MC GROUP

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัท แม็คกรุ๊ป จำกัด (มหาชน)

มีผลใช้บังคับเมื่อวันที่ 11 พฤษภาคม 2566

สารบัญ

1 นโยบายและระเบียบปฏิบัติด้านไอที

1.1 วัตถุประสงค์

นโยบายเทคโนโลยีสารสนเทศนี้ได้กำหนดมุมมองในระดับสูงถึงวิธีที่แม็คกรุ๊ปเพื่อสร้างความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ นโยบายนี้จะช่วยให้แม็คกรุ๊ปสามารถทำงานได้ตามมาตรฐานอุตสาหกรรมที่เหมาะสมและตามแนวทางปฏิบัติที่ดีที่สุด

นโยบายนี้เป็นของฝ่ายเทคโนโลยีสารสนเทศและได้รับการรับรองในระดับผู้จัดการ

คำแถลงการณ์ในนโยบายนี้ได้แบ่งระหว่างมาตรฐานขั้นต่ำซึ่งถูกคาดหวังให้อยู่ในข้อความที่ถูกระบุว่า '**จะต้อง**' และแนะนำแนวทางปฏิบัติที่ดีที่สุดที่ถูกระบุว่า '**ควร**'

1.2 ขอบเขต

นโยบายนี้มีผลบังคับใช้กับพนักงานของแม็คกรุ๊ปและระบบที่เฉพาะเจาะจงกับแม็คกรุ๊ปทั้งหมด เป็นการสำคัญอย่างยิ่งที่พนักงานของแม็คกรุ๊ปทุกคนจะเข้าใจถึงภาระหน้าที่ของตนในนโยบายนี้ และปฏิบัติตามข้อกำหนดที่เกี่ยวข้องทั้งหมดเพื่อปกป้องความเป็นส่วนตัวของข้อมูลที่แม็คกรุ๊ปครอบครอง และรักษาแนวทางปฏิบัติที่ดีเพื่อลดความเสี่ยงขององค์กร

1.3 แถลงการณ์ถึงความสำคัญของการรักษาความปลอดภัยต่อองค์กร

นโยบายด้านความมั่นคงขององค์กรถือเป็นเรื่องสำคัญอย่างยิ่งในองค์กรในปัจจุบัน ตั้งแต่การถือกำเนิดขึ้นของการสื่อสารทางอิเล็กทรอนิกส์และเครือข่าย ภาคเอกชน ภาครัฐบาล รัฐบาล หรือองค์กรที่ไม่แสวงหาผลกำไรจำเป็นต้องมีการรักษาความปลอดภัยของข้อมูลอย่างมั่นคงเพื่อรักษาระดับความต่อเนื่องอันสูงสำหรับกระบวนการทางธุรกิจและระบบสารสนเทศ ความต่อเนื่องทางธุรกิจนั้นเกี่ยวข้องกับการปกป้องระบบข้อมูลจากกรณีของฮาร์ดแวร์และซอฟต์แวร์ทั่วไป โดยทำให้มั่นใจอย่างยิ่งว่าระบบเหล่านั้นปลอดภัยจากอันตรายทั้งภายในและภายนอก

1.4 การรักษาความปลอดภัยในการเข้าถึง

แม็คกรุ๊ปมีช่องทางการเข้าถึงอยู่สองช่องทางหลัก:

- การเข้าถึงทางกายภาพ (ไปยังสำนักงาน ห้องคอมพิวเตอร์ ฯลฯ)
- การเข้าถึงทางอิเล็กทรอนิกส์ (ไปยังเครือข่าย ระบบข้อมูล ฯลฯ)

ช่องทางการเข้าถึงแต่ละช่องทางควรมีการจำแนกประเภท (เช่น ต่ำ ปานกลาง สูง) เพื่อบ่งชี้ถึงความเสี่ยงต่อข้อมูลของแม็คกรุ๊ป

แผนธุรกิจในการเข้าถึงและเหตุผลของความจำเป็นเฉพาะประเภทในการเข้าถึงนั้นต้องแจ้งให้ผู้จัดการไอทีทราบ บุคคลที่ 3 คนใดก็ตามที่เข้าถึงเครือข่ายของแม็คกรุ๊ปจากระยะไกลควรให้ความมั่นใจว่าการรักษาความปลอดภัยของพวกเขามีความสอดคล้องกับนโยบายรักษาความปลอดภัยของบริษัท เพื่อลดความเสี่ยงต่อเหตุการณ์ด้านความปลอดภัยต่อแม็คกรุ๊ป

ข้อมูลสำคัญหรือข้อมูลที่ละเอียดอ่อนจะต้องถูกจัดเก็บไว้ในพื้นที่ปลอดภัยที่ได้รับการป้องกันโดยการควบคุมความปลอดภัยที่เหมาะสม ในการประเมินความเสี่ยงควรระบุถึงระดับการป้องกันที่เหมาะสมที่จะถูกนำมาใช้เพื่อรักษาความปลอดภัยของข้อมูลที่ได้รับการจัดเก็บไว้

1.5 สิทธิพิเศษทางด้านไอที

สิทธิ์การเข้าถึงทางด้านไอทีทั้งหมดต้องได้รับการอนุมัติจากเจ้าของเทคโนโลยีที่เกี่ยวข้องก่อนการอนุญาตให้เข้าถึง คำร้องขอเหล่านี้ต้องถูกทำขึ้นและได้รับการอนุมัติผ่านแบบฟอร์มคำขอบริการด้านไอทีและบัตรผ่านของระบบช่วยเหลือที่เกี่ยวข้อง สิทธิในการเข้าถึงด้านไอทีประกอบด้วย:

- การเข้าถึงของผู้ดูแลระบบโดเมน
- การเข้าถึงของผู้ดูแลระบบฐานข้อมูล
- การเข้าถึงของผู้ดูแลระบบภายในไปยังเซิร์ฟเวอร์ในขอบเขต
- การจัดการอุปกรณ์เครือข่าย
- การบริหารจัดการ Internet
- การบริหารจัดการ Wi-Fi
- การบริหารจัดการ Navision
- การบริหารจัดการ SAP
- การบริหารจัดการ POS
- การบริหารจัดการ Citrix (การเข้าถึงระยะไกล)
- การบริหารจัดการ โฟลเดอร์ที่ใช้งานร่วมกันในเซิร์ฟเวอร์

