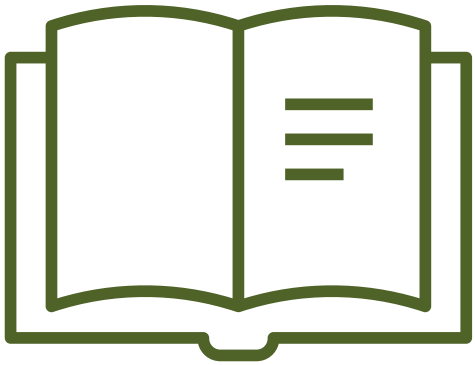
COMANCHE
INTERNATIONAL PUBLIC COMPANY LIMITED



นโยบายและคู่มือปฏิบัติงานสารสนเทศ

บริษัท โคแมนชี่ อินเตอร์เนชั่นแนล จำกัด (มหาชน)

สารบัญ

นโยบายสารสนเทศ (Information Technology Policy)

บริษัท โคแมนชี่ อินเตอร์เนชั่นแนล จำกัด(มหาชน) (“บริษัทฯ”) ตระหนักถึงความสำคัญของเทคโนโลยีสารสนเทศ จึงได้จัดทำนโยบายสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้อง โดยมีวัตถุประสงค์เพื่อให้ผู้ใช้งาน และบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ เพื่อการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ ได้อย่างมีประสิทธิภาพและมีมาตรฐาน

1. นโยบาย/การบริหาร และระเบียบปฏิบัติงานที่สำคัญ (Policy/Governance and IT Policy)

การกำกับดูแลและความรับผิดชอบอย่างเป็นทางการ

1. การแต่งตั้งผู้รับผิดชอบอย่างเป็นทางการ:

แต่งตั้ง "คณะกรรมการความมั่นคงปลอดภัยด้านสารสนเทศ" หรือ "ผู้จัดการฝ่ายสารสนเทศ (Chief Information Officer - CIO)" หรือตำแหน่งเทียบเท่า เป็นผู้รับผิดชอบนโยบายความมั่นคงปลอดภัยด้าน IT อย่างเป็นทางการ มีอำนาจในการอนุมัติ ติดตาม และบังคับใช้นโยบาย

2. ทบทวนนโยบาย:

กำหนดให้มีการทบทวนนโยบายนี้อย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญทางธุรกิจและเทคโนโลยี

2. นโยบายรักษาความปลอดภัยด้านสารสนเทศและการรักษาความปลอดภัยข้อมูล

1. การควบคุมทางกายภาพ (Physical Control):

จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์เครือข่าย (Network) เป็นต้น ไว้ในห้องเฉพาะหรือพื้นที่หวงห้าม โดยมีป้ายบอกชัดเจน หรือ ตู้ rack server ที่มีการล็อคและจำการการเข้าถึง

2. การกำหนดสิทธิการเข้าถึง (Access Control) ตามหลัก Need-to-Know:

กำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ให้เหมาะสมกับหน้าที่และความรับผิดชอบ และจำกัดการเข้าถึงเครือข่ายหรือบริการคอมพิวเตอร์ที่ไม่เกี่ยวข้องกับงานที่ได้รับมอบหมาย โดยอิงตามหลักการ "สิทธิที่จำเป็นต้องใช้เท่านั้น (Need-to-Know / Least Privilege)" หากผู้ใช้ต้องการสิทธิในการเข้าถึงระบบงานใด ต้องกรอกแบบฟอร์มและขออนุมัติจากหัวหน้างานและส่วนงานที่เกี่ยวข้องก่อน

3. การควบคุมการเข้าถึงและนำข้อมูลออกจากฐานข้อมูลโดยตรง (Direct Database Access Control):

จำกัดการเข้าถึงฐานข้อมูลที่สำคัญโดยตรง (เช่น การใช้ SQL Query) ให้เฉพาะบุคลากร IT ที่ได้รับมอบหมายและต้องมีเหตุผลทางธุรกิจที่ชัดเจนเท่านั้น

ห้าม บุคลากรนำข้อมูลออกจากฐานข้อมูลโดยตรงเพื่อจุดประสงค์ที่ไม่เกี่ยวข้องกับการทำงาน หรือโดยปราศจากการอนุมัติจากผู้รับผิดชอบข้อมูล (Data Owner) อย่างเป็นลายลักษณ์อักษร

จัดให้มีระบบบันทึก (Logging) การเข้าถึงฐานข้อมูลโดยตรงทั้งหมด เพื่อตรวจสอบย้อนหลัง

4. ระบบตรวจสอบตัวตน (Identification and Authentication):

จัดให้มีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งาน โดยให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ไม่ใช่ Account รวม

5. ระบบป้องกันไวรัสและภัยคุกคาม:

จัดซื้อระบบตรวจจับและป้องกันไวรัสคอมพิวเตอร์ (Antivirus Software) ให้เพียงพอต่อความต้องการ

จัดให้มีระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก รวมถึงระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย

6. ลิขสิทธิ์ซอฟต์แวร์:

จัดซื้อซอฟต์แวร์ให้เพียงพอสำหรับการใช้งานและถูกต้องตามลิขสิทธิ์

7. ห้ามการกระทำที่ผิดกฎหมาย/ก่อความเสียหาย:

ห้ามนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

8. การสื่อสารนโยบาย:

กำหนดวิธีการสื่อสารนโยบายสารสนเทศให้พนักงานทุกคนทราบอย่างทั่วถึง

3. การกำหนดรหัสผ่าน (Password Management Policy)

1. ความยาวและองค์ประกอบของรหัสผ่าน:

กำหนดให้ใช้รหัสผ่านที่มีความยาวอย่างน้อย 12 ตัวอักษร โดยต้องประกอบด้วยอักขระอย่างน้อย 3 ใน 4 ประเภทต่อไปนี้: ตัวอักษรพิมพ์เล็ก, ตัวอักษรพิมพ์ใหญ่, ตัวเลข, และอักขระพิเศษ

2. ข้อห้ามในการตั้งรหัสผ่าน:

ตั้งรหัสผ่านที่ยากต่อการเดา ห้ามใช้ ข้อมูลส่วนตัว (ชื่อ, วันเกิด), คำในพจนานุกรม, หรืออักขระที่เรียงกัน (เช่น 123456, abcde)

3. ความลับของรหัสผ่าน:

ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น (ยกเว้นผู้ดูแลระบบตามความจำเป็นภายใต้การควบคุมที่เข้มงวด) และไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น หรือใช้รหัสผ่านเดียวกันกับระบบงานที่ไม่ใช่ของบริษัทฯ

4. การเปลี่ยนรหัสผ่าน:

กำหนดให้พนักงานทุกคนเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ หรืออย่างน้อยทุก ๆ 180 วัน

4. การประเมินและบริหารความเสี่ยงด้าน IT (IT Risk Assessment)

1. จัดให้มีการประเมินความเสี่ยงด้าน IT และความปลอดภัยของข้อมูลอย่างเป็นทางการ อย่างน้อยปีละ 1 ครั้ง เพื่อระบุภัยคุกคาม จุดอ่อน และผลกระทบต่อสินทรัพย์สารสนเทศที่สำคัญ

2. กำหนดมาตรการควบคุมและแผนปฏิบัติการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

3. ทบทวนและปรับปรุงการประเมินความเสี่ยงเมื่อมีการเปลี่ยนแปลงระบบงานหรือเทคโนโลยีสำคัญ

5. การจัดประเภทข้อมูล (Data Classification)

1. กำหนดและจัดทำกรอบการจำแนกประเภทข้อมูล (เช่น ข้อมูลลับสูงสุด, ข้อมูลลับ, ข้อมูลภายใน, ข้อมูลสาธารณะ) เพื่อให้มั่นใจว่ามาตรการรักษาความปลอดภัยเหมาะสมกับระดับความอ่อนไหวของข้อมูล

2. กำหนดสิทธิการเข้าถึง การจัดเก็บ การประมวลผล และการทำลายข้อมูลตามประเภทที่จัดไว้

6. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

1. จัดให้มีคำบรรยายลักษณะงาน (Job Description) ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่ายไอทีเป็นลายลักษณ์อักษร

2. กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน

3. จัดให้มีการฝึกอบรมภายในเพื่อถ่ายทอดความรู้เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น

7. การควบคุมการเข้าถึงและการป้องกันความเสียหาย (Physical Security)

1. กำหนดพื้นที่วางเครื่องแม่ข่ายให้เป็นสัดส่วน มีป้ายบอกชัดเจน

2. จัดหาตู้ใส่เครื่องแม่ข่าย (Server Rack) ที่สามารถล็อคกุญแจได้เพื่อควบคุมการเข้าถึงอุปกรณ์จากผู้ไม่เกี่ยวข้อง

3. จัดให้มีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์แม่ข่ายที่สำคัญ เพื่อทำให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

4. จัดให้มีอุปกรณ์ตรวจจับควันและระบบดับเพลิงอัตโนมัติ (Sprinkler) เพื่อให้สามารถป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา (ตามมาตรฐานของอาคาร)

หมายเหตุ: ผู้ควบคุมกุญแจสำหรับเข้าห้องหรือเปิด Server Rack คือ Head of Development

8. นโยบายการใช้งานระบบอินเตอร์เน็ต (Internet Usage Policy)

1. ผู้ใช้ต้องไม่ใช้เครือข่ายอินเตอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว หรือเข้าสู่เว็บไซต์ที่ไม่เหมาะสม (ผิดศีลธรรม, ผิดกฎหมาย, เป็นภัยต่อสังคม)

2. ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

3. ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านเครือข่ายอินเตอร์เน็ต

4. ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

5. ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ตก่อนนำข้อมูลไปใช้งาน

6. เครื่องคอมพิวเตอร์ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและเปิดระบบการอุดช่องโหว่ของระบบปฏิบัติการ (Patch / Fix Update) เสมอ

7. ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเตอร์เน็ต ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น

9. การแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

1. การพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ที่ส่งผลกระทบกับผู้ใช้งานจำนวนมาก (อาทิเช่น อัพเกรดระบบ, ปิดเครื่องแม่ข่ายเพื่อบำรุงรักษา, เปลี่ยนแปลงอุปกรณ์เครือข่ายตัวหลัก) ต้องจัดทำเป็นลายลักษณ์อักษร และได้รับอนุมัติจากผู้มีอำนาจก่อนเสมอ

2. ต้องจัดการประเมินผลกระทบก่อนการเปลี่ยนแปลงระบบ หรืออุปกรณ์ที่เกี่ยวข้อง หรือทำการทดสอบระบบใหม่ภายในวงจำกัดก่อนเริ่มใช้งานจริง โดยผู้ที่ขอแก้ไขเปลี่ยนแปลงและผู้ใช้รายอื่นที่เกี่ยวข้องจะต้องมีส่วนร่วมในการทดสอบระบบ

10. การสำรองข้อมูลและการเตรียมพร้อมกรณีฉุกเฉิน (Business Continuity Plan – BCP)

1. มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพในเวลาที่ต้องการ

2. จัดให้มีการบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน

3. จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกสถานที่ (off-site backup)

4. ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ การตั้งค่า (Configuration) ข้อมูลในฐานข้อมูล เป็นต้น

5. จัดให้มีการทดสอบการเรียกข้อมูลสำรอง (Data backup restoration) อย่างน้อยปีละ 1 ครั้ง

6. จัดให้มีการสื่อสารและซ้อมแผนรองรับสถานการณ์ฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

11. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation Planning and Control)

1. จัดให้มีการตรวจสอบการทำงานของเครื่องแม่ข่ายและจัดทำรายงาน System Monitor and Logging ทุกเดือนเพื่อตรวจสอบประสิทธิภาพการทำงานของระบบ

2. กำหนดให้มีการบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบของผู้ดูแลระบบ บันทึกการพยายามเข้าสู่ระบบจากบุคคลภายนอก

3. จัดให้มีการทำสำรองข้อมูลตามที่ได้กำหนดไว้ในแผนรองรับสถานการณ์ฉุกเฉิน

12. การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง (Asset Management System)

1. การจัดซื้อทรัพย์สิน: ทรัพย์สิน เช่น เครื่องใช้หรืออุปกรณ์ต่าง ๆ ภายในบริษัท พนักงานจะต้องทำการกรอกแบบฟอร์มสั่งซื้อ และหัวหน้าแผนกจะเป็นผู้พิจารณาถึงความเหมาะสมและทำการลงนามเสนอซื้อ ก่อนส่งให้ผู้มีอำนาจอนุมัติพิจารณาลงนามอนุมัติ

2. ทะเบียนทรัพย์สิน: จัดให้มีทะเบียนทรัพย์สินโดยมีข้อมูลสำคัญ: วันที่จัดซื้อ/อายุการใช้งาน/ผู้ครอบครอง/มูลค่าทรัพย์สิน/สถานที่นำไปใช้

