์กร

7.6 ไม่ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

7.7 ห้ามโพสต์ ดาวน์โหลดไฟล์รูปภาพ หรือข้อมูลใดๆ บนอินทราเน็ต หรือ เว็บไซต์อื่นๆ ที่เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้อง (เอกสารแนบท้าย)

7.8 ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็น จดหมายอิเล็กทรอนิกส์ (e-mail) การสนทนา (Chat) หรือการติดต่อสื่อสารใดๆ (Digital Communication) ให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการ โดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือหรือจดหมายของบริษัท เช่น การรักษาความลับของเอกสาร ห้ามส่งเอกสารความลับผ่านทางจดหมายอิเล็กทรอนิกส์ยกเว้นได้รับการเข้ารหัสโดยได้รับการยืนยันจากฝ่ายสารสนเทศ

7.9 ให้ใช้ข้อความสุภาพในการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) การสนทนา (Chat) หรือการสื่อสารทางอิเล็กทรอนิกส์อื่นๆ (Digital Communication)

7.10 ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อองค์กรหรือบุคคลอื่นๆ

7.11 ห้ามส่งไฟล์รูปภาพ ข้อความ หรือไฟล์ที่เกี่ยวข้องกับเรื่องลามกอนาจาร

7.12 ห้ามส่งจดหมายอิเล็กทรอนิกส์หรือการสื่อสารทางอิเล็กทรอนิกส์ใดๆ ที่ไม่เกี่ยวข้องกับธุรกรรมขององค์กร

7.13 ไม่อนุญาตให้ผู้ใช้งานใช้ e-mail อื่นใดที่ฝ่ายสารสนเทศไม่ได้กำหนดให้ใช้ ในการทำธุรกรรมที่เกี่ยวกับองค์กร

8. บทลงโทษ

ผู้ใช้งานจะต้องไม่กระทำการ ดังต่อไปนี้

8.1 เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

8.2 กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้ เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

8.3 ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

8.4 กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

8.5 กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

8.6 จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามข้อ 8

ผู้ใดปฏิบัติฝ่าฝืนหรือละเว้นต่อการปฏิบัติตามระเบียบของฝ่ายสารสนเทศ จนทำให้บริษัทได้รับความเสียหาย ซึ่งเข้าตามลักษณะความผิดทางวินัย ให้ถือว่าผู้ใช้งานผู้นั้นมีความผิด และต้องถูกลงโทษตามระเบียบของบริษัท ว่าด้วยเรื่อง “วินัยและโทษทางวินัย” ในกรณีร้ายแรง จะถูกนำเสนอต้นสังกัดเพื่อดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้อง (เอกสารแนบท้าย)

เอกสารแนบท้าย

พระราชบัญญัติและกฎหมายที่เกี่ยวข้อง

ธุรกรรมทางอิเล็กทรอนิกส์

ก. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551

ข. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ค. พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551

ง. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

จ. พระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554

ฉ. พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ พ.ศ. 2549

ช. พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ของสถาบันการเงินเฉพาะกิจ พ.ศ. 2559

คุ้มครองข้อมูลส่วนบุคคล

ก. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540

ข. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ.2553

ทรัพย์สินทางปัญญาที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์

ก. พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

ข. พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558

ค. พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 3) พ.ศ. 2558

ง. พระราชบัญญัติสิทธิบัตร พ.ศ. 2552

จ. พระราชบัญญัติเครื่องหมายการค้า พ.ศ. 2534

กฎหมายต่างประเทศ

ก. UNCITRAL
   1) United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)
   2) UNCITRAL Model Law on Electronic Signatures (2001)
   3) UNCITRAL Model Law on Electronic Commerce (1996)

ข. Singapore
   1) Personal Data Protection Act 2012 (PDPA)

ค. OECD
   1) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)

ง. APEC
   1) APEC Privacy Framework

กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ก. พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550

ข. กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. 2551

ค. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

ง. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

จ. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ฉ. ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

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

ข้อมูลอ้างอิง

ETDA (Electronic Transactions Development Agency (Public Organization)

URL: https://ictlawcenter.etda.or.th/laws