1.5.1 การเข้าถึงของผู้ใช้ในบริการด้านไอทีและแอพพลิเคชันทางธุรกิจ

คำขอสำหรับการเข้าถึงบริการด้านไอทีและแอพพลิเคชันทางธุรกิจต้องเป็นไปตามการขอและกระบวนการอนุมัติพิเศษสำหรับแอพพลิเคชันที่เกี่ยวข้องตามที่ระบุไว้ในหัวข้อ "กระบวนการจัดการสิทธิด้านไอที"

1.5.2 การเข้าถึงโฟลเดอร์ที่ใช้งานร่วมกัน

คำขอในการเข้าถึงโฟลเดอร์ที่ใช้งานร่วมกันในเซิร์ฟเวอร์ของบริษัทจะต้องได้รับการอนุมัติจากผู้จัดการสายงานที่เกี่ยวข้องพร้อมกับการอนุมัติจากฝ่ายไอทีผ่านแบบฟอร์มคำขอใช้บริการด้านไอทีและบัตรผ่านระบบช่วยเหลือที่เกี่ยวข้อง เฉพาะผู้ดูแลระบบระบบไอทีเท่านั้นที่สามารถให้สิทธิหรือแก้ไขการเข้าถึงโฟลเดอร์เหล่านี้ได้

1.5.3 การเข้าถึงทางกายภาพในทรัพยากรทางคอมพิวเตอร์

การเข้าถึงพื้นที่รักษาความปลอดภัยเช่นห้องอุปกรณ์ไอทีต้องได้รับการควบคุมอย่างเหมาะสม และการเข้าถึงทางกายภาพสู่สิ่งปลูกสร้างต้องถูกจำกัดให้เฉพาะผู้ที่ได้รับมอบอำนาจเท่านั้น พนักงานที่ทำงานในพื้นที่รักษาความปลอดภัยควรพร้อมที่จะตรวจตราทุกคนที่ไม่รู้จักและ/หรือไม่สวมตราเครื่องหมาย แต่ละแผนกต้องตรวจสอบให้แน่ใจว่าประตูและหน้าต่างได้รับการรักษาความปลอดภัยอย่างเหมาะสม

ตราเครื่องหมาย/กุญแจ (ควรถูกลงชื่อ/ตรวจสอบอย่างสม่ำเสมอ) และรหัสการเข้าออก ฯลฯ ต้องได้รับการเก็บรักษาไว้โดยพนักงานที่ได้รับอนุญาตให้เข้าถึงพื้นที่เหล่านั้นและไม่ควรมีการให้ยืม/มอบให้กับบุคคลอื่น
บุคลากรที่ทำงานในพื้นที่ที่ปลอดภัยต้อมีความรู้เกี่ยวกับปัญหาด้านสุขภาพและความปลอดภัยทั้งหมดในพื้นที่รักษาความปลอดภัย เช่น การไล่ก๊าซ และปฏิบัติตามกระบวนการที่เกี่ยวข้องทั้งหมด

ผู้มาติดต่อในพื้นที่รักษาความปลอดภัยจะต้องลงชื่อเข้าและออกพร้อมกับเวลาที่เข้ามาและออกไป และจำเป็นต้องแขวนป้ายประจำตัว พนักงานของแม็คกรุ๊ปควรตรวจสอบผู้มาติดต่อทั้งหมดที่เข้าถึงพื้นที่ไอทีที่มีการรักษาความปลอดภัยอยู่ตลอดเวลา

ควรมีการประเมินความเสี่ยงเกี่ยวกับสภาพแวดล้อมและสถานที่รอบๆ บริเวณ จุดสำคัญที่ต้องพิจารณาได้แก่:

- ธุรกิจในท้องถิ่นที่มีความเสี่ยงสูง เช่น งานเกี่ยวกับแก๊ส
- ความเสี่ยงด้านสิ่งแวดล้อม
- ที่ตั้งของสำนักงานในอาคารที่ใช้ร่วมกัน

1.5.4 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

1.5.5 ความปลอดภัยของสายไฟและสายเคเบิล

สายไฟและสายเคเบิลที่มีข้อมูลหรือรองรับพื้นที่ทางธุรกิจที่สำคัญจะต้องได้รับการปกป้องจากการดักข้อมูลหรือความเสียหาย สายไฟควรถูกแยกออกจากสายเคเบิลเครือข่ายเพื่อป้องกันการรบกวน

สายเคเบิลเครือข่ายควรได้รับการปกป้องโดยท่อส่งและหากเป็นไปได้ให้หลีกเลี่ยงเส้นทางที่ผ่านทางสาธารณะหรือบริเวณที่มีความเสี่ยงด้านสิ่งแวดล้อมสูงขึ้น การเข้าถึงแผงต่อควรได้รับการจำกัดเฉพาะสมาชิกที่ได้รับอนุญาตเท่านั้น

1.5.6 การบำรุงรักษาอุปกรณ์

บันทึกประวัติการรักษาอุปกรณ์ควรได้รับการเก็บรักษาไว้เพื่อช่วยให้สามารถตัดสินใจเกี่ยวกับเวลาที่เหมาะสมในการเปลี่ยนอุปกรณ์ได้เมื่ออุปกรณ์มีอายุการใช้งานมากขึ้น

การบำรุงรักษาอุปกรณ์ต้องเป็นไปตามคำแนะนำของผู้ผลิต ต้องมีการจัดทำเป็นเอกสารและเตรียมพร้อมให้แก่เจ้าหน้าที่ฝ่ายสนับสนุนเพื่อใช้ในการจัดซ่อม เช่น เซิร์ฟเวอร์ที่อยู่ภายใต้ข้อตกลงการสนับสนุนและการบำรุงรักษา

ระดับของสัญญาการบำรุงรักษาในสถานที่ต้องเชื่อมโยงกับความสำคัญของระบบต่อธุรกิจ และเกี่ยวข้องกับการสนับสนุนแผนการกู้คืนความเสียหายและแผนธุรกิจต่อเนื่อง

1.5.7 ความรับผิดชอบของพนักงานและผู้ทำสัญญา

ความรับผิดชอบตกเป็นของผู้ใช้ในการป้องกันการเข้าถึงระบบแม็คกรุ๊ปโดยไม่ได้รับอนุญาต โดยการ:

- ใช้รหัสผ่านที่รัดกุม
- ไม่ทิ้งสิ่งใดไว้บนหน้าจอที่อาจมีข้อมูลการเข้าถึง เช่น ชื่อล็อกอินและรหัสผ่าน
- ตรวจดูให้แน่ใจว่าได้มีการล็อกเอาท์ออกจากเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งาน

ผู้ทำสัญญาทุกคนในสถานที่ต้องปฏิบัติตามนโยบายความปลอดภัยของแม็คกรุ๊ป และต้องถูกควบคุมดูแลอยู่ตลอดเวลา

หากจำเป็นต้องเข้าถึงระบบข้อมูลเพื่อปฏิบัติหน้าที่ การเข้าถึงข้อมูลที่ได้รับอนุญาตควรถูกจำกัดเพื่อให้แน่ใจว่ามีเพียงข้อมูลที่จำเป็นเท่านั้นที่จะได้รับการจัดเตรียมให้

การควบคุมที่จำเป็นทั้งหมดเพื่อปกป้องข้อมูลของแม็คกรุ๊ปต้องได้รับการทำสัญญากับผู้จัดจ้างหรือบุคคลที่ 3

1.5.8 การบริหารการเข้าถึง การออกใบรับรอง และการสิ้นสุด

ผู้ใช้แต่ละรายต้องได้รับการจัดสรรสิทธิการเข้าถึงและการอนุญาตไปยังระบบคอมพิวเตอร์และข้อมูลที่

- เหมาะสมกับงานที่คาดว่าพวกเขาจะกระทำ
- มีการเข้าสู่ระบบที่ไม่ซ้ำกันซึ่งจะไม่ถูกใช้ร่วมกันหรือถูกเปิดเผยแก่ผู้ใช้รายอื่น
- มีรหัสผ่านเฉพาะที่จะถูกร้องขอในการเข้าสู่ระบบใหม่แต่ละครั้ง

สิทธิในการเข้าถึงของผู้ใช้ต้องได้รับการตรวจสอบเป็นระยะ (ทุกสองปี) โดยผู้ที่ได้รับมอบอำนาจเพื่อให้แน่ใจว่าได้มีการจัดสรรสิทธิที่เหมาะสม บัญชีที่มีสิทธิพิเศษจะถูกจัดให้แก่ผู้ใช้ที่จำเป็นต่องานบริหารจัดการระบบเท่านั้น

คำขอเพื่อเข้าถึงระบบคอมพิวเตอร์ของแม็คกรุ๊ป ต้องได้รับการอนุมัติโดยผู้จัดการสายงาน ผู้ดูแลข้อมูล หรือผู้ที่ได้รับมอบอำนาจอื่นๆ ที่ระบุ เช่น สำหรับใบสมัครเพื่อขออนุมัติโดยเฉพาะ

เมื่อพนักงานได้ออกจากบริษัท การเข้าถึงระบบไอทีและข้อมูลของพวกเขาจะถูกระงับในวันสิ้นสุดการทำงานของพนักงาน การปิดใช้งานบัญชีจะเป็นไปตามขั้นตอนเฉพาะที่อธิบายไว้ใน "กระบวนการจัดการสิทธิด้านไอที"

1.5.9 การเข้าถึงแอพพลิเคชัน ฐานข้อมูล และระบบปฏิบัติการ

การเข้าถึงระบบปฏิบัติการต้องถูกควบคุมโดยกระบวนการล็อกอินที่ปลอดภัย การควบคุมการเข้าถึงที่ถูกกำหนดไว้ในส่วนการจัดการโพรไฟล์ผู้ใช้และส่วนของรหัสผ่านจะถูกนำมาใช้งาน

ขั้นตอนการเข้าสู่ระบบต้องได้รับการป้องกันโดย:

- จำนวนครั้งที่ไม่สำเร็จและล็อคบัญชีหากเกินจำนวนนั้น
- ตัวอักษรของรหัสผ่านจะถูกซ่อนโดยสัญลักษณ์
- แสดงคำเตือนทั่วไปเพื่อเตือนว่าอนุญาตให้ใช้งานเฉพาะผู้ใช้ที่ได้รับสิทธิเท่านั้น
- หากเป็นไปได้ อย่าเก็บข้อมูลการเข้าสู่ระบบก่อนหน้านี้ไว้ ตัวอย่างเช่น ชื่อผู้ใช้

การเข้าใช้งานระบบปฏิบัติการทั้งหมดจะผ่านล็อกอินไอดีที่ไม่ซ้ำกัน ซึ่งจะได้รับการตรวจสอบในช่วงเวลาที่กำหนด (และสามารถสืบหาถึงบุคคลที่รับผิดชอบได้)

ผู้ดูแลระบบต้องมีบัญชีผู้ดูแลระบบส่วนตัวที่สามารถได้รับการบันทึกและตรวจสอบได้ บัญชีผู้ดูแลระบบต้องไม่ถูกใช้งานโดยบุคคลทั่วไปในกิจกรรมประจำวัน

1.5.10 การตั้งค่าความปลอดภัยเฉพาะระบบ

ระบบไอทีที่เฉพาะต้องมีการตั้งค่าความปลอดภัยส่วนบุคคลในการนำมาใช้เพื่อเพิ่มความปลอดภัยและปกป้องระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

เพื่อให้เอกสารนี้เป็นไปโดยย่อและหลีกเลี่ยงการอัปเดตบ่อยครั้ง การตั้งค่าความปลอดภัยเหล่านี้จะถูกอธิบายไว้ในเอกสารนโยบายแยกต่างหาก "IT System Specific Security Procedures"

1.5.11 การจัดการโพรไฟล์ผู้ใช้งาน

1.5.11.1 การเพิ่มเติม การปรับเปลี่ยน และการลบผู้ใช้งาน

การจัดสรร การแก้ไข และการต่ออายุโพรไฟล์ของผู้ใช้งานควรถูกควบคุมโดยขั้นตอนการจัดการอย่างเป็นทางการซึ่งอนุญาตให้แผนกไอทีหรือระบบช่วยเหลือตรวจสอบข้อมูลประจำตัวของผู้ร้องขอได้

1.5.11.2 การตรวจสอบผู้ใช้เป็นระยะ (การดูแลทำบัญชีต่าง ๆ)

สิทธิในการเข้าถึงของผู้ใช้ต้องได้รับการตรวจสอบเป็นระยะ (ทุกปี) โดยผู้ที่ได้รับมอบอำนาจ เพื่อให้แน่ใจว่ามีการจัดสรรสิทธิที่เหมาะสม บัญชีที่มีสิทธิพิเศษจะถูกจัดให้แก่ผู้ใช้ที่จำเป็นต่องานบริหารจัดการระบบเท่านั้น

