นโยบายการจัดการความปลอดภัยทางด้านสารสนเทศและไซเบอร์

ฝ่ายสารสนเทศ | วันที่มีผลบังคับใช้ 29 กุมภาพันธ์ 2567 | ฉบับที่ 01, แก้ไขครั้งที่ 04

จัดทำโดย	สอบทานโดย	อนุมัติโดย
นางสาวนฤมล ชื่นชูจิตร์	**นายสันติ บางอ้อ**	**นายประเสริฐ บุญสัมพันธ์**
ผู้จัดการอาวุโส	**ประธาน**	**ประธาน**
ฝ่ายสารสนเทศ	**คณะกรรมการกำกับดูแลกิจการ**	**คณะกรรมการบริษัท**

คำนำ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทโทรีเซนไทย เอเยนต์ซีส์ จำกัด (มหาชน) หรือต่อไปนี้เรียกว่า "บริษัท" สามารถดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ และมีความมั่นคงปลอดภัย สอดคล้องกับนโยบายทางธุรกิจ และป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเครือข่ายระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง รวมถึงการถูกคุกคามจากภัยต่างๆ ซึ่งอาจส่งผลกระทบต่อระบบธุรกิจของบริษัทให้ได้รับความเสียหายได้ ดังนั้นเพื่อให้ระบบสารสนเทศของบริษัทคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความสมบูรณ์ถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) จึงเห็นสมควรกำหนดนโยบายความปลอดภัยทางด้านระบบสารสนเทศและไซเบอร์ เพื่อให้ผู้ปฏิบัติงานและหน่วยงานต่างๆ ใช้ในการดำเนินงานอย่างเคร่งครัด

คำนิยาม

คำศัพท์	ความหมาย
บริษัท / องค์กร	บริษัทโทรีเซนไทย เอเยนต์ซีส์ จำกัด (มหาชน) บริษัทย่อย และบริษัทในเครือ ที่ใช้ระบบสารสนเทศ และระบบเครือข่ายร่วมกัน
การกู้คืน	การนำข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบสารสนเทศที่เกิดความเสียหายกลับมาใช้งานได้ครบถ้วนถูกต้อง ตามเงื่อนไขที่กำหนด
การสำรองข้อมูล	การคัดลอกหรือทำสำเนาข้อมูล เช่น ไฟล์, ฐานข้อมูล, ระบบคอมพิวเตอร์ ไปยังสถานที่เก็บอื่นๆ เพื่อเตรียมนำมาใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหาย สูญหาย หรือเกิดภัยพิบัติ
ศูนย์คอมพิวเตอร์	สถานที่ที่ใช้ในการจัดวางอุปกรณ์สารสนเทศที่มีการประมวลผล หรือจัดเก็บสารสนเทศที่มีการรักษาระดับความมั่นคงปลอดภัยสูง
พื้นที่ควบคุม	พื้นที่ที่มีระบบสารสนเทศที่สำคัญของบริษัท เช่น ศูนย์คอมพิวเตอร์
การพิสูจน์และยืนยันตัวตน	กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล (อ้างอิงจากจากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562)

คำศัพท์	ความหมาย
การปฏิบัติงานจากระยะไกล	การเข้าสู่ระบบสารสนเทศของบริษัทจากภายนอก
ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (อ้างอิงจากพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
เจ้าของข้อมูลส่วนบุคคล	บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล
ผู้ควบคุมข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
เหตุการณ์ผิดปกติ	เหตุการณ์ใดๆ ที่ส่งผลกระทบต่อการรักษาความปลอดภัยของระบบสารสนเทศ
เจ้าหน้าที่	พนักงานประจำ พนักงานสัญญาจ้าง พนักงานชั่วคราว
ผู้ใช้งาน	ลูกจ้าง เจ้าหน้าที่ ผู้ปฏิบัติงาน ผู้บริหารของกลุ่มบริษัท หรือบุคคลภายนอกที่ได้รับสิทธิ์ให้ใช้งานระบบสารสนเทศของบริษัท
บัญชีผู้ใช้งาน	ชุดอักษรหรือตัวเลขที่กำหนดขึ้นมา เพื่อใช้ในการเข้าใช้งานระบบสารสนเทศที่กำหนดสิทธิ์การใช้งานเอาไว้
รหัสผ่าน	ชุดอักษรหรือตัวเลขหรืออักขระ ที่ใช้ในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

1. ความมั่นคงปลอดภัยของสารสนเทศ

1.1. นโยบายความปลอดภัยสารสนเทศ

<u>วัตถุประสงค์และขอบเขต</u>

เพื่ออธิบายถึงวัตถุประสงค์และขอบเขตของนโยบายความปลอดภัยของสารสนเทศ รวมถึงทิศทางของผู้บริหารในการรักษาความปลอดภัยและการใช้ข้อมูลสารสนเทศอย่างเหมาะสม เพื่อให้มีความปลอดภัยทางด้านระบบสารสนเทศสำหรับการสนับสนุนการดำเนินงานทางธุรกิจ สอดคล้องกับกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

ทางบริษัทให้ความสำคัญกับการปกป้องระบบสารสนเทศ รวมถึงการเตรียมความพร้อมในการรองรับภัยคุกคามทางไซเบอร์ โดยการดำเนินนโยบายดังกล่าว จะมุ่งเน้นให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 นอกจากนี้ บริษัทยังให้ความสำคัญถึงเรื่องการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ดังนั้นนโยบายความปลอดภัยฉบับนี้ จึงครอบคลุมถึงการปกป้องข้อมูลขององค์กร ตลอดจนข้อมูลส่วนบุคคล เนื่องด้วยข้อมูลถือว่าเป็นทรัพย์สินที่มีความสำคัญในการดำเนินธุรกิจขององค์กร หากข้อมูลที่สำคัญขององค์กรไม่มีความปลอดภัย

ไม่สามารถรักษาความลับได้ และไม่มีความพร้อมใช้งาน ก็จะส่งผลกระทบทั้งในด้านการเงิน ความน่าเชื่อถือ หรือภาพลักษณ์ชื่อเสียงขององค์กร

<u>เนื้อหานโยบายและการดำเนินการ</u>

1.1.1. การจัดทำนโยบายความปลอดภัยทางด้านสารสนเทศและไซเบอร์

นโยบายฉบับนี้ได้ถูกจัดทำตามวัตถุประสงค์และขอบเขต และได้รับการอนุมัติจากผู้บริหาร หรือคณะกรรมการ ซึ่งมีการประกาศใช้และถือเป็นหลักปฏิบัติทั่วทั้งองค์กร โดยให้มีผลบังคับใช้กับบุคลากรในบริษัททุกระดับชั้น ตั้งแต่ผู้บริหาร พนักงาน ครอบคลุมถึงบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศและทรัพย์สินของบริษัท

1.1.2. การทบทวนนโยบายความปลอดภัยทางด้านสารสนเทศและไซเบอร์

นโยบายฉบับนี้ต้องได้รับการปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงที่อาจเกิดในอนาคต ซึ่งอาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การเปลี่ยนโครงสร้างของเทคโนโลยีในองค์กร การแก้ไขกฎหมายเพิ่มเติม การเปลี่ยนทิศทางด้านเทคโนโลยีสารสนเทศ

2. โครงสร้างความปลอดภัยสารสนเทศ

2.1. โครงสร้างความมั่นคงปลอดภัยสารสนเทศในองค์กร

เพื่อกำหนดกรอบการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศในบริษัท ให้เป็นไปอย่างมีแบบแผน และมีความชัดเจน รวมถึงการกำหนดบทบาทหน้าที่ในการบริหารจัดการความปลอดภัย

2.1.1. กำหนดบทบาทและหน้าที่ด้านความมั่นคงปลอดภัยของสารสนเทศและไซเบอร์

แต่งตั้งกลุ่มหรือคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และมอบหมายหน้าที่ ความรับผิดชอบด้านความมั่นคงปลอดภัย

2.1.1.1. หน่วยงานภายใน

<u>1) แผนกเทคโนโลยีสารสนเทศ</u>

- กำหนดนโยบายแนวทางการปฏิบัติ ตลอดจนแผนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศและไซเบอร์ ให้สอดคล้องกับการดำเนินการทางธุรกิจ
- รับผิดชอบด้านความปลอดภัยทางสารสนเทศ และเป็นผู้นำในการดำเนินงานทั้งหมดที่เกี่ยวข้องกับความปลอดภัยของสารสนเทศในบริษัท
- ดูแลโครงสร้างพื้นฐานทางด้านสารสนเทศ ระบบแอปพลิเคชั่นทางด้านธุรกิจ ให้สามารถดำเนินงานได้อย่างราบรื่น
- บริหารจัดการเฝ้าระวังการโจมตีทางสารสนเทศ โดยจัดให้มีระบบป้องกัน, ตรวจสอบและแจ้งเตือน ผู้บุกรุก หรือระบบกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์ ตลอดจนการกำหนดแนวทางการดำเนินการ เมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ เพื่อให้ธุรกิจสามารถกลับมาดำเนินการได้อย่างต่อเนื่อง
- เป็นที่ปรึกษาและช่วยเหลือในการพัฒนาหรือจัดวางระบบต่างๆ รวมถึงจัดกิจกรรมให้ความรู้ เพื่อสร้างความตระหนักรู้ในด้านความมั่นคงปลอดภัยสารสนเทศ และภัยจากการคุกคามทางไซเบอร์

2) หัวหน้าแผนก / หัวหน้าฝ่าย

- กำหนดบทบาทหน้าที่ ความรับผิดชอบ ต่อทรัพย์สินรวมถึงบริหารจัดการทรัพย์สินที่อยู่ภายใต้การดูแลให้คงสภาพการป้องกันความลับ ความสมบูรณ์ และความพร้อมใช้งานของทรัพย์สินนั้นๆ
- สื่อสารและเน้นย้ำถึงความสำคัญของการรักษาความปลอดภัยของสารสนเทศต่อพนักงานที่อยู่ภายใต้การกำกับดูแล
- ตอบสนองต่อเหตุการณ์ความปลอดภัยสารสนเทศ ซึ่งเป็นเหตุการณ์ที่ส่งผลกระทบในทางลบต่อหน่วยงานหรือทั้งองค์กร รวมถึงการให้ความร่วมมือในการสอบสวน หรือเสนอแนวทางในการแก้ไข

3) คณะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- ให้คำแนะนำ และความรู้ในการปฏิบัติตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล แก่บุคคลหรือหน่วยงานอื่นๆ ที่เกี่ยวข้อง
- ติดต่อประสานงานกับหน่วยงานต่าง ๆ ภายในองค์กร เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล รวมถึงต้องมีการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของแต่ละแผนก ให้เป็นไปตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล
- ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่มีปัญหา เกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล หรือเกิดคำร้องเรียนขึ้นในองค์กร

4) เจ้าของข้อมูลส่วนบุคคลและสารสนเทศ / เจ้าของทรัพย์สิน

- กำหนดลำดับชั้นความลับของข้อมูล จัดทำมาตราการ และขั้นตอนควบคุมการเข้าถึงข้อมูล พร้อมทั้งแจ้งให้ผู้เกี่ยวข้องรับทราบเมื่อมีการเปลี่ยนแปลง
- แจ้งแผนกเทคโนโลยีสารสนเทศ เมื่อพบเหตุที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ หรือมีการเปลี่ยนแปลงสิทธิ์การเข้าถึง อันเนื่องจากการการโอนย้าย, ลาออก และการเปลี่ยนอำนาจหน้าที่

5) พนักงาน / ผู้ใช้งาน

- เรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายความปลอดภัยทางด้านระบบสารสนเทศและไซเบอร์อย่างเคร่งครัด
- รักษาความลับของข้อมูลสารสนเทศขององค์กร
- รักษาความลับของข้อมูลส่วนบุคคล และความยินยอมที่ได้รับจากเจ้าของข้อมูลส่วนบุคคล
- รายงานเหตุการณ์การละเมิดความปลอดภัยทางด้านสารสนเทศและไซเบอร์ต่อผู้บังคับบัญชา และแผนกเทคโนโลยีสารสนเทศให้ทราบโดยทันทีเมื่อพบเหตุ เพื่อช่วยเหลือในการตอบสนองต่อเหตุการณ์นั้นๆ
- ใช้งานข้อมูลและทรัพย์สินขององค์กรอย่างมีประสิทธิภาพ ถูกต้องตามที่ได้รับอนุญาต หรือได้รับมอบหมายสิทธิ์การเข้าถึง

2.1.1.2. หน่วยงานภายนอก

- เข้าถึงระบบสารสนเทศตามที่ได้รับสิทธิ์เท่านั้น
- ข้อมูลสารสนเทศที่ได้รับจากการเก็บรวมรวบหรือเข้าถึงระหว่างที่ปฏิบัติงานกับองค์กร ให้ถือเป็นความลับ ห้ามเปิดเผย ส่งต่อ หรือแก้ไขข้อมูลสารสนเทศที่ได้มา โดยไม่ได้รับความยินยอมจากหน่วยงานที่ดูแลการดำเนินงาน
- รายงานเหตุการณ์การละเมิดความปลอดภัยทางด้านสารสนเทศและไซเบอร์ที่เกิดขึ้นทันที ให้แก่หน่วยงานที่ทำหน้าที่กำกับดูแลงานและแผนกเทคโนโลยีสารสนเทศ

2.2. การจัดชั้นความลับของสารสนเทศ

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อให้สารสนเทศได้รับการป้องกันอย่างเหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศที่มีต่อองค์กร

<u>เนื้อหานโยบายและการดำเนินการ</u>

ข้อมูลสารสนเทศต้องมีการกำหนดชั้นความลับ โดยพิจารณาจากระดับความสำคัญ กฎหมาย และระดับความอ่อนไหว โดยการป้องกันจะต้องพิจารณาทั้ง 3 ด้านคือ การรักษาความลับ การรักษาความสมบูรณ์และความพร้อมใช้งาน ทั้งนี้การควบคุมป้องกันจะเริ่มตั้งแต่กระบวนการการสร้าง การนำไปใช้ การเก็บรักษา และการทำลาย

2.2.1. ชั้นเปิดเผยได้

เป็นข้อมูลที่ทุกคนสามารถเข้าถึงได้ ทั้งบุคคลภายในและภายนอกองค์กร หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย เช่นข้อมูลบริษัทที่ปรากฏในหน้าเว็บไซต์บริษัท

2.2.2. ชั้นใช้ภายในองค์กร

เป็นข้อมูลที่พนักงานทุกคน หรือผู้ได้รับสิทธิ์สามารถเข้าถึงได้ โดยผู้ได้รับสิทธิ์อาจเป็นบุคคลภายนอกก็ได้

2.2.3. ชั้นเฉพาะหน่วยงานหรือเฉพาะกลุ่ม

เป็นข้อมูลที่ไม่สามารถเปิดเผยให้พนักงานทุกคนรับทราบ โดยข้อมูลประเภทนี้จะถูกกำหนดให้กับผู้เกี่ยวข้องและมีความจำเป็นต้องใช้ข้อมูลในการปฏิบัติงานได้รับทราบเท่านั้น ซึ่งอาจมีการกำหนดการเข้ารหัสข้อมูล หรือหากต้องการเปิดเผยให้บุคคล ภายนอกองค์กรรับทราบ ก็สามารถกระทำได้ก็ต่อเมื่อเป็นบุคคลที่ได้รับสิทธ์ในการเข้าถึงข้อมูล

2.2.4. ชั้นข้อมูลลับ

เป็นข้อมูลที่มีผลทางธุรกิจขององค์กร ข้อมูลจะถูกใช้งานกับผู้ใช้บางกลุ่ม โดยข้อมูลประเภทนี้จำเป็นต้องเข้ารหัสและบุคคลที่เข้าถึงได้ จะต้องเป็นบุคคลที่ได้รับสิทธิ์ซึ่งได้รับการอนุมัติการนำไปใช้จากผู้บริหาร

2.2.5. ชั้นข้อมูลส่วนบุคคล

เป็นข้อมูลที่สามารถระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม การใช้ข้อมูลจะต้องใช้ตามวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้เท่านั้น

2.3. การควบคุมอุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก

วัตถุประสงค์และขอบเขต

เพื่อรักษาความมั่นคงปลอดภัยจากการปฏิบัติงานหรือเข้าถึงระบบจากระยะไกล

เนื้อหานโยบายและการดำเนินการ

2.3.1. อุปกรณ์สื่อสารแบบพกพา

เพื่อควบคุมการนำอุปกรณ์สื่อสารแบบพกพามาใช้งานเกี่ยวกับข้อมูลขององค์กรให้เป็นไปอย่างปลอดภัย ซึ่งมีแนวทางการปฏิบัติดังนี้

- อุปกรณ์ที่นำมาใช้จะต้องได้รับการลงทะเบียนเข้าใช้งานจากหน่วยงานเทคโนโลยีสารสนเทศ โดยมีการกำหนดสิทธิ์การเข้าถึงข้อมูล เพื่อให้มีความปลอดภัยทางไซเบอร์และข้อมูลส่วนบุคคล
- อุปกรณ์ต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ และมีการปรับปรุงข้อมูลไวรัสให้เป็นปัจจุบันอยู่เสมอ
- มีการตรวจสอบความพร้อมของอุปกรณ์ว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ มีการติดตั้งโปรแกรมตามความจำเป็นและเป็นโปรแกรมที่ถูกต้องตามลิขสิทธิ์
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการดูแล และป้องกันอุปกรณ์พกพาที่ได้รับ
- หากเกิดความเสียหายต่ออุปกรณ์พกพา อันเนื่องมาจากความประมาทของผู้ใช้งาน ผู้นำไปใช้จะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

2.3.2. การปฏิบัติงานจากระยะไกล

เพื่อควบคุมการเข้าถึงระบบหรือข้อมูลภายในบริษัทจากสถานที่อื่น เช่น การทำงานจากที่บ้าน ต้องมีการป้องกันข้อมูลที่ได้รับการเข้าถึง การประมวลผล หรือการจัดเก็บ จากสถานที่ดังกล่าว

- บุคคลที่ต้องการปฏิบัติงานจากระยะไกล จะต้องได้รับการอนุมัติจากหัวหน้าแผนกที่บุคคลนั้นสังกัด และหัวหน้าแผนกเทคโนโลยีสารสนเทศ โดยสิทธิ์ที่ได้รับจะอยู่ภายใต้หลักความจำเป็นต้องรู้ และความจำเป็นต้องใช้งาน
- วิธีการเข้าถึงระบบหรือข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ
- มีการกำหนด Session Timeout เพื่อตัดผู้ใช้งานออกจากระบบ เมื่อไม่มีการใช้งานหรือปล่อยหน้าจอทิ้งไว้ ตามระยะเวลาที่กำหนด
- ผู้ใช้งานที่มีการปฏิบัติงานจากระยะไกล จะต้องปฏิบัติตามนโยบายความปลอดภัยทางด้านระบบสารสนเทศและไซเบอร์ เช่นเดียวกับการปฏิบัติงานภายในบริษัท
- มีการบันทึกรายละเอียดของกิจกรรมที่มีการดำเนินการระหว่างการเข้าถึงระบบหรือข้อมูล ซึ่งการบันทึกดังกล่าวต้องมีข้อมูลที่สามารถระบุตัวบุคคล และเวลาที่เข้าใช้ได้

2.4. การบริหารความเสี่ยงด้านความปลอดภัยสารสนเทศและไซเบอร์

วัตถุประสงค์และขอบเขต

เพื่อให้บริษัทมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ สำหรับเป็นแนวทางในการป้องกัน ตรวจสอบ ตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้น และลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

เนื้อหานโยบายและการดำเนินการ

2.4.1. การประเมินความเสี่ยงและจัดการความเสี่ยง

- กำหนดเกณฑ์การยอมรับความเสี่ยง และเกณฑ์สำหรับการประเมินความเสี่ยงด้านระบบสารสนเทศและไซเบอร์
- ระบุความเสี่ยงที่เกี่ยวข้อง และกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการ
- ประเมินผลกระทบและความรุนแรง หากความเสี่ยงที่ระบุไว้เกิดขึ้น
- ประเมินความเป็นไปได้หรือโอกาส ที่ความเสี่ยงที่ระบุไว้จะเกิดขึ้น
- กำหนดแนวทางในการจัดการ ควบคุม โอนหรือกระจาย และป้องกันความเสี่ยง ให้สอดคล้องกับผลการประเมินความเสี่ยง เพื่อให้ความเสี่ยงที่เหลืออยู่ในระดับที่ยอมรับได้
- มีการตรวจสอบและประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเสนอหรือเกิดการเปลี่ยนแปลงที่สำคัญ โดยประเมินถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้นต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อหาแนวทางในการจัดการ

2.4.2. การติดตามและทบทวนความเสี่ยง

- กำหนดให้มีกระบวนการการติดตามความเสี่ยงทางด้านระบบสารสนเทศและไซเบอร์
- รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยง ตามรอบระยะเวลาที่กำหนด

3. การบริหารจัดการทรัพย์สิน

3.1. หน้าที่ความรับผิดชอบต่อทรัพย์สิน

เพื่อให้มีการระบุทรัพย์สินของบริษัท และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม ทั้งนี้เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลหรือควบคุมทรัพย์สินแทน แต่ความรับผิดชอบสูงสุดในทรัพย์สินดังกล่าวยังคงเป็นของเจ้าของทรัพย์สิน

3.1.1. การจัดการบัญชีทรัพย์สิน

ต้องมีการจัดทำ และปรับปรุงบัญชีทรัพย์สินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโอนย้ายสิทธิ์เจ้าของทรัพย์สิน พร้อมทั้งระบุผู้ที่ถือครองทรัพย์สิน

3.1.2. ความเป็นเจ้าของทรัพย์สิน

ในการจัดทำทะเบียนทรัพย์สิน แต่ละหน่วยงานจะต้องกำหนดเจ้าของทรัพย์สินที่มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้นๆ เจ้าของทรัพย์สินต้องสอบทานความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สิน ตลอดจนการแจ้งถึง การเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับทรัพย์สินให้ผู้ดูแลทรัพย์สินทราบ

3.1.3. การใช้งานทรัพย์สินอย่างเหมาะสม

ต้องมีการระบุจัดทำเป็นลายลักษณ์อักษรให้ความยินยอมจาก ผู้ใช้งาน พนักงาน หรือหน่วยงานภายนอก ตามข้อกำหนดในการใช้งานข้อมูลและทรัพย์สินสารสนเทศ

3.1.4. การคืนทรัพย์สิน

พนักงานและลูกจ้างของหน่วยงานภายนอกทั้งหมด ต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้าง หมดสัญญา หรือสิ้นสุดข้อตกลงจ้าง หากทรัพย์สินพบความชำรุดเสียหาย ผู้ถือครองจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

3.2. การจัดการสื่อที่ใช้ในการบันทึกข้อมูล

- เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูล โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล สื่อบันทึกข้อมูลต่างๆ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม
- มีการลงทะเบียน เพื่อควบคุมการใช้งาน
- ขั้นตอนการใช้งานต้องปฏิบัติตามให้สอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนดไว้
- ประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่หรือมีการเปลี่ยนแปลงสินทรัพย์ที่สำคัญเกิดขึ้น
- สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย โดยต้องปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลาย โดยอ้างอิงจากมาตราฐานซึ่งเป็นที่ยอมรับในสากล
- การขนย้ายสื่อบันทึกข้อมูล ต้องมีการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

4. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

4.1. นโยบายพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้ง และพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูล และสารสนเทศซึ่งเป็นทรัพย์สินของบริษัท รวมถึงการกำหนดมาตราการการป้องกันที่เหมาะสม ตามระดับความสำคัญและความเสี่ยงของแต่ละพื้นที่

<u>เนื้อหานโยบายและการดำเนินการ</u>

4.1.1. ขอบเขต หรือบริเวณโดยรอบทางกายภาพ

ศูนย์คอมพิวเตอร์อยู่ในพื้นที่ควบคุม การเข้าถึงจะต้องเป็นผู้ได้รับอนุญาต พื้นที่โดยรอบมีระบบรักษาความปลอดภัยตามมาตราฐานของศูนย์คอมพิวเตอร์

4.1.2. การควบคุมการเข้า-ออกทางกายภาพ

- มีการลงทะเบียนผู้ใช้งานที่มีสิทธิ์ผ่านเข้า-ออก เพื่อปฏิบัติหน้าที่ตามงานสิทธิ์ที่ได้รับ

● อนุญาตให้ผ่านเข้า-ออกเฉพาะผู้ที่มีหน้าที่ปฏิบัติงานภายในพื้นที่ หรือ ผู้ที่ได้รับอนุญาตตามความจำเป็นเท่านั้น โดยต้องมีเหตุผลเพียงพอในการขออนุญาต

● มีการพิสูจน์และยืนยันตัวตนเพื่อควบคุมการเข้า-ออกพื้นที่ เช่น บันทึกวันและเวลาการเข้า-ออกพื้นที่ การใช้บัตรเพื่อเข้า - ออกพื้นที่

● ในกรณีของบุคคลภายนอก จะต้องมีเจ้าหน้าที่ของฝ่ายสารสนเทศอยู่กับบุคคลที่มาติดต่อตลอดเวลา

4.1.3. การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน พื้นที่ทำงาน และอุปกรณ์ต่างๆ

มีการจัดเตรียมอุปกรณ์รักษาความปลอดภัยในการเข้าถึงศูนย์คอมพิวเตอร์ ดังนี้

● มีระบบควบคุมการเข้า - ออกพื้นที่ ด้วยคีย์การ์ด ประตูจะถูกล็อคเสมอ

● ติดตั้งกล้องวงจรปิด และบันทึกภาพภายในห้องตลอดเวลา โดยสามารถดูข้อมูลย้อนหลังได้ 21 วัน

4.1.4. การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม

● มีระบบป้องกันอัคคีภัย มีอุปกรณ์ดักจับควัน และถังดับเพลิงอุปกรณ์อิเล็กทรอนิคส์

● มีระบบตรวจจับน้ำล้น เพื่อแจ้งเตือนให้ผู้ดูแลรับทราบปัญหาได้ทันที

● มีระบบควบคุมอุณหภูมิและความชื้น โดยจะมีแอร์ 3 ชุด ทำงานสลับกัน และตั้งค่าให้เหมาะสมกับการทำงานของอุปกรณ์คอมพิวเตอร์

● มีระบบสำรองไฟฟ้า และระบบป้องกันจากความไม่เสถียรของไฟฟ้า

● ระบบกล้องวงจรปิด เพื่อใช้ในการตรวจสอบความผิดปกติภายในศูนย์คอมพิวเตอร์

● จัดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา

4.2. นโยบายเกี่ยวกับการจัดการของอุปกรณ์

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต อันเนื่องมากจากการสูญหาย การเสียหาย การโจรกรรม หรือการกระทำที่เป็นอันตรายต่อทรัพย์สิน เจ้าหน้าที่หรือผู้ใช้งานต้องดูแลและป้องกันอุปกรณ์ของบริษัท เพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายต่างๆ รวมถึงการความเสี่ยงการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

<u>เนื้อหานโยบายและการดำเนินการ</u>

4.2.1. การติดตามการทำงานของเครื่องแม่ข่าย

● มีการจัดทำรายงานสถานะการทำงานของเครื่องแม่ข่ายต่างๆ รวมถึงอุปกรณ์รอบข้างทุกวัน

● จัดทำรายงานสรุปสถานะของเครื่องแม่ข่าย ให้ทางผู้บริหารรับทราบทุกๆ 6 เดือน

4.2.2. ระบบและอุปกรณ์สนับสนุนการทำงาน

● อุปกรณ์คอมพิวเตอร์และเครือข่ายที่สาคัญ ต้องมีอุปกรณ์สำรองไฟฟ้าฉุกเฉิน เพื่อให้ระบบสามารถทำงานได้ต่อเนื่อง หรือสิ้นสุดการทำงานอย่างเหมาะสม เมื่อระบบไฟฟ้าขัดข้อง

● มีระบบและเจ้าหน้าที่เฝ้าระวัง และรายงานเมื่อพบข้อผิดพลาด

● ติดตั้งระบบแจ้งเตือน เมื่อระบบสนับสนุนการทำงานภายในศูนย์คอมพิวเตอร์ ทำงานผิดปกติหรือหยุดการทำงาน

- จัดให้มีการตรวจสอบ หรือทดสอบระบบและอุปกรณ์สนับสนุนอย่างน้อยปีละ 2 ครั้ง เพื่อให้มั่นใจได้ว่าระบบและอุปกรณ์สามารถทำงานได้ตามปกติ

4.2.3. การบำรุงรักษาอุปกรณ์

- กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต หรือมาตราฐานการบำรุงรักษา
- บันทึกปัญหา และวิธีการแก้ไขปัญหาของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- บันทึกกิจกรรมการบำรุงอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบ หรือประเมินภายหลัง

5. การเข้ารหัสข้อมูล

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อรักษาความปลอดภัยของข้อมูล และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม สามารถป้องกันการเข้าถึง เปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับ หรือมีความสำคัญ ทั้งในด้านความลับและความถูกต้องของข้อมูล

<u>เนื้อหานโยบายและการดำเนินการ</u>

5.1. การใช้มาตรการเข้ารหัสข้อมูล

จัดให้มีนโยบายควบคุมการใช้งานระบบการเข้ารหัสข้อมูลที่คำนึงถึงชนิด และวิธีการเข้ารหัสข้อมูลที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับ หรือมีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการดำเนินนโยบาย และการบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล โดยผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญ เช่น

- กำหนดรูปแบบ Wireless Security ให้เป็น WPA/WPA2 (WIFI Protected Access) ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายคอมพิวเตอร์สาธารณะ ควรได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น VPN
- รหัสผ่านต่าง ๆ ที่เก็บอยู่ในระบบฐานข้อมูล จะถูกเข้ารหัสไว้เจ้าของรหัส รวมถึงซอฟต์แวร์เจ้าของข้อมูลส่วนบุคคลเท่านั้น ที่ทราบรหัสผ่านดังกล่าว

6. การควบคุมการเข้าถึง

6.1. การควบคุมการเข้าถึงตามความต้องการทางธุรกิจ

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ เพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสมจำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็น และความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความปลอดภัย

เนื้อหานโยบายและการดำเนินการ

6.1.1. การควบคุมการเข้าถึง

ต้องกำหนดสิทธิ์ในการเข้าถึงสารสนเทศ ระบบประมวลผลสารสนเทศ และสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ ตามวัตถุประสงค์ทางธุรกิจ ภายใต้หลักความจำเป็นต้องรู้ และความจำเป็นต้องใช้งาน พร้อมทั้งบันทึกรายการการเข้าถึงและนำรายการดังกล่าว มาทบทวนตามความต้องการทางธุรกิจ และความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ โดยการบันทึกนั้นจะต้องประกอบด้วยข้อมูลที่สามารถระบุตัวบุคคล ระยะเวลา และกิจกรรมที่ดำเนินการได้

6.2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์และขอบเขต

เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

เนื้อหานโยบายและการดำเนินการ

6.2.1. การลงทะเบียนและการเพิกถอนทะเบียนผู้ใช้งาน

1) พนักงานทุกคนที่มีสิทธิ์เข้าใช้งานระบบข้อมูลต้องมีบัญชีผู้ใช้งานเฉพาะบุคคลในการเข้าสู่ระบบ

2) บัญชีผู้ใช้งานเป็นข้อมูลเฉพาะบุคคล ไม่มีการแชร์การใช้งานร่วมกับบุคคลอื่น

3) ในกรณีที่พนักงานลาออก บัญชีผู้ใช้งานรายนั้นต้องไม่ถูกนำกลับมาใช้ใหม่

4) หากมีความจำเป็นต้องใช้ชื่อผู้ใช้งานร่วมกัน (Share Use Account) ต้องกำหนดสิทธิ์ให้ต่ำที่สุด เช่น สามารถอ่านข้อมูลได้อย่างเดียว (Read Only)

6.2.2. การจัดการสิทธิการเข้าถึงของผู้ใช้งาน

1) ในการร้องขอเพื่อเข้าใช้งานระบบใด ๆ ผู้บังคับบัญชาในหน่วยงานต้องทำการพิจารณาให้ความเห็นชอบ

2) บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น

3) ผู้ดูแลระบบต้องดำเนินการปรับปรุงสิทธิ์ หลังจากได้รับแจ้งจากหน่วยงานต้นสังกัด ในกรณีที่ผู้ใช้งานลาออก เปลี่ยนตำแหน่งงาน โอนย้าย สิ้นสุดการว่าจ้าง ฯลฯ

6.2.3. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

ต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง โดยทางฝ่ายเทคโนโลยีสารสนเทศ จะทำรายการข้อมูลผู้ใช้งานและสิทธิ์การเข้าใช้งาน เพื่อให้ทางเจ้าของระบบงานนั้นๆ ตรวจสอบและยืนยันความถูกต้อง หากพบความผิดปกติใดๆ ให้แจ้งฝ่ายเทคโนโลยีสารสนเทศ เพื่อปรับปรุงข้อมูลให้ถูกต้อง

6.3. หน้าที่ความรับผิดชอบของผู้ใช้งาน

วัตถุประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต และมุ่งเน้นให้ผู้ใช้งานระบบสารสนเทศ มีความรับผิดชอบในการป้องกันข้อมูลที่ใช้ในการพิสูจน์และยืนยันตัวตน

เนื้อหานโยบายและการดำเนินการ

6.3.1. การใช้ข้อมูลการพิสูจน์และยืนยันตัวตนซึ่งเป็นข้อมูลลับ

- ผู้ใช้งานต้องเก็บรักษารหัสผ่าน สำหรับการเข้าใช้งานระบบสารสนเทศให้เป็นความลับ ห้ามเปิดเผยหรือแบ่งปันให้บุคคลอื่นทราบ
- เมื่อผู้ใช้งานได้รับข้อมูลรหัสผ่าน ซึ่งเป็นค่าเริ่มต้น (Default) ควรมีการแก้ไขทันทีเมื่อเข้าใช้งานระบบครั้งแรก
- ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีความยาวอย่างน้อย 8 ตัวอักษร ซึ่งประกอบด้วยตัวอักษร สัญลักษณ์ และตัวเลข ไม่ใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน เช่น วันเดือนปีเกิด หมายเลขโทรศัพท์
- ผู้ใช้งานต้องตรวจสอบว่าสิทธิ์ที่ตนได้รับในการเข้าใช้ระบบเหมาะสมกับหน้าที่ที่ตนรับผิดชอบหรือไม่ หากพบว่าสิทธิ์ที่ ได้รับไม่เหมาะสม จะต้องแจ้งผู้บังคับบัญชาให้รับทราบ เพื่อพิจารณาและปรับเปลี่ยนให้เหมาะสม
- ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแลรักษาบัญชีการใช้งานและรหัสผ่านของตนเอง รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้
- ผู้ใช้งานต้องหลีกเลี่ยงการเก็บบันทึกข้อมูลการตรวจสอบความลับ เว้นแต่สามารถเก็บไว้อย่างปลอดภัย
- ไม่จดรหัสผ่านลงในกระดาษหรือไฟล์เอกสารที่ไม่มีการป้องกันการเข้าถึง
- ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานและรหัสผ่านของตนทั้งหมด หากผู้ใช้งานสงสัยว่า บัญชีผู้ใช้งานหรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อฝ่ายเทคโนโลยีสารสนเทศ และดำเนินการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที

7. การบริหารจัดการด้านการสื่อสารข้อมูลและดำเนินการ

วัตถุประสงค์และขอบเขต

1) ป้องกันข้อมูลในระบบสารสนเทศ โครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัท ให้มีความปลอดภัย สามารถใช้งานการสื่อสารได้อย่างมีประสิทธิภาพ

2) ให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคง ปลอดภัยรวมถึงการป้องกันข้อมูลสารสนเทศจากภัยคุกคามในรูปแบบต่างๆ

3) เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในบริษัท และถ่ายโอนข้อมูลกับภายนอก

เนื้อหานโยบายและการดำเนินการ

7.1. การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย

7.1.1. ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย

- ป้องกันระบบเครือข่ายภายในให้ปลอดจากการเข้าถึงและการดัดแปลงโดยไม่ได้รับอนุญาต
- จำกัดการเข้าถึงระบบเครือข่าย และระบบสารสนเทศที่เชื่อมต่ออยู่กับระบบเครือข่าย โดยกำหนดให้ผู้ใช้งานในเครือข่ายสามารถเข้าถึงระบบสารสนเทศผ่านทางเครือข่ายที่ได้รับการอนุญาตเท่านั้น

- ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต
- การเข้าถึงอุปกรณ์เครือข่ายเพื่อการตรวจสอบและปรับแต่งระบบทั้งทางกายภาพ และการเข้าถึงจากระยะไกลต้องมีการควบคุม และทำได้เพียงแต่เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ในกรณีที่ต้องกำหนดสิทธิการเข้าถึงแบบชั่วคราวแก่บุคคลภายนอก ต้องให้มีผู้ควบคุม ตรวจสอบและยกเลิกสิทธิการเข้าถึงทันทีที่ปฏิบัติงานเสร็จ
- ต้องมี Security Log เพื่อตรวจสอบเหตุการณ์และปัญหาที่เกิดขึ้น
- สำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์เครือข่ายทุกครั้งที่มีการเปลี่ยนแปลงค่า

7.1.2. การจัดแบ่งเครือข่าย

- แยกระบบเครือข่ายภายใน และภายนอกออกจากกัน เพื่อควบคุมการเข้าถึงระบบหรือข้อมูลสารสนเทศภายในบริษัท
- จัดทำแผนผังเครือข่าย ซึ่งมีรายละเอียดเกี่ยวข้องกับขอบเขตของระบบเครือข่ายภายในและการเชื่อมต่อไปยังภายนอกบริษัท พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ประเมินประสิทธิภาพของระบบเครือข่ายอย่างน้อยปีละ 1 ครั้ง และวางแผนในการปรับปรุงระบบเครือข่ายให้สามารถรองรับปริมาณงานที่จะขยายตัวในอนาคต

7.2. การถ่ายโอนข้อมูลสารสนเทศ

- ต้องมีการถ่ายโอนสารสนเทศด้วยวิธีการที่ปลอดภัย และเหมาะสมกับประเภทชั้นของสารสนเทศตามที่บริษัทกำหนด
- การรับ-ส่งข้อมูลหรือไฟล์อิเล็กทรอนิกส์ที่เป็นความลับระหว่างหน่วยงานภายในหรือภายนอกบริษัท ต้องได้รับการเข้ารหัสข้อมูลตามนโยบายและการดำเนินการการเข้ารหัสข้อมูล
- กำหนดให้มีข้อตกลงในการรักษาความลับหรือไม่เปิดเผยความลับอย่างเป็นลักษณ์อักษร กับผู้ให้บริการภายนอก (Confidentiality or Non-Disclosure Agreements)

8. การจัดหา การพัฒนา และการบำรุงรักษาระบบ

8.1. การกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อควบคุมการพัฒนา หรือการแก้ไขเปลี่ยนแปลงข้อมูลระบบสารสนเทศ ให้มั่นใจได้ว่าการดำเนินการนั้นๆ ได้คำนึงถึงความปลอดภัยและความเป็นข้อมูลส่วนบุคคล มีการประเมินความเสี่ยง รวมถึงการควบคุมที่สอดคล้องตามหลักการที่เป็นมาตรฐานสากล โดยจะครอบคลุมตั้งแต่ขั้นตอนการร้องขอจนถึงการนำระบบงานหรือข้อมูลไปใช้งานจริง

8.2. กระบวนการพัฒนาระบบ

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมทั้งกระบวนการการพัฒนาระบบสารสนเทศ

<u>เนื้อหานโยบายและการดำเนินการ</u>

8.2.1. กระบวนการในการควบคุมการเปลี่ยนแปลงระบบ

- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร โดยอาจเป็น Electronic Transaction เช่น อีเมล และต้องได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ
- ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน การรักษาความปลอดภัย และการทำงานของระบบงานที่เกี่ยวข้อง
- ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

8.2.2. การทดสอบเพื่อรับรองระบบ

- มีการจัดทำแผนการทดสอบ โดยต้องจัดทำทั้งระบบเดิมและระบบที่มีการปรับปรุง
- ผู้ที่ร้องขอ และหน่วยงานเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้อง ต้องมีส่วนร่วมในการทดสอบเพื่อให้มั่นใจว่าระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลง มีการทำงานที่มีประสิทธิภาพ ประมวลผลถูกต้อง และเป็นไปตามความต้องการ ก่อนที่จะโอนย้ายไปใช้งานจริง

8.3. ข้อมูลสำหรับการทดสอบ

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

<u>เนื้อหานโยบายและการดำเนินการ</u>

1) สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการใช้งานจริง มีการแยกส่วนออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

2) ไม่นำข้อมูลส่วนบุคคลมาใช้ทดสอบระบบงาน ก่อนได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หากมีความจำเป็นต้องนำข้อมูลที่มีความอ่อนไหว มาใช้ทดสอบระบบงาน ต้องไม่มีข้อมูลที่สามารถระบุตัวบุคคลได้

3) มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อทำการทดสอบ ต้องมีการควบคุมการเข้าถึงข้อมูลเหมือนกับการควบคุมบนระบบใช้งานจริง ให้เป็นไปตามชั้นความลับและการคุ้มครองข้อมูลส่วนบุคคล

9. การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการภายนอก (IT Outsourcing)

วัตถุประสงค์และขอบเขต

เพื่อให้มีการป้องกันทรัพย์สินของบริษัทที่มีการเข้าถึงโดยผู้รับดำเนินการภายนอก

เนื้อหานโยบายและการดำเนินการ

1) ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท กำหนดหน้าที่ความรับผิดชอบ และจัดทำเป็นลายลักษณ์อักษร เมื่อผู้รับดำเนินการภายนอกมีความจำเป็นต้องเข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท

2) ต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

3) หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

4) มีการตรวจประเมินผู้ให้บริการจากภายนอกทุกปี โดยจัดทำในแบบฟอร์มการประเมินและคัดเลือกผู้ขาย/ผู้ให้บริการ

10. การบริหารจัดการสถานการณ์ความมั่นคงปลอดภัยด้านระบบสารสนเทศและไซเบอร์

วัตถุประสงค์และขอบเขต

เพื่อให้มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล ซึ่งรวมถึงเหตุการณ์ภัยคุกคามทางไซเบอร์ ให้ได้รับการดำเนินการที่เหมาะสมทันการณ์

เนื้อหานโยบายและการดำเนินการ

10.1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ

ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติ เพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท

10.2. การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและการเก็บรวบรวมหลักฐาน

1) กำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยด้านระบบสารสนเทศ และไซเบอร์อย่างชัดเจน

2) ผู้ใช้งานระบบสารสนเทศของบริษัทมีหน้าที่ในการรายงานเหตุละเมิดหรือจุดอ่อนด้านความมั่นคงใดๆ ที่พบเห็นหรือต้องสงสัยต่อผู้บังคับบัญชาและ/ หรือฝ่ายเทคโนโลยีสารสนเทศโดยทันที เพื่อให้สามารถแก้ไขปัญหาได้อย่างทันท่วงทีหรือจำกัดความเสียหายที่อาจเกิดขึ้น ตัวอย่างของเหตุละเมิดความมั่นคงที่ต้องรายงาน เช่น

- พบไวรัส หรือโปรแกรมไม่ประสงค์ดีต่าง ๆ
- ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือสูญหาย
- มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน
- การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่าย
- เหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัยขององค์กร

3) ข้อมูลและหลักฐานที่เกี่ยวข้องกับเหตุละเมิดความมั่นคงที่เกิดขึ้นทั้งหมด ต้องได้รับการบันทึกและจัดเก็บอย่างปลอดภัยตามกฎ หรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

10.3. การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

หากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ประเมินแล้วพบว่าการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล จะแจ้งเหตุละเมิดแก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ โดยต้องมีรายละเอียดดังนี้

1) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล

2) ช่องทางติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือบุคคลที่ได้รับมอบหมายให้ประสานงาน

3) ผลกระทบที่อาจเกิดขึ้น

4) แนวทางเยียวยาความเสียหาย มาตรการที่จะป้องกัน ระงับ แก้ไขเหตุละเมิด

นอกจากนี้ บริษัทจะทำการแจ้งเหตุดังกล่าวไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามหน้าที่ของบริษัทในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

11. ความมั่นคงปลอดภัยทางด้านระบบสารสนเทศและไซเบอร์ ของการบริหารจัดการความต่อเนื่องทางธุรกิจ

11.1. ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อป้องกันการหยุดชะงักในการดำเนินธุรกิจของบริษัท อันเนื่องมาจากมาจากความล้มเหลวหรือการหยุดทำงานของระบบ ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม ลดความรุนแรงของผลกระทบให้อยู่ในระดับที่ยอมรับได้ และให้สามารถดำเนินธุรกิจของบริษัทต่อไปได้

<u>เนื้อหานโยบายและการดำเนินการ</u>

11.1.1. การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

ต้องจัดทำแผนเตรียมความพร้อม เพื่อรับมือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นได้ ทั้งจากวิธีการทางอิเล็กทรอนิกส์และวิธีทางกายภาพ ซึ่งการทำแผนต้องวิเคราะห์และประเมินความเสี่ยงที่กระทบต่อการดำเนินธุรกิจขององค์กร โดยต้องมีรายละเอียดอย่างน้อยดังนี้

1) กำหนดหน้าที่และความรับผิดชอบของบุคคลที่เกี่ยวข้อง

2) กำหนดขั้นตอนการปฏิบัติในการกู้คืนระบบสารสนเทศ

3) กำหนดขั้นตอนการปฏิบัติในการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้

4) กำหนดให้ทบทวนหรือปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

5) กำหนดให้ทำการทดสอบแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

6) กำหนดช่องทางการสื่อสารไปยังพนักงานทุกคน เพื่อให้รับทราบถึงแผนการดำเนินการเมื่อเกิดเหตุฉุกเฉิน

11.2. การเตรียมอุปกรณ์ประมวลผลสำรอง

วัตถุประสงค์และขอบเขต

เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

เนื้อหานโยบายและการดำเนินการ

1) ประเมินและกำหนดระบบสารสนเทศสำหรับระบบสำคัญ รวมไปถึงจัดเตรียมอุปกรณ์ที่สามารถทำงานทดแทนได้อย่างเหมาะสม

2) กำหนดสถานที่และเตรียมพื้นที่ให้อยู่ในสภาพพร้อมใช้งานสำหรับ ระบบทำงานทดแทน

3) กำหนดให้มีการทดสอบระบบปฏิบัติงานสำรองอย่างสม่ำเสมอ เพื่อมั่นใจได้ว่าจะสามารถทำงานทดแทนระบบหลักได้เมื่อมีความจำเป็นต้องใช้งาน

12. การปฏิบัติตามข้อกำหนด

12.1. การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและสัญญาจ้าง

วัตถุประสงค์และขอบเขต

เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ รวมทั้งการคุ้มครองข้อมูลส่วนบุคคล

เนื้อหานโยบายและการดำเนินการ

1) พนักงานทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบายกฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยมีรายการดังต่อไปนี้เป็นอย่างน้อย

- นโยบายความปลอดภัยทางด้านระบบสารสนเทศและไซเบอร์ของบริษัท
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- พระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์
- พระราชบัญญัติลิขสิทธิ์
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

2) ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัท ถือเป็นสินทรัพย์ของบริษัท (ยกเว้นข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์) ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้ เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

3) เพื่อวัตถุประสงค์ในการบริหารจัดการ และรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งาน เพื่อให้มั่นใจว่ามีการใช้งานตรงตามนโยบายต่าง ๆ ของบริษัทที่กำหนดไว้

4) บริษัทขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่ต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตามบริษัท จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้น

5) ห้ามผู้ใช้งาน ใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

6) ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ ในการใช้งานทรัพย์สินทางปัญญาที่บริษัทจัดหามาใช้งาน

7) ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ ข้อมูลหรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดสิทธิ์บนอุปกรณ์อิเล็กทรอนิกส์ของบริษัทโดยเด็ดขาด

12.2. การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและรายละเอียดทางเทคนิค

ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงาน ตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้

ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่ ตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมถึงการตรวจสอบระบบโดยใช้ซอฟต์แวร์ค้นหาช่องโหว่ และทดสอบการโจมตีระบบ เพื่อตรวจสอบข้อบกพร่องของระบบด้วย