3. การตรวจนับ: จัดให้มีการตรวจนับทรัพย์สินปีละครั้งอย่างน้อย

4. การควบคุม Software และ License (เพิ่มเติม):

จัดให้มีทะเบียนคุม Software และ License ทั้งหมดที่ใช้งานในองค์กร โดยมีข้อมูลสำคัญ: ชื่อ Software, เลขที่ License, วันหมดอายุ, จำนวนสิทธิการใช้งานที่ถูกต้อง, และผู้รับผิดชอบ Software นั้นๆ

มีการตรวจสอบทะเบียนคุมนี้อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการใช้งาน Software ทั้งหมดเป็นไปตามเงื่อนไขลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

13. การควบคุมผู้ให้บริการ IT ภายนอก (Third-Party Service Control)

1. กำหนดให้มีการทำสัญญาหรือข้อตกลงที่ระบุข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการ IT ภายนอก (Vendors, Outsourced IT) อย่างชัดเจน

2. บริษัทฯ ต้องมีการตรวจสอบและประเมินมาตรการรักษาความปลอดภัยของผู้ให้บริการภายนอกก่อนและระหว่างการใช้งาน

14. นโยบายการบริหารจัดการความเสี่ยงด้านสารสนเทศ (Information Security Risk Management Policy)

นิยาม

ระบบข้อมูลสารสนเทศถือเป็น ทรัพย์สินทางการบริหารที่มีความสำคัญสูงสุด ต่อการดำเนินงานของบริษัท บริษัทตระหนักดีว่า แม้จะมีคู่มือปฏิบัติการ แต่ความเสี่ยงจากปัจจัยภายนอก (ภัยพิบัติ, การโจมตี) และปัจจัยภายใน (อุปกรณ์ขัดข้อง, ความผิดพลาดของบุคลากร) ยังคงมีอยู่ ซึ่งอาจส่งผลให้การทำงานหยุดชะงักและเกิดความเสียหายร้ายแรงได้

ดังนั้น จึงได้กำหนดนโยบายการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Security Plan) ขึ้น เพื่อให้เป็นกรอบแนวทางที่ชัดเจนในการป้องกัน แก้ไข และฟื้นฟูระบบให้กลับมาดำเนินการได้อย่างรวดเร็ว

วัตถุประสงค์ (Objectives)

1. สร้างความเข้าใจที่เป็นเอกภาพ ระหว่างผู้บริหารและผู้ปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยของฐานข้อมูลสารสนเทศ

2. กำหนดแนวทางมาตรฐาน ในการดูแลรักษาระบบความมั่นคงปลอดภัยของข้อมูลให้มีเสถียรภาพและมีความพร้อมใช้งาน (Availability) สูงสุด

3. ทำให้การปฏิบัติงานเป็นไปอย่าง มีระบบและต่อเนื่อง (Business Continuity) และสามารถแก้ไขสถานการณ์ฉุกเฉินได้อย่างทันท่วงที

4. ลดความเสียหาย และเตรียมความพร้อมรับมือสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบข้อมูลสารสนเทศ

แนวทางการป้องกันความเสียหายจากเหตุการณ์ต่าง ๆ (Risk Mitigation)

1. ภัยจากสิ่งแวดล้อมและสถานที่ตั้ง

อัคคีภัย (Fire):

- ห้ามกระทำการใด ๆ ที่อาจนำไปสู่การเกิดอัคคีภัยในพื้นที่ปฏิบัติงานและห้อง Server

- ประสานงานกับผู้บริหารอาคารให้มีการติดตั้งเครื่องตรวจจับควันและเครื่องดับเพลิงอัตโนมัติที่ได้มาตรฐาน
- จัดซื้อถังดับเพลิงชนิดที่ใช้สำหรับอุปกรณ์อิเล็กทรอนิกส์ (เช่น สารสะอาด) และเตรียมให้พร้อมใช้งานและอยู่ในจุดที่เข้าถึงง่าย
- เจ้าหน้าที่ทุกคนต้องศึกษาเส้นทางหนีไฟและให้ความร่วมมือในการซ้อมหนีไฟตามกำหนด

อุทกภัยและความชื้น (Flood and Moisture):

- ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่ายหลักนอกบริเวณที่น้ำท่วมถึง
- ตรวจสอบการรั่วซึมจากเครื่องปรับอากาศ ท่อน้ำ ฝ้าเพดาน หรือบริเวณหน้าต่างอย่างสม่ำเสมอเพื่อป้องกันน้ำฝนหรือน้ำค้างสะสม

อุณหภูมิที่ไม่เหมาะสม (Temperature):

- ติดตั้งเครื่องปรับอากาศในห้อง Server ที่สามารถทำงานได้ต่อเนื่อง 24 ชั่วโมง
- ตั้งอุณหภูมิให้อยู่ในระดับที่เหมาะสมต่อการทำงานของอุปกรณ์
- ติดตั้งอุปกรณ์ตั้งเวลา (Timer) หรือระบบควบคุมอัตโนมัติเพื่อสำรองการทำงานของเครื่องปรับอากาศ

2. การรักษาความปลอดภัยทางกายภาพ (Physical Security)

- การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย
- ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้อง Server โดยเด็ดขาด
- ติดตั้งกล้องวงจรปิด (CCTV) บริเวณประตูทางเข้าออกสำนักงานของบริษัท และจุดสำคัญอื่นๆที่เกี่ยวข้องกับระบบสารสนเทศ

3. การจัดการระบบเครือข่ายและกระแสไฟฟ้า

ระบบอินเตอร์เน็ตขัดข้อง:

- ดำเนินการตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารอย่างสม่ำเสมอ เพื่อให้สามารถใช้งานได้ตลอดเวลา
- จัดให้มี เครือข่ายอินเทอร์เน็ตสำรอง (Backup Internet Link) เพื่อใช้งานทดแทนทันทีที่เครือข่ายหลักขัดข้อง

ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ:

- แยกไฟระบบคอมพิวเตอร์แม่ข่ายออกจากสายไฟหลักที่ผ่านสะพานไฟเข้าสู่หน่วยงาน เพื่อควบคุมการจ่ายไฟโดยเฉพาะ
- ติดตั้ง เครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (Uninterruptible Power Supply - UPS) ที่มีประสิทธิภาพ
- เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย

4. การรักษาความปลอดภัยทางตรรกะ (Logical Security)

การบุกรุกหรือโจมตีภายนอก (Intrusion/Attack):