1.5.12 การจัดประเภทข้อมูลและคำจำกัดความที่ใช้

ข้อมูลลับ เป็นคำสามัญที่แสดงถึงข้อมูลที่ถูกจัดประเภทว่าถูกจำกัด ตามรูปแบบการจำแนกประเภทที่กำหนดไว้ในแนวนโยบายนี้ คำนี้มักถูกใช้แทนกันกับข้อมูลที่ละเอียดอ่อน

ข้อมูลของสถาบัน หมายถึงข้อมูลทั้งหมดที่เป็นของหรือถูกขึ้นทะเบียนโดยแม็คกรุ๊ป

ข้อมูลไม่สาธารณะ หมายถึงข้อมูลใดๆ ที่จัดเป็นข้อมูลส่วนตัวหรือข้อมูลที่ถูกจำกัด ตามรูปแบบการจำแนกประเภทที่กำหนดไว้ในแนวนโยบายนี้

ข้อมูลที่ละเอียดอ่อน เป็นคำสามัญที่แสดงถึงข้อมูลที่ถูกจัดประเภทว่าถูกจำกัด ตามรูปแบบการจำแนกประเภทที่กำหนดไว้ในแนวนโยบายนี้ คำนี้มักถูกใช้แทนกันกับข้อมูลลับ

การจัดประเภทข้อมูลควรได้รับดำเนินการโดยผู้ดูแลข้อมูลที่เหมาะสม

1.5.13 นโยบายและขั้นตอนการเป็นเจ้าของข้อมูล

คุณภาพและความถูกต้องของการตัดสินใจของบริษัทอาจไม่ได้ดีไปกว่าคุณภาพของข้อมูลที่เป็นพื้นฐานในการตัดสินใจเหล่านั้น ดังนั้น ข้อมูลของเราจะได้รับการวางแผนสำหรับการเก็บ ประมวลผล จัดการ และป้องกันในฐานะทรัพยากรที่มีค่า แม็คกรุ๊ปเป็นเจ้าของข้อมูลทั้งหมดที่ถูกเก็บรวบรวมโดยและภายในแม็คกรุ๊ป โดยไม่คำนึงถึงวิธีการจัดเก็บหรือขนาดของคอลเลกชัน ข้อมูลนี้เป็นสินทรัพย์ที่มีค่าของบริษัทซึ่งจะถูกใช้งานในการสนับสนุนธุรกิจของแม็คกรุ๊ป

1.5.13.1 เจ้าของข้อมูลหรือผู้ดูแลข้อมูล

ผู้ดูแลข้อมูล เป็นพนักงานระดับสูงของแม็คกรุ๊ป ที่ดูแลวงจรชีวิตของข้อมูลสถาบันอย่างน้อยหนึ่งชุด

1.5.13.2 ฟังก์ชันการจัดการข้อมูล

การจัดการข้อมูลคือการพัฒนา การบำรุงรักษา และการควบคุมฐานข้อมูล ผู้จัดการข้อมูลสามารถยกเลิกหรือเพิ่มสิทธิการเข้าถึงและกำหนดระดับการเข้าถึงที่เหมาะสมเพื่อให้บุคลากรสามารถรับข้อมูลที่ต้องการได้โดยไม่ต้องเข้าถึงเนื้อหาที่ละเอียดอ่อน ผู้จัดการข้อมูลต้องวางแผนล่วงหน้าสำหรับการเติบโตรวมทั้งความต้องการในการเข้าถึงดังต่อไปนี้:

ข้อมูล	เงื่อนไข	การบริหาร
โฟลเดอร์ที่ใช้งานร่วมกันในเซิร์ฟเวอร์กลาง	ข้อมูลที่อนุญาติให้อยู่บนเซิร์ฟเวอร์กลางจะต้องมีอายุและการเรียกใช้ล่าสุดน้อยกว่า 2 ปี นับจากวันที่ปัจจุบัน	โดยข้อมูลที่มากกว่า 2 ปีจะได้รับการสำรองไปยังหน่วยงานด้านนอกที่เชื่อถือได้ การเรียกคืนข้อมูลจะใช้เวลา 1 วันทำการ นับจากวันที่ร้องขอ
	ข้อมูลที่อยู่บนเซิร์ฟเวอร์กลางอายุน้อยกว่า 3 ปี และมีการใช้งานพื้นที่มากกว่าหรือเท่ากับ 80% ของพื้นที่โดยรวมทั้งหมด	จะต้องได้รับการขยายพื้นที่ เพื่อให้เพียงพอต่อปริมาณการใช้งานในอนาคต

1.5.13.3 คำจำกัดความของระดับความลับ

ข้อมูลทั้งหมดของแม็คกรุ๊ป แบ่งออกเป็น 2 ประเภทหลักๆ ดังนี้:

- ข้อมูลสาธารณะของแม็คกรุ๊ป
- ข้อมูลลับของแม็คกรุ๊ป

ข้อมูลสาธารณะของแม็คกรุ๊ป เป็นข้อมูลที่ได้รับการประกาศว่าเป็นความรู้สาธารณชนโดยบุคคลที่มีอำนาจในการดำเนินการดังกล่าว และสามารถถูกส่งมอบให้กับทุกคนได้อย่างอิสระโดยไม่มีความเสียหายใดๆ ต่อแม็คกรุ๊ป

ข้อมูลลับของแม็คกรุ๊ป ประกอบไปด้วยข้อมูลอื่นๆ ทั้งหมด ซึ่งเป็นข้อมูลต่อเนื่องที่เป็นที่เข้าใจกันว่าข้อมูลบางอย่างนั้นมีความละเอียดอ่อนกว่าข้อมูลอื่นๆ และควรได้รับความคุ้มครองอย่างปลอดภัยมากขึ้น รวมทั้งข้อมูลที่ควรได้รับความคุ้มครองอย่างใกล้ชิด เช่น ความลับทางการค้า โปรแกรมการพัฒนา เป้าหมายการเข้าซื้อที่มีศักยภาพ และข้อมูลอื่นๆ ที่เป็นส่วนสำคัญต่อความสำเร็จของบริษัทของเรา นอกจากนี้ข้อมูลลับของแม็คกรุ๊ปยังมีข้อมูลที่ไม่สำคัญ เช่น สมุดโทรศัพท์ข้อมูลทั่วไปขององค์กร ข้อมูลบุคลากร ฯลฯ ซึ่งไม่จำเป็นต้องมีการป้องกันอย่างเข้มงวด

ส่วนย่อยของข้อมูลลับของแม็คกรุ๊ป คือ "ข้อมูลกลุ่มบุคคลที่สามของแม็คกรุ๊ป" ข้อมูลลับนี้เป็นของหรือเกี่ยวข้องกับบริษัทอื่นซึ่งถูกมอบหมายให้แก่แม็คกรุ๊ปโดยบริษัทดังกล่าวภายใต้ข้อตกลงและสัญญาอื่นๆ ที่ไม่เปิดเผยข้อมูล

ตัวอย่างของข้อมูลประเภทนี้รวมทุกอย่างตั้งแต่ความพยายามร่วมในการพัฒนา ไปจนถึงรายชื่อผู้ขาย คำสั่งซื้อของลูกค้า และข้อมูลผู้จัดจำหน่าย ข้อมูลในประเภทนี้มีตั้งแต่ข้อมูลที่ละเอียดอ่อนมากไปจนถึงข้อมูลเกี่ยวกับข้อเท็จจริงที่ว่าเราได้เชื่อมต่อผู้จัดหา/ผู้ขายเข้ากับเครือข่ายของแม็คกรุ๊ป เพื่อสนับสนุนการดำเนินงานของเรา

บุคลากรของแม็คกรุ๊ป ได้รับการสนับสนุนให้ใช้วิจารณญาณในการรักษาข้อมูลลับของกลุ่มบุคคลที่สามให้อยู่ในขอบเขตที่เหมาะสม หากพนักงานไม่แน่ใจถึงความละเอียดอ่อนของข้อมูลบางส่วน เขา/เธอควรติดต่อผู้จัดการของตน

1.5.13.4 สิทธิในการเข้าถึง

ผู้ที่ได้รับมอบอำนาจสามารถเข้าถึงข้อมูลสำหรับธุรกิจหรือข้อมูลส่วนบุคคลได้โดยมีเงื่อนไขว่าพวกเขาจะ:

- ไม่ทำอันตรายต่อความปลอดภัยของบริษัทหรือข้อมูลลูกค้าที่เป็นความลับใดๆ ซึ่งอาจมีอยู่ในคอมพิวเตอร์
- ไม่ละเมิดนโยบายใดๆ ของบริษัท
- ไม่มีส่วนร่วมในกิจกรรมที่ผิดกฎหมายหรือกิจกรรมโลกีย์

- ไม่มีส่วนร่วมในผลประโยชน์ทางธุรกิจภายนอก

1.5.14 ข้อกำหนดในการตั้งชื่อสำหรับบัญชีผู้ใช้งาน

เพื่อรับประกันการตั้งชื่อบัญชีผู้ใช้งานที่ตรงตามหลักการภายในระบบไอทีของแม็คกรุ๊ป ข้อกำหนดในการตั้งชื่อสำหรับบัญชีผู้ใช้งานต่อไปนี้ต้องถูกนำมาใช้เมื่อมีการสร้างบัญชีผู้ใช้งาน

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

ประเภท	กฎ	ตัวอย่าง
บัญชีที่ใช้ร่วมกัน	ชื่อที่เป็นกลางโดยไม่ระบุตัวบุคคล อาจจะเป็นชื่อแผนก หรือชื่อประเภทการใช้งาน ในกรณีที่มีชื่อผู้ใช้ซ้ำกันหรือหลายมีบัญชีที่จำเป็นสำหรับวัตถุประสงค์เดียวกัน หมายเลขการทำงานจะถูกเพิ่มเข้ามา	Shared account for Accounting in Navision = account, account1, account2
บัญชีผู้ใช้งาน SAP	อักษรไม่เกินแปดตัวแรกของชื่อตามด้วยจุดและอักษรสามตัวแรกของนามสกุล	Somchai Thongdee = somchai.tho

1.5.15 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

พารามิเตอร์	คำอธิบาย	การตั้งค่า
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
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"

1.5.16 นโยบายเกี่ยวกับการใช้งานซอฟต์แวร์มาตรฐาน การอนุญาตให้ใช้งานซอฟต์แวร์ และลิขสิทธิ์

แม็คกรุ๊ปใช้ซอฟต์แวร์ในทุกด้านของธุรกิจเพื่อสนับสนุนงานที่ดำเนินการโดยพนักงานของบริษัท ซอฟต์แวร์ทุกชิ้นจำเป็นจะต้องได้รับใบอนุญาตในทุกกรณี

ซอฟต์แวร์คอมพิวเตอร์ต้องถูกซื้อผ่านทางไอที และถูกติดตั้งโดยพนักงานแผนกไอที แผนกไอทีต้องสร้างรายการของซอฟต์แวร์ที่ถูกติดตั้งและต้องมีการอัปเดตรายการนี้ ใบอนุญาตซอฟต์แวร์ทั้งหมดควรได้รับการจัดเก็บไว้ในสถานที่ส่วนกลางที่มีการรักษาความปลอดภัย

แชร์แวร์ ฟรีแวร์ และ โปรแกรมสาธารณะ ขึ้นต่อนโยบายและขั้นตอนเดียวกันกับซอฟต์แวร์อื่นๆ ผู้ใช้งานจะต้องไม่ติดตั้งซอฟต์แวร์ฟรีหรือซอฟต์แวร์เพื่อการประเมินผลโดยไม่ได้รับการอนุมัติล่วงหน้า

พนักงานต้องไม่ทำสำเนาของซอฟต์แวร์คอมพิวเตอร์ที่เป็นของแม็คกรุ๊ปเพื่อการใช้งานส่วนตัว

1.5.17 การตรวจสอบเครือข่าย

การจัดการเครือข่ายมีความสำคัญต่อการจัดหาบริการด้านไอทีของแม็คกรุ๊ป และควรใช้งานการควบคุมดังต่อไปนี้:

- ความรับผิดชอบในการดำเนินงานของเครือข่ายควรถูกแยกออกจากกิจกรรมการดำเนินงานด้วยคอมพิวเตอร์หากเป็นไปได้
- เครือข่ายต้องได้รับการตรวจสอบอย่างละเอียดสำหรับปัญหาต่างๆ
- ต้องมีการควบคุมเพื่อป้องกันข้อมูลที่ส่งผ่านเครือข่ายตามสมควร เช่น การเข้ารหัส

สถาปัตยกรรมเครือข่ายต้องได้รับการจัดทำเป็นเอกสารและถูกจัดเก็บไว้ด้วยการตั้งค่าระบบของส่วนประกอบฮาร์ดแวร์และซอฟต์แวร์ทั้งหมดที่ประกอบกันขึ้นเป็นเครือข่าย

เครือข่ายไร้สายต้องใช้การควบคุมอย่างเข้มงวดเพื่อปกป้องข้อมูลที่ส่งผ่านเครือข่ายและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเข้ารหัสลับต้องถูกนำมาใช้งานในเครือข่ายเพื่อป้องกันไม่ให้ข้อมูลถูกดักจับ มาตรฐานสำหรับเครือข่ายไร้สายจะได้รับการควบคุมและบำรุงรักษาโดยแผนกไอที และการใช้งานระบบเครือข่ายทั้งหมดจะต้องเป็นไปตามมาตรฐานเหล่านี้

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

1.5.18 การเข้าถึงจากระยะไกล

ในกรณีที่จำเป็นต้องมีการเข้าถึงเครือข่ายของแม็คกรุ๊ปจากระยะไกล แอพพลิเคชันจะต้องถูกดำเนินการผ่านแผนกไอที โดยผ่านบัตรผ่านของระบบช่วยเหลือ การเข้าถึงเครือข่ายจากระยะไกลต้องได้รับการรักษาความปลอดภัยโดยใช้แอพพลิเคชันที่มีความปลอดภัย เช่น FortiClient สำหรับ VPN และ ซิทริกซ์

บริษัทคู่ค้าหรือผู้จัดหาที่เป็นบุคคลที่สาม จะต้องไม่ได้รับรายละเอียดเกี่ยวกับวิธีเข้าถึงเครือข่ายของแม็คกรุ๊ปหากไม่ได้รับอนุญาตจากฝ่ายไอที การเปลี่ยนแปลงใดๆ ในการเชื่อมต่อของผู้จัดหาจะต้องถูกส่งต่อไปยังฝ่ายไอทีโดยตรงเพื่อให้การเข้าถึงสามารถอัพเดตหรือถูกยกเลิกได้

1.5.19 การป้องกันไวรัส

ซอฟต์แวร์ป้องกันมัลแวร์จะต้องได้รับการติดตั้งและบำรุงรักษาในเวิร์กสเตชันและเซิร์ฟเวอร์ทั้งหมด และจะต้องถูกจัดเตรียมไว้ในจุดที่เหมาะสมบนเครือข่าย การตรวจสอบต้องมีขึ้นเป็นระยะเพื่อให้แน่ใจว่าการอัปเดตได้ถูกเปิดใช้งาน

การตรวจสอบระบบทุกระบบที่จำเป็นต่อธุรกิจอย่างสม่ำเสมอจะต้องเกิดขึ้นเพื่อกำหนดซอฟต์แวร์ทั้งหมดที่ทำงานอยู่ในระบบ ไฟล์หรือซอฟต์แวร์ใดๆ ที่ไม่ได้รับอนุญาตจะต้องได้รับการตรวจสอบอย่างเป็นทางการและถูกลบออกไปตามสมควร

เพื่อป้องกันระบบจากมัลแวร์ เครื่องคอมพิวเตอร์ตั้งโต๊ะและแล็ปท็อปไม่ควรได้สิทธิพิเศษของผู้จัดการระบบ ข้อยกเว้นนั้นจำเป็นในบางครั้งและผู้ใช้งานที่มีสิทธิการเข้าถึงของผู้จัดการระบบจะต้องไม่:

- ติดตั้งซอฟต์แวร์จากแหล่งภายนอกใดๆ รวมทั้งจากอินเทอร์เน็ต ซีดี/ดีวีดีรอม หน่วยความจำยูเอสบี ฟล็อปปี้ดิสก์ ฯลฯ บนเวิร์กสเตชัน
- เพิ่มสกรีนเซฟเวอร์หรือยูทิลิตี้ลงในเวิร์กสเตชัน มัลแวร์สามารถถูกดำเนินการผ่านอีเมลหลอกลวงและผู้ใช้งานต้องระมัดระวังในการป้องกันสิ่งนี้ ผู้ใช้งานต้องไม่ส่งต่ออีเมล์ที่อ้างว่าเป็นคำเตือนซึ่งอีเมล์เหล่านี้มักเป็นอีเมล์ลูกโซ่

1.5.20 การตรวจสอบความปลอดภัยสำหรับการบำรุงรักษาไอดีของผู้ใช้งานและการควบคุมรหัสผ่าน

บันทึกการตรวจสอบควรถูกเก็บไว้อย่างน้อยหกเดือนซึ่งจะบันทึกข้อยกเว้นและเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยอื่นๆ ที่เป็นไปได้ในทางเทคนิคและเป็นประโยชน์ในการดำเนินการดังกล่าว บันทึกการตรวจสอบควรประกอบด้วยข้อมูลดังต่อไปนี้:

- เอกลักษณ์ของระบบ
- ไอดีของผู้ใช้งาน
- การเข้าสู่ระบบที่ประสบความสำเร็จ/ไม่สำเร็จ
- การออกจากระบบที่ประสบความสำเร็จ/ไม่สำเร็จ
- การเข้าถึงแอพพลิเคชันที่ไม่ได้รับอนุญาต
- การเปลี่ยนแปลงการกำหนดค่าระบบ
- การใช้บัญชีแบบพิเศษ (เช่น การจัดการบัญชี การเปลี่ยนแปลงนโยบาย การกำหนดค่าอุปกรณ์)

การเข้าถึงบันทึกต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาตซึ่งอาจส่งผลให้ข้อมูลที่บันทึกถูกแก้ไขหรือถูกลบออก

ควรตรวจสอบข้อผิดพลาดของระบบผ่านระบบช่วยเหลือไอที และติดตามและตรวจสอบผ่านระบบที่เหมาะสม การดำเนินการที่สำคัญระหว่างการแก้ไขปัญหาความผิดพลาดควรได้รับการบันทึกและอ้างอิงโยงกับกรณีที่คล้ายกันก่อนหน้านี้

กระบวนการบันทึกที่ผิดพลาดควรได้รับการป้อนเข้าสู่กระบวนการจัดการเหตุการณ์ของระบบเพื่อการดำเนินการขั้นต่อไปหากจำเป็น

1.6 การเปลี่ยนแปลงโปรแกรม

การดำเนินการเปลี่ยนแปลงแอพพลิเคชันซอฟต์แวร์ เครือข่าย และโครงสร้างพื้นฐานต้องใช้ขั้นตอนการควบคุมการเปลี่ยนแปลงอย่างเป็นทางการ ขั้นตอนการควบคุมการเปลี่ยนแปลงควร:

- มีโครงสร้างศูนย์รวมที่ซึ่งการเปลี่ยนแปลงที่ได้รับการเสนอทั้งหมดต้องถูกส่งไป
- มีเส้นทางการตรวจสอบคำขอโดยระบุว่ามีการตัดสินใจอย่างไรสำหรับแต่ละคนและเพราะอะไร
- ตรวจสอบให้แน่ใจว่าการเปลี่ยนแปลงจะไม่สร้างความเสียหายกับการควบคุมและขั้นตอนที่มีอยู่
- ตรวจสอบให้แน่ใจว่าการเปลี่ยนแปลงถูกอนุมัติอย่างเป็นทางการจากจากคณะกรรมการที่ปรึกษาด้านการเปลี่ยนแปลง
- ตรวจสอบให้แน่ใจว่าเอกสารของระบบและขั้นตอนของผู้ใช้จะได้รับการอัปเดตเมื่อมีการเปลี่ยนแปลง
- การควบคุมการเปลี่ยนแปลงต้องถูกนำไปใช้กับการเปลี่ยนแปลงในการเข้าถึงแอพพลิเคชันและข้อมูลที่อยู่บนไฟล์เซิร์ฟเวอร์

โปรดดู "ขั้นตอนการจัดการการเปลี่ยนแปลงแอพพลิเคชัน" และ "ขั้นตอนการจัดการการเปลี่ยนแปลงโครงสร้างพื้นฐาน"

1.7 การพัฒนาโปรแกรม

การดำเนินการเปลี่ยนแปลงแอพพลิเคชันซอฟต์แวร์ เครือข่าย และโครงสร้างพื้นฐานต้องใช้ขั้นตอนการควบคุมการเปลี่ยนแปลงอย่างเป็นทางการ ขั้นตอนการควบคุมการเปลี่ยนแปลงควร:

- มีโครงสร้างศูนย์รวมที่ซึ่งการเปลี่ยนแปลงที่ได้รับการเสนอทั้งหมดต้องถูกส่งไป
- มีเส้นทางการตรวจสอบคำขอโดยระบุว่ามีการตัดสินใจอย่างไรสำหรับแต่ละคนและเพราะอะไร
- ตรวจสอบให้แน่ใจว่าการเปลี่ยนแปลงจะไม่สร้างความเสียหายกับการควบคุมและขั้นตอนที่มีอยู่

- ตรวจสอบให้แน่ใจว่าการเปลี่ยนแปลงถูกอนุมัติอย่างเป็นทางการจากจากคณะกรรมการที่ปรึกษาด้านการเปลี่ยนแปลง
- ตรวจสอบให้แน่ใจว่าเอกสารของระบบและขั้นตอนของผู้ใช้จะได้รับการอัปเดตเมื่อมีการเปลี่ยนแปลง
- การควบคุมการเปลี่ยนแปลงต้องถูกนำไปใช้กับการเปลี่ยนแปลงในการเข้าถึงแอพพลิเคชันและข้อมูลที่อยู่บนไฟล์เซิร์ฟเวอร์

1.8 การปฏิบัติการทางคอมพิวเตอร์

1.8.1 การประมวลผลของงาน

การประมวลผลของงานต้องถูกกระทำโดยผู้ใช้งานที่ได้รับอนุญาต

1.8.2 การสำรองข้อมูลและการกู้คืน

จำเป็นต้องมีการสำรองข้อมูลทางธุรกิจที่สำคัญอย่างสม่ำเสมอเพื่อให้มั่นใจว่าแม็คกรุ๊ปจะสามารถกู้คืนจากภัยพิบัติ ระบบล้มเหลว หรือข้อผิดพลาดอื่นๆได้ ขั้นตอนการสำรองข้อมูลได้ถูกนำเสนอในขั้นตอนการกู้คืนภัยพิบัติ

พนักงานทุกคนต้องทำให้แน่ใจว่าข้อมูลทางธุรกิจที่จำเป็นทั้งหมดที่มีอยู่ในพีซีและแล็ปท็อปได้รับการสำรองไว้

1.8.3 การจัดการอุบัติการณ์และปัญหา

ระบบข้อมูลและข้อมูลของแม็คกรุ๊ปต้องได้รับการปกป้องจากอุบัติการณ์ด้านความปลอดภัยที่เกิดขึ้นจริงหรือที่สงสัยว่าอาจเกิดขึ้นได้ คำนิยามของอุบัติการณ์คือเหตุการณ์อันไม่พึงประสงค์ที่ก่อให้เกิดหรือมีศักยภาพก่อความเสียหายในทรัพย์สิน ชื่อเสียง และ/หรือบุคลากรขององค์กร

การจัดการเหตุการณ์ในด้านไอทีนั้นเกี่ยวข้องกับการบุกรุก ความเป็นอันตราย และการใช้ทรัพยากรสารสนเทศและข้อมูลอย่างไม่ถูกต้อง และความต่อเนื่องของระบบสารสนเทศที่สำคัญและกระบวนการ

เหตุการณ์และจุดอ่อนด้านความปลอดภัยของข้อมูลจะต้องถูกรายงานไปยังจุดศูนย์กลางการติดต่อที่ได้รับการเสนอชื่อภายในแผนกไอทีโดยเร็วที่สุดเท่าที่จะเป็นไปได้และจะต้องมีการปฏิบัติตามขั้นตอนการตอบสนองต่ออุบัติการณ์และขั้นตอนการยกระดับ

1.9 การบริหารสินทรัพย์ไอที

สำหรับระบบข้อมูลที่จะถูกนำมาใช้อย่างมีประสิทธิภาพ มีไหวพริบ และถูกต้องตามกฎหมาย สินทรัพย์ที่ประกอบด้วยระบบเหล่านั้นจะต้องได้รับการควบคุมอย่างถูกต้อง การจัดการสินทรัพย์ไม่จำกัดเพียงแค่การครอบคลุมข้อมูลที่แม็คกรุ๊ปรักษาไว้ แต่ยังเกี่ยวข้องกับผู้คนที่ใช้งาน และกระบวนการที่พวกเขาปฏิบัติตาม และคอมพิวเตอร์ทางกายภาพที่ถูกใช้ในการเข้าถึง นโยบายการจัดการสินทรัพย์ควรกำหนดประเด็นเหล่านี้ทั้งหมดเนื่องจากสามารถจำกัดความลับ คุณภาพ และความพร้อมใช้งานของข้อมูล

1.9.1 การทำรายการสินทรัพย์

การทำรายการหรือการลงทะเบียนสินทรัพย์ข้อมูลที่สำคัญทั้งหมดที่แม็คกรุ๊ปกำหนดขึ้นสำหรับตำแหน่งที่ตั้งแต่ละแห่งต้องถูกสร้างขึ้น และควรประกอบไปด้วยประเภท สถานที่ตั้ง เจ้าของสินทรัพย์ที่ถูกกำหนดหากมีการเกี่ยวข้อง

1.9.2 การใช้สินทรัพย์ที่ยอมรับได้

นโยบายการใช้งานที่ยอมรับได้สำหรับสินทรัพย์ ระบบ และบริการต้องได้รับการจัดทำเป็นเอกสารและนำมาใช้จริง สิ่งนี้ควรนำมาใช้กับพนักงาน ผู้ทำสัญญา และกลุ่มบุคคลที่สาม และการใช้ระบบต้องเป็นไปตามเงื่อนไขในการยอมรับนโยบายการใช้งานที่เหมาะสม

แม็คกรุ๊ปอนุญาตให้ใช้งานอินเทอร์เน็ตเพื่อการใช้งานส่วนบุคคลที่สมเหตุผลและมีความรับผิดชอบ และผู้ใช้งานที่ต้องเผชิญกับนโยบายการใช้อินเทอร์เน็ตที่เหมาะสมต้องมั่นใจว่าได้ตระหนักถึงความรับผิดชอบของตนในขณะที่ใช้งานอินเทอร์เน็ต สิ่งนี้ควรรวมถึงการใช้เว็บไซต์เครือข่ายสังคมออนไลน์ที่เหมาะสมด้วย

1.10 การจัดการความต่อเนื่องทางธุรกิจ

การวางแผนต่อเนื่องทางธุรกิจ (BCP) เป็นกระบวนการขององค์กรที่ออกแบบมาเพื่อปกป้องกระบวนการและบริการทางธุรกิจที่สำคัญจากผลกระทบของความล้มเหลวหรือภัยพิบัติที่สำคัญของระบบ และเพื่อให้มั่นใจได้ถึงการเริ่มต้นใหม่ตามเวลาที่กำหนดและตามลำดับความสำคัญของเหตุการณ์ต่อเนื่องทางธุรกิจใดๆ

- ระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการสูญเสียระบบไอทีที่อาจเกิดขึ้นกับการบริการของบริษัท
- พัฒนาแผนการลดผลกระทบจากการสูญเสียระบบไอทีที่อาจเกิดขึ้นบริการของตน
- ตรวจสอบให้แน่ใจว่าระบบไอทีที่สนับสนุนบริการของพวกเขาสามารถถูกกู้คืนได้ภายในกรอบเวลาที่ยอมรับได้

แผนการเหล่านี้สามารถถูกใช้โดยแผนกไอทีเพื่อมุ่งเน้นและจัดลำดับความสำคัญของการกู้คืนระบบ

1.10.1 ความต่อเนื่องทางธุรกิจและการประเมินความเสี่ยง

กลยุทธ์และแผนการรักษาความต่อเนื่องทางธุรกิจของแม็คกรุ๊ปต้องได้รับการพัฒนาขึ้นบนพื้นฐานของการประเมินความเสี่ยง (ความน่าจะเป็นและผลกระทบ) ที่เหมาะสม ต้องมีการระบุเหตุการณ์ที่อาจเป็นสาเหตุของการขัดจังหวะกระบวนการทางธุรกิจพร้อมกับความน่าจะเป็นและผลกระทบของการขัดจังหวะดังกล่าว และผลกระทบเหล่านั้นต่อความมั่นคงทางสารสนเทศ

1.10.2 การพัฒนาและการดำเนินแผนการต่อเนื่อง

แผนการต้องได้รับการพัฒนาและดำเนินการเพื่อรักษาหรือกู้คืนการดำเนินงาน และต้องทำให้มั่นใจได้ว่ามีข้อมูลอยู่ในระดับที่ต้องการและอยู่ในช่วงเวลาที่กำหนดหลังจากการหยุดชะงักหรือความล้มเหลวของกระบวนการทางธุรกิจที่สำคัญ

1.10.3 การทดสอบการดูแลรักษาและการประเมินแผนความต่อเนื่องทางธุรกิจ

ต้องมีการทดสอบแผนความต่อเนื่องทางธุรกิจอย่างน้อยปีละครั้งและมีการปรับปรุงตามการทดสอบหรือตามการเปลี่ยนแปลงที่สำคัญของระบบสารสนเทศ การจัดบุคลากร โครงสร้างองค์กร หรือสภาพแวดล้อมทางธุรกิจ เพื่อให้มั่นใจได้ว่ามันมีประสิทธิภาพและสอดคล้องกับข้อกำหนดทั้งหมดสำหรับความปลอดภัยของข้อมูล

ผู้ให้บริการรายอื่นที่ต้องพึ่งพาความต่อเนื่องทางธุรกิจจะต้องถูกทดสอบอย่างน้อยปีละครั้งเพื่อให้มั่นใจว่าจะสามารถปฏิบัติตามพันธสัญญาของพวกเขาได้

1.10.4 การดำเนินการตอบสนองเหตุการณ์ ความมั่นคงปลอดภัย ทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ระบบป้องกันผู้บุกรุก

1. ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทาการตรวจสอบ มีดังนี้
    a. มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
    b. ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
    c. ระดับความรุนแรงมากน้อยเพียงใด

d. หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

2. ระบบไฟร์วอลล์
   a. ดำเนินการตรวจระบบป้องกันการบุกรุกอย่างน้อยเดือนละ 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. ศึกษาหาวิธีแก่ไขเครื่องคอมพิวเตอร์ ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่าย
   c. ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก่ไขเครื่องนั้นทันที

1.10.5 การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

1. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ ให้แก่ผู้ใช้งาน
2. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ เกิดความมั่นคงปลอดภัย
3. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ โดยไม่คาดคิด

แนวปฏิบัติ

1. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

2. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่าเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน
3. ประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนาไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
4. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้อง ดำเนินการอย่างไร
5. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน
6. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของหน่วยงาน และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 11 พฤษภาคม 2566

(นางไขศรี เนื่องสิกขาเพียร)

ประธานกรรมการ