SC GROUP

นโยบายความปลอดภัยสารสนเทศ

(IT Policy)

1. ข้อกำหนดทั่วไป

1.1. วัตถุประสงค์ของนโยบาย

นโยบายความปลอดภัยสารสนเทศฉบับนี้ จัดทำขึ้นเพื่อใช้เป็นแนวทางและกฎเกณฑ์ปฏิบัติสำหรับการจัดการทรัพย์สินข้อมูลสารสนเทศของบริษัท มีวัตถุประสงค์เพื่อปกป้องทรัพย์สินข้อมูลสารสนเทศบริษัท

1.2. ขอบเขตของนโยบาย

นโยบายฉบับนี้ครอบคลุมบริษัทและบริษัทในเครือ ทั้งนี้ บริษัทในเครือจะต้องนำนโยบายฉบับนี้ไปใช้หรือไปเป็นแนวทางในการจัดทำนโยบาย หลักเกณฑ์และขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

1.3. ผู้ที่ต้องปฏิบัติตามนโยบายฉบับนี้

กรรมการ ผู้บริหารและพนักงานทุกระดับของบริษัท รวมถึงบุคคลหรือนิติบุคคลอื่นๆ ที่ปฏิบัติงานแทนหรือทำในนามบริษัท เช่น บุคคลภายนอกที่ได้รับการว่าจ้างในลักษณะสัญญาชั่วคราว เป็นต้น มีหน้าที่ต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

1.4. ความถี่ในการทบทวนนโยบาย

ทุก 1 ปี หรือ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2. หลักการทั่วไป

การนำเทคโนโลยีเข้ามาใช้เพื่อรองรับการเพิ่มขึ้นของปริมาณการทำธุรกรรม ทั้งในเรื่องของการบริหารจัดการ การจัดเก็บข้อมูลและการประมวลผลข้อมูล ทำให้การดำเนินงานมีความสะดวกรวดเร็ว มีประสิทธิภาพ และเพิ่มโอกาสแข่งขันในทางธุรกิจได้มากขึ้น อย่างไรก็ตาม เทคโนโลยีอาจนำมาซึ่งความเสี่ยงและภัยคุกคามหลายรูปแบบ ซึ่งหากไม่มีการบริหารจัดการความปลอดภัยสารสนเทศที่เหมาะสมและรัดกุมเพียงพอก็อาจทำให้ข้อมูลสารสนเทศที่ขึ้นอยู่กับเทคโนโลยีเหล่านั้นถูกเปิดเผย แก้ไขเปลี่ยนแปลง ทำลาย หรือทำให้สูญหาย และอาจส่งผลกระทบต่อการดำเนินธุรกิจ ความไว้วางใจจากลูกค้า ภาพลักษณ์และชื่อเสียงของบริษัทได้

3. นิยาม

3.1. ข้อมูลสารสนเทศ (Information)

หมายถึง ข้อมูลและสารสนเทศทั้งที่อยู่ในรูปเอกสารและข้อเท็จจริงที่อยู่ในรูปแบบต่างๆเช่นข้อมูลที่อยู่ในแบบฟอร์มของบริษัทรวมถึงที่อยู่ในระบบสารสนเทศระบบเครือข่ายอุปกรณ์คอมพิวเตอร์หรือสื่อในการจัดเก็บข้อมูลของบริษัทไม่ว่าข้อมูลเหล่านี้จะอยู่ในรูปแบบใดๆเช่นในรูปของเอกสารที่จัดพิมพ์เทปแม่เหล็กข้อมูลออนไลน์หรือรูปแบบอื่นๆคำว่า “ข้อมูล” ที่ระบุในนโยบายฉบับนี้มีความหมายรวมถึง “สารสนเทศ”

3.2. ระบบสารสนเทศ (Information System)

หมายถึง ระบบงานคอมพิวเตอร์ระบบการสื่อสารระบบข้อมูลต่างๆที่มีการบันทึกประมวลผลเรียกดูหรือมีการโอนย้ายผ่านระบบดังกล่าวรวมไปถึงโปรแกรมข้อกำหนดของระบบและกระบวนการต่างๆที่ใช้ในการปฏิบัติงานและการบำรุงรักษาระบบ

3.3. การให้บริการจากหน่วยงานภายนอก (External Party Services)

หมายถึง การให้บริการเก็บรักษาข้อมูลการให้บริการประมวลผลข้อมูลผู้จัดจำหน่ายฮาร์ดแวร์และซอฟต์แวร์ปรึกษาทางด้านธุรกิจและด้านความปลอดภัยรวมถึงประเภทของการให้บริการอื่นที่ไม่ได้ให้บริการอยู่ภายในบริษัทด้วย เช่นการให้บริการด้านอินเทอร์เน็ตและระบบเครือข่ายงานที่เชื่อมต่อกันทั่วโลก

3.4. เจ้าของข้อมูล (Information Owner)

หมายถึง ผู้บริหารของหน่วยงานทางธุรกิจที่ทำหน้าที่รับผิดชอบต่อการสร้างข้อมูลหรือความเชื่อถือได้ของข้อมูล

3.5. ผู้ใช้ข้อมูล (Information User)

หมายถึง กลุ่มบุคคลต่างๆ ไม่ว่าจะเป็นพนักงานผู้ให้บริการ/จำหน่ายระบบคู่สัญญาหรือผู้อื่นที่มีสิทธิในการใช้ข้อมูลในการปฏิบัติงานประจำวัน

3.6. หน่วยงานดูแลข้อมูล (Information Custodians)

หมายถึง บุคคลหรือหน่วยงานที่ได้รับมอบหมายจากเจ้าของข้อมูลให้ทำหน้าที่รับผิดชอบดูแลข้อมูล

4. ข้อกำหนดเฉพาะ

4.1. โครงสร้างด้านความปลอดภัยสารสนเทศภายในองค์กร (Internal organization)

4.1.1. ความรับผิดชอบของผู้บริหารของบริษัทต่อความปลอดภัยสารสนเทศ

4.1.1.1. ความรับผิดชอบของผู้บริหารของบริษัท ต่อความปลอดภัยสารสนเทศนั้น ผู้บริหารของบริษัทต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความปลอดภัยสารสนเทศ โดยพิจารณาในเรื่องต่าง ๆ ดังต่อไปนี้

- สอบทานและอนุมัตินโยบายความปลอดภัยสารสนเทศ มาตรฐาน และระเบียบปฏิบัติที่มีการเปลี่ยนแปลงหรือเพิ่มเติม
- ตรวจสอบสถานภาพปัจจุบันและเหตุการณ์ที่กระทบกับ ความปลอดภัยสารสนเทศของบริษัท
- อนุมัติโครงการที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ
- กำหนดนโยบายและเป้าหมายความปลอดภัยด้านสารสนเทศและการปกป้องข้อมูลของบริษัท
- ประเมินความเหมาะสมด้านค่าใช้จ่ายและคุณภาพในการปกป้องข้อมูล

4.1.2. หน้าที่ความรับผิดชอบทางด้านการรักษาความปลอดภัยสารสนเทศ

4.1.2.1. เจ้าของข้อมูล (Information Owner) คือผู้จัดการ/ผู้บริหารหน่วยงานทางธุรกิจซึ่งมีหน้าที่รับผิดชอบ ทรัพย์สินข้อมูลของบริษัท ซึ่งหน้าที่ความรับผิดชอบโดยสังเขป ได้แก่

- กำหนดการจัดชั้นข้อมูล และมีการตรวจตราข้อมูลเป็นระยะๆเพื่อพิจารณาว่าการจัดชั้นข้อมูลนั้น เหมาะสมกับความต้องการทางธุรกิจ

- มีการตรวจตราให้มั่นใจว่าการควบคุมความปลอดภัยที่เหมาะสมกับระดับความสำคัญของข้อมูล
- มีการตรวจตราให้มั่นใจว่ามีการจัดชั้นข้อมูลในสื่อประเภทต่างๆ
- กำหนดกฎเกณฑ์ในการให้สิทธิและตรวจทานสิทธิการเข้าใช้ข้อมูล ณ ปัจจุบัน
- กำหนดความต้องการด้านการสำรองและการกู้ข้อมูล
- ดำเนินการที่เหมาะสมหากมีเหตุการณ์ละเมิดความปลอดภัย

4.1.2.2. ผู้ใช้ข้อมูล (Information User) คือ ผู้ที่นำข้อมูลมาใช้งาน ซึ่งได้แก่พนักงาน ผู้ให้บริการ/ จำหน่ายระบบคู่สัญญา ผู้ให้บริการแก่บริษัท หรือผู้ที่ได้รับอนุญาต ซึ่งหน้าที่ความรับผิดชอบโดยสังเขป ได้แก่

- รักษาความลับของข้อมูลและรหัสผ่านระบบ
- รายงานเหตุการณ์การละเมิดความปลอดภัยให้กับหน่วยงานต้นสังกัดและฝ่ายเทคโนโลยีสารสนเทศ
- ปฏิบัติตามแนวทางระเบียบปฏิบัติและนโยบายความปลอดภัยสารสนเทศของบริษัท
- ใช้งานข้อมูลและทรัพย์สินทางข้อมูลของบริษัท อย่างรับผิดชอบและใช้สำหรับงานที่ได้รับอนุญาตเท่านั้น

4.1.2.3. หน่วยงานดูแลข้อมูล (Information Custodian) คือ ผู้ที่ได้รับมอบอำนาจหน้าที่จากเจ้าของข้อมูลในการดูแลและ/หรือสนับสนุนข้อมูลของบริษัทเนื่องจากเจ้าของข้อมูลอาจขาดความชำนาญหรือทรัพยากรที่จำเป็นในการทำงานทางด้านดูแลข้อมูลหน่วยงานดูแลข้อมูลอาจจะเป็นพนักงานผู้ให้บริการ/จำหน่ายระบบคู่สัญญาหรือบุคคลภายนอกที่ได้รับอนุญาตรายละเอียดการมอบหมายหน้าที่จะถูกระบุไว้ในข้อตกลงระดับการให้บริการระหว่างเจ้าของข้อมูลและหน่วยงานดูแลข้อมูลซึ่งหน้าที่ความรับผิดชอบของหน่วยงานดูแลข้อมูลโดยสังเขป ได้แก่

- สำรองข้อมูลตามความต้องการของเจ้าของข้อมูล
- กู้ข้อมูลและทำให้ธุรกิจสามารถใช้ข้อมูลได้
- นำระบบรักษาความปลอดภัยไปใช้กับระบบปฏิบัติการโปรแกรมประยุกต์ต่างๆและข้อมูลที่เกี่ยวข้องตามระดับความสำคัญของข้อมูลที่ถูกประมวลผล
- ให้ความร่วมมือกับเจ้าของข้อมูลในการพัฒนาการจัดการและดูแลรักษาข้อมูล

4.2. โครงสร้างด้านความปลอดภัยสารสนเทศที่เกี่ยวข้องกับบุคคลภายนอก (External parties)

4.2.1. การประเมินความเสี่ยงจากการเข้าถึงข้อมูลของบุคคลภายนอก

4.2.1.1. ในกรณีที่มีความจำเป็นทางด้านธุรกิจที่ต้องมีการเชื่อมต่อเครือข่ายกับบุคคลภายนอก บริษัทจะต้องทำการประเมินความเสี่ยงเพื่อศึกษาถึงผลกระทบด้านความปลอดภัยและจัดให้มี การควบคุมที่จำเป็นก่อนการอนุญาตให้มีการเข้าถึงข้อมูลของบริษัท

4.2.1.2. นโยบายความปลอดภัยสารสนเทศของบริษัท มีผลบังคับใช้กับบุคคลภายนอก รวมถึงผู้ตรวจสอบภายนอก ซึ่งต้องปฏิบัติตามนโยบายในลักษณะเดียวกับพนักงาน เช่น การกำหนดขอบเขตการเข้าถึงข้อมูลเท่าที่จำเป็นสำหรับการทำงาน เป็นต้น

4.2.2. ข้อกำหนดด้านความปลอดภัยในสัญญาการใช้บริการจากบุคคลภายนอก

4.2.2.1. การอนุมัติสัญญาการใช้บริการจากบุคคลภายนอกที่เกี่ยวข้องกับการจัดการข้อมูลของบริษัทต้องทำโดยฝ่ายกฎหมายฝ่ายเทคโนโลยีสารสนเทศและหน่วยงานทางธุรกิจของบริษัทที่รับผิดชอบในการเลือกใช้บริการจากบุคคลภายนอก

4.2.2.2. ในกรณีที่มีผู้ให้บริการระบบต้องการที่จะเข้าถึงข้อมูลที่สำคัญของบริษัทฝ่ายเทคโนโลยีสารสนเทศต้องมีการตรวจตราให้มั่นใจว่าทางผู้ให้บริการจะใช้ข้อมูลเท่าที่จำเป็นและผู้ให้บริการนั้นๆมีการจัดการด้านความปลอดภัยสารสนเทศการป้องกันระบบหรือการควบคุมการประมวลผลข้อมูลของบริษัทอย่างเหมาะสมส่วนฝ่ายกฎหมายต้องมีการตรวจตราให้มั่นใจว่าคู่สัญญาต้องมีพันธะสัญญาในการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศและระเบียบปฏิบัติบริษัทโดยพันธะสัญญาดังกล่าวต้องส่งให้ฝ่ายกฎหมายของบริษัทเห็นชอบก่อน

4.2.2.3. สัญญาสำหรับการใช้บริการจากบุคคลภายนอกทั้งหมดต้องประกอบด้วย

- ข้อตกลงในส่วนของนโยบายและการควบคุมด้านความปลอดภัย
- การกำหนดระดับการให้บริการและความพร้อมใช้ในการให้บริการ
- สิทธิของบริษัทในการตรวจสอบสภาพแวดล้อมของผู้ให้บริการจากบุคคลภายนอกในส่วนของการควบคุมความปลอดภัยกับข้อมูลและระบบของบริษัท
- ข้อกำหนดทางด้านกฎหมายเกี่ยวกับการปกป้องข้อมูลและความลับ

4.3. การจัดชั้นข้อมูล (Information Classification)

4.3.1. แนวทางการปฏิบัติในการจัดชั้นข้อมูล

4.3.1.1. ทรัพย์สินที่เป็นข้อมูลของบริษัทต้องมีการแบ่งประเภทตามที่กำหนดในแบบแผนของการจัดชั้นข้อมูลซึ่งการจัดชั้นข้อมูลทำให้หน่วยงานทางธุรกิจสามารถพิจารณาถึงความเหมาะสมของการควบคุมที่มีต่อข้อมูลนั้นๆได้รวมถึงการลงