MC GROUP

บริษัท แม็คกรุ๊ป จำกัด (มหาชน)

Mc group public company limited.

นโยบาย
ความมั่นคงปลอดภัยข้อมูลสารสนเทศ
(Information Security Policy)

คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(ISMS Committee: ISMS-C)

MC GROUP

ประกาศ

บริษัท แม็คกรุ๊ป จำกัด (มหาชน) (“บริษัท”) ได้จัดทำ “นโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security Policy)” เป็นลายลักษณ์อักษรขึ้น เพื่อเป็นแนวทางการปฏิบัติที่ชัดเจนตามข้อกำหนด กฎเกณฑ์ ข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศ การปกป้องความเป็นส่วนตัวของข้อมูลที่บริษัทครอบครอง และรักษาแนวทางปฏิบัติที่ดีเพื่อลดความเสี่ยงขององค์กร รวมถึงเพื่อป้องกันและลดการกระทำความผิดที่อาจเกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ โดยไม่คาดคิด

บริษัทจึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนสารสนเทศนี้ เพื่อให้กรรมการ ผู้บริหาร และพนักงาน ของบริษัท แม็คกรุ๊ป จำกัด (มหาชน) และบริษัทย่อยทุกท่านปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด

(นางไขศรี เนื่องสิกขาเพียร)

ประธานกรรมการบริษัท

บริษัท แม็คกรุ๊ป จำกัด (มหาชน)

สารบัญ

1. นโยบายการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security Policy)

1.1. บททั่วไป

- นโยบายเทคโนโลยีสารสนเทศนี้ได้กำหนดมุมมองในระดับสูงถึงวิธีที่แม็คกรุ๊ปเพื่อสร้างความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ นโยบายนี้จะช่วยให้แม็คกรุ๊ปสามารถทำงานได้ตามมาตรฐานอุตสาหกรรมที่เหมาะสมและตามแนวทางปฏิบัติที่ดีที่สุด
- นโยบายนี้เป็นของฝ่ายเทคโนโลยีสารสนเทศและได้รับการรับรองในระดับผู้จัดการ
- คำแถลงการณ์ในนโยบายนี้ได้แบ่งระหว่างมาตรฐานขั้นต่ำซึ่งถูกคาดหวังให้อยู่ในข้อความที่ถูกระบุว่า 'จะต้อง' และแนะนำแนวทางปฏิบัติที่ดีที่สุดที่ถูกระบุว่า 'ควร'
- ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์ต่อเชื่อมของบริษัทฯ จัดหาเพื่อให้บริการที่เกี่ยวข้องกับกิจการของบริษัทฯ เท่านั้น ไม่อนุญาตให้ใช้ในกิจการที่ไม่เกี่ยวข้องกับกิจการของบริษัทฯ
- การเข้าใช้งานระบบคอมพิวเตอร์และการต่อเชื่อมทางอินเทอร์เน็ตของบริษัทฯ จะต้องปฏิบัติตามนโยบายฯ ฉบับนี้ โดยจะมีการลงทะเบียนก่อนการเข้าใช้งาน
- อนุญาตให้ใช้สื่อบันทึกประเภท Flash Drive/Removable Media/External Hard Disk ในกรณีที่มีการร้องขอจากผู้ใช้บริการ โดยจะต้องแจ้งให้หัวหน้างาน หรือผู้ที่ได้รับมอบหมายรับทราบ อย่างเป็นลายลักษณ์อักษรก่อนการใช้งาน และจะต้องมีการ Format ก่อนการใช้งานทุกครั้ง โดยในการนำส่งให้ลูกค้าจะจัดส่งในรูปแบบระดับชั้นความลับ (Confidential)
- ในการขออนุญาตเข้าใช้งาน ให้หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานของผู้ที่จะขอใช้บริการเป็นผู้ขอ โดยปฏิบัติตามนโยบายฯ ฉบับนี้
- ผู้เข้าใช้งานจะต้องทำความเข้าใจและลงนามเพื่อยืนยันตาม **นโยบายการอนุญาตให้ใช้ทรัพย์สินขององค์กร (Acceptable Use Policy)** ว่าจะปฏิบัติตามนโยบายที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
- นโยบายฯ ฉบับนี้ ถือเป็นส่วนหนึ่งของข้อกำหนดในการปฏิบัติงานของผู้ใช้ทุกคน และจะถือเป็นการผิดวินัยการทำงานเช่นเดียวกันหากไม่ปฏิบัติตาม
- บริษัทฯ ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อทางอินเทอร์เน็ต ให้ปฏิบัติตาม พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และกฎหมายประกอบอื่น ๆ ที่เกี่ยวข้อง

อ้างอิงตาม **เอกสารข้อมูลข้อกำหนดด้านกฎหมายและระเบียบข้อบังคับที่องค์กรประยุกต์ใช้** บริษัทฯ ไม่สนับสนุน หรือยินยอมให้ผู้ใช้งานของบริษัทฯ กระทำผิดต่อพระราชบัญญัติและกฎหมายประกอบอื่น ๆ

- หากพบว่าผู้ใช้มีการละเมิดนโยบายฯ ฉบับนี้ จะถูกลงโทษตามกฎระเบียบฯ ของบริษัทฯ รวมไปถึงการส่งตัวเพื่อดำเนินคดีตามกฎหมายหากการละเมิดนั้นผิดต่อกฎหมายของประเทศ
- กำหนดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และรวมถึงเอกสารการปฏิบัติงาน (Operation Procedure) และปรับปรุงให้ทันสมัยอยู่เสมอ **อย่างน้อยปีละ 1 ครั้ง** (ในกรณีปรับปรุงเอกสารนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ ต้องดำเนินการทบทวนและปรับปรุงเอกสาร Information Security Policy ฉบับ Public ให้เป็นปัจจุบัน)

1.1.1 ขอบเขต

นโยบายนี้มีผลบังคับใช้กับพนักงานของแม็คกรุ๊ปและระบบที่เฉพาะเจาะจงกับแม็คกรุ๊ปทั้งหมด เป็นการสำคัญอย่างยิ่งที่พนักงานของแม็คกรุ๊ปทุกคนจะเข้าใจถึงภาระหน้าที่ของตนในนโยบายนี้ และปฏิบัติตามข้อกำหนดที่เกี่ยวข้องทั้งหมดเพื่อปกป้องความเป็นส่วนตัวของข้อมูลที่แม็คกรุ๊ปครอบครอง และรักษาแนวทางปฏิบัติที่ดีเพื่อลดความเสี่ยงขององค์กร

1.2. นโยบายหน้าที่และความรับผิดชอบของผู้ใช้งาน (User Responsibility)

ผู้ใช้งานมีหน้าที่เกี่ยวข้องกับการบริหารจัดการการใช้งานระบบคอมพิวเตอร์ ดังนี้

- การจัดการรหัสผ่าน (Password) ให้สอดคล้องตาม **นโยบายการจัดการและการใช้งานรหัสผ่าน (Password Management)**
- การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended Use Equipment) ดังนี้
    - กำหนดให้มีมาตรการควบคุมดูแลและป้องกันอุปกรณ์ทางกายภาพและทางลอจิคัล เมื่อไม่มีพนักงานดูแล
    - กำหนดให้มีมาตรการควบคุมการเข้าถึงอุปกรณ์หรือระบบคอมพิวเตอร์ โดยการตั้งค่า Automatic Log Off หรือ Screen Saver เพื่อให้ระบบคอมพิวเตอร์ทำการล็อคหน้าจอโดยอัตโนมัติ โดยตั้งค่าล็อคหน้าจอน้อยกว่าหรือไม่เกิน 15 นาที ยกเว้น ระบบคอมพิวเตอร์ที่มีการเฝ้าระวังอยู่ตลอดเวลา
    - หน้าที่และความรับผิดชอบของผู้ใช้งานในการป้องกันการเข้าถึงในทุกระดับโดยไม่ได้รับอนุญาต
    - ห้ามให้บุคคลภายนอกใช้งานเครื่องคอมพิวเตอร์ของบริษัทฯ โดยไม่ได้รับอนุญาต

- ต้องไม่ใช้เครื่องคอมพิวเตอร์ในทางที่ก่อหรือจะก่อให้เกิดความเสียหายต่อผู้อื่น ต่อบริษัทฯ ผิดกฎหมาย หรือศีลธรรมอันดี เช่น
  - การเข้าถึงข้อมูล เครือข่าย หรือระบบงานโดยมิชอบ หรือโดยไม่ได้รับอนุญาต
  - การรบกวน หรือก่อความรำคาญต่อเครือข่าย หรือระบบงาน
  - การดักรับ หรือดักจับข้อมูลของผู้อื่น
  - การลักลอบถอดรหัสผ่าน
  - การปลอมแปลง หรือเปลี่ยนแปลงข้อมูลโดยมิชอบหรือโดยไม่ได้รับอนุญาต
  - การเผยแพร่รูปภาพ ข้อความ หรือเสียงที่ไม่เหมาะสม
  - การกระทำสิ่งใดที่ผิดกฎหมาย หรือส่อเจตนาไปในทางที่ผิดจากพฤติกรรมการใช้งานปกติ

1.3. นโยบายการบริหารจัดการโครงการ (Project Management)

- ในการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ระบุความเสี่ยงและมาตรการควบคุมที่จำเป็นด้านความมั่นคงปลอดภัยสารสนเทศ รวมทั้งมีการบริหารจัดการความเสี่ยงที่เกิดขึ้นตลอดระยะเวลาโครงการ
  หมายเหตุ: โครงการ/บริการ หมายความถึง ระบบงาน/งานเครือข่าย ซึ่งจะเป็นเครื่องมือที่จะช่วยให้หน่วยงานสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ หรือบริการที่ต้องการพัฒนาขึ้นใหม่เรียบร้อยแล้ว

1.4. นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook Device Policy)

- อุปกรณ์คอมพิวเตอร์แบบพกพาต้องได้รับการติดตั้ง Application จาก Application Store ที่น่าเชื่อถือ
- ห้ามนำเข้า หรือเผยแพร่ข้อมูลสำคัญของบริษัทฯ ที่อาจจะส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ เช่น ข้อมูลรหัสผ่าน เป็นต้น
- ติดตั้ง Application และ Plugins ต้องได้รับการควบคุม ดังต่อไปนี้
  - ห้ามติดตั้ง Application และ Plugins ใด ๆ ที่สุ่มเสี่ยงกับการกระทำผิดกฎหมาย และผิดลิขสิทธิ์
  - ห้ามติดตั้ง Application และ Plugins ใด ๆ ที่โปรแกรมป้องกันไวรัสในอุปกรณ์คอมพิวเตอร์แบบพกพาตรวจจับว่ามีความเสี่ยงด้านความมั่นคงปลอดภัย
- ห้าม Jailbreak หรือ Root อุปกรณ์คอมพิวเตอร์แบบพกพา
- ไม่อนุญาตให้พนักงานในคณะทำงาน ISMS ใช้งาน USB Drive storage ต่างๆ ที่เป็นของส่วนตัวหรือไม่ได้ลงทะเบียนขออนุญาตจากฝ่ายบริหาร การได้รับอนุญาตจำเป็นต้องบันทึกไว้ในระบบ Kace และมีการอนุมัติจากหัวหน้างาน และฝ่ายบริหารอย่างเป็นลายลักษณ์อักษร

- กำหนดให้ตั้งค่า Lock Screen ของเครื่องโทรศัพท์ ด้วย PIN ที่เป็นรหัสที่เดาสุ่มได้ยาก ความยาวอย่างน้อย 8 ตัวเลข หรือใช้วิธีการยืนยันตัวตนก่อนใช้งานเครื่องที่ดีกว่า เช่น Password หรือ Fingerprint เป็นต้น
- อุปกรณ์ที่ไม่มีพนักงานดูแล กำหนดให้มีมาตรการควบคุมดูแลและป้องกันอุปกรณ์โดยการตั้งค่า Automatic Log Off หรือ Screen Saver เพื่อให้ระบบคอมพิวเตอร์ทำการล็อคหน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้มีการใช้งานเกินกว่า 15 นาที ยกเว้นระบบคอมพิวเตอร์ที่มีการเฝ้าระวังอยู่ตลอดเวลา
- อุปกรณ์คอมพิวเตอร์แบบพกพาที่บริษัทฯ จัดให้ต้องเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตไร้สายเพื่อเชื่อมต่อเข้าสู่เครือข่ายสาธารณะที่บริษัทกำหนดให้เท่านั้น
- พนักงานต้องปฏิบัติตาม **นโยบายการควบคุมการเข้าถึง (Access Control)** อย่างเคร่งครัด
- พนักงานต้องปฏิบัติตาม **ระเบียบปฏิบัติงานการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)** อย่างเคร่งครัด
- กำหนดให้ดำเนินการตรวจสอบและเฝ้าระวังการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาของผู้ใช้
- ต้องจัดให้มีการอบรมสร้างความตระหนักเกี่ยวกับเรื่องการใช้งานอุปกรณ์คอมพิวเตอร์พกพา (Mobile Device Security) สำหรับผู้ใช้งาน

1.5. นโยบายการให้นำอุปกรณ์ส่วนตัวมาใช้ทำงาน (Bring Your Own Device (BYOD))

- สำหรับพนักงานที่ได้รับอนุมัติต้องจัดเก็บอุปกรณ์ส่วนตัวที่นำมาใช้ทำงานในที่ปลอดภัยไม่วางทิ้งไว้ในที่เสี่ยงต่อการสูญหาย
- อุปกรณ์ส่วนตัวที่นำมาใช้ทำงานต้องเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตไร้สายเพื่อเชื่อมต่อเข้าสู่เครือข่ายสาธารณะที่บริษัทฯ กำหนดให้เท่านั้น
- อุปกรณ์ส่วนตัวที่นำมาใช้ทำงานอ้างอิงการติดตั้ง OS, Software, Application และ Plugins ต้องไม่สุ่มเสี่ยงกับการกระทำผิดกฎหมายและผิดลิขสิทธิ์จากแหล่งที่น่าเชื่อถือได้เท่านั้น
- อุปกรณ์ส่วนตัวที่นำมาใช้ทำงานต้องติดตั้งโปรแกรมป้องกันไวรัสพร้อมทั้งดำเนินการสแกน และอัปเดตให้เป็นปัจจุบันอยู่เสมอ
- ห้ามติดตั้ง Software, Application และ Plugins ที่หลีกเลี่ยงการตรวจสอบจากโปรแกรมกันป้องกันไวรัส
- เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต อุปกรณ์ต้องได้รับการป้องกันด้วยรหัสผ่านโดยใช้คุณสมบัติของอุปกรณ์

- และต้องมีรหัสผ่านตามแนวทางการตั้งรหัสผ่านที่ปลอดภัยเช่น Finger Scan, Retina Scan, Bio Metric Scan เป็นต้น เพื่อเข้าถึงเครือข่ายของบริษัทฯ
- ห้ามนำเข้าหรือเผยแพร่ข้อมูลสำคัญของบริษัทฯ ที่อาจจะส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ เช่น ข้อมูลรหัสผ่าน หรือ ค่าข้อมูลของระบบ (Configuration) เป็นต้น
- พนักงานต้องปฏิบัติตาม **นโยบายการควบคุมการเข้าถึง (Access Control)** อย่างเคร่งครัด
- พนักงานต้องปฏิบัติตาม **ระเบียบปฏิบัติงานการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)** อย่างเคร่งครัด
- เมื่อเลิกใช้ หรือส่งซ่อมอุปกรณ์ส่วนตัวที่นำมาใช้ทำงาน พนักงานหรือหน่วยงานผู้รับผิดชอบต้องถอดถอนสิทธิ์และทำลายข้อมูลใน Drive ที่ดำเนินการจัดเก็บข้อมูลของบริษัทฯ ในอุปกรณ์ส่วนตัว
- พนักงานต้องยินยอมให้บริษัทฯ ดำเนินการตรวจสอบและเฝ้าระวังการใช้งานอุปกรณ์ส่วนตัวที่นำมาใช้ทำงานที่เกี่ยวข้องกับบริษัทฯ
- จัดให้มีการอบรมสร้างความตระหนักเกี่ยวกับเรื่องการใช้งานอุปกรณ์ส่วนตัว (BYOD) ที่นำมาใช้ให้มีความมั่นคงปลอดภัยในการทำงาน สำหรับพนักงาน
- ห้าม Jailbreak หรือ Root อุปกรณ์
- กำหนดหรือแนะนำให้ตั้งค่า Lock Screen สำหรับโทรศัพท์ ด้วย PIN ที่เป็นรหัสที่เดาสุ่มได้ยาก ความยาวอย่างน้อย 4 ตัวเลข หรือใช้วิธีการยืนยันตัวตนก่อนใช้งานเครื่องที่ดีกว่า เช่น Password หรือ Fingerprint เป็นต้น กำหนดให้ตั้งค่า Automatically Lock Screen Timeout สำหรับโทรศัพท์ เป็น 1 นาที
- กำหนดหรือแนะนำให้มีการใช้งาน Session Timeout/Idle Timeout สำหรับระบบปฏิบัติการ และ/หรืออุปกรณ์เครือข่าย โดยตั้งค่าไม่เกิน 15 นาที หรือตามความเหมาะสมของข้อมูลที่อยู่ภายในระบบและอุปกรณ์ **ยกเว้น** ระบบคอมพิวเตอร์ที่มีการเฝ้าระวังอยู่ตลอดเวลา

1.6. นโยบายสำหรับการใช้งานเครือข่ายไร้สาย (Wireless Access Policy)

- ผู้ดูแลระบบเครือข่ายไร้สายต้องจัดแบ่งเครือข่ายไร้สายตามรูปแบบการใช้งานเครือข่ายตามความต้องการของบริษัทฯ
- สำหรับการให้บริการเครือข่ายไร้สายเพื่อเชื่อมต่อเข้าสู่บริการภายในของบริษัทฯ ผู้ดูแลระบบเครือข่ายไร้สายต้องจัดเตรียมระบบการยืนยันตัวตนผู้ใช้งานก่อนเข้าใช้งานระบบเครือข่ายไร้สาย และต้องปรับปรุงระบบให้มีการเข้ารหัสการเชื่อมต่อในรูปแบบ WPA2-PSK เป็นอย่างน้อย

- สำหรับการให้บริการเครือข่ายไร้สายเพื่อเชื่อมต่อเข้าสู่เครือข่ายสาธารณะ ผู้ดูแลระบบเครือข่ายไร้สายต้องจัดเตรียมระบบการยืนยันตัวตนผู้ใช้งานก่อนเข้าใช้งานระบบเครือข่ายไร้สาย
- กำหนดให้มีการแบ่งแยก และควบคุมเครือข่ายไร้สายกับเครือข่าย LAN ด้วยอุปกรณ์ Firewall เพื่อควบคุมการเข้าถึงที่เหมาะสม
- ห้ามพนักงานนำ Access Point ส่วนตัวมาเชื่อมต่อเครือข่าย LAN เพื่อกระจายสัญญาณ
- ห้ามพนักงานปลอม SSID (Rouge SSID) ซ้ำกับ SSID ที่บริษัทฯ กำหนด
- ต้องใช้การเชื่อมต่อที่มีการเข้ารหัสสำหรับการใช้บริการที่มีการรับส่งข้อมูลระดับชั้นลับ เช่น HTTPS หรือ SSH เป็นต้น
- ในการเข้าถึงเครือข่ายจากภายนอก จะต้องเข้าผ่านระบบ VPN เท่านั้น

1.7. นโยบายการใช้งานจากเครือข่ายภายนอก (Teleworking Policy)

- กำหนดให้มีการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้บริการได้และบริการใดที่ไม่อนุญาตให้ผู้ใช้งานสามารถใช้บริการได้
- จัดให้มีการขออนุญาตเข้าใช้งานบริการเครือข่ายก่อนเข้าใช้งาน เพื่อที่จะกำหนดว่าบุคคลใดสามารถเข้าถึงระบบหรือเครือข่ายใด ให้สอดคล้องตาม **ระเบียบปฏิบัติงานการบริหารจัดการการเชื่อมต่อเครือข่ายและงานบริการเครือข่าย (Network Security Control)**
- กำหนดมาตรการควบคุม ช่องทางและเงื่อนไขในการเชื่อมต่อเพื่อเข้าใช้งานที่มีความมั่นคงปลอดภัย ก่อนเปิดให้บริการใช้งานระบบจากระยะไกลทั้งแบบ Mobile Computing และ Teleworking โดยพิจารณาถึงภัยคุกคามช่องโหว่ และความเสี่ยง
- จัดให้มีมาตรการควบคุมและพิสูจน์ตัวตนก่อนที่อนุญาตให้ผู้ใช้งานที่อยู่ภายนอกบริษัทฯ เข้าใช้งานเครือข่ายและระบบสารสนเทศของบริษัทฯ ได้จากอุปกรณ์หรือสถานที่ที่ได้อนุญาตแล้ว
- กำหนดให้มีการเข้าผ่านระบบ VPN ก่อนการเข้าถึงระบบปฏิบัติงานทุกครั้ง
- ในการปฏิบัติงาน ผู้ใช้หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์ของผู้อื่นในการเข้าสู่บริการทั้งแบบ Mobile Computing และ Teleworking
- ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการใช้งานให้เป็นไปตาม **นโยบายการควบคุมการเข้าถึง (Access Control)**

- เครื่องคอมพิวเตอร์ที่มีการเชื่อมต่อเข้าถึงจากระยะไกลต้องมีมาตรการป้องกันโปรแกรมไม่ประสงค์ดีตาม **นโยบายการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls of Malicious Code and Mobile Code)**
- หากพบเหตุการณ์การละเมิดนโยบายทางด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศของบริษัทฯ ผู้ใช้งานดำเนินการแจ้งเหตุตาม **ระเบียบปฏิบัติงานการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident Management)** และดำเนินการแก้ไขป้องกันที่เหมาะสม

1.8. นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)

- กำหนดให้มีการจัดทำ **ระเบียบปฏิบัติงานการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**
- กำหนดให้มีการจัดระดับชั้นความลับของข้อมูล (Information Classification) หมายรวมถึงการสร้างความมั่นคงปลอดภัยให้แก่ข้อมูลซึ่งอยู่ในเอกสารระบบ (Security of System Documentation) เพื่อกำหนดมาตรการควบคุมที่เหมาะสม
- โดยระบุพนักงานที่มีหน้าที่ดูแลรับผิดชอบ ผู้มีสิทธิ์หรืออำนาจในการอนุมัติ
- กำหนดให้มีการจัดทำป้าย (Labeling) หรือระบุสารสนเทศแต่ละระดับอย่างชัดเจน โดยติดป้ายหรือระบุคำอธิบายที่มีความสัมพันธ์กับระดับชั้นความลับของข้อมูลสารสนเทศ
- การเก็บรักษา (Storage) จัดเก็บสารสนเทศไว้ในสถานที่ หรือบันทึกข้อมูลลงในเครื่องคอมพิวเตอร์ที่ปลอดภัย ป้องกันภัยคุกคามต่อข้อมูลตามระดับชั้นความลับของข้อมูลสารสนเทศ รวมถึงบริหารจัดการหรือการกำหนดการเข้าถึงสารสนเทศอย่างเหมาะสมตาม **ระเบียบปฏิบัติงานการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**
- กำหนดแนวทางการจัดการสารสนเทศ (Handling) โดยคำนึงถึงความปลอดภัย และป้องกันภัยคุกคามที่ส่งผลกระทบต่อการเข้าถึง หรือความเสียหายของสารสนเทศ
- การทำลายสารสนเทศ (Disposal) กำหนดผู้อนุมัติให้ทำลายสารสนเทศ และวิธีการทำลายสารสนเทศตามระดับชั้นความลับของข้อมูลตาม **ระเบียบปฏิบัติงานการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**

- ไม่อนุญาตให้ดำเนินการสำเนาข้อมูลของลูกค้าบนระบบทดสอบ (POC) มายังระบบใช้งานจริง (Production) หรือ จากระบบใช้งานจริงมายังบนระบบทดสอบ (POC) **ยกเว้น** กรณีที่เจ้าของข้อมูลร้องขอและมีการยืนยันอย่างเป็นลายลักษณ์อักษร

1.9 นโยบายการควบคุมการเข้าถึง (Access Control)

- ต้องมีกระบวนการลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and Deregistration) อย่างเป็นทางการและปฏิบัติตามเพื่อเป็นการให้สิทธิ์การเข้าถึง
- กำหนดให้มีการแยกหน้าที่และความรับผิดชอบ (Segregation of Duties) ของผู้เกี่ยวข้องในระบบงานต่าง ๆ เพื่อป้องกันไม่ให้ผู้ใดสามารถเข้าถึงระบบงานทั้งหมด และสามารถเปลี่ยนแปลงแก้ไข หรือดำเนินการใด ๆ โดยต้องได้รับอนุญาตจากหน่วยงาน/บุคคล หรือสามารถตรวจสอบได้จากระบบ
- ให้มีการจัดทำ **ระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน (User Access Management)** อย่างเป็นลายลักษณ์อักษร และปรับปรุงเนื้อหาตามรอบระยะเวลาที่กำหนดไว้
- กำหนดการเข้าถึงระบบสารสนเทศหลักและสนับสนุนประมวลผลด้านกระบวนการทางธุรกิจ ทั้งทางลอจิคัล (Logical Access) ให้สอดคล้องตาม **ระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน (User Access Management)** และกำหนดการเข้าถึงทางกายภาพ (Physical Access) ได้แก่ พื้นที่ปฏิบัติงานของบริษัทฯ ให้สอดคล้องตาม **นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security)** เพื่อควบคุมการเข้าถึงหรือวิธีการเข้าถึงสารสนเทศอย่างมั่นคงปลอดภัย ตามสิทธิ์ของผู้ใช้งาน หรือ กลุ่มผู้ใช้งานอย่างชัดเจน
- ให้ใช้เครื่องคอมพิวเตอร์ หรือ Mobile Device หรือ อุปกรณ์ส่วนตัวมาใช้ทำงาน (Bring Your Own Device (BYOD) หรืออุปกรณ์ประกอบอื่นที่เชื่อมต่อเข้ากับระบบปฏิบัติการ ระบบงาน ระบบเครือข่ายของบริษัทฯ โดยต้องปฏิบัติตาม **นโยบายการใช้งานจากเครือข่ายภายนอก (Teleworking Policy)** และ **นโยบายการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls of Malicious Code and Mobile Code)**
- การเข้าใช้งานระบบงานต่าง ๆ จะต้องได้รับอนุญาตจากเจ้าของระบบ โดยให้หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน เป็นผู้ขอสิทธิ์ในการใช้ เพื่อให้มีการระบุและพิสูจน์ตัวตนของผู้ใช้งานตาม **นโยบายการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User Identification and Authentication)**
- ควรกำหนดคุณสมบัติหรือวิธีการล็อกอินเข้าใช้ระบบให้มีความปลอดภัย (Secure Log On) เมื่อมีระบบใหม่ที่ได้รับการอนุมัติให้จัดหาและติดตั้ง พิจารณากำหนดคุณสมบัติ เช่น

- การบันทึกข้อมูลความสำเร็จหรือการล้มเหลวในการล็อกอินแต่ละครั้งของผู้ใช้งาน (เพื่อใช้ในการตรวจสอบในภายหลัง)
- การไม่แสดงข้อมูลรหัสผ่านให้เห็นบนจอในขณะที่ผู้ใช้งานใส่ข้อมูลรหัสผ่านของตน
- การแสดงผลข้อผิดพลาดเท่าที่จำเป็น รายละเอียดข้อมูลอื่น ๆ ของระบบต้องไม่แสดงออกมา
- การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services) ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น
- ผู้ใช้งาน ที่จะเข้าถึงระบบที่สำคัญผ่าน Application หรือ Software ในการบริหารจัดการต่าง ๆ หรือเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ จากทั้งเครือข่ายสาธารณะ (Public Network) หรือเครือข่ายส่วนตัว (Private Network) ต้องปฏิบัติตาม **ระเบียบปฏิบัติงานการควบคุมการเข้าถึง (Access Control)**
- ต้องมีการทบทวน **นโยบายการควบคุมการเข้าถึง (Access Control)** ตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ **อย่างน้อยปีละ 1 ครั้ง**
- ห้ามพนักงานเข้าถึงระบบงานหรือข้อมูลของลูกค้าภายหลังจากการส่งมอบบริการให้กับลูกค้าเสร็จสิ้น ยกเว้นกรณีระบุในสัญญาการให้บริการ หรือมีการร้องขอความช่วยเหลือตามกระบวนการการร้องขอตาม **ระเบียบปฏิบัติงานการบริหารจัดการปัญหาการใช้งานและการร้องขอ (Incident and Service Request Management)**

10.1.1 สิทธิพิเศษทางด้านไอที

- สิทธิ์การเข้าถึงทางด้านไอทีทั้งหมดต้องได้รับการอนุมัติจากเจ้าของเทคโนโลยีที่เกี่ยวข้องก่อนการอนุญาตให้เข้าถึง คำร้องขอเหล่านี้ต้องถูกทำขึ้นและได้รับการอนุมัติผ่านแบบฟอร์มคำขอบริการด้านไอทีและบันทึกในระบบช่วยเหลือที่เกี่ยวข้อง (Kace) ทั้งนี้ สิทธิในการเข้าถึงด้านไอทีประกอบด้วย:
- การเข้าถึงของผู้ดูแลระบบโดเมน
- การเข้าถึงของผู้ดูแลระบบฐานข้อมูล
- การเข้าถึงของผู้ดูแลระบบภายในไปยังเซิร์ฟเวอร์ในขอบเขต
- การจัดการอุปกรณ์เครือข่าย
- การบริหารจัดการ Internet
- การบริหารจัดการ Wi-Fi
- การบริหารจัดการ Navision
- การบริหารจัดการ SAP

- การบริหารจัดการ POS
- การบริหารจัดการ Citrix
- การเข้าถึงระยะไกล Remote ทุกชนิด (VPN, TeamViewer, AnyDesk)
- การบริหารจัดการ โฟลเดอร์ที่ใช้งานร่วมกันในเซิร์ฟเวอร์
- การเข้าถึงของผู้ใช้ในบริการด้านไอทีและแอพพลิเคชันทางธุรกิจ
- คำขอสำหรับการเข้าถึงบริการด้านไอทีและแอพพลิเคชันทางธุรกิจต้องเป็นไปตามการขอและกระบวนการอนุมัติพิเศษสำหรับแอพพลิเคชันที่เกี่ยวข้องตามที่ระบุไว้ในหัวข้อ กระบวนการจัดการ" "สิทธิด้านไอที
- การใช้งานอุปกรณ์ USB drive storage

10.1.2 การเข้าถึงโฟลเดอร์ที่ใช้งานร่วมกัน

- คำขอในการเข้าถึงโฟลเดอร์ที่ใช้งานร่วมกันในเซิร์ฟเวอร์ของบริษัทจะต้องได้รับการอนุมัติจากผู้จัดการสายงานที่เกี่ยวข้องพร้อมกับการอนุมัติจากฝ่ายไอทีผ่านแบบฟอร์มคำขอใช้บริการด้านไอทีและบัตรผ่านระบบช่วยเหลือที่เกี่ยวข้อง เฉพาะผู้ดูแลระบบระบบไอทีเท่านั้นที่สามารถให้สิทธิหรือแก้ไขการเข้าถึงโฟลเดอร์เหล่านี้ได้

1.11 นโยบายการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User Identification and Authentication)

- ระบบสารสนเทศต้องมีการจำกัดการเข้าถึง (Information Access Restriction) โดยอนุญาตให้เข้าถึงเฉพาะผู้ที่มีสิทธิ์เท่านั้นจัดให้มีการลงทะเบียน (User Registration) เพื่อพิสูจน์ตัวตนของผู้ใช้งานสำหรับระบบสารสนเทศ ให้สอดคล้องกับระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

- ผู้ใช้งานต้องมีบัญชีผู้ใช้งานหรือรหัสประจำตัวของผู้ใช้งานเฉพาะ และไม่ซ้ำกับคนอื่น รวมถึงไม่นำบัญชีผู้ใช้งานเดิมกลับมาใช้งานอีกครั้ง เมื่อมีการเข้าถึงระบบสารสนเทศ จะต้องมีการพิสูจน์ตัวตนที่ปลอดภัย (Authentication) เพื่อยืนยันว่าเป็นผู้ที่ได้รับสิทธิ์เข้าถึงข้อมูลสารสนเทศที่แท้จริง **ยกเว้น** ระบบที่มีการจำกัดเรื่องลิขสิทธิ์การใช้งาน

- ต้องมีการกำหนดสิทธิ์การใช้งานระบบสารสนเทศ (Privileged Management) ตามบทบาทหน้าที่ความรับผิดชอบ และพนักงานต้องจัดเก็บบัญชีผู้ใช้งานหรือรหัสประจำตัวผู้ใช้งานเป็นความลับ หากมีการละเมิดการเข้าถึงระบบสารสนเทศหรือละเมิดการใช้งาน บริษัทฯ จะจัดส่งหลักฐานการละเมิดไปยังบัญชีผู้ใช้งานหรือรหัสประจำตัวผู้ใช้งานดังกล่าว

- กรณีที่มีความจำเป็นต้องอนุญาตให้บุคคลหลายบุคคลเข้าถึงข้อมูลโดยมีรหัสผู้ใช้งานเหมือนกันได้ ในกรณีเช่นนี้ ผู้ใช้งานร่วมกันต้องรับผิดชอบต่อเหตุการณ์ที่เกิดขึ้น ให้สอดคล้องกับ **นโยบายการควบคุมการเข้าถึง (Access Control)**

- หากจะต้องมีการเลิกใช้บัญชีผู้ใช้งานและรหัสผ่าน ให้แจ้งกับหัวหน้าหน่วยงานของบริษัทฯ โดยตรงเพื่อทำเรื่องขอเลิกใช้โดยจะต้องกระทำ **ภายใน 3 วันก่อนที่จะเลิกใช้งาน**_หรือทันทีที่ได้รับทราบ ให้สอดคล้องกับ **ระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน (User Access Management)**

- กำหนดให้ดำเนินการทบทวนบัญชีผู้ใช้งานและสิทธิ์การเข้าถึง (Review of User Access Rights) **อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลง**

1.12 นโยบายการใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities)

- ให้มีการทำรายการ **Software Baseline** และติดตั้งซอฟต์แวร์ดังกล่าวตามที่กำหนดไว้เท่านั้น บริษัทฯ ไม่อนุญาตให้พนักงานติดตั้งหรือใช้ซอฟต์แวร์ที่อยู่นอกเหนือรายการ **Software Baseline** รวมถึงซอฟต์แวร์ประเภท Portable Software บนเครื่องคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ ของบริษัทฯ นอกจากได้รับอนุญาตจากผู้มีอำนาจแล้วเท่านั้น
- ดำเนินการติดตั้งซอฟต์แวร์ ตามความจำเป็นโดยพิจารณาถึงหน้าที่และความรับผิดชอบในการดำเนินงานของผู้ใช้งาน
- จัดให้มีการป้องกันการเข้าถึง Software Utilities โดยผู้ที่ไม่ได้รับอนุญาต
- ก่อนการติดตั้งซอฟต์แวร์ ซอฟต์แวร์ประเภทฟรีแวร์ หรือ Software Utilities ผู้ดูแลระบบมีแนวทางการตรวจสอบ ดังนี้
    - ศึกษาหรือทดสอบก่อนว่าเป็นซอฟต์แวร์ที่น่าเชื่อถือหรือไม่
    - มีการประมวลผลที่ถูกต้องหรือไม่
    - มีผู้ใช้งานอยู่ในจำนวนที่มากพอหรือไม่
    - มีผู้ผลิตซอฟต์แวร์อย่างชัดเจนหรือไม่
    - มีผู้ร่วมอาชีพหรือสายงานเดียวกันด้านสารสนเทศให้การรับรองหรือไม่
    - สามารถรายงานผลหากพบข้อผิดพลาดจากการใช้งานได้หรือไม่
    - มีการใช้งานกันมาเป็นระยะเวลานานพอแล้วหรือไม่
- ติดตั้งในระบบถึงความเหมาะสม เงื่อนไขและต้องไม่ละเมิดลิขสิทธิ์ก่อนการติดตั้ง ให้ปฏิบัติและดำเนินการตาม **นโยบายการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls of Malicious Code and Mobile Code)**

1.13 นโยบายการติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เทคโนโลยีสารสนเทศของบริษัทฯ (Installation of Software on Operational Systems)

- จัดทำ **Software Baseline** สำหรับเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่มีความสำคัญไว้อย่างเป็นลายลักษณ์อักษร และทบทวนปรับปรุงเนื้อหา อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่สำคัญ
- เมื่อมีการติดตั้งซอฟต์แวร์สำหรับเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่มีความสำคัญ ผู้รับผิดชอบพิจารณาตั้งค่าให้ตั้งค่าให้สอดคล้องตามที่กำหนดไว้ เช่น การกำหนดค่ามีผลกระทบการการทำงานของระบบ เป็นต้น ผู้รับผิดชอบต้องขออนุมัติเพื่อยกเว้นการกำหนดค่าดังกล่าว
- กำหนดให้มีการสุ่มตรวจเครื่องคอมพิวเตอร์ของพนักงานภายในบริษัทฯ การตั้งค่าของเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่มีความสำคัญ เพื่อให้มีความสอดคล้องกับความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

1.14 นโยบายการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls of Malicious Code and Mobile Code)

- การติดตั้งโปรแกรมต้องดำเนินการติดตั้งตาม **รายการ Software Baseline** เพื่อป้องกันใช้งานโปรแกรมชนิดเคลื่อนที่ (Mobile Code) นอกเหนือจาก ที่บริษัทฯ กำหนดขึ้น
- จัดให้มีการติดตั้งโปรแกรมป้องกันไวรัส และซอฟต์แวร์ไม่ประสงค์ดี สำหรับเครื่องคอมพิวเตอร์ที่เกี่ยวข้องตามรายการของ Software Baseline ที่บริษัทฯ กำหนดขึ้น และดำเนินการตาม **ระเบียบปฏิบัติงานการควบคุมซอฟต์แวร์ที่ไม่ประสงค์ดี (Control of Malicious Code and Mobile Code)** กรณีที่ไม่มีการติดตั้งโปรแกรมป้องกันไวรัส ให้มีการตั้งค่าความปลอดภัยของเครื่องคอมพิวเตอร์นั้น ๆ ตามที่ผู้บังคับบัญชาเห็นสมควรและได้รับการอนุมัติจากผู้บังคับบัญชา
- จัดให้มีการกำหนดมาตรการสำหรับตรวจจับและป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี

1.15 นโยบายการจัดการและการใช้งานรหัสผ่าน (Password Management)

- พนักงานต้องมีการกำหนดรหัสผ่าน (Password) ดังนี้
  - ต้องใช้การระบุและพิสูจน์ตัวตนของผู้ใช้งานตามนโยบายการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User Identification and Authentication) และรหัสผ่านที่เป็นของตนเองในการแสดงตนเข้าใช้งานหรือปฏิบัติงานในระบบข้อมูลตามสิทธิ์ที่ได้รับเท่านั้น
  - เก็บรักษาบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้เป็นความลับ

- บริษัทฯ ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และผู้ใช้ทุกคนมีหน้าที่ในการป้องกันรหัสผ่านอย่างเคร่งครัด
- กำหนดให้ใช้แนวทางการตั้งรหัสผ่านที่ปลอดภัย ดังนี้
  - เมื่อได้รับรหัสผ่านในครั้งแรกต้องเปลี่ยนรหัสผ่านใหม่ทันทีให้เป็นความลับเฉพาะตัว ในกรณีที่รหัสผ่านถูกเปิดเผยแล้ว พนักงานจะต้องทำการเปลี่ยนรหัสผ่านใหม่ทันที
  - **รหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักขระ** สำหรับระบบซึ่งมีการใช้งานหลังการประกาศใช้งานนโยบายฯ ฉบับนี้ ซึ่งประกอบด้วย ตัวอักษร ตัวเลข หรือสัญลักษณ์อื่นใดที่ยากต่อการคาดเดา **ยกเว้น** ระบบงานที่มีข้อจำกัดของอุปกรณ์
  - ไม่กำหนดรหัสผ่านจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือคำศัพท์ที่ปรากฏในพจนานุกรม
  - หลีกเลี่ยงรหัสผ่านที่เดาได้ง่าย เช่น ชื่อบุคคล สถานที่ ฯลฯ
- หลีกเลี่ยงการเก็บบันทึกรหัสผ่านลงในกระดาษ ไฟล์ข้อมูล ยกเว้นว่ามีขั้นตอนหรือวิธีการเก็บรักษาความลับของรหัสผ่านที่สามารถพิสูจน์ได้ว่าปลอดภัย
- กำหนดให้เปลี่ยนรหัสผ่านเป็นประจำทุก ๆ 90 วัน ขึ้นอยู่กับความเหมาะสม หรือข้อจำกัดของระบบงาน/อุปกรณ์

- ผู้ดูแลระบบด้านระบบปฏิบัติการจัดให้มีระบบบริหารจัดการรหัสผ่าน (Password Management System) ที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ โดยระบบดังกล่าวต้องสามารถกำหนดการตั้งรหัสผ่านได้ตามแนวการจัดการรหัสผ่าน (Password) ซึ่งกำหนดไว้ใน **นโยบายหน้าที่และความรับผิดชอบของผู้ใช้งาน (User Responsibility) กรณีที่บางระบบไม่สามารถดำเนินการ**ได้ตามแนวทางดังกล่าวอันเนื่องมาจากข้อจำกัดของระบบ ผู้ดูแลระบบต้องบริหารจัดการความมั่นคงปลอดภัยโดยใช้มาตรการอื่นทดแทน

1.16 นโยบายการเข้ารหัส (Cryptographic) และ การจัดการกุญแจ (Key Management)

- กำหนดระดับชั้นข้อมูลสารสนเทศและพิจารณาใช้งานการเข้ารหัสตามระดับชั้นข้อมูลสารสนเทศตาม **ระเบียบปฏิบัติงานการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Data Classification)** และต้องกำหนดมาตรการเข้ารหัสตาม **ระเบียบปฏิบัติงานการควบคุมการเข้ารหัส (Cryptographic Control)**
- การเข้ารหัสจะต้องใช้เทคนิคที่เป็นมาตรฐานสากล หรือตามที่กฎหมายกำหนด โดยพิจารณาถึงความแข็งแกร่ง (Strength) ของอัลกอริทึมที่ใช้รวมถึงความเหมาะสมในการนำมาใช้งาน

- กำหนดมาตรการในการบริหารจัดการการเข้ารหัสของข้อมูลและบริหารจัดการกุญแจเข้ารหัส (Key Management) ตาม **ระเบียบปฏิบัติงานการควบคุมการเข้ารหัส (Cryptographic Control)**

1.17 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

- จัดเก็บข้อมูลของบริษัทฯ อย่างปลอดภัยสอดคล้องตามระดับชั้นความลับของข้อมูลตาม **นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**
- ไม่เปิดโอกาสให้ผู้ไม่เกี่ยวข้องเข้าถึงข้อมูลของบริษัทฯ ในคอมพิวเตอร์ ทั้งโดยเจตนาหรือไม่เจตนา
- ห้ามติดตั้งและใช้งานโปรแกรมที่มีความเสี่ยงต่อการเคลื่อนย้ายข้อมูลที่ไม่ปลอดภัย
- เมื่อมีการใช้งาน Printer หรือใช้งานอุปกรณ์อื่น ๆ นำออกหรือส่งผ่านข้อมูลสำคัญ ผู้ใช้งานต้องกำกับดูแลจนกระทั่งดำเนินการต่อข้อมูลนั้นเรียบร้อย รวมถึงการฉายภาพ การนำเสนอข้อมูลผ่าน Presentation ในที่สาธารณะ เพื่อให้มั่นใจว่าข้อมูลสำคัญไม่รั่วไหลไปยังผู้ที่ไม่ได้รับอนุญาต
- ภายหลังปฏิบัติงานเสร็จสิ้นพนักงานต้องจัดเก็บเครื่องคอมพิวเตอร์ที่มีข้อมูลสำคัญไว้ในที่เหมาะสม ปลอดภัย และป้องกันผู้ไม่เกี่ยวข้องเข้าถึงได้ ตาม **นโยบายการจัดวางและป้องกันอุปกรณ์ (Equipment Security)**
- หากเกิดการชำรุด เสียหาย หรือสูญหายของเครื่องคอมพิวเตอร์ที่ใช้งาน เมื่อสอบสวนแล้วและพบว่าเกิดจากความประมาท ขาดการระมัดระวังและดูแลอย่างเพียงพอ พนักงานหรือผู้รับผิดชอบต้องรับผิดชอบความเสียหายที่เกิดขึ้น
- ไม่อนุญาตให้นำเครื่องคอมพิวเตอร์ไปใช้งานเพื่อการอื่นใดที่ไม่เกี่ยวข้องกับงานตามภารกิจหรือหน้าที่ความรับผิดชอบ
- ก่อนส่งอุปกรณ์ให้ผู้ให้บริการภายนอกซ่อม ผู้ดูแลอุปกรณ์ต้องดำเนินการลบหรือป้องกันข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์ สื่อบันทึกข้อมูลแบบเคลื่อนที่ (Removable Storage Media)
- สำรองข้อมูลในเครื่องคอมพิวเตอร์ที่สำคัญหรือใช้งานอย่างสม่ำเสมอเพื่อป้องกันจากการสูญหายของข้อมูลในกรณีต่าง ๆ เช่น ฮาร์ดดิสก์เสีย ไฟกระชากจนทำให้ฮาร์ดดิสก์พัง หรืออื่น ๆ
- เมื่อมีการนำไปใช้งานนอกสถานที่ เพื่อป้องกันการสูญหาย และห้ามปล่อยเครื่องคอมพิวเตอร์ทิ้งไว้โดยไม่มีผู้ดูแล
- ห้ามทิ้งเครื่องคอมพิวเตอร์ไว้ในรถยนต์ที่สามารถมองเห็นได้โดยผู้อื่นจากภายนอก

1.18 นโยบายการบริหารจัดการความเปลี่ยนแปลง (Change Management)

- จัดให้มีการขออนุมัติใช้งาน ติดตั้ง ปรับปรุง หรือแก้ไข งานบริการประมวลผลสารสนเทศ โดยให้หน่วยงานที่รับผิดชอบในการดำเนินการเปลี่ยนแปลงทำการประเมินผลกระทบที่จะเกิดขึ้นรวมทั้งผลกระทบด้านความปลอดภัยจากการเปลี่ยนแปลง รวมทั้งจัดทำแผนถอยหลังกลับ (Roll Back Plan) ก่อนที่จะมีการขออนุมัติจากผู้ที่มีอำนาจหรือระดับผู้บริหารที่ รับผิดชอบในเรื่องดังกล่าว
- กำหนดให้มีการจัดทำ **ระเบียบปฏิบัติงานการบริหารจัดการเปลี่ยนแปลง (Change Management)**
- การเปลี่ยนแปลงระบบหรือโครงสร้างพื้นฐานที่มีผลกระทบต่อลูกค้าและผู้ใช้งานที่เกี่ยวข้อง ต้องมีการสื่อสารรายละเอียดให้ลูกค้าและผู้ใช้งานที่เกี่ยวข้องรับทราบ
- การเปลี่ยนแปลง ติดตั้ง ปรับปรุง หรือแก้ไข งานบริการประมวลผลสารสนเทศโดยผู้ให้บริการภายนอก (Supplier) จะต้องมีการประเมินผลกระทบที่จะเกิดขึ้นรวมทั้ง ผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศจากการเปลี่ยนแปลง รวมทั้งจัดทำแผนถอยหลังกลับ (Roll Back Plan) เสนอต่อหน่วยงานที่รับผิดชอบ (Owner) ก่อน เพื่อให้หน่วยงานที่รับผิดชอบ (Owner) ดำเนินการทำเรื่องขออนุมัติจากผู้ที่มีอำนาจหรือระดับผู้บริหารที่รับผิดชอบในเรื่องดังกล่าว

1.19 นโยบายการสำรองข้อมูล (Backup Management)

- จัดให้มีการสำรองข้อมูลให้ครบถ้วน เช่น ข้อมูลสารสนเทศ ข้อมูลค่า Configuration เป็นต้น เพื่อให้ระบบมีความพร้อมใช้งานได้อย่างต่อเนื่องตาม **ระเบียบปฏิบัติงานการสำรองข้อมูล** รวมถึงมีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกสถานที่และทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ เพื่อให้ข้อมูลที่สำรองมีความพร้อมใช้
- กำหนดระยะเวลาการสำรองข้อมูล ทั้งศูนย์ข้อมูลหลัก (Data Center: DC) และ ศูนย์สำรองข้อมูล (Disaster Recovery Site: DR Site) ในการจัดเก็บข้อมูลสำรองเป็นรูปแบบ เป็นจำนวน 7 Copy

1.20 นโยบายการจัดการความมั่นคงปลอดภัยสำหรับเครือข่าย (Network Security Management)

- การบริหารจัดการสิทธิ์การเข้าใช้งานระบบเครือข่ายของบริษัทต้องปฏิบัติตาม **ระเบียบปฏิบัติงานการบริหารจัดการการเชื่อมต่อเครือข่ายและงานบริการเครือข่าย (Network Security Control)** และการทบทวนสิทธิ์การเข้าถึงตาม **ระเบียบปฏิบัติงานการควบคุมการเข้าถึงระบบของผู้ใช้งาน (User Access Management)**
    - มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการ สำหรับบริการเครือข่าย รวมถึงการกำหนดระดับการให้บริการเครือข่ายภายในของ

บริษัทฯ หรือบริการที่ได้รับจากผู้ให้บริการภายนอก ตาม**นโยบายการควบคุมผู้ให้บริการจากภายนอก (Supplier Management)**

- จัดให้มีการแยกสภาพแวดล้อมสำหรับระบบสำคัญ (Sensitive System Isolation) โดยทำการแยกเครือข่ายออกจากระบบอื่น (Segregation in Networks)
- การเชื่อมต่อเครือข่ายจากระยะไกล (Teleworking) ผู้ใช้งานจากระยะไกล (Remote User) หรือจากการเชื่อมต่อผ่านอุปกรณ์ Mobile Device ที่ทำการเชื่อมต่อเครือข่ายจะมีการระบุตัวตนหรือยืนยันตัวตน (Authentication) ผ่านกลไกของ VPN (Virtual Private Network) เพื่อเข้าถึงเครือข่ายของบริษัทฯ
- ต้องมีการบันทึกกิจกรรมและการเฝ้าระวังเหตุการณ์ผิดปกติต่าง ๆ ของการใช้งานระบบเครือข่าย ตาม **ระเบียบปฏิบัติงานการจัดเก็บ เฝ้าระวัง ตรวจสอบการวิเคราะห์และจัดการกับข้อมูลล็อก (Log Monitoring and Management)** และ **วิธีปฏิบัติงานการเทียบเวลาระบบคอมพิวเตอร์ (Clock Synchronization)**
- ต้องมีการทบทวน Firewall Policy ปีละ 1 ครั้ง

1.21 นโยบายการบริหารจัดการถ่ายโอนข้อมูล (Transfer Management Policy)

- ต้องมีการป้องกันจากการถูกดักจับ คัดลอก แก้ไข และการทำลายข้อมูลต้องมีการป้องกันการส่งข้อมูลที่สำคัญตามวิธีการที่องค์กรกำหนด
- ข้อตกลงในการถ่ายโอนข้อมูลสารสนเทศ (Agreements on Information Transfer) ดำเนินการอย่างน้อยดังนี้
    - มีการกำหนดวิธีการติดต่อสื่อสารข้อมูล และมีการแจ้งให้ผู้รับ-ส่งทราบ
    - มีบันทึกเกี่ยวกับการติดต่อสื่อสารข้อมูลที่สามารถติดตามและสอบกลับได้
    - การทำข้อตกลงในการถ่ายโอนข้อมูลต้องคำนึงถึงนโยบาย และกฎหมายที่เกี่ยวข้อง
    - มีการระบุความสำคัญของข้อมูล ตามระดับชั้นข้อมูล
    - การส่งข้อความทางอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม ตามระดับชั้นข้อมูล
- ก่อนการแลกเปลี่ยนสารสนเทศระหว่างบริษัทฯ ต้องมีการประเมินความเสี่ยงที่เกี่ยวข้องในการดำเนินการแลกเปลี่ยนสารสนเทศนั้น
- เมื่อมีการแลกเปลี่ยนสารสนเทศระหว่างบริษัทฯ ต้องผ่านการอนุมัติผู้บริหารระดับสูงหรือผู้บริหารตามระดับชั้น (ระดับการอนุมัติขึ้นอยู่กับระดับความสำคัญของข้อมูลที่ต้องการแลกเปลี่ยน) อย่างเป็นลายลักษณ์

อักษร และลงนามในข้อตกลงระหว่างกันในการที่จะไม่เปิดเผยความลับขององค์กร (Non-Disclosure Agreement) ระหว่างบริษัทฯ สำหรับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems)

- มีการกำหนดช่องทางการแลกเปลี่ยนสารสนเทศหรือสื่อบันทึกข้อมูลสารสนเทศระหว่างบริษัทฯ กับหน่วยงานภายนอก ด้วยวิธีการที่มีความมั่นคงปลอดภัยและสอดคล้องตาม **นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)**
- กำหนดให้มีการจัดทำ**เอกสารไม่เปิดเผยความลับขององค์กร (Non-Disclosure Agreement)** เพื่อใช้ในการลงนามสำหรับข้อตกลงการไม่เปิดเผยความลับของบริษัทฯ

1.22. นโยบายการควบคุมการสื่อสาร Electronic Messaging (Control of Electronic Messaging)

- ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์ การสนทนา หรือการติดต่อสื่อสารใด ๆ ให้ถือเสมือนเป็นการส่งจดหมายแบบเป็นทางการ
- ต้องใช้งานอีเมลแอดเดรสของบริษัทฯ เพื่อการติดต่อหรือใช้เพื่อการปฏิบัติงานตามความรับผิดชอบของตนเองที่ได้รับมอบหมายเท่านั้น ห้ามมิให้ใช้อีเมลของบริษัทฯ เพื่อหาผลประโยชน์ส่วนตน
- ห้ามใช้อีเมลแอดเดรสอื่น ๆ เพื่อติดต่อธุรกิจหรืองานของบริษัทฯ โดยไม่ได้รับอนุญาต
- ใช้ความระมัดระวังและตรวจสอบอีเมลแอดเดรสของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งข้อมูลสำคัญผิดตัวผู้รับและทำให้ข้อมูลเกิดการรั่วไหล
- ควรระบุชื่อของผู้ส่ง ตำแหน่ง และข้อมูลติดต่อกลับไว้ในอีเมลทุกฉบับที่ส่งไปเพื่อเป็นข้อมูลในการติดต่อกลับ
- จำกัดการส่งหรือส่งต่อข้อมูลทางอีเมลไปยังผู้รับหรือกลุ่มผู้รับอีเมลเท่าที่มีความจำเป็นต้องรับทราบข้อมูลในอีเมลนั้นเท่านั้น
- ใช้คำที่สุภาพในการส่งอีเมล ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อบริษัทฯ หรือบุคคลอื่น ๆ
- ควรสำรองข้อมูลอีเมลตามความจำเป็นอย่างสม่ำเสมอ
- ห้ามเข้าถึงข้อมูลอีเมลของผู้อื่นโดยไม่ได้รับอนุญาต
- ห้ามรับหรือส่งอีเมลแทนผู้อื่นโดยไม่ได้รับอนุญาต
- ห้ามลงทะเบียนด้วยอีเมลแอดเดรสของบริษัทฯ ไว้ตามที่อยู่เว็บไซต์ต่าง ๆ ที่ไม่มีความเกี่ยวข้องกับภารกิจงานของตนเอง

- ห้ามส่งอีเมลที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) หรือที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter) หรือที่มีลักษณะเป็นการละเมิดต่อกฎหมาย ทรัพย์สินทางปัญญา หรือสิทธิ์ของบุคคลอื่น หรือที่มีโปรแกรมไม่ประสงค์ดีไปให้กับผู้อื่นโดยเจตนา
- ห้ามปลอมแปลงหรือสวมรอยใช้อีเมลของผู้อื่น

1.23 นโยบายการรักษาความมั่นคงปลอดภัยในการพัฒนาระบบงาน (Information Systems Acquisition, Development and Maintenance Policy)

- กำหนดให้มีการระบุความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศตั้งแต่เริ่มระยะเวลาโครงการสำหรับการพัฒนาระบบใหม่และการปรับปรุงระบบเดิม
- ให้ปฏิบัติตามหลักการวิศวกรรมระบบที่น่าเชื่อถือและมีความมั่นคงปลอดภัย ตาม **เอกสารแนวทาง Principles for Engineering Secure Systems** โดยผู้พัฒนาต้องระบุหลักการที่นำมาพัฒนาหรือปรับปรุงหรือการประยุกต์กับการพัฒนา
- ต้องมีการควบคุมความมั่นคงปลอดภัยข้อมูลสารสนเทศของระบบงานที่มีการใช้งานในเครือข่ายสาธารณะ เพื่อป้องกันเรื่องการฉ้อโกง (Fraud) การละเมิดสัญญา การเปิดเผยและแก้ไขโดยไม่ได้รับอนุญาตให้สอดคล้องตาม **เอกสารแนวทาง Principles for Engineering Secure Systems**
- ระบบงานต้องมีการพัฒนาให้ครอบคลุมเรื่อง การส่งผ่านข้อมูลระหว่างเครือข่ายให้มีความมั่นคงปลอดภัย เช่น การใช้งานโปรโตคอลที่มีความปลอดภัย การใช้งานใบรับรองอิเล็กทรอนิกส์ (Certification Authority) เป็นต้น
- กำหนดขั้นตอนการปฏิบัติสำหรับการเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบและทดสอบกระบวนการของระบบสารสนเทศนั้นก่อนตรวจรับระบบงาน ตาม **นโยบายการบริหารจัดการความเปลี่ยนแปลง (Change Management)**
- ต้องมีการทบทวนและทดสอบภายหลังมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบสำคัญ เพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยขององค์กร
- ไม่อนุญาตการดำเนินการเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูป และจำกัดการเปลี่ยนแปลงเท่าที่จำเป็นและต้องมีการควบคุมอย่างรัดกุม
- จัดให้มีการแยกสภาพแวดล้อมสำหรับการพัฒนาระบบ การทดสอบระบบ และระบบที่ใช้งานจริง (Separation of Development, Test and Operational Facilities) ไม่ให้อยู่สภาพแวดล้อมเดียวกัน เพื่อหลีกเลี่ยงการเข้าถึง Operational System โดยไม่ได้รับอนุญาต

- กำหนดให้มีการแบ่งแยกหน้าที่และความรับผิดชอบ (Segregation of Duties) ระหว่างบุคคลหรือหน่วยงาน โดยจัดให้มีการตรวจสอบความถูกต้องระหว่างกัน ไม่ให้บุคคลคนเดียวปฏิบัติงานตั้งแต่ต้นจนจบเพื่อป้องกันความเสี่ยงต่อข้อผิดพลาดและการทุจริตหรือการกระทำที่ไม่เหมาะสม เช่น แยกหน้าที่การพัฒนาระบบหรือจัดทำระบบทดสอบออกจากหน้าที่ของผู้มีอำนาจอนุมัติหรือดำเนินการนำระบบออกสู่การให้บริการ เป็นต้น
- หากบริษัทฯ ต้องมีการจัดจ้างผู้ให้บริการภายนอกเป็นผู้ดำเนินการพัฒนาระบบใหม่ให้มีกำกับดูแลเฝ้าระวัง พร้อมทั้งแจ้งให้ผู้ให้บริการภายนอกทราบถึง **นโยบายการรักษาความมั่นคงปลอดภัยในการพัฒนาระบบงาน (Information Systems Acquisition, Development and Maintenance Policy)** ก่อนการพัฒนา
- ต้องมีการดำเนินการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบในระหว่างที่ระบบอยู่ในช่วงการพัฒนา
- จัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่หรือปรับปรุงเพิ่มเติมตาม **ระเบียบปฏิบัติงานการตรวจรับระบบงาน (System Acceptance)** รวมถึงการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบตามที่กำหนดไว้ในช่วงการพัฒนา
- หากต้องมีการใช้ข้อมูลของบริษัทฯ ในการทดสอบ จะต้องบริหารจัดการตาม **นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)** และปฏิบัติตาม **นโยบายการบริหารจัดการแลกเปลี่ยนข้อมูล (Information Transfer Management)**

1.24 นโยบายการควบคุมผู้ให้บริการจากภายนอก (Supplier Management)

- จัดให้มีการคัดเลือกผู้ให้บริการภายนอกก่อนการจัดจ้างเพื่อให้ เข้าถึง ดำเนินการ ติดตั้ง สื่อสาร เชื่อมต่อ หรือให้บริการโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศต่อข้อมูลสารสนเทศขององค์กร เช่น การตรวจสอบคุณสมบัติทางการเงินของบริษัทฯ ผู้ให้บริการภายนอกซึ่งแสดงถึงความน่าเชื่อถือของบริษัทฯ เป็นต้น โดยหน่วยงานที่เกี่ยวข้อง
- กรณีจัดจ้างผู้ให้บริการภายนอกที่ เข้าถึง ดำเนินการ ติดตั้ง สื่อสาร เชื่อมต่อ หรือให้บริการโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศต่อข้อมูลสารสนเทศของบริษัทฯ ต้องควบคุมและบริหารจัดการผู้ให้บริการภายนอกตาม **ระเบียบปฏิบัติงานการบริหารจัดการผู้ให้บริการภายนอก (Supplier Management)** จะต้องปฏิบัติตามข้อกำหนด ดังนี้
  1. พิจารณาเพิ่มข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศในระหว่างการดำเนินการโครงการ
  2. ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้องในด้านความมั่นคงปลอดภัยสารสนเทศ และลงนามในสัญญารักษาความลับ (NDA) และ AUP

3. กรณีผู้ให้บริการภายนอกมีการจ้างช่วง ดำเนินการดังต่อไปนี้
   3.1 ดำเนินการแจ้งรายชื่อผู้รับการจ้างช่วงต่อหัวหน้าโครงการเพื่อขออนุญาตให้เข้าดำเนินการ
   3.2 กรณีมีการเปลี่ยนแปลงต่อการดำเนินการโครงการ เช่น รายละเอียดโครงการ ผู้รับจ้างช่วงในระหว่างดำเนินโครงการ เป็นต้น ผู้ให้บริการภายนอกต้องแจ้งและดำเนินการตาม **ระเบียบปฏิบัติงานการบริหารจัดการผู้ให้บริการภายนอก (Supplier Management)**

- จัดให้มีการประเมินความเสี่ยงผู้ให้บริการภายนอกในด้านการเข้าถึงระบบสารสนเทศ ในกรณีที่เป็นผู้ให้บริการภายนอกรายใหม่หรือรายเดิมที่เข้าถึงระบบใหม่ตาม **ระเบียบปฏิบัติงานการบริหารจัดการผู้ให้บริการภายนอก (Supplier management)** และต้องประเมินความเสี่ยงของผู้ให้บริการภายนอกตามกระบวนการประเมินความเสี่ยงตามรอบระยะเวลาให้สอดคล้องตาม **ระเบียบปฏิบัติงานการประเมินความเสี่ยง (Risk Assessment)**
- ต้องมีการระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก
- ต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกในเรื่องความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการโครงสร้างพื้นฐานของระบบสำหรับ สารสนเทศขององค์กรโดยผู้ให้บริการภายนอก โดยจัดให้มีการทำ Service Level Agreement ที่ครอบคลุมถึงข้อตกลงด้านความปลอดภัยในการให้บริการโดยหน่วยงานภายนอก ได้แก่ คุณลักษณะและรายละเอียดของการให้บริการ, มาตรการจัดการด้านความมั่นคงปลอดภัยในการให้บริการ โดยข้อตกลงนี้เป็นที่ยอมรับของทั้งสองฝ่าย และกำหนดให้มีการทบทวน Service Level Agreement ดังกล่าวอย่างน้อยปีละ 1 ครั้ง
- ต้องจัดให้มีการควบคุมด้านความปลอดภัยในการถ่ายโอนข้อมูล เครื่องมือ อุปกรณ์ระหว่างบริษัทฯ กับผู้ให้บริการภายนอกให้เกิดความมั่นคงปลอดภัย
- มีการทบทวนรายงานผลปฏิบัติงานของผู้ให้บริการภายนอก (รวมถึงมีการประชุมร่วมกันตามเงื่อนไขที่ระบุใน Agreement)
- แลกเปลี่ยนข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident) ระหว่างบริษัทฯ กับผู้ให้บริการภายนอกเพื่อเสริมองค์ความรู้และเตรียมการป้องกัน โดยดำเนินการตามขอบเขตของ Agreement อย่างเคร่งครัด
- ติดตามผล และสนับสนุนการแก้ไขปัญหาและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) ร่วมกับผู้ให้บริการภายนอกตามขอบเขตที่ตกลงกันไว้

- หน่วยงานที่เกี่ยวข้องต้องดำเนินการติดตาม ทบทวน และตรวจสอบการปฏิบัติการของผู้ให้บริการภายนอก
- การเปลี่ยนแปลงผู้ให้บริการภายนอกต้องพิจารณาจากผลการปฏิบัติงาน ความเหมาะสมของการเปลี่ยนแปลงตามความจำเป็น และกรณีที่มีความจำเป็นในการเปลี่ยนแปลงแก้ไขสัญญา หรือข้อตกลงร่วมกัน หากต้องดำเนินการเปลี่ยนแปลงใด ๆ ต้องได้รับอนุมัติจากผู้มีอำนาจก่อนเปลี่ยนแปลง รวมถึงการพิจารณาความเสี่ยงที่อาจกระทบต่อธุรกิจของบริษัทฯ ระหว่างการเปลี่ยนแปลง

1.25. นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

- บุคคลภายนอกที่มาติดต่อกับบริษัทฯ จะต้องมีการแลกบัตร และต้องรอเจ้าหน้าที่ของบริษัทฯ มารับที่บริเวณต้อนรับก่อน แล้วจึงจะพาไปตามบริเวณต่าง ๆ ตามที่กำหนดไว้
- พนักงานของบริษัทฯ จะต้องติดบัตรประจำตัวพนักงานตลอดเวลาที่อยู่ในบริษัทฯ และติดไว้ในที่ที่สังเกตเห็นได้อย่างชัดเจน เช่น ที่หน้าอกเสื้อ หรือ กระเป๋าเสื้อ หรือ ใส่สายคล้องไว้ที่คอ เป็นต้น
- จัดให้มีการกำหนดว่า พื้นที่ หรือ บริเวณใดในเขตสำนักงานเป็นบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas) อ้างอิง **เอกสารสนับสนุน MS Scope and Secure Area**
- ปฏิบัติตาม **ระเบียบปฏิบัติงานการควบคุมการเข้าถึงพื้นที่สำนักงาน และแนวทางการปฏิบัติงานในพื้นที่การรักษาความมั่นคงปลอดภัย สำหรับ บริษัท แม็คกรุ๊ป จำกัด (มหาชน)**

1.26 นโยบายการจัดทำบัญชีทรัพย์สินและกำหนดผู้รับผิดชอบ (Inventory and Ownership of Assets Policy)

- จัดให้มีการจัดทำทะเบียนทรัพย์สินของระบบข้อมูล รวมทั้งต้องกำหนดผู้รับผิดชอบ ระบบข้อมูลดังกล่าวของลูกค้า ตลอดจนจัดบัญชีทรัพย์สินของระบบและโครงสร้างพื้นฐานต่าง ๆ ซึ่งสนับสนุนระบบข้อมูล และของลูกค้า

1.27 นโยบายการจัดวางและป้องกันอุปกรณ์ (Equipment Security)

- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์ ควรต้องมีการจัดวางในพื้นที่มีการควบคุมการเข้าถึงโดยผู้ไม่ได้รับอนุญาตและมีความมั่นคงปลอดภัย
- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์ใด ๆ ที่มีข้อมูลสำคัญตามที่ กฎหมาย สัญญา มาตรฐานสากล กำหนดให้มีการจัดเก็บและควบคุมการเข้าถึงแยกออกจากระบบอื่น ๆ
- มีมาตรการควบคุมเพื่อลดความเสี่ยงจากช่องโหว่ทางกายภาพ

- การนำอุปกรณ์ประมวลผลสารสนเทศ เครื่องคอมพิวเตอร์ อุปกรณ์ เครื่องมือ ของบริษัทฯ ไปใช้งานนอกสถานที่ (Security of Equipment Off-Premises) จะต้องมีการขออนุญาตจากบริษัทฯ ผ่านช่องทาง E-mail พร้อมทั้งลงนามใน **แบบฟอร์ม MCG-ISMS-FM-2567-033 ใบขออนุญาตนำทรัพย์สินของบริษัทออกนอกบริษัท** และได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร ก่อนนำอุปกรณ์ดังกล่าวออกไปใช้งานภายนอกบริษัทฯ และจัดเก็บหลักฐานเพื่อใช้ในการตรวจสอบและยืนยันการดำเนินการ
- ผู้ใช้งานที่นำอุปกรณ์ไปใช้งานนอกบริษัทฯ มีความตระหนัก พึงระวัง รักษา หวงแหน รักษาข้อมูล เครื่องคอมพิวเตอร์ หรืออุปกรณ์ซึ่งเป็นทรัพย์สินของบริษัทฯ เสมือนเช่นทรัพย์สินของตนเอง และพิจารณาความเสี่ยงของการปฏิบัติงานภายนอกบริษัทฯ
- ก่อนการนำอุปกรณ์กลับมาใช้ใหม่ หรือกำจัดอุปกรณ์ (Secure Disposal or Re-Use of Equipment) ให้ทำลายข้อมูลสำคัญและลบซอฟต์แวร์ลิขสิทธิ์ทั้งหมดที่อยู่ในสื่อบันทึกดังกล่าวก่อนโดยดำเนินการตามระดับชั้นของข้อมูลที่อยู่ในสื่อบันทึก สอดคล้องตาม นโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling)

1.28 นโยบายการกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment)

- กรณีมีการยกเลิกสัญญาระหว่างลูกค้ากับบริษัทฯ ให้ดำเนินแจ้งลูกค้าอย่างเป็นทางการถึงการล้างข้อมูลของลูกค้าบนระบบและโครงสร้างพื้นฐานต่าง ๆ เมื่อได้รับคำยืนยันเรียบร้อยแล้ว จึงดำเนินการล้างข้อมูลทั้งหมดนั้นที่เป็นส่วนของระบบข้อมูล ของลูกค้าออกจากระบบ รวมทั้งแจ้งผลการดำเนินการอย่างเป็นทางการให้ลูกค้าได้รับทราบ

1.29 นโยบายการบริหารจัดการการถ่ายโอนข้อมูลเพื่อการใช้งานโพรโทคอล FTP/sFTP

- กำหนดให้ระบบรองรับ FTP/sFTP โดยตั้งค่าเป็น Secure Shell (SSH)
- กำหนดการตั้งค่า Symmetric Key ในการ เข้า/ถอด รหัสไฟล์ เพื่อการแลกเปลี่ยนข้อมูลผ่าน FTP/sFTP บนระบบ
- กำหนดการตั้งค่า FTP Server ให้รองรับการเข้ารหัสลับข้อมูล เพื่อป้องกันการถูกดักจับ (Sniffer) จากผู้ไม่ประสงค์ดี โดยการเข้ารหัสการส่งข้อมูลตั้งแต่ AES128-CTR ขึ้นไป
- กำหนด Firewall Policy เพื่อกำหนดต้นทางที่จะ Connect เข้ามาที่ระบบเสมอ
- กำหนดให้ผู้ใช้บริการต้องใช้ Username/Password ที่ผู้ดูแลระบบของบริษัทฯ สร้างให้เท่านั้น
- ต้องมีการกำหนดสิทธิ์ในการเข้าถึงไฟล์ให้กับผู้ใช้งาน ผู้ดูแลระบบต้องกำหนดสิทธิ์เท่าที่จำเป็นเท่านั้น โดยกำหนดสิทธิ์การเข้าใช้งานได้เฉพาะ Path ที่กำหนดเท่านั้น

- กำหนดให้ระบบลบไฟล์ที่อัปโหลด (Upload) มาแล้วมากกว่า 120 วัน โดยอัตโนมัติ เพื่อช่วยในการบริการจัดการพื้นที่ของระบบ และลดความเสี่ยงที่เกิดขึ้น
- กำหนดเปิดใช้งานการบันทึก Log บน Server ของบริษัทฯ เพื่อตั้งค่าระบบให้บันทึกการทำงานต่าง ๆ ที่เกิดขึ้นกับระบบ เช่น การล็อกอินเข้าใช้งาน หรือวิเคราะห์ในกรณีที่ระบบเกิดปัญหา เช่น การติดตามหา IP Address ของผู้ที่โจมตีระบบ เพื่อทำให้ระบบมีความสอดคล้องตาม พรบ.คอมพิวเตอร์ พ.ศ. 2550 ซึ่งระบุว่า ผู้ให้บริการจะต้องสามารถระบุตัวตนของผู้ใช้งานได้ พร้อมเก็บข้อมูลการจราจรคอมพิวเตอร์ไม่น้อยกว่า 90 วัน ในระยะเวลา 1 ปี
- อัปเดตเวอร์ชันของซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่อทำให้ระบบมีประสิทธิภาพและลดปัญหาช่องโหว่ที่อาจเกิดขึ้นต่อระบบได้

1.30 นโยบายการบริหารจัดการการแลกเปลี่ยนข้อมูลในรูปแบบส่วนต่อประสานโปรแกรมประยุกต์ หรือ Application Programming Interface (API)

- กำหนดให้บริษัทฯ ต้องศึกษาและจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับ API ให้สอดคล้องกับมาตรฐานสากล ระเบียบปฏิบัติงาน ข้อเสนอแนะมาตรฐาน และกฎหมายอ้างอิงตาม **นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)**
- กำหนดรูปแบบสถาปัตยกรรม (Architectural Style) หรือเกณฑ์วิธีของการสื่อสารข้อมูล (Protocol) สำหรับ API มาตรฐานของบริษัทฯ เป็น REST (Representational State Transfer) ในการแลกเปลี่ยนข้อมูลของบริษัทฯ เพื่อการสื่อสารระหว่างซอฟต์แวร์ที่ได้มาตรฐานสากล ปลอดภัย เสถียร และมีประสิทธิภาพ
- กำหนดให้ระบบรองรับการแลกเปลี่ยนข้อมูลรูปแบบ API โดยตั้งค่าเป็น HTTPS
- กำหนดให้ระบบรองรับการเข้ารหัสลับข้อมูล เพื่อป้องกันการถูกดักจับ (Sniffer) จากผู้ไม่ประสงค์ดี
- กำหนด Firewall Policy เพื่อกำหนดต้นทางที่จะเชื่อมต่อ (Connect) ต้องเข้ามาด้วย HTTPS Protocol เสมอ เพื่อความถูกต้องสมบูรณ์ ปลอดภัย ตลอดจนสามารถเก็บข้อมูลของผู้ใช้บริการไว้เป็นความลับได้
- กำหนดให้บริษัทฯ จัดทำเอกสาร API Specification สำหรับพัฒนา และเผยแพร่ให้แก่ผู้ใช้บริการ ที่ผู้ดูแลระบบของบริษัทฯ จัดทำให้เท่านั้น สำหรับการยืนยันตัวตนทางด้านผู้ใช้บริการ (Client Authentication) โดยคำนึงถึงและปฏิบัติตามมาตรฐานสากล หรือแนวปฏิบัติที่ดีที่เหมาะสมกับรูปแบบสถาปัตยกรรมหรือเกณฑ์วิธีของการสื่อสารข้อมูลที่ใช้ รวมถึงควบคุมการเข้าถึง API Specification ให้สอดคล้องกับวัตถุประสงค์ของการให้บริการ API
- กำหนดเปิดใช้งานการบันทึก Application Log บน Server ของบริษัทฯ เพื่อตั้งค่าระบบให้บันทึกการทำงานต่าง ๆ ที่เกิดขึ้นกับระบบ เช่น การล็อกอินเข้าใช้งาน หรือวิเคราะห์ในกรณีที่ระบบเกิดปัญหา เช่น การติดตาม

หา IP Address ของผู้ที่โจมตีระบบ เพื่อทำให้ระบบมีความสอดคล้องตาม พรบ.คอมพิวเตอร์ พ.ศ. 2550 ซึ่งระบุว่า ผู้ให้บริการจะต้องสามารถระบุตัวตนของผู้ใช้งานได้ พร้อมเก็บข้อมูลการจราจรคอมพิวเตอร์ไม่น้อยกว่า 90 วัน ในระยะเวลา 1 ปี

- กำหนดให้บริษัทฯ ต้องศึกษา ประเมิน และคัดเลือกรูปแบบโครงสร้างข้อความในการแลกเปลี่ยนข้อมูล (Structured Data Format for Data Exchanging) ที่เหมาะสม เช่น JSON (JavaScript Object Notation) และ XML (Extensible Markup Language) โดยพิจารณาจากปัจจัยต่าง ๆ เช่น รูปแบบสถาปัตยกรรมหรือเกณฑ์วิธีของการสื่อสารข้อมูลที่ใช้ มาตรฐานข้อความที่ใช้ ข้อจำกัดของทรัพยากรด้านเทคโนโลยีสารสนเทศที่มีอยู่ แนวทางการใช้งานในปัจจุบันของผู้ใช้บริการ ระดับของความซับซ้อนของข้อมูล และความสามารถเฉพาะตัวของรูปแบบโครงสร้างข้อความในการแลกเปลี่ยนข้อมูลแต่ละประเภทเอกสาร
- อัปเดตเวอร์ชันของซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่อทำให้ระบบมีประสิทธิภาพและลดปัญหาช่องโหว่ที่อาจเกิดขึ้นต่อระบบได้

1.31 นโยบายการบริหารจัดการการใช้บริการระบบคลาวด์ Information Security For Use of Cloud Services

การใช้บริการคลาวด์อาจเกี่ยวข้องกับความรับผิดชอบร่วมกันในเรื่องความปลอดภัยของข้อมูลและความพยายามในการทำงานร่วมกันระหว่างผู้ให้บริการคลาวด์และองค์กรที่ทำหน้าที่เป็นลูกค้าบริการคลาวด์ จำเป็นอย่างยิ่งที่จะต้องกำหนดและดำเนินการความรับผิดชอบสำหรับทั้งผู้ให้บริการคลาวด์และองค์กรซึ่งทำหน้าที่เป็นลูกค้าบริการคลาวด์อย่างเหมาะสม ทีมรักษาความปลอดภัยจะต้องกำหนดนโยบายมาเพื่อควบคุมความเสี่ยง ดังนี้

- จะต้องป้องกันและบำรุงรักษากระบวนการในการได้มา ใช้ จัดการ และยกเลิกการใช้งานจากบริการคลาวด์ เจ้าหน้าที่ควรกำหนดวิธีการที่สอดคล้องกับระบบ Change Management และให้มีการบันทึกไว้เพื่อให้เป็นไปตามข้อกำหนดด้านความปลอดภัยข้อมูลขององค์กร
- ทีมรักษาความปลอดภัยควรกำหนดและสื่อสารถึงความตั้งใจที่จะจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลที่เกี่ยวข้องกับการใช้บริการคลาวด์ อาจเป็นส่วนขยายหรือเป็นส่วนหนึ่งของแนวทางที่มีอยู่สำหรับวิธีที่องค์กรจัดการบริการที่จัดทำโดยบุคคลภายนอก
- ไม่อนุญาตให้พนักงานใช้ระบบ Cloud ส่วนบุคคล หากมีความจำเป็นจะต้องทำการขออนุมัติจากฝ่ายบริหารก่อน โดยจะต้องประเมินความเสี่ยงทุกครั้ง และจะต้องติดตามความเสี่ยงอยู่เป็นประจำหากมีการใช้งาน
- ข้อกำหนดด้านความปลอดภัยข้อมูลที่เกี่ยวข้องทั้งหมดที่เกี่ยวข้องกับการใช้บริการคลาวด์จะต้องถูกสื่อสารให้กับทีมงานหรือเจ้าหน้าที่ที่ได้รับผิดชอบในการดูแลอย่างเป็นประจำ

- เกณฑ์การเลือกบริการคลาวด์และขอบเขตการใช้บริการคลาวด์ จะต้องเป็นไปตามข้อกำหนดของเจ้าหน้าที่ ที่เชี่ยวชาญ และผ่านการเห็นชอบจากฝ่ายบริหาร ก่อนการจัดซื้อหรือการใช้บริการจะต้องมีการจัดทำ Security Requirement เพื่อคำนึงถึงสิ่งที่องค์กรต้องการให้ผู้ให้บริการรับรองความปลอดภัยต่าง ๆ เช่น SLA, สัญญาการให้บริการ, การผ่านการรับรองความปลอดภัยต่าง ๆ เป็นต้น
- บทบาทและความรับผิดชอบที่เกี่ยวข้องกับการใช้และการจัดการบริการคลาวด์จะต้องถูกจำแนกและจัดการอย่างปลอดภัย
- ผู้ให้บริการจะต้องระบุการควบคุมความปลอดภัยของข้อมูลที่ได้รับการจัดการโดยผู้ให้บริการระบบคลาวด์ และที่ได้รับการจัดการโดยองค์กรในฐานะลูกค้าบริการระบบคลาวด์
- จะต้องมีคู่มือวิธีใช้ความสามารถด้านความปลอดภัยของข้อมูลที่ผู้ให้บริการระบบคลาวด์มอบให้
- จะต้องคำนึงถึงวิธีขอรับการรับประกันเกี่ยวกับการควบคุมความปลอดภัยของข้อมูลที่ดำเนินการโดยผู้ให้บริการระบบคลาวด์
- เจ้าหน้าที่จะต้องคำนึงถึงวิธีจัดการการควบคุม อินเทอร์เฟซ และการเปลี่ยนแปลงบริการเมื่อองค์กรใช้บริการคลาวด์หลายบริการ โดยเฉพาะจากผู้ให้บริการคลาวด์ที่แตกต่างกัน
- จะต้องคำนึงถึงขั้นตอนในการจัดการเหตุการณ์ความปลอดภัยของข้อมูลที่เกิดขึ้นเกี่ยวกับการใช้บริการคลาวด์
- กำหนดให้มีแนวทางในการติดตาม ทบทวน และประเมินการใช้บริการคลาวด์อย่างต่อเนื่องเพื่อจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล
- จะต้องมีวิธีการเปลี่ยนแปลงหรือหยุดการใช้บริการคลาวด์ รวมถึงกลยุทธ์การออกจากบริการคลาวด์
- จะต้องคำนึงถึงข้อตกลงบริการคลาวด์ที่มักถูกกำหนดไว้ล่วงหน้าและไม่เปิดให้เจรจา สำหรับบริการคลาวด์ทั้งหมด องค์กรควรตรวจสอบข้อตกลงการบริการคลาวด์กับผู้ให้บริการคลาวด์ ข้อตกลงบริการคลาวด์ควรจัดการกับข้อกำหนดการรักษาความลับ ความสมบูรณ์ ความพร้อมใช้งาน และการจัดการข้อมูลขององค์กร โดยมีวัตถุประสงค์ระดับบริการคลาวด์ที่เหมาะสมและวัตถุประสงค์เชิงคุณภาพบริการคลาวด์ องค์กรควรดำเนินการประเมินความเสี่ยงที่เกี่ยวข้องเพื่อระบุความเสี่ยงที่เกี่ยวข้องกับการใช้บริการคลาวด์ ความเสี่ยงตกค้างใดๆ ที่เกี่ยวข้องกับการใช้บริการคลาวด์ควรได้รับการระบุและยอมรับอย่างชัดเจนโดยฝ่ายบริหารที่เหมาะสมขององค์กร ข้อตกลงระหว่างผู้ให้บริการคลาวด์และองค์กรซึ่งทำหน้าที่เป็นลูกค้าบริการคลาวด์ควรรวมข้อกำหนดต่อไปนี้สำหรับการปกป้องข้อมูลขององค์กรและความพร้อมใช้งานของบริการ
- การนำเสนอโซลูชั่นตามมาตรฐานที่อุตสาหกรรมยอมรับสำหรับสถาปัตยกรรมและโครงสร้างพื้นฐานจะต้องถูกนำไปวิเคาะห์ทุกครั้งในการเลือกใช้บริการ

- จะต้องจัดให้มีการจัดการควบคุมการเข้าถึงบริการคลาวด์ให้ตรงตามความต้องการขององค์กร
- การใช้โซลูชันการตรวจสอบและป้องกันมัลแวร์ จะต้องถูกนำมาเป็นข้อมูลที่ควรพิจารณา
- ควรคำนึงการประมวลผลและจัดเก็บข้อมูลที่ละเอียดอ่อนขององค์กรในสถานที่ที่ได้รับอนุมัติ (เช่น ประเทศหรือภูมิภาคเฉพาะ) หรือภายในหรืออยู่ภายใต้เขตอำนาจศาลเฉพาะ
- ผู้ให้บริการจะต้องให้การสนับสนุนเฉพาะในกรณีที่เกิดเหตุการณ์ความปลอดภัยของข้อมูลในสภาพแวดล้อมบริการคลาวด์
- ควรคำนึงถึงบริการที่ทำสัญญาช่วงเพิ่มเติมกับซัพพลายเออร์ภายนอก (หรือห้ามไม่ให้บริการคลาวด์ทำสัญญาช่วง
- ผู้ให้บริการจะต้องสนับสนุนองค์กรในการรวบรวมหลักฐานดิจิทัล โดยคำนึงถึงกฎหมายและข้อบังคับสำหรับหลักฐานดิจิทัลในเขตอำนาจศาลต่าง ๆ
- องค์กรซึ่งทำหน้าที่เป็นลูกค้าบริการคลาวด์ ควรพิจารณาว่าข้อตกลงควรกำหนดให้ผู้ให้บริการคลาวด์ต้องแจ้งเตือนล่วงหน้าก่อนที่ลูกค้าสำคัญจะส่งผลกระทบต่อการเปลี่ยนแปลงวิธีการส่งมอบบริการให้กับองค์กรหรือไม่ รวมถึง การเปลี่ยนแปลงโครงสร้างพื้นฐานทางเทคนิค (เช่น การย้ายตำแหน่ง การกำหนดค่าใหม่ หรือการเปลี่ยนแปลงฮาร์ดแวร์หรือซอฟต์แวร์) ที่ส่งผลกระทบหรือเปลี่ยนแปลงข้อเสนอบริการคลาวด์, การประมวลผลหรือจัดเก็บข้อมูลในเขตอำนาจศาลทางภูมิศาสตร์หรือกฎหมายใหม่, การใช้ผู้ให้บริการเพียร์คลาวด์หรือผู้รับเหมาช่วงอื่น ๆ

1.32 นโยบายการบริหารจัดการการจัดการการตั้งค่า Configuration Management

- จะต้องมีการระบุส่วนประกอบการตั้งค่าอุปกรณ์ IT ทั้งหมด (รายการการกำหนดค่า) และการรวมไว้ในฐานข้อมูลการจัดการการกำหนดค่า เพื่อเป็นประโยชน์ต่อการเปลี่ยนแปลงการตั้งค่า
- ควรมีการจัดทำรายการการตั้งค่าสินทรัพย์ไอที ควรประกอบด้วย Hardware Software Information Personnel Service
- จะต้องคำนึงถึงความปลอดภัยของสถานที่จัดเก็บข้อมูล Configuration และควรมีการจำกัดสิทธิ์การเข้าถึง
- จะต้องคำนึงถึงผลลัพท์ของการกู้คือเสมอ หากมีความจำเป็นจะต้องกู้คืนหรือเรียกใช้งาน
- การจัดเก็บข้อมูล Configuration จะต้องมีการวางแผน คำนึงถึงความเป็นไปได้ของพื้นที่จัดเก็บ ความปลอดภัย และผู้ใช้งานอย่างสม่ำเสมอ
- การเปลี่ยนแปลง Configuration ทุก ๆ อุปกรณ์ จะต้องมีการจัดทำ Change Management อยู่เสมอ

- การจัดทำรายการ Configuration ควรคำนึงถึง Version ของ Configuration หรือ รายการก่อนหน้าที่สามารถรับรองว่าใช้งานได้
- ควรมีการลำดับความสำคัญของอุปกรณ์ที่จำเป็นจะต้องมีการสำรองข้อมูล Configuration และควรมีการจัดทำอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง
- Configuration ที่ไม่ได้ใช้งานจะต้องถูกทำลายอย่างปลอดภัย
- จะต้องมีการตรวจสอบ ตรวจทานอุปกรณ์ต่าง ๆ เพื่อติดตามว่าได้มีการใช้งาน Configuration แบบใด เพื่อป้องกันความผิดพลาด อย่างน้อยปีละ 1 ครั้ง

1.33 นโยบายการบริหารจัดการการใช้งานระบบป้องการข้อมูลรั่วไหล Data Leakage Prevention

- จะต้องระบุและจำแนกข้อมูลตามความสำคัญ อ้างอิง “การจำแนกประเภทและการจัดการข้อมูล”
- จะต้องคำนึงถึงการจัดประเภทข้อมูลเกี่ยวข้องกับการระบุประเภทต่าง ๆ และจัดหมวดหมู่ตามความอ่อนไหว คุณค่า และผลกระทบที่อาจเกิดขึ้นกับองค์กร
- ระบุข้อมูลที่สำคัญที่สุด ทีมรักษาความปลอดภัยใช้มาตรการรักษาความปลอดภัยต่าง ๆ เช่น การเข้ารหัสและการควบคุมการเข้าถึง เพื่อป้องกันการเข้าถึงและการโจรกรรมโดยไม่ได้รับอนุญาต การเข้ารหัสเป็นกระบวนการแปลงข้อมูลเป็นรูปแบบที่ไม่สามารถอ่านได้ เพื่อให้เฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงได้ด้วยคีย์ถอดรหัสที่เหมาะสม การควบคุมการเข้าถึงจะจำกัดผู้ที่สามารถเข้าถึงข้อมูลโดยต้องมีการรับรองความถูกต้อง เช่น รหัสผ่านหรือการตรวจสอบยืนยันทางชีวภาพ
- จะต้องใช้การเข้ารหัสเพื่อปกป้องข้อมูลและไฟล์ที่สำคัญ
- การเข้ารหัสทำงานโดยใช้อัลกอริธึมทางคณิตศาสตร์ที่ซับซ้อนกับข้อมูล โดยแปลงเป็นสตริงอักขระต้องเป็นไปตาม “นโยบายการเข้ารหัส (Cryptographic) และ การจัดการกุญแจ (Key Management)”
- ระบบ DLP ที่ใช้งานจะต้องเปิดใช้งานการควบคุมการเข้าถึง
- การควบคุมการเข้าถึงเป็นมาตรการรักษาความปลอดภัยที่จำกัดการเข้าถึงข้อมูลที่ละเอียดอ่อนโดยไม่พึงประสงค์ และรับรองว่าข้อมูลดังกล่าวจะพร้อมใช้งานสำหรับบุคคลที่ได้รับอนุญาตเท่านั้นซึ่งจำเป็นต้องใช้ข้อมูลดังกล่าวเพื่อปฏิบัติหน้าที่ของตน การควบคุมการเข้าถึงอาจมีได้หลายรูปแบบ รวมถึงบัญชีที่มีการป้องกันด้วยรหัสผ่าน การตรวจสอบสิทธิ์แบบหลายปัจจัย และการควบคุมการเข้าถึงตามบทบาท
- ด้วยการใช้การควบคุมการเข้าถึง องค์กรสามารถลดความเสี่ยงของการสูญหายของข้อมูลอันเนื่องมาจากข้อผิดพลาดของมนุษย์หรือการโจมตีที่เป็นอันตราย การควบคุมการเข้าถึงสามารถช่วยป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลที่ละเอียดอ่อน ลดความเสี่ยงของภัยคุกคามจากภายใน และจำกัดความเสียหายที่

เกิดจากการละเมิดข้อมูล ทั้งนี้องค์กรจะต้องดำเนินการประเมินความเสี่ยงการใช้งานระบบ DLP และขั้นตอนที่มีอยู่เพื่อป้องกันข้อมูลรั่วไหล

- ตรวจสอบการเข้าถึงข้อมูล ทีมรักษาความปลอดภัยต้อง การตรวจสอบการเข้าถึงข้อมูลเกี่ยวข้องกับการติดตามว่าใครเข้าถึงข้อมูลที่ละเอียดอ่อน เข้าถึงเมื่อใด และทำอะไรกับข้อมูลนั้น ด้วยการตรวจสอบการเข้าถึงข้อมูลทีมรักษาความปลอดภัยจะต้องระบุการละเมิดข้อมูลที่อาจเกิดขึ้นได้อย่างรวดเร็ว และดำเนินการเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตเพิ่มเติม และรายงานต่อคณะกรรมการ ISMS
- ทีมรักษาความปลอดภัยจะต้องตั้งค่าความพยายามในการเข้าถึงการบันทึก และการวิเคราะห์บันทึกของระบบสามารถช่วยระบุความพยายามในการเข้าถึงที่ไม่ได้รับอนุญาต และจัดทำบันทึกว่าใครเข้าถึงข้อมูลที่ละเอียดอ่อนและเมื่อใด การตรวจสอบบันทึกกิจกรรมของผู้ใช้สามารถให้ข้อมูลเชิงลึกเกี่ยวกับวิธีที่ผู้ใช้โต้ตอบกับข้อมูลที่ละเอียดอ่อน และระบุจุดอ่อนด้านความปลอดภัยหรือการละเมิดนโยบายที่อาจเกิดขึ้น เครื่องมือตรวจสอบแบบเรียลไทม์ จะต้องตรวจจับกิจกรรมที่น่าสงสัยและแจ้งเตือนทีมรักษาความปลอดภัยถึงการละเมิดข้อมูลที่อาจเกิดขึ้นเมื่อเกิดขึ้น
- ให้ความรู้แก่พนักงาน ทีมรักษาความปลอดภัยจะต้องให้ความตระหนักรู้แก่พนักงานซึ่งเป็นองค์ประกอบสำคัญของกลยุทธ์ DLP ที่มีประสิทธิผล ภัยคุกคามที่เลวร้ายที่สุดหลายประการต่อโครงสร้างพื้นฐานด้านไอทีขององค์กรจำเป็นต้องมีข้อผิดพลาดจากมนุษย์จึงจะทำให้เกิดความเสียหายได้จริง ตัวอย่างเช่น การโจมตีด้วยแรนซัมแวร์มักกำหนดให้พนักงานคลิกลิงก์ที่ติดไวรัสหรือดาวน์โหลดไฟล์แนบที่ติดไวรัส การโจมตีจากวงในอาจเกี่ยวข้องกับพนักงานที่จงใจหรือไม่ตั้งใจทำให้ข้อมูลที่ละเอียดอ่อนรั่วไหล
- ทีมรักษาความปลอดภัยจะต้องให้ความรู้แก่พนักงานเกี่ยวกับแนวทางปฏิบัติที่ดีที่สุดด้านความปลอดภัยทางไซเบอร์ องค์กรสามารถลดความเสี่ยงของการสูญหายหรือการโจรกรรมข้อมูลที่เกิดจากข้อผิดพลาดของมนุษย์ ซึ่งอาจรวมถึงการฝึกอบรมเกี่ยวกับวิธีการระบุอีเมลฟิชชิ่ง วิธีหลีกเลี่ยงการคลิกลิงก์หรือไฟล์แนบที่น่าสงสัย วิธีใช้รหัสผ่านที่ปลอดภัย และวิธีใช้การตรวจสอบสิทธิ์แบบหลายปัจจัย
- การดำเนินการตามขั้นตอนการตอบสนองเหตุการณ์ต้องเป็นไปตาม ขั้นตอนการจัดการเหตุการณ์ด้านความปลอดภัย
- แผนตอบสนองต่อเหตุการณ์ การละเมิดข้อมูล ต่อเหตุการณ์โดยทั่วไปประกอบด้วยขั้นตอนต่อไปนี้:
    - การระบุ: ระบุลักษณะและขอบเขตของการละเมิดข้อมูล รวมถึงข้อมูลที่ถูกบุกรุก จำนวนบุคคลที่ได้รับผลกระทบ และวิธีการละเมิดเกิดขึ้น

- การกักกัน: ควบคุมการละเมิดและจำกัดการแพร่กระจายของข้อมูลที่ถูกบุกรุก ซึ่งอาจเกี่ยวข้องกับการแยกระบบที่ได้รับผลกระทบ การปิดบริการที่ได้รับผลกระทบ หรือการดำเนินการอื่น ๆ เพื่อป้องกันข้อมูลสูญหายเพิ่มเติม
- การแจ้งเตือน: แจ้งบุคคลที่ได้รับผลกระทบ หน่วยงานกำกับดูแล และผู้มีส่วนได้ส่วนเสียอื่น ๆ ตามที่กฎหมายและนโยบายของบริษัทกำหนด การแจ้งเตือนควรตรงเวลา ถูกต้อง และให้ข้อมูลที่ชัดเจนเกี่ยวกับลักษณะของการละเมิดและขั้นตอนในการดำเนินการแก้ไข
- การสอบสวน: ดำเนินการสอบสวนอย่างละเอียดเพื่อระบุสาเหตุของการละเมิด ขอบเขตของความเสียหาย และรายละเอียดอื่น ๆ ที่เกี่ยวข้อง ซึ่งอาจเกี่ยวข้องกับการวิเคราะห์ทางนิติเวชของระบบที่ได้รับผลกระทบ การสัมภาษณ์พนักงาน และเทคนิคการสืบสวนอื่น ๆ
- การแก้ไข: ดำเนินการแก้ไขเพื่อป้องกันไม่ให้การละเมิดที่คล้ายกันเกิดขึ้นในอนาคต ซึ่งอาจรวมถึงการแพตช์ช่องโหว่ อัปเกรดการควบคุมความปลอดภัย หรือแก้ไขนโยบายและขั้นตอนต่าง ๆ

1.34 นโยบายการบริหารจัดการการกรองเว็บ Web Filtering

- อุปกรณ์กรองเว็บคืออุปกรณ์หรือซอฟต์แวร์ที่ใช้ในการกรองการรับส่งข้อมูลทางอินเทอร์เน็ตสำหรับเนื้อหา ทีมรักษาความปลอดภัย ใช้ฮาร์ดแวร์และซอฟต์แวร์สำหรับการตรวจสอบไฟร์วอลล์ซึ่งจะตรวจสอบและกรองการรับส่งข้อมูลตาม URL แอปพลิเคชัน และสามารถระบุและตรวจสอบโปรโตคอลได้ บริการจำแนกประเภทเว็บไซต์ใช้เพื่อจัดหมวดหมู่เว็บไซต์ จากนั้นกฎจะถูกตั้งค่าบนไฟร์วอลล์ซึ่งจะบล็อกไซต์ที่ถูกจัดประเภทไว้ในหมวดหมู่นั้น
- นโยบายการกรองเว็บต้องทำตามขั้นตอนรักษาความปลอดภัยขององค์กรและดำเนินการโดยผู้เชี่ยวชาญ
- องค์กรมีสิทธิ์ตรวจสอบการใช้งานอินเทอร์เน็ตจากคอมพิวเตอร์และอุปกรณ์ทั้งหมดที่เชื่อมต่อกับเครือข่ายองค์กร
- องค์กรมีสิทธิ์บล็อกการเข้าถึงเว็บไซต์อินเทอร์เน็ตและโปรโตคอลที่ถือว่าไม่เหมาะสมสำหรับสภาพแวดล้อม
- โปรโตคอลและหมวดหมู่ของเว็บไซต์ต่อไปนี้จะถูกบล็อก มีดังต่อไปนี้
  - เนื้อหาสำหรับผู้ใหญ่/ทางเพศอย่างโจ่งแจ้ง
  - โฆษณาและป๊อปอัป
  - การประมูล
  - แชทและการส่งข้อความโต้ตอบแบบทันที
  - ลัทธิและไสยศาสตร์

- ไซต์ที่ตายแล้ว
- การพนัน
- ยาเสพติดผิดกฎหมาย
- การแชร์ไฟล์แบบเพียร์ทูเพียร์
- ไซต์ที่เป็นอันตรายรวมถึงบอทเน็ต คีย์ล็อกเกอร์ สแปม เนื้อหาไดนามิก ฟิชชิ่ง การฉ้อโกง และสปายแวร์
- ดาวน์โหลดซอฟต์แวร์อันตราย
- เนื้อหาที่น่ารังเกียจและน่ารังเกียจ
- ความรุนแรง และความเกลียดชัง

- ทีมรักษาความปลอดภัยจะตรวจสอบและแนะนำการเปลี่ยนแปลงกฎการกรองเว็บและโปรโตคอล เป็นประจำทุกปี การเปลี่ยนแปลงกฎการกรองเว็บและโปรโตคอลจะถูกบันทึกไว้ในแบบฟอร์มการจัดการการเปลี่ยนแปลง และอัปเดตนโยบายการตรวจสอบและการกรองการใช้อินเทอร์เน็ต และผู้จัดการแผนกจะได้รับแจ้งถึงการเปลี่ยนแปลงนี้เพื่อแจ้งให้พนักงานของตนทราบ
- พนักงานอาจได้รับอนุญาตให้เข้าถึงไซต์ที่ถูกบล็อกได้หากเหมาะสมและจำเป็นสำหรับวัตถุประสงค์ทางธุรกิจ และหากเว็บไซต์นั้นเป็นไปตามมาตรฐานกฎหมายและความปลอดภัย ข้อยกเว้นจะไม่ใช้กับผู้รับเหมาบุคคลที่สามที่ต้องการเข้าถึง

1.35 นโยบายการบริหารจัดการข่าวกรองด้านภัยคุกคาม Threat Intelligence

- ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความปลอดภัยของข้อมูลควรได้รับการรวบรวมและวิเคราะห์เพื่อสร้างข้อมูลภัยคุกคามโดยทีมรักษาความปลอดภัย เพื่อให้ความตระหนักรู้เกี่ยวกับสภาพแวดล้อมภัยคุกคามขององค์กร เพื่อให้สามารถดำเนินการบรรเทาผลกระทบได้อย่างเหมาะสม
- ข้อมูลเกี่ยวกับภัยคุกคามที่มีอยู่หรือที่เกิดขึ้นใหม่จะถูกรวบรวมและวิเคราะห์เพื่ออำนวยความสะดวกในการดำเนินการโดยอาศัยข้อมูลเพื่อป้องกันภัยคุกคามไม่ให้ก่อให้เกิดอันตรายต่อองค์กร และลดผลกระทบของภัยคุกคามดังกล่าว
- ข้อมูลภัยคุกคามสามารถแบ่งออกเป็นสามชั้น ซึ่งควรพิจารณาทั้งหมด:
  - ข้อมูลอัจฉริยะด้านภัยคุกคามเชิงกลยุทธ์: การแลกเปลี่ยนข้อมูลระดับสูงเกี่ยวกับภาพรวมภัยคุกคามที่เปลี่ยนแปลงไป (เช่น ประเภทของผู้โจมตีหรือประเภทการโจมตี)
  - ข้อมูลภัยคุกคามทางยุทธวิธี: ข้อมูลเกี่ยวกับวิธีการ เครื่องมือ และเทคโนโลยีของผู้โจมตีที่เกี่ยวข้อง
  - ข้อมูลภัยคุกคามเชิงปฏิบัติการ: รายละเอียดเกี่ยวกับการโจมตีเฉพาะ รวมถึงตัวบ่งชี้ทางเทคนิค

- ข่าวกรองด้านภัยคุกคามควรจะคำนึงถึง
  - เกี่ยวข้อง เช่น เกี่ยวข้องกับการคุ้มครององค์กร
  - เจาะลึก เช่น ช่วยให้องค์กรมีความเข้าใจที่ถูกต้องและละเอียดเกี่ยวกับภาพรวมภัยคุกคาม
  - ตามบริบท เพื่อให้การรับรู้สถานการณ์ เช่น การเพิ่มบริบทให้กับข้อมูลตามเวลาของเหตุการณ์ สถานที่ที่เกิดขึ้น ประสบการณ์ก่อนหน้านี้ และการเกิดในองค์กรที่คล้ายคลึงกัน
  - นำไปปฏิบัติได้ เช่น องค์กรสามารถดำเนินการกับข้อมูลได้อย่างรวดเร็วและมีประสิทธิภาพ
- กิจกรรมข่าวกรองภัยคุกคามควรประกอบด้วย
  - การสร้างวัตถุประสงค์สำหรับการผลิตข้อมูลภัยคุกคาม (บันทึกใน การประชุม หรือ การประชุมรายสัปดาห์ใน War room หรือ ช่องทางสื่อสารที่ได้กำหนด)
  - การระบุ คัดกรอง และคัดเลือกแหล่งข้อมูลภายในและภายนอกที่จำเป็นและเหมาะสมในการให้ข้อมูลที่จำเป็นสำหรับการผลิตข้อมูลภัยคุกคาม
  - รวบรวมข้อมูลจากแหล่งที่เลือกซึ่งอาจทั้งภายในและภายนอก
  - การประมวลผลข้อมูลที่รวบรวมเพื่อเตรียมพร้อมสำหรับการวิเคราะห์
  - การวิเคราะห์ข้อมูลเพื่อทำความเข้าใจว่าเกี่ยวข้องและมีความหมายต่อองค์กรอย่างไร
  - การสื่อสารและแบ่งปันให้กับบุคคลที่เกี่ยวข้องในรูปแบบที่สามารถเข้าใจได้
- ข้อมูลภัยคุกคามควรได้รับการวิเคราะห์และใช้ในภายหลัง
  - ทีมรักษาความปลอดภัยต้องใช้กระบวนการเพื่อรวมข้อมูลที่รวบรวมจากแหล่งข่าวกรองภัยคุกคามเข้าสู่กระบวนการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลขององค์กร
  - เป็นข้อมูลเพิ่มเติมสำหรับการควบคุมเชิงป้องกันและตรวจจับทางเทคนิค เช่น ไฟร์วอลล์ ระบบตรวจจับการบุกรุก หรือโซลูชันป้องกันมัลแวร์
  - เป็นข้อมูลเข้าสู่กระบวนการและเทคนิคการทดสอบความปลอดภัยของข้อมูล

1.36 นโยบายเกี่ยวกับการใช้งานซอฟต์แวร์มาตรฐาน การอนุญาตให้ใช้งานซอฟต์แวร์ และลิขสิทธิ์

- แม็คกรุ๊ปใช้ซอฟต์แวร์ในทุกด้านของธุรกิจเพื่อสนับสนุนงานที่ดำเนินการโดยพนักงานของบริษัท ซอฟต์แวร์ทุกชิ้นจำเป็นจะต้องได้รับใบอนุญาตในทุกกรณี
- ซอฟต์แวร์คอมพิวเตอร์ต้องถูกซื้อผ่านทางไอที และถูกติดตั้งโดยพนักงานแผนกไอที แผนกไอทีต้องสร้างรายการของซอฟต์แวร์ที่ถูกติดตั้งและต้องมีการอัปเดตรายการนี้ ใบอนุญาตซอฟต์แวร์ทั้งหมดควรได้รับการจัดเก็บไว้ในสถานที่ส่วนกลางที่มีการรักษาความปลอดภัย

- แชร์แวร์ ฟรีแวร์ และ โปรแกรมสาธารณะ ขึ้นต่อนโยบายและขั้นตอนเดียวกันกับซอฟต์แวร์อื่นๆ ผู้ใช้งานจะต้องไม่ติดตั้งซอฟต์แวร์ฟรีหรือซอฟต์แวร์เพื่อการประเมินผลโดยไม่ได้รับการอนุมัติล่วงหน้า
- พนักงานต้องไม่ทำสำเนาของซอฟต์แวร์คอมพิวเตอร์ที่เป็นของแม็คกรุ๊ปเพื่อการใช้งานส่วนตัว

ภาคผนวก

ระเบียบปฏิบัติงานการควบคุมการเข้าถึงพื้นที่สำนักงาน และแนวทางการปฏิบัติงานในพื้นที่การรักษาความมั่นคงปลอดภัย สำหรับ บริษัท แม็คกรุ๊ป จำกัด (มหาชน)

การเข้าถึงพื้นที่รักษาความปลอดภัยเช่นห้องอุปกรณ์ไอทีต้องได้รับการควบคุมอย่างเหมาะสม และการเข้าถึงทางกายภาพสู่สิ่งปลูกสร้างต้องถูกจำกัดให้เฉพาะผู้ที่ได้รับมอบอำนาจเท่านั้น พนักงานที่ทำงานในพื้นที่รักษาความปลอดภัยควรพร้อมที่จะตรวจตราทุกคนที่ไม่รู้จักและ/หรือไม่สวมตราเครื่องหมาย แต่ละแผนกต้องตรวจสอบให้แน่ใจว่าประตูและหน้าต่างได้รับการรักษาความปลอดภัยอย่างเหมาะสม

- ตราเครื่องหมาย/กุญแจ (ควรถูกลงชื่อ/ตรวจสอบอย่างสม่ำเสมอ) และรหัสการเข้าออก ฯลฯ ต้องได้รับการเก็บรักษาไว้โดยพนักงานที่ได้รับอนุญาตให้เข้าถึงพื้นที่เหล่านั้นและไม่ควรมีการให้ยืม/มอบให้กับบุคคลอื่น บุคลากรที่ทำงานในพื้นที่ที่ปลอดภัยต้อมีความรู้เกี่ยวกับปัญหาด้านสุขภาพและความปลอดภัยทั้งหมดในพื้นที่รักษาความปลอดภัย เช่น การไล่ก๊าซ และปฏิบัติตามกระบวนการที่เกี่ยวข้องทั้งหมด
- ผู้มาติดต่อในพื้นที่รักษาความปลอดภัยจะต้องลงชื่อเข้าและออกพร้อมกับเวลาที่เข้ามาและออกไป และจำเป็นต้องแขวนป้ายประจำตัว พนักงานของแม็คกรุ๊ปควรตรวจสอบผู้มาติดต่อทั้งหมดที่เข้าถึงพื้นที่ไอทีที่มีการักษาความปลอดภัยอยู่ตลอดเวลา
- ควรมีการประเมินความเสี่ยงเกี่ยวกับสภาพแวดล้อมและสถานที่รอบๆ บริเวณ จุดสำคัญที่ต้องพิจารณาได้แก่:
    - ธุรกิจในท้องถิ่นที่มีความเสี่ยงสูง เช่น งานเกี่ยวกับแก๊ส
    - ความเสี่ยงด้านสิ่งแวดล้อม
    - ที่ตั้งของสำนักงานในอาคารที่ใช้ร่วมกัน

ความปลอดภัยของอุปกรณ์

อุปกรณ์คอมพิวเตอร์ทั่วไปทั้งหมดต้องอยู่ในตำแหน่งทางกายภาพที่เหมาะสมซึ่ง:

- ลดความเสี่ยงจากอันตรายทางสิ่งแวดล้อม เช่น ความร้อน ไฟ ควัน น้ำ ฝุ่น และการสั่นสะเทือน
- ลดความเสี่ยงในการถูกโจรกรรม ตัวอย่างเช่น อุปกรณ์จำพวกพวกแล็ปท็อปควรได้รับการยึดติดกับโต๊ะทำงานหากจำเป็น
- อำนวยความสะดวกด้านเวิร์กสเตชันที่จัดการข้อมูลที่มีความสำคัญในตำแหน่ง เพื่อกำจัดความเสี่ยงต่อการที่บุคคลอื่นๆ ซึ่งไม่ได้รับอนุญาตได้รู้เห็นข้อมูล

- คอมพิวเตอร์ตั้งโต๊ะไม่ควรเก็บข้อมูลของผู้ใช้ไว้ในฮาร์ดไดรฟ์ภายในเครื่อง ข้อมูลของผู้ใช้ควรถูกจัดเก็บไว้ในเซิร์ฟเวอร์เครือข่ายเพื่อให้แน่ใจว่าข้อมูลที่สูญหายจากการถูกขโมยหรือเสียหายจากการถูกเข้าถึงโดยไม่ได้รับอนุญาตจะสามารถถูกเรียกกลับคืนมาได้โดยสมบูรณ์ ข้อมูลผู้ใช้ที่ต้องอยู่ในฮาร์ดดิสก์ของเครื่องแล็ปท็อปต้องได้รับการสำรองข้อมูลเป็นประจำ
- แล็ปท็อปและอุปกรณ์เคลื่อนที่จะต้องถูกนำออกจากโต๊ะทำงานและเก็บไว้อย่างปลอดภัยหากถูกทิ้งไว้ในสำนักงานหลังจากเวลาทำการปกติ
- ในกรณีที่บริษัทเป็นเจ้าของอุปกรณ์ที่สูญหายหรือถูกโจรกรรม จำเป็นต้องดำเนินการดังต่อไปนี้:
    - แจ้งแผนกไอทีและหัวหน้างานของท่านให้ทราบทันทีเกี่ยวกับความสูญเสียหรือความเสียหายต่อเครื่องคอมพิวเตอร์
    - ภายใน 24 ชั่วโมงหลังจากเกิดความสูญเสียหรือความเสียหายต่อเครื่องคอมพิวเตอร์ ให้ส่งรายงานที่เป็นลายลักษณ์อักษร ให้แก่ผู้ตรวจการและแผนกไอทีในทันที โดยระบุถึงสถานการณ์การสูญหายหรือความเสียหาย
- หากพบว่าการสูญหายหรือความเสียหายต่ออุปกรณ์เกิดจากความประมาท การใช้งานที่ไม่ถูกต้อง หรือความไม่รับผิดในการใช้งานของพนักงาน บริษัทจะเรียกเก็บเงินจากพนักงานสำหรับ:
    - จำนวนเงินที่จำเป็นในการซ่อมแซมอุปกรณ์ในกรณีที่เกิดความเสียหาย หรือ
    - ราคาตามบัญชีหรือราคาตามตลาดของอุปกรณ์ในขณะที่เกิดความเสียหาย แล้วแต่ว่าจำนวนใดจะสูงกว่า
    - พนักงานสามารถซื้ออุปกรณ์ที่มีรุ่นปีและสภาพอุปกรณ์เดียวกัน เพื่อทดแทนอุปกรณ์ที่สูญหายหรือเสียหายภายใน 30 วันได้ สภาพของอุปกรณ์ที่จะนำมาแทนที่ต้องได้รับการอนุมัติโดยผู้จัดการไอที
- อุปกรณ์ทั้งหมดต้องได้รับการทำเครื่องหมายการรักษาความปลอดภัยและมีหมายเลขอุปกรณ์ที่ไม่ซ้ำกัน หมายเลขอุปกรณ์นี้ควรได้รับการบันทึกไว้ในบัญชีสินทรัพย์
- อุปกรณ์เซิร์ฟเวอร์ควรได้รับการป้องกันจากเหตุไฟฟ้าดับโดยใช้แหล่งพลังงานสำรอง ตัวอย่างเช่น อุปกรณ์ไฟฟ้าสำรอง(ยูพีเอส) ควรมีการทดสอบเป็นประจำเพื่อให้ยูพีเอสทำงานได้อย่างถูกต้อง
- อุปกรณ์ที่สำคัญควรถูกทำสัญญาการบำรุงรักษาที่เหมาะสมกับผู้จัดหาที่ได้รับการอนุมัติ

ความปลอดภัยของสายไฟและสายเคเบิล

- สายไฟและสายเคเบิลที่มีข้อมูลหรือรองรับพื้นที่ทางธุรกิจที่สำคัญจะต้องได้รับการปกป้องจากการดักข้อมูลหรือความเสียหาย สายไฟควรถูกแยกออกจากสายเคเบิลเครือข่ายเพื่อป้องกันการรบกวน

- สายเคเบิลเครือข่ายควรได้รับการปกป้องโดยท่อส่งและหากเป็นไปได้ให้หลีกเลี่ยงเส้นทางที่ผ่านทางสาธารณะหรือบริเวณที่มีความเสี่ยงด้านสิ่งแวดล้อมสูงขึ้น การเข้าถึงแผงต่อควรได้รับการจำกัดเฉพาะสมาชิกที่ได้รับอนุญาตเท่านั้น

การบำรุงรักษาอุปกรณ์

- บันทึกประวัติการรักษาอุปกรณ์ควรได้รับการเก็บรักษาไว้เพื่อช่วยให้สามารถตัดสินใจเกี่ยวกับเวลาที่เหมาะสมในการเปลี่ยนอุปกรณ์ได้เมื่ออุปกรณ์มีอายุการใช้งานมากขึ้น
- การบำรุงรักษาอุปกรณ์ต้องเป็นไปตามคำแนะนำของผู้ผลิต ต้องมีการจัดทำเป็นเอกสารและเตรียมพร้อมให้แก่เจ้าหน้าที่ฝ่ายสนับสนุนเพื่อใช้ในการจัดซ่อม เช่น เซิร์ฟเวอร์ที่อยู่ภายใต้ข้อตกลงการสนับสนุนและการบำรุงรักษา
- ระดับของสัญญาการบำรุงรักษาในสถานที่ต้องเชื่อมโยงกับความสำคัญของระบบต่อธุรกิจ และเกี่ยวข้องกับการสนับสนุนแผนการกู้คืนความเสียหายและแผนธุรกิจต่อเนื่อง

ความรับผิดชอบของพนักงานและผู้ทำสัญญา

ความรับผิดชอบตกเป็นของผู้ใช้ในการป้องกันการเข้าถึงระบบแม็คกรุ๊ปโดยไม่ได้รับอนุญาต โดยการ:

- ใช้รหัสผ่านที่รัดกุม
- ไม่ทิ้งสิ่งใดไว้บนหน้าจอที่อาจมีข้อมูลการเข้าถึง เช่น ชื่อล็อกอินและรหัสผ่าน
- ตรวจดูให้แน่ใจว่าได้มีการล็อกเอาท์ออกจากเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งาน
- ผู้ทำสัญญาทุกคนในสถานที่ต้องปฏิบัติตามนโยบายความปลอดภัยของแม็คกรุ๊ป และต้องถูกควบคุมดูแลอยู่ตลอดเวลา
- หากจำเป็นต้องเข้าถึงระบบข้อมูลเพื่อปฏิบัติหน้าที่ การเข้าถึงข้อมูลที่ได้รับอนุญาตควรถูกจำกัดเพื่อให้แน่ใจว่ามีเพียงข้อมูลที่จำเป็นเท่านั้นที่จะได้รับการจัดเตรียมให้
- การควบคุมที่จำเป็นทั้งหมดเพื่อปกป้องข้อมูลของแม็คกรุ๊ปต้องได้รับการทำสัญญากับผู้จัดจ้างหรือบุคคลที่ 3

การบริหารการเข้าถึง การออกใบรับรอง และการสิ้นสุด

- ผู้ใช้แต่ละรายต้องได้รับการจัดสรรสิทธิการเข้าถึงและการอนุญาตไปยังระบบคอมพิวเตอร์และข้อมูลที่เหมาะสมกับงานที่คาดว่าพวกเขาจะกระทำ
- มีการเข้าสู่ระบบที่ไม่ซ้ำกันซึ่งจะไม่ถูกใช้ร่วมกันหรือถูกเปิดเผยแก่ผู้ใช้รายอื่น

- มีรหัสผ่านเฉพาะที่จะถูกร้องขอในการเข้าสู่ระบบใหม่แต่ละครั้ง
- สิทธิในการเข้าถึงของผู้ใช้ต้องได้รับการตรวจสอบเป็นระยะ (ทุกสองปี) โดยผู้ที่ได้รับมอบอำนาจเพื่อให้แน่ใจว่าได้มีการจัดสรรสิทธิที่เหมาะสม บัญชีที่มีสิทธิพิเศษจะถูกจัดให้แก่ผู้ใช้ที่จำเป็นต่องานบริหารจัดการระบบเท่านั้น
- คำขอเพื่อเข้าถึงระบบคอมพิวเตอร์ของแม็คกรุ๊ป ต้องได้รับการอนุมัติโดยผู้จัดการสายงาน ผู้ดูแลข้อมูล หรือผู้ที่ได้รับมอบอำนาจอื่นๆ ที่ระบุ เช่น สำหรับใบสมัครเพื่อขออนุมัติโดยเฉพาะ
- เมื่อพนักงานได้ออกจากบริษัท การเข้าถึงระบบไอทีและข้อมูลของพวกเขาจะถูกระงับในวันสิ้นสุดการทำงานของพนักงาน การปิดใช้งานบัญชีจะเป็นไปตามขั้นตอนเฉพาะที่อธิบายไว้ใน "กระบวนการจัดการสิทธิด้านไอที"

การเข้าถึงแอพพลิเคชัน ฐานข้อมูล และระบบปฏิบัติการ

การเข้าถึงระบบปฏิบัติการต้องถูกควบคุมโดยกระบวนการล็อกอินที่ปลอดภัย การควบคุมการเข้าถึงที่ถูกกำหนดไว้ในส่วนการจัดการโพรไฟล์ผู้ใช้และส่วนของรหัสผ่านจะถูกนำมาใช้งาน

ขั้นตอนการเข้าสู่ระบบต้องได้รับการป้องกันโดย:

- จำนวนครั้งที่ไม่สำเร็จและล็อคบัญชีหากเกินจำนวนนั้น
- ตัวอักษรของรหัสผ่านจะถูกซ่อนโดยสัญลักษณ์
- แสดงคำเตือนทั่วไปเพื่อเตือนว่าอนุญาตให้ใช้งานเฉพาะผู้ใช้ที่ได้รับสิทธิเท่านั้น
- หากเป็นไปได้ อย่าเก็บข้อมูลการเข้าสู่ระบบก่อนหน้านี้ไว้ ตัวอย่างเช่น ชื่อผู้ใช้
- การเข้าใช้งานระบบปฏิบัติการทั้งหมดจะผ่านล็อกอินไอดีที่ไม่ซ้ำกัน ซึ่งจะได้รับการตรวจสอบในช่วงเวลาที่กำหนด (และสามารถสืบหาถึงบุคคลที่รับผิดชอบได้)
- ผู้ดูแลระบบต้องมีบัญชีผู้ดูแลระบบส่วนตัวที่สามารถได้รับการบันทึกและตรวจสอบได้ บัญชีผู้ดูแลระบบต้องไม่ถูกใช้งานโดยบุคคลทั่วไปในกิจกรรมประจำวัน

การตั้งค่าความปลอดภัยเฉพาะระบบ

ระบบไอทีที่เฉพาะต้องมีการตั้งค่าความปลอดภัยส่วนบุคคลในการนำมาใช้เพื่อเพิ่มความปลอดภัยและปกป้องระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

เพื่อให้เอกสารนี้เป็นไปโดยย่อและหลีกเลี่ยงการอัปเดตบ่อยครั้ง การตั้งค่าความปลอดภัยเหล่านี้จะถูกอธิบายไว้ในเอกสารนโยบายแยกต่างหาก “IT System Specific Security”

การจัดการโพรไฟล์ผู้ใช้งาน

- การเพิ่มเติม การปรับเปลี่ยน และการลบผู้ใช้งาน
    - การจัดสรร การแก้ไข และการต่ออายุโพรไฟล์ของผู้ใช้งานควรถูกควบคุมโดยขั้นตอนการจัดการอย่างเป็นทางการซึ่งอนุญาตให้แผนกไอทีหรือระบบช่วยเหลือตรวจสอบข้อมูลประจำตัวของผู้ร้องขอได้
- การตรวจสอบผู้ใช้เป็นระยะ (การดูแลทำบัญชีต่างๆ)
    - สิทธิในการเข้าถึงของผู้ใช้ต้องได้รับการตรวจสอบเป็นระยะ (ทุกปี) โดยผู้ที่ได้รับมอบอำนาจ เพื่อให้แน่ใจว่ามีการจัดสรรสิทธิที่เหมาะสม บัญชีที่มีสิทธิพิเศษจะถูกจัดให้แก่ผู้ใช้ที่จำเป็นต่องานบริหารจัดการระบบเท่านั้น

นโยบายและขั้นตอนการเป็นเจ้าของข้อมูล

คุณภาพและความถูกต้องของการตัดสินใจของบริษัทอาจไม่ได้ดีไปกว่าคุณภาพของข้อมูลที่เป็นพื้นฐานในการตัดสินใจเหล่านั้น ดังนั้น ข้อมูลของเราจะได้รับการวางแผนสำหรับการเก็บ ประมวลผล จัดการ และป้องกันในฐานะทรัพยากรที่มีค่า แม็คกรุ๊ปเป็นเจ้าของข้อมูลทั้งหมดที่ถูกเก็บรวบรวมโดยและภายในแม็คกรุ๊ป โดยไม่คำนึงถึงวิธีการจัดเก็บหรือขนาดของคอลเลกชั่น ข้อมูลนี้เป็นสินทรัพย์ที่มีค่าของบริษัทซึ่งจะถูกใช้งานในการสนับสนุนธุรกิจของแม็คกรุ๊ป

เจ้าของข้อมูลหรือผู้ดูแลข้อมูล

ผู้ดูแลข้อมูล เป็นพนักงานระดับสูงของแม็คกรุ๊ป ที่ดูแลวงจรชีวิตของข้อมูลสถาบันอย่างน้อยหนึ่งชุด

ฟังก์ชันการจัดการข้อมูล

การจัดการข้อมูลคือการพัฒนา การบำรุงรักษา และการควบคุมฐานข้อมูล ผู้จัดการข้อมูลสามารถยกเลิกหรือเพิ่มสิทธิการเข้าถึงและกำหนดระดับการเข้าถึงที่เหมาะสมเพื่อให้บุคลากรสามารถรับข้อมูลที่ต้องการได้โดยไม่ต้องเข้าถึงเนื้อหาที่ละเอียดอ่อน ผู้จัดการข้อมูลต้องวางแผนล่วงหน้าสำหรับการเติบโตรวมทั้งความต้องการในการเข้าถึงดังต่อไปนี้:

ข้อมูล	เงื่อนไข	การบริหาร
โฟลเดอร์ที่ใช้งานร่วมกันในเซิร์ฟเวอร์กลาง	ข้อมูลที่อนุญาติให้อยู่บนเซิร์ฟเวอร์กลางจะต้องมีอายุและการเรียกใช้ล่าสุดน้อยกว่า 3 ปี นับจากวันที่ปัจจุบัน	โดยข้อมูลที่มากกว่า 2 ปีจะได้รับการสำรองไปยังหน่วยงานด้านนอกที่เชื่อถือได้ การเรียกคืนข้อมูลจะใช้เวลา 1 วันทำการ นับจากวันที่ร้องขอ

ข้อมูล	เงื่อนไข	การบริหาร
	ข้อมูลที่อยู่บนเซิร์ฟเวอร์กลาง อายุน้อยกว่า 3 ปี และมีการใช้งานพื้นที่มากกว่าหรือเท่ากับ 80% ของพื้นที่โดยรวมทั้งหมด	จะต้องได้รับการขยายพื้นที่ เพื่อให้เพียงพอต่อปริมาณการใช้งานในอนาคต

สิทธิในการเข้าถึง

ผู้ที่ได้รับมอบอำนาจสามารถเข้าถึงข้อมูลสำหรับธุรกิจหรือข้อมูลส่วนบุคคลได้โดยมีเงื่อนไขว่าพวกเขาจะ:

- ไม่ทำอันตรายต่อความปลอดภัยของบริษัทหรือข้อมูลลูกค้าที่เป็นความลับใดๆ ซึ่งอาจมีอยู่ในคอมพิวเตอร์
- ไม่ละเมิดนโยบายใดๆ ของบริษัท
- ไม่มีส่วนร่วมในกิจกรรมที่ผิดกฎหมายหรือกิจกรรมโลกีย์
- ไม่มีส่วนร่วมในผลประโยชน์ทางธุรกิจภายนอก

ข้อกำหนดในการตั้งชื่อสำหรับบัญชีผู้ใช้งาน

เพื่อรับประกันการตั้งชื่อบัญชีผู้ใช้งานที่ตรงตามหลักการภายในระบบไอทีของแม็คกรุ๊ป ข้อกำหนดในการตั้งชื่อสำหรับบัญชีผู้ใช้งานต่อไปนี้ต้องถูกนำมาใช้เมื่อมีการสร้างบัญชีผู้ใช้งาน

ประเภท	กฎ	ตัวอย่าง
บัญชีผู้ใช้งานส่วนบุคคล ที่ไม่ได้รับสิทธิพิเศษ	ชื่อต้นและอักษรตัวแรกของนามสกุล ถูกคั่นด้วยจุด (.) ในกรณีที่มีชื่อผู้ใช้ซ้ำกัน ตัวอักษรของนามสุลจะถูกเพิ่มจนกว่าจะมีการสร้างชื่อบัญชีผู้ใช้ที่ไม่ซ้ำกัน	Somchai Thongdee = Somchai.T, Somchai.Th, Somchai.Tho
บัญชีผู้ใช้งานส่วนบุคคล ที่ได้รับสิทธิพิเศษ เช่น) (ผู้ดูแลระบบ	กฎเดียวกันกับด้านบน เพียงแต่เปลี่ยนจากนามสกุลเป็นคำว่า local	Somchai Thongdee = Somchai.local

ประเภท	กฎ	ตัวอย่าง
ที่อยู่อีเมล์ส่วนบุคคล	กฎเดียวกันกับบัญชีผู้ใช้ตามด้วยโดเมนของอีเมล์	Somchai Thongdee = somchai.t@mcgroupnet.com
บัญชีบริการ	ชื่อบริการ คั่นด้วย . ตามด้วยคำว่า service	Service account for Kaspersky virus protection = kaspersky.service
กล่องข้อความและรายชื่ออีเมล์แบบกลุ่มที่ใช้ร่วมกัน	จะได้รับการเห็นชอบและอนุมัติจากฝ่ายบริหารด้านไอทีเป็นรายบุคคล	Shared mailbox for HR = hr@mcgroupnet.com
บัญชีที่ใช้ร่วมกัน	ชื่อที่เป็นกลางโดยไม่ระบุตัวบุคคล อาจจะเป็นชื่อแผนก หรือชื่อประเภทการใช้งาน ในกรณีที่มีชื่อผู้ใช้ซ้ำกันหรือหลายมีบัญชีที่จำเป็นสำหรับวัตถุประสงค์เดียวกัน หมายเลขการทำงานจะถูกเพิ่มเข้ามา	Shared account for Accounting in Navision = account, account1, account2
บัญชีผู้ใช้งาน SAP	อักษรไม่เกินแปดตัวแรกของชื่อตามด้วยจุดและอักษรสามตัวแรกของนามสกุล	Somchai Thongdee = somchai.tho

พารามิเตอร์ของรหัสผ่าน / ความปลอดภัยของรหัสผ่าน

การจัดสรรและการต่ออายุรหัสผ่านควรได้รับการควบคุมผ่านขั้นตอนการจัดการอย่างเป็นทางการซึ่งอนุญาตให้ฝ่ายไอทีหรือระบบช่วยเหลือตรวจสอบข้อมูลประจำตัวของผู้ร้องขอ ผู้ใช้งานทุกคนต้องใช้รหัสผ่านที่รัดกุมในการเข้าสู่ระบบและแอพพลิเคชันด้านไอที

บัญชีผู้ใช้แอคทีฟไดเร็กตอรีที่แม็คกรุ๊ปอยู่ภายใต้นโยบายรหัสผ่านที่มีพารามิเตอร์ดังต่อไปนี้:

พารามิเตอร์	คำอธิบาย	การตั้งค่า
รหัสผ่านต้องเป็นไปตามข้อกำหนดที่ซับซ้อน	รหัสผ่านต้องมีอักขระอย่างน้อยสามประเภทต่อไปนี้: • ตัวพิมพ์ใหญ่ (A ถึง Z) • ตัวพิมพ์เล็ก (a ถึง z) • ตัวเลข (0 ถึง 9) • อักขระพิเศษ !เช่น), $, #,%) • อักขระยูนิโค้ดใดๆที่จัดอยู่ในประเภทตัวอักษร แต่ไม่ใช่ตัวพิมพ์ใหญ่หรือตัวพิมพ์เล็ก (เช่นภาษาไทย)	เปิด
ความยาวขั้นต่ำของรหัสผ่าน	จำนวนอักขระอย่างน้อยที่สุดที่อาจใช้เป็นรหัสผ่าน	8 ตัวอักษร
อายุสูงสุดของรหัสผ่าน	เวลาจนกว่าผู้ใช้จะถูกบังคับให้เปลี่ยนรหัสผ่าน	90 วัน
อายุต่ำสุดของรหัสผ่าน	เวลาที่สามารถเปลี่ยนรหัสผ่านได้อีกครั้งหลังจากการเปลี่ยนรหัสผ่านสำเร็จ	1 วัน
รีเซ็ตตัวนับการล็อกบัญชีหลังจาก	เวลาที่ต้องผ่านไปหลังจากความพยายามในการเข้าสู่ระบบล้มเหลวก่อนที่ตัวนับความพยายามในการเข้าสู่ระบบที่ล้มเหลวจะถูกรีเซ็ตเป็นศูนย์	60 นาที
บังคับใช้งานประวัติของรหัสผ่าน	จำนวนของรหัสผ่านที่พึ่งใช้ซึ่งไม่สามารถใช้เป็นรหัสผ่านใหม่ได้	5 ครั้ง
เกณฑ์การล็อกบัญชี	จำนวนครั้งในการเข้าสู่ระบบที่ล้มเหลวซึ่งจะทำให้บัญชีผู้ใช้งานถูกล็อก	3 ครั้ง
ระยะเวลาการล็อกบัญชี	จำนวนนาทีที่บัญชีที่ถูกล็อคยังคงถูกล็อคก่อนที่จะถูกปลดล็อกโดยอัตโนมัติ	60 นาที

พารามิเตอร์	คำอธิบาย	การตั้งค่า
การตรวจสอบสิทธิ์แบบหลายปัจจัย (MFA)	มาตรการรักษาความปลอดภัยเพิ่มเติมเพื่ออนุมัติการเข้าสู่ระบบในอุปกรณ์แยกต่างหากโดยใช้รหัสที่มีให้โดยแอป (แนะนำ) หรือผ่านทาง SMS	เปิด (ถ้ามีตัวเลือก)

ควรเปลี่ยนรหัสผ่านเป็นประจำทุกช่วงเวลา เช่น ทุก 90 วันหรือในทันทีหากมีความเสี่ยงต่อการถูกบุกรุก รหัสผ่านควรได้รับความคุ้มครองและผู้ใช้งานไม่ควรกระทำการดังนี้:

- เปิดเผยรหัสผ่านให้กับผู้ใดก็ตาม
- ใช้ฟังก์ชั่น 'จดจำรหัสผ่าน' ในแอพพลิเคชันบางอย่าง
- จดรหัสผ่านหรือเก็บรหัสผ่านไว้ในที่ที่เสี่ยงต่อการถูกขโมย
- เก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์โดยไม่มีการเข้ารหัส
- ใช้รหัสผ่านเดียวกันเพื่อเข้าถึงระบบต่างๆ
- ใช้รหัสผ่านเดียวกันสำหรับระบบภายในและภายนอกที่ทำงาน
- ข้อยกเว้นในนโยบายรหัสผ่านด้านบนต้องได้รับการอนุมัติจากผู้บริหารระดับสูงของแม็คกรุ๊ป จะถูกอธิบายไว้ในเอกสารนโยบายแยกต่างหาก ที่เรียกว่า "IT User Exception List Policy"

การตรวจสอบเครือข่าย

การจัดการเครือข่ายมีความสำคัญต่อการจัดหาบริการด้านไอทีของแม็คกรุ๊ป และควรใช้งานการควบคุมดังต่อไปนี้:

- ความรับผิดชอบในการดำเนินงานของเครือข่ายควรถูกแยกออกจากกิจกรรมการดำเนินงานด้วยคอมพิวเตอร์หากเป็นไปได้
- เครือข่ายต้องได้รับการตรวจสอบอย่างละเอียดสำหรับปัญหาต่างๆ
- ต้องมีการควบคุมเพื่อป้องกันข้อมูลที่ส่งผ่านเครือข่ายตามสมควร เช่น การเข้ารหัส
- สถาปัตยกรรมเครือข่ายต้องได้รับการจัดทำเป็นเอกสารและถูกจัดเก็บไว้ด้วยการตั้งค่าระบบของส่วนประกอบฮาร์ดแวร์และซอฟต์แวร์ทั้งหมดที่ประกอบกันขึ้นเป็นเครือข่าย
- เครือข่ายไร้สายต้องใช้การควบคุมอย่างเข้มงวดเพื่อปกป้องข้อมูลที่ส่งผ่านเครือข่ายและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเข้ารหัสลับต้องถูกนำมาใช้งานในเครือข่ายเพื่อป้องกันไม่ให้ข้อมูลถูกดักจับ มาตรฐาน

สำหรับเครือข่ายไร้สายจะได้รับการควบคุมและบำรุงรักษาโดยแผนกไอที และการใช้งานระบบเครือข่ายทั้งหมดจะต้องเป็นไปตามมาตรฐานเหล่านี้

ประเภทเครื่อข่าย	เงื่อนไข
เครื่องข่ายสาย	จำกัดให้ใช้งานได้กับอุปกรณ์ของแม็คกรุ๊ปที่ได้รับการอนุญาติแล้วเท่านั้น เช่น - อุปกรณ์เครื่องเซิร์ฟเวอร์จะต้องติดตั้งอยู่ในห้องที่มีการควบคุมการเข้าถึงเป็นพิเศษ - คอมพิวเตอร์ทั้งแบบตั้งโต๊ะและพกพา จะต้องเข้าร่วมระบบ Domain - โทรศัพท์ตั้งโต๊ะ, ปริ้นเตอร์, กล้องวงจรปิด และอื่นๆ จะต้องได้รับการบันทึกและอนุญาติจากเจ้าหน้าที่เครื่อข่าย

การเข้าถึงจากระยะไกล

ในกรณีที่จำเป็นต้องมีการเข้าถึงเครือข่ายของแม็คกรุ๊ปจากระยะไกล แอพพลิเคชันจะต้องถูกดำเนินการผ่านแผนกไอทีโดยผ่านบัตรผ่านของระบบช่วยเหลือ การเข้าถึงเครือข่ายจากระยะไกลต้องได้รับการรักษาความปลอดภัยโดยใช้แอพพลิเคชันที่มีความปลอดภัย เช่น FortiClient สำหรับ VPN และ Citrix

บริษัทคู่ค้าหรือผู้จัดหาที่เป็นบุคคลที่สาม จะต้องไม่ได้รับรายละเอียดเกี่ยวกับวิธีเข้าถึงเครือข่ายของแม็คกรุ๊ปหากไม่ได้รับอนุญาตจากฝ่ายไอที การเปลี่ยนแปลงใดๆ ในการเชื่อมต่อของผู้จัดหาจะต้องถูกส่งต่อไปยังฝ่ายไอทีโดยตรงเพื่อให้การเข้าถึงสามารถอัพเดตหรือถูกยกเลิกได้

การตรวจสอบความปลอดภัยสำหรับการบำรุงรักษาไอดีของผู้ใช้งานและการควบคุมรหัสผ่าน

บันทึกการตรวจสอบควรถูกเก็บไว้อย่างน้อยหกเดือนซึ่งจะบันทึกข้อยกเว้นและเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยอื่นๆ ที่เป็นไปได้ในทางเทคนิคและเป็นประโยชน์ในการดำเนินการดังกล่าว บันทึกการตรวจสอบควรประกอบด้วยข้อมูลดังต่อไปนี้:

- เอกลักษณ์ของระบบ
- ไอดีของผู้ใช้งาน
- การเข้าสู่ระบบที่ประสบความสำเร็จ/ไม่สำเร็จ

- การออกจากระบบที่ประสบความสำเร็จ/ไม่สำเร็จ
- การเข้าถึงแอพพลิเคชันที่ไม่ได้รับอนุญาต
- การเปลี่ยนแปลงการกำหนดค่าระบบ
- การใช้บัญชีแบบพิเศษ (เช่น การจัดการบัญชี การเปลี่ยนแปลงนโยบาย การกำหนดค่าอุปกรณ์)
- การเข้าถึงบันทึกต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาตซึ่งอาจส่งผลให้ข้อมูลที่บันทึกถูกแก้ไขหรือถูกลบออก
- ควรตรวจสอบข้อผิดพลาดของระบบผ่านระบบช่วยเหลือไอที และติดตามและตรวจสอบผ่านระบบที่เหมาะสม การดำเนินการที่สำคัญระหว่างการแก้ไขปัญหาความผิดพลาดควรได้รับการบันทึกและอ้างอิงโยงกับกรณีที่คล้ายกันก่อนหน้านี้
- กระบวนการบันทึกที่ผิดพลาดควรได้รับการป้อนเข้าสู่กระบวนการจัดการเหตุการณ์ของระบบเพื่อการดำเนินการขั้นต่อไปหากจำเป็น

ระเบียบการปฏิบัติการทางคอมพิวเตอร์

การประมวลผลของงาน

การประมวลผลของงานต้องถูกกระทำโดยผู้ใช้งานที่ได้รับอนุญาต

การสำรองข้อมูลและการกู้คืน

จำเป็นต้องมีการสำรองข้อมูลทางธุรกิจที่สำคัญอย่างสม่ำเสมอเพื่อให้มั่นใจว่าแม็คกรุ๊ปจะสามารถกู้คืนจากภัยพิบัติ ระบบล้มเหลว หรือข้อผิดพลาดอื่นๆได้ ขั้นตอนการสำรองข้อมูลได้ถูกนำเสนอในขั้นตอนการกู้คืนภัยพิบัติ พนักงานทุกคนต้องทำให้แน่ใจว่าข้อมูลทางธุรกิจที่จำเป็นทั้งหมดที่มีอยู่ในพีซีและแล็ปท็อปได้รับการสำรองไว้

การจัดการอุบัติการณ์และปัญหา

ระบบข้อมูลและข้อมูลของแม็คกรุ๊ปต้องได้รับการปกป้องจากอุบัติการณ์ด้านความปลอดภัยที่เกิดขึ้นจริงหรือที่สงสัยว่าอาจเกิดขึ้นได้ คำนิยามของอุบัติการณ์คือเหตุการณ์อันไม่พึงประสงค์ที่ก่อให้เกิดหรือมีศักยภาพก่อความเสียหายในทรัพย์สิน ชื่อเสียง และ/หรือบุคลากรขององค์กร

การจัดการเหตุการณ์ในด้านไอทีนั้นเกี่ยวข้องกับการบุกรุก ความเป็นอันตราย และการใช้ทรัพยากรสารสนเทศและข้อมูลอย่างไม่ถูกต้อง และความต่อเนื่องของระบบสารสนเทศที่สำคัญและกระบวนการ

เหตุการณ์และจุดอ่อนด้านความปลอดภัยของข้อมูลจะต้องถูกรายงานไปยังจุดศูนย์กลางการติดต่อที่ได้รับการเสนอชื่อภายในแผนกไอทีโดยเร็วที่สุดเท่าที่จะเป็นไปได้และจะต้องมีการปฏิบัติตามขั้นตอนการตอบสนองต่ออุบัติการณ์และขั้นตอนการยกระดับ

การจัดการความต่อเนื่องทางธุรกิจ

การวางแผนต่อเนื่องทางธุรกิจ (BCP) เป็นกระบวนการขององค์กรที่ออกแบบมาเพื่อปกป้องกระบวนการและบริการทางธุรกิจที่สำคัญจากผลกระทบของความล้มเหลวหรือภัยพิบัติที่สำคัญของระบบ และเพื่อให้มั่นใจได้ถึงการเริ่มต้นใหม่ตามเวลาที่กำหนดและตามลำดับความสำคัญของเหตุการณ์ต่อเนื่องทางธุรกิจใดๆ

- ระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการสูญเสียระบบไอทีที่อาจเกิดขึ้นกับการบริการของบริษัท
- พัฒนาแผนการลดผลกระทบจากการสูญเสียระบบไอทีที่อาจเกิดขึ้นบริการของตน
- ตรวจสอบให้แน่ใจว่าระบบไอทีที่สนับสนุนบริการของพวกเขาสามารถถูกกู้คืนได้ภายในกรอบเวลาที่ยอมรับได้
- แผนการเหล่านี้สามารถถูกใช้โดยแผนกไอทีเพื่อมุ่งเน้นและจัดลำดับความสำคัญของการกู้คืนระบบ

ความต่อเนื่องทางธุรกิจและการประเมินความเสี่ยง

กลยุทธ์และแผนการรักษาความต่อเนื่องทางธุรกิจของแม็คกรุ๊ปต้องได้รับการพัฒนาขึ้นบนพื้นฐานของการประเมินความเสี่ยง (ความน่าจะเป็นและผลกระทบ) ที่เหมาะสม ต้องมีการระบุเหตุการณ์ที่อาจเป็นสาเหตุของการขัดจังหวะกระบวนการทางธุรกิจพร้อมกับความน่าจะเป็นและผลกระทบของการขัดจังหวะดังกล่าว และผลกระทบเหล่านั้นต่อความมั่นคงทางสารสนเทศ

การพัฒนาและการดำเนินแผนการต่อเนื่อง

แผนการต้องได้รับการพัฒนาและดำเนินการเพื่อรักษาหรือกู้คืนการดำเนินงาน และต้องทำให้มั่นใจได้ว่ามีข้อมูลอยู่ในระดับที่ต้องการและอยู่ในช่วงเวลาที่กำหนดหลังจากการหยุดชะงักหรือความล้มเหลวของกระบวนการทางธุรกิจที่สำคัญ

การทดสอบการดูแลรักษาและการประเมินแผนความต่อเนื่องทางธุรกิจ

ต้องมีการทดสอบแผนความต่อเนื่องทางธุรกิจอย่างน้อยปีละครั้งและมีการปรับปรุงตามการทดสอบหรือตามการเปลี่ยนแปลงที่สำคัญของระบบสารสนเทศ การจัดบุคลากร โครงสร้างองค์กร หรือสภาพแวดล้อมทางธุรกิจ เพื่อให้มั่นใจได้ว่ามันมีประสิทธิภาพและสอดคล้องกับข้อกำหนดทั้งหมดสำหรับความปลอดภัยของข้อมูล

ผู้ให้บริการรายอื่นที่ต้องพึ่งพาความต่อเนื่องทางธุรกิจจะต้องถูกทดสอบอย่างน้อยปีละ 1 ครั้งเพื่อให้มั่นใจว่าจะสามารถปฏิบัติตามพันธสัญญาของพวกเขาได้

การดำเนินการตอบสนองเหตุการณ์ ความมั่นคงปลอดภัย ทางระบบสารสนเทศ

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ ให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ระบบป้องกันผู้บุกรุก

1. ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทาการตรวจสอบ มีดังนี้
    a. มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
    b. ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
    c. ระดับความรุนแรงมากน้อยเพียงใด
    d. หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี
2. ระบบไฟร์วอลล์
    a. ดำเนินการตรวจระบบป้องกันการบุกรุก่อย่างน้อยเดือนละ ๑ ครั้ง
    b. ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้อง ตรวจสอบมีดังต่อไปนี้
        i. Packet ที่ไฟร์วอลล์ได้ทาการ Block
        ii. ลักษณะของ Packet ที่ถูก Block
        iii. Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก
    c. กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา
3. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์
    a. ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ตสิ่งที่ต้องตรวจสอบมีดังนี้
        i. มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
        ii. มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
        iii. มีการส่งมัลแวร์ จากเครือข่ายภายในไปยังภายนอกหรือไม่
    b. ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่าย

c. ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

- เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ ให้แก่ผู้ใช้งาน
- เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ เกิดความมั่นคงปลอดภัย
- เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ โดยไม่คาดคิด

แนวปฏิบัติ

- จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง
- จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่าเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน
- ประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนาไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
- ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้อง ดำเนินการอย่างไร
- สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน
- ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของหน่วยงาน และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

Document History

เลขที่การแก้ไข	วันที่แก้ไข วัน-เดือน-ปี	เปลี่ยนแปลงโดย	ข้อสังเกต
1.0	22/2/2567	วิชาติ อร่ามศรี	เวอร์ชั่นแรก
1.1	03-05-2567	วิชาติ อร่ามศรี	1.ยกเลิก นโยบายการอนุญาตให้ใช้ทรัพย์สินขององค์กร (Acceptable Use Policy)
2.0	25/12/2567	วิชาติ อร่ามศรี	ปรับปรุง Mobile policy

MC GROUP	**ชนิดเอกสาร:** นโยบาย	**เลขที่เอกสาร:** MCG-ISMS-PL-2568-002
	หน่วยงาน: บริษัท แม็คกรุ๊ป จำกัด (มหาชน)	**ชั้นความลับ:** Public
	หัวข้อเรื่อง: ความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security Policy)	**แก้ไขครั้งที่:** 2.0
	หัวข้อควบคุม: ISO/IEC 27001 – 2022	**วันที่บังคับใช้:** 8/1/2568

การอนุมัติ

ลายเซ็นด้านล่างแสดงถึงการอนุมัติเอกสารนี้เพื่อใช้ในพื้นที่ปฏิบัติงานของส่วนที่กำหนด

จัดทำโดย:	วิชาติ อร่ามศรี, รองผู้อำนวยการ แผนกสนับสนุนโครงสร้างและระบบปฏิบัติการ	
ลายเซ็น: วิชาติ อร่ามศรี วันที่: 25/12/2567		

ตรวจสอบโดย:	นพดล ตั้งเด่นชัย, ประธานเจ้าหน้าที่ แผนกเทคโนโลยีสารสนเทศ	
ลายเซ็น: นพดล หั่งเด่นชัย วันที่: 08/01/2568		

อนุมัติโดย:	นพดล ตั้งเด่นชัย, ประธานเจ้าหน้าที่ แผนกเทคโนโลยีสารสนเทศ	
ลายเซ็น นพดล หั่งเด่นชัย วันที่: 08/01/2568		