- ติดตั้งและดูแลอุปกรณ์ Firewall เพื่อป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตเข้าสู่เครือข่ายภายในบริษัท
- ตรวจสอบประวัติ (Log) การบุกรุกจากบุคคลภายนอกอย่างสม่ำเสมอ
- ตรวจสอบปริมาณข้อมูลบนเครือข่ายที่มีปริมาณมากผิดปกติ เพื่อวิเคราะห์หาสาเหตุและป้องกัน

การกำหนดรหัสผ่าน (Password Policy):

- รหัสผ่านต้องมีความยาวขั้นต่ำ อย่างน้อย 8 อักขระ
- รหัสผ่านต้องยากต่อการเดา ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 1234, หรือ abcd
- ห้ามเปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น
- ห้ามใช้รหัสตนเองร่วมกับผู้อื่น

ไวรัสคอมพิวเตอร์ (Computer Virus/Malware):

- ติดตั้งโปรแกรมป้องกันไวรัสและมีการ Update ข้อมูลไวรัสให้เป็นปัจจุบันอยู่เสมอ
- ระมัดระวังภัยจากการเปิดไฟล์บันทึกข้อมูลต่าง ๆ เช่น USB Flash Drive และ ไม่เปิดไฟล์ที่มีนามสกุลแปลก
- ใช้ความระมัดระวังในการเปิด e-mail โดย ห้ามเปิดไฟล์ที่ไม่ทราบแหล่งที่มา หรือถ้าไม่ทราบแหล่งที่มาควรลบทิ้งทันที
- หลีกเลี่ยงการดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ และหลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น
- ใช้โปรแกรมเพื่อทำาการตรวจหาไวรัสอย่างน้อย สัปดาห์ละ 1 ครั้ง

5. การบริหารจัดการโครงสร้างพื้นฐานและเทคโนโลยีสมัยใหม่

เพื่อให้ระบบสารสนเทศมีความยืดหยุ่น ลดความเสี่ยง และง่ายต่อการดูแลรักษา บริษัทมีแนวทางดังนี้:

การปรับเปลี่ยนระบบสู่คลาวด์ (Cloud Transformation):

- พิจารณาย้ายระบบหรือโปรแกรมภายในจาก Physical Server ไปสู่ระบบคลาวด์ (On-Cloud Service) ในส่วนที่เหมาะสม เพื่อลดภาระการดูแลรักษาอุปกรณ์ (Hardware)
- ใช้ประโยชน์จากระบบคลาวด์ในการสำรองข้อมูล (Backup) และการกู้คืนระบบ (Disaster Recovery) เพื่อสร้างความต่อเนื่องในการทำงาน (Business Continuity) และลดค่าใช้จ่ายในระยะยาว

การจัดการตู้จัดเก็บอุปกรณ์เครือข่าย (Network Rack Management):

- Physical Security: จัดเตรียมตู้ Rack ที่มีความแข็งแรงและมีระบบล็อกที่แน่นหนา เพื่อป้องกันการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต
- Access Control: กำหนดผู้มีสิทธิ์ถือครองกุญแจตู้ Rack อย่างชัดเจน (เช่น IT Manager หรือผู้ที่ได้รับมอบหมายเท่านั้น) และมีการบันทึกการเข้าใช้งาน
- Organization & Labeling: จัดระเบียบสายสัญญาณและติดป้ายชื่อ (Labeling) อุปกรณ์ทุกชิ้นให้ชัดเจน เพื่อความรวดเร็วและแม่นยำในการตรวจสอบเมื่อเกิดปัญหา (Troubleshooting)
- Power Protection: ติดตั้งเครื่องสำรองไฟฟ้า (UPS) ภายในตู้ Rack เพื่อป้องกันความเสียหายของอุปกรณ์ Network จากปัญหาไฟกระชากหรือไฟดับ

ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ (Incident Response)

1. กรณีเครื่องลูกข่าย (Client Workstation)

เมื่อพบเหตุขัดข้องที่ทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือผู้ดูแลทราบทันที

กรณีติดไวรัสคอมพิวเตอร์:

- เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องโดยเร็วที่สุด
- ให้เจ้าหน้าที่ผู้ใช้เครื่อง กำจัดไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส
- แจ้งเจ้าหน้าที่ที่เกี่ยวข้องเพื่อเข้าตรวจสอบและยืนยันความปลอดภัย
- ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึก ให้ดึงสาย (LAN) ออกจากจุดรวมสายในชั้นนั้นออกให้หมด

2. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย (Server and Network Equipment)
   - ไฟฟ้าดับ/ไฟฟ้าตก: ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า (UPS)
   - ไฟไหม้: ปิดระบบจ่ายไฟทันที และใช้น้ำยาดับเพลิงที่เหมาะสมฉีดควบคุมเพลิงโดยเร็วที่สุด พร้อมทั้งรีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย
   - การขัดข้องทั่วไป: ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ (Server) และระบบเครือข่ายโดยเร็วที่สุด
   - อุปกรณ์ด้านฮาร์ดแวร์เสีย: ให้รีบจัดหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด
   - ผู้ดูแลระบบต้อง แจ้งผู้บังคับบัญชาทราบถึงเหตุขัดข้องและมาตรการแก้ไขโดยเร็วที่สุด
3. หลักการปฏิบัติของบุคลากรในกรณีเกิดอัคคีภัย
   - เมื่อพบอัคคีภัยให้ แจ้งเจ้าหน้าที่รักษาความปลอดภัยของอาคารทันที
   - ปฏิบัติตามแผนซ้อมหนีไฟ ที่ได้รับการฝึกอบรมมาอย่างเคร่งครัด
4. ระบบป้องกันและการแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า (Power Management)
   - เปิดเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาการใช้งาน
   - เมื่อเกิดกระแสไฟฟ้าดับให้ รีบทำการบันทึกข้อมูล (Save) ทันที
   - ดำเนินการปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่เกี่ยวข้องอย่างถูกต้องตามขั้นตอน
   - เริ่มการทำงานของระบบอีกครั้ง เมื่อแน่ใจว่าระบบไฟฟ้าทำงานเป็นปกติและมีเสถียรภาพแล้วเท่านั้น

15. นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนด และมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

นิยาม

อุปกรณ์พกพา หมายถึง อุปกรณ์คอมพิวเตอร์ประเภทพกพา

อุปกรณ์คอมพิวเตอร์ประเภทพกพา หมายถึง อุปกรณ์ประมวลผล คอมพิวเตอร์ซึ่งมีหน่วยประมวลผลข้อมูลภายในโดยทั่วไปเป็นอุปกรณ์คอมพิวเตอร์ขนาดเล็กที่สามารถพกพา หรือเคลื่อนย้ายไปกับตัวบุคคลได้โดยง่ายและมีน้ำหนักเบา เช่น เครื่องคอมพิวเตอร์โน๊ตบุ๊ค

แนวปฏิบัติทั่วไป

1. ผู้ใช้ควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร
2. ผู้ใช้ต้องปฏิบัติตามนโยบายสารสนเทศของบริษัทอย่างเคร่งครัด
3. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ไอทีเท่านั้น
4. หากจำเป็นต้องส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อม ผู้ใช้งานจะต้องแจ้งเจ้าหน้าที่ไอทีก่อนเสมอ
5. ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ
6. ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และอุปกรณ์
7. กรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
8. ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้
9. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
10. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
11. ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์
12. การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
13. ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน
14. ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
15. ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
16. ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็กโทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
17. ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
18. การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

แนวปฏิบัติการป้องกันความปลอดภัยทางด้านกายภาพ

1. ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2. ผู้ใช้ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อนความชื้น ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

3. ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน

แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

1. ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

2. ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในนโยบายสารสนเทศของบริษัท

3. ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) ให้ทำการล็อคหน้าจอโดยอัตโนมัติเมื่อไม่มีการใช้งานเกิน 30 นาที และกำหนดให้ใส่รหัสผ่านใหม่อีกครั้งเมื่อต้องการใช้งาน

4. ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

1. ผู้ใช้ต้องทำการ Update ระบบปฏิบัติการเว็บบราวเซอร์และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

2. ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

3. หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

1. ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

2. ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

3. แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

4. แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

การส่งเครื่องคอมพิวเตอร์แบบพกพาเข้ารับการซ่อม

วัตถุประสงค์

เพื่อกำหนดขั้นตอนที่ชัดเจนในการส่งเครื่องคอมพิวเตอร์แบบพกพาเข้ารับการซ่อม เพื่อให้การดำเนินการเป็นไปอย่างรวดเร็วและเป็นไปตามระเบียบปฏิบัติขององค์กร

ขั้นตอนทั่วไป

1. พนักงานที่พบปัญหาต้อง แจ้งเจ้าหน้าที่ไอที ก่อนเสมอ

2. พนักงานต้องจัดทำ ใบแจ้งซ่อมสินทรัพย์ และนำส่งเครื่องคอมพิวเตอร์แบบพกพาให้แก่เจ้าหน้าที่ไอที

3 .เจ้าหน้าที่ไอทีจะรับเครื่องเพื่อดำเนินการตามขั้นตอนต่อไป

กรณีที่ 1: เครื่องคอมพิวเตอร์ยังอยู่ในระยะประกัน

เจ้าหน้าที่ไอทีจะดำเนินการประสานงานกับผู้ให้บริการ (Call Center หรือศูนย์ซ่อม) เพื่อดำเนินการนัดหมายการซ่อม (แบบนำส่งซ่อม หรือ On-site Service)

กรณีที่ 2: เครื่องคอมพิวเตอร์หมดระยะประกัน

1. เจ้าหน้าที่ไอทีจะดำเนินการติดต่อร้านซ่อมภายนอก เพื่อขอใบเสนอราคาและส่งเครื่องเข้ารับการซ่อม
2. การอนุมัติค่าใช้จ่าย:
   - มูลค่าซ่อมไม่เกิน 5,000 บาท: ให้เบิกจ่ายโดยใช้เงินสดย่อย
   - มูลค่าซ่อมเกิน 5,000 บาท: ให้เปิดใบขอซื้อ (PR) และใบสั่งซื้อ (PO) เพื่อขออนุมัติตามระเบียบ
3. เจ้าหน้าที่ไอทีจะแจ้งกำหนดวันส่งคืนเครื่องแก่พนักงานหลังการซ่อมเสร็จสิ้น

กรณีที่ 3: กรณีฉุกเฉิน (เครื่องหมดประกันและจำเป็นต้องใช้งานด่วน)

1. พนักงานสามารถนำเครื่องส่งร้านซ่อมภายนอกด้วยตนเองได้
2 .พนักงานต้องให้ร้านซ่อมจัดทำ ใบเสนอราคา และ แจ้งค่าใช้จ่ายให้เจ้าหน้าที่ไอทีรับทราบทันที
3. การเบิกจ่ายและการสำรองเงิน:
   - พนักงานสามารถนำหลักฐานการชำระเงินมาเบิกคืนจากฝ่ายบัญชี/การเงินได้
   - หากไม่มีเงินสำรองจ่าย สามารถแจ้งเจ้าหน้าที่บัญชีและการเงินเพื่อขอโอนเงินทดรองจ่ายเข้าบัญชีพนักงานก่อน และทำเอกสารหลักฐานส่งให้ฝ่ายบัญชีภายหลัง
4. ใบเสร็จรับเงินค่าซ่อมจะต้องออกในนาม บริษัท เท่านั้น

เอกสารที่เกี่ยวข้อง

- ใบแจ้งซ่อมสินทรัพย์

16. การควบคุมการปฏิบัติตามกฎหมายและกฎเกณฑ์ (Compliance)

1. กำหนดให้ฝ่าย IT มีหน้าที่ติดตาม ตรวจสอบ และทบทวนกฎหมาย กฎเกณฑ์ ข้อบังคับ และสัญญาที่เกี่ยวข้องกับ IT และข้อมูลของบริษัทฯ เพื่อให้มั่นใจว่าระบบและกระบวนการปฏิบัติงานเป็นไปตามข้อกำหนดเหล่านั้น

2. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายและกฎหมาย (Audit) ภายในหรือภายนอกอย่างสม่ำเสมอ

17. นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Secure Media Handling Policy)

นิยาม

สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Storage Media): หมายถึง สื่อที่ใช้สำหรับบันทึกข้อมูลที่สามารถเคลื่อนย้ายออกจากอุปกรณ์หลักได้โดยง่าย เช่น USB Flash Drive, External Hard Disk Drive (HDD/SSD), CD/DVD, Secure Digital (SD) Cards, และเทปสำรองข้อมูล (Backup Tapes)

ข้อมูลลับ/ข้อมูลสำคัญ (Confidential/Sensitive Data): ข้อมูลที่หากมีการเปิดเผย สูญหาย หรือถูกแก้ไขโดยไม่ได้รับอนุญาต จะส่งผลกระทบต่อชื่อเสียง ฐานะทางการเงิน หรือการดำเนินงานของบริษัท

วัตถุประสงค์

เพื่อกำหนดมาตรการและแนวทางปฏิบัติที่รัดกุมในการ บริหารจัดการและควบคุมสื่อบันทึกข้อมูล (Data Storage Media) ทุกประเภท เพื่อป้องกันการสูญหาย การเข้าถึงโดยไม่ได้รับอนุญาต การเปลี่ยนแปลงแก้ไข หรือการนำสารสนเทศไปใช้ในทางที่ไม่เหมาะสมและป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อบันทึกข้อมูลที่เป็นทรัพย์สินของบริษัท

การบริหารและจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

ข้อกำหนด	รายละเอียดการปฏิบัติงาน
การจัดเก็บในระหว่างการใช้งาน	ข้อมูลลับ/ข้อมูลสำคัญ สื่อบันทึก และอุปกรณ์ที่จัดเก็บข้อมูล ต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในห้องที่ไม่ได้ล็อกกุญแจ หากไม่อยู่ในพื้นที่ให้จัดเก็บในตู้/ลิ้นชักที่ล็อกได้
การควบคุมการเคลื่อนย้าย	- ห้ามบุคคลใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลสำคัญออกจากพื้นที่ทำงานโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากเจ้าหน้าที่ผู้มีอำนาจ - การนำสื่อบันทึกข้อมูลสำคัญออกนอกองค์กร (เช่น External Hard Disk สำหรับสำรองข้อมูล) ต้องมีการขออนุญาต และบันทึกรายการอย่างเป็นทางการ
ความมั่นคงปลอดภัยในการจัดเก็บ	- ผู้ใช้ต้องจัดเก็บสื่อบันทึกข้อมูลสำคัญไว้ใน สถานที่ที่มีความมั่นคงปลอดภัยทางกายภาพสูง - ปฏิบัติตามข้อกำหนดและคำแนะนำจากผู้ผลิตเกี่ยวกับการจัดเก็บสื่อบันทึกข้อมูล เช่น หลีกเลี่ยงสถานที่ที่มีอุณหภูมิสูง, ความชื้นสูง หรือมีสนามแม่เหล็กสูง
การขึ้นทะเบียนและการควบคุม	สื่อบันทึกข้อมูลสำคัญที่ใช้ในการสำรองข้อมูล หรือมีการใช้งานถาวร ต้องมีการขึ้นบัญชีรายชื่อ (Inventory) และควบคุมสถานะ เพื่อป้องกันการสูญหายและตรวจสอบได้

การทำลายหรือกำจัดสื่อบันทึกข้อมูล (Secure Disposal of Media)

การทำลายหรือกำจัดสื่อบันทึกข้อมูลต้องดำเนินการอย่างมั่นคงปลอดภัยเมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไป และต้องผ่านขั้นตอนปฏิบัติที่กำหนดไว้อย่างเป็นทางการ ดังนี้:

- **การอนุมัติ:** ต้องได้รับความเห็นชอบจากเจ้าของข้อมูลและผู้มีอำนาจอนุมัติ ก่อนดำเนินการทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล
- **การทำลายข้อมูลอิเล็กทรอนิกส์ (Data Sanitization):**
  > ก่อนการเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์ (ฮาร์ดดิสก์/คอมพิวเตอร์): ต้องทำการลบข้อมูลที่บันทึกอยู่ใน อุปกรณ์อย่างถาวร
  > สำหรับข้อมูลทั่วไป: ควรใช้วิธีการเขียนทับ (Overwriting) อย่างน้อย 1 ครั้ง
  > สำหรับข้อมูลลับ/ข้อมูลสำคัญของบริษัท: ต้องใช้วิธีการเขียนทับซ้ำ (Secure Multiple Overwriting) อย่างน้อย 3 ครั้งหรือมากกว่า เพื่อป้องกันการกู้คืนข้อมูล
  > สำหรับ SSD/Flash Storage ให้ใช้คำสั่ง Secure Erase ที่รองรับโดยผู้ผลิต
- **การทำลายทางกายภาพ (Physical Destruction):**
  > สื่อบันทึกข้อมูลที่ไม่สามารถลบข้อมูลได้อย่างมั่นคงปลอดภัย (เช่น CD/DVD/เทปสำรองข้อมูล) หรือฮาร์ดดิสก์ที่ใช้จัดเก็บข้อมูลลับ ควรถูก ทำลายทางกายภาพ (เช่น การบด, การเจาะ, การเผา)

- การจ้างบริษัทภายนอก:

> ควรมีการเก็บรวบรวมและกำจัดสื่อบันทึกข้อมูลโดย บริษัทรับทำลายสื่อบันทึกข้อมูลที่มีความเชี่ยวชาญ>ต้องพิจารณาเลือกบริษัทที่มีมาตรการสำหรับทำลายสื่อบันทึกข้อมูลแต่ละประเภทอย่างมั่นคงปลอดภัยและ น่าเชื่อถือ

> ต้องพิจารณาเลือกบริษัทที่มีมาตรการสำหรับทำลายสื่อบันทึกข้อมูลแต่ละประเภทอย่างมั่นคงปลอดภัยและน่าเชื่อถือ

> บริษัทต้องจัดให้มีบุคลากรผู้ทำหน้าที่ในการ สอดส่องและดูแล การกำจัดหรือการทำลายสื่อบันทึกข้อมูล (ทั้งทำลายเองและจ้างบริษัทภายนอก)

- **การบันทึกรายการ (Documentation):**

> ต้องมีการบันทึกข้อมูลการทำลายสื่อบันทึกข้อมูลสำคัญอย่างละเอียด เช่น วันที่และเวลา, ประเภทของสื่อบันทึกข้อมูล, ชื่อข้อมูลที่ถูกทำลาย, และชื่อผู้อนุมัติ

- สภาพแวดล้อมในการปฏิบัติงาน:

> ผู้ปฏิบัติงานต้องทำลายสื่อบันทึกข้อมูล, เอกสาร, และอุปกรณ์สำนักงาน ภายใต้ สิ่งแวดล้อมที่ได้มีการควบคุมและปลอดภัย เพื่อป้องกันการรั่วไหลในกระบวนการทำลาย

บทลงโทษกรณีฝ่าฝืน กฎ ระเบียบ ข้อบังคับ นโยบายสารสนเทศ

ผู้บังคับบัญชาจะเป็นผู้พิจารณาความผิด และลงโทษพนักงานที่ฝ่าฝืน กฎ ระเบียบ ข้อบังคับ นโยบายสารสนเทศ โดยพนักงานที่กระทำความผิดจะได้รับการพิจารณาลงโทษหนักเบาตามลักษณะของความผิดตามควรแก่กรณีเป็นราย ๆ ไป ซึ่งอาจเป็นโทษสถานใดสถานหนึ่ง หรือหลายสถาน ดังต่อไปนี้

1. ตักเตือนด้วยวาจา
2. ตักเตือนเป็นหนังสือ
3. พักงานโดยไม่จ่ายค่าจ้าง
4. ให้ออก ปลดออก ไล่ออก

คู่มือปฏิบัติงานแผนกสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคลากรที่เกี่ยวข้องตระหนักถึงความสำคัญของ การรักษาความปลอดภัยด้านสารสนเทศ (Information Security) และเพื่อให้เจ้าหน้าที่แผนกสารสนเทศมี ขั้นตอนการปฏิบัติงานที่เป็นมาตรฐาน สามารถประสานงานและดูแลระบบได้อย่างมีประสิทธิภาพ ทันสมัย และเป็นไปตามข้อกำหนดทางกฎหมาย

ขั้นตอนการใช้งานระบบอินเทอร์เน็ต (Secure Internet Usage Policy)

1. การควบคุมการเชื่อมต่อ:
   - เจ้าหน้าที่ไอทีต้องกำหนดเส้นทางการเชื่อมต่อการใช้งานอินเทอร์เน็ต ผ่านระบบรักษาความปลอดภัยที่บริษัทจัดไว้เท่านั้น (เช่น ผ่านระบบ Firewall, Secure Web Gateway, หรือ Proxy Server) เสมอ
2. การจัดการผู้ใช้งานภายนอก (Guest Access):
   - หากบุคคลภายนอกมีความจำเป็นต้องใช้งานอินเทอร์เน็ต จะต้องแจ้งพนักงานที่เกี่ยวข้องเพื่อขอรับรหัสผ่านสำหรับแขก (Guest Wi-Fi/Access)
   - เจ้าหน้าที่ไอทีต้องจัดเก็บข้อมูลการลงทะเบียนของผู้ใช้งานภายนอก (เช่น ชื่อ-นามสกุล, เบอร์โทรศัพท์, วันที่/เวลาใช้งาน) เพื่อประโยชน์ในการอ้างอิงและปฏิบัติตามกฎหมาย
3. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Retention):
   - เจ้าหน้าที่ไอทีต้องจัดให้มีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log file) อย่างถูกต้องและปลอดภัย ตามระยะเวลา และข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (พ.ร.บ. คอมพิวเตอร์) อย่างเคร่งครัด

ขั้นตอนการสำรองข้อมูลและการเตรียมพร้อมกรณีฉุกเฉิน (Business Continuity Plan – BCP)

1. การทดสอบการกู้คืนข้อมูล (Data Restoration Test):
   - เจ้าหน้าที่ฝ่ายไอทีต้องทำการทดสอบการเรียกข้อมูลสำรอง (Data Backup Restoration) อย่างน้อยปีละ 1 ครั้ง หรือตามความถี่ที่กำหนดในนโยบาย BCP
   - การทดสอบต้องดำเนินการร่วมกับหัวหน้าแผนกเจ้าของข้อมูล เพื่อยืนยันความสมบูรณ์และความถูกต้องของข้อมูลที่กู้คืน (Integrity)
   - จัดให้มีการทดสอบความต่อเนื่องของระบบงานหลัก (Application and System Restoration Test) โดยร่วมกับฝ่ายพัฒนาโปรแกรม
2. การบันทึกและการรายงาน:
   - เจ้าหน้าที่ไอทีต้องจัดทำ บันทึกการปฏิบัติงานและผลการทดสอบ รวมถึงปัญหาที่พบ และแนวทางการแก้ไข เพื่อใช้สำหรับการตรวจสอบ (Audit Trail) และการปรับปรุงประสิทธิภาพในครั้งต่อไป

มาตรฐานการติดตั้งระบบปฏิบัติการและโปรแกรม (System and Software Installation Standard)

1. ลิขสิทธิ์ซอฟต์แวร์ (Software Licensing):

- เครื่องคอมพิวเตอร์ทุกเครื่องที่ใช้ในองค์กรจะต้องมี ลิขสิทธิ์ของระบบปฏิบัติการและโปรแกรมสำเร็จรูปต่าง ๆ อย่างถูกต้องตามกฎหมาย เสมอ

2. การตั้งค่าความปลอดภัยเบื้องต้น:

- โปรแกรมพักหน้าจอ (Screen Lock/Screen Saver): กำหนดการตั้งค่าให้โปรแกรมพักหน้าจอทำงานหากไม่มีผู้ใช้งานไม่เกิน 15-30 นาที (Idle Time) และตั้งค่าให้ระบบ ถามรหัสผ่านทุกครั้ง ก่อนการเริ่มใช้งานอีกครั้ง (Resume with password)

3. การกำหนดชื่อผู้ใช้และสิทธิ์ (User and Privilege Management):

- บัญชีผู้ใช้งานทั่วไป (Standard User Account): สร้างชื่อผู้ใช้สำหรับพนักงานเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์ตามปกติ โดยมีสิทธิ์จำกัด
- บัญชีผู้ดูแลระบบ (System Admin Account): สร้างชื่อผู้ใช้แบบ System Admin เพื่อใช้เข้าระบบในกรณีฉุกเฉินหรือการบำรุงรักษาเท่านั้น และต้องควบคุมการเข้าถึงรหัสผ่านอย่างเข้มงวด
- รหัสผ่าน: กำหนดรหัสผ่านให้ยากแก่การคาดเดาและเป็นไปตามหลักเกณฑ์ที่ระบุไว้ใน "นโยบายการกำหนดรหัสผ่าน" ของบริษัท

4. การรายงานปัญหา:

- หากพบปัญหาที่ไม่สามารถดำเนินการติดตั้งหรือแก้ไขได้ตามมาตรฐาน ให้แจ้งหัวหน้าแผนกหรือหัวหน้าฝ่ายที่เกี่ยวข้องเพื่อหาแนวทางแก้ไขทันที

ขั้นตอนการตรวจสอบและควบคุมความสอดคล้อง (IT Compliance & Auditing)

การตรวจสอบ:

- เจ้าหน้าที่ไอทีทำการสุ่มตรวจเครื่องคอมพิวเตอร์ของผู้ใช้ (Surprise Check) สำหรับพนักงานที่ปฏิบัติงานในสำนักงาน
- สำหรับพนักงานที่ไม่ได้ปฏิบัติงานในสำนักงานเป็นประจำ ให้กำหนดวัน-เวลาที่แน่นอนของการตรวจสอบล่วงหน้าเพื่อความสะดวกในการประสานงาน

รายการที่ต้องตรวจสอบ:

- การตั้งรหัสผ่านตามนโยบายสารสนเทศ (ความยาว, ความซับซ้อน, ความถี่ในการเปลี่ยน)
- การติดตั้งโปรแกรมที่ ละเมิดลิขสิทธิ์ หรือโปรแกรมที่ไม่ได้รับอนุญาต
- การตั้งค่าพักหน้าจอ (Screen Lock) และการตั้งให้ถามรหัสผ่านตามที่กำหนด
- สิทธิ์การใช้งานระบบสารสนเทศต่าง ๆ ในองค์กร (สิทธิ์ต้องสอดคล้องกับหน้าที่ความรับผิดชอบ)
- ทรัพย์สินและอุปกรณ์ไอทีที่อยู่ในความครอบครอง (ตรวจสอบความสอดคล้องตามทะเบียนทรัพย์สิน)

การบันทึกผล:

- เจ้าหน้าที่ไอทีต้องพิมพ์ ผลการตรวจสอบ และให้พนักงานที่ถูกตรวจสอบ ลงนามรับรองผล เพื่อยืนยันการรับทราบ และนำผลดังกล่าวไปปรับปรุงแก้ไข

ขั้นตอนการขอใช้งานอีเมลและระบบงานใหม่ (Email and New System Access Request)

การขออนุมัติ:

- พนักงานที่ต้องการใช้งานอีเมล หรือขอเข้าใช้งานระบบสารสนเทศใหม่ ต้องกรอกแบบฟอร์มขอเปิด/เข้าใช้งาน ที่กำหนด
- พนักงานส่งแบบฟอร์มให้เจ้าหน้าที่ไอทีเพื่อดำเนินการ

การสร้างบัญชี:

- เจ้าหน้าที่ไอทีประสานงานเพื่อขออนุมัติจาก หัวหน้าแผนก/ผู้มีอำนาจ ให้ลงนามอนุมัติ
- เจ้าหน้าที่ไอทีดำเนินการสร้างอีเมล/บัญชีผู้ใช้ ตามรายละเอียดที่ได้รับอนุมัติ

การแจ้งรายละเอียด:

- เจ้าหน้าที่ไอทีแจ้งรายละเอียดการเข้าใช้งานและรหัสผ่านเริ่มต้นให้พนักงานผู้ขออนุมัติทราบ พร้อมเน้นย้ำให้ เปลี่ยนรหัสผ่านทันที ในการเข้าใช้งานครั้งแรก

เอกสารอ้างอิง:

- แบบฟอร์มขอเปิดใช้งานอีเมล/แบบฟอร์มขอสิทธิ์เข้าถึงระบบ (Access Request Form)

ขั้นตอนการดำเนินการ กรณีพนักงานลาออก (Off-boarding Procedures)

เมื่อเจ้าหน้าที่ไอทีได้รับข้อมูลจากแผนกบุคคลถึงกำหนดการลาออกของพนักงาน ให้ดำเนินการดังนี้ โดยเร็วที่สุด:

การเรียกคืนทรัพย์สิน:

- เรียกคืนและตรวจสอบทรัพย์สินไอทีทั้งหมดที่พนักงานถือครอง (เช่น โน้ตบุ๊ก, โทรศัพท์มือถือบริษัท, คีย์การ์ด) โดยอาศัยข้อมูลจากทะเบียนทรัพย์สินของแผนกบุคคล

การจัดการบัญชีอีเมล:

- ระงับการใช้งาน (De-activate) บัญชีอีเมลทันที ในวันที่พนักงานพ้นสภาพ
- ให้เก็บรักษา (Retention) Mailbox/ข้อมูลอีเมลดังกล่าวไว้เป็นระยะเวลาที่กำหนด (เช่น 1-3 เดือน) เพื่อให้ผู้ที่ได้รับมอบหมายสามารถเข้าถึงและตรวจสอบข้อมูลในกรณีจำเป็น

การยกเลิกสิทธิ์การเข้าถึง (Access Revocation):

- ตรวจสอบ สิทธิ์การเข้าถึงข้อมูลในระบบสารสนเทศทั้งหมด (เช่น โปรแกรมบัญชี, ระบบ ERP, Shared Drives, ระบบคลาวด์)
- ดำเนินการ ยกเลิก/ลบ/เพิกถอนสิทธิ์ ต่าง ๆ ทั้งหมด และ/หรือประสานงานผู้เกี่ยวข้องเพื่อยกเลิกสิทธิ์การเข้าถึงระบบสนเทศ โดยมีผลในวันที่พนักงานพ้นสภาพ

แบบฟอร์มขอเปิดใช้งานอีเมล

แบบฟอร์มขอเปิดใช้งานอีเมล

วันที่ _____

ขออนุมัติเปิดใช้งานอีเมลสำหรับ

ชื่อ-นามสกุล ภาษาไทย : _____

First-Last Name : _____

ตำแหน่ง : _____ แผนก : _____

ชื่ออีเมล : _____ @comancheinternational.com (ต้องลงท้ายด้วยโดเมนของบริษัทเท่านั้น)

เริ่มใช้งาน : _____

.....	.....	.....
(.....)	(.....)	(.....)
ผู้ขออนุมัติ	**หัวหน้าฝ่าย/แผนก (รับทราบ)**	**ผู้อนุมัติ**
วันที่.....	วันที่.....	วันที่.....

ใบแจ้งซ่อมสินทรัพย์

ใบแจ้งซ่อมสินทรัพย์

เลขที่เอกสาร _____

วันที่ _____

แจ้งซ่อมทรัพย์สิน จากแผนก _____ ผู้ดูแล _____

ลำดับที่	รหัสสินทรัพย์	ชื่อสินทรัพย์/ยี่ห้อ/รุ่น/สี	หมายเหตุ

อาการที่เสีย

_____

_____

_____

.....	.....	.....
(.....)	(.....)	(.....)
ผู้ขออนุมัติ	หัวหน้าฝ่าย/แผนก (รับทราบ)	ผู้อนุมัติ
วันที่.....	วันที่.....	วันที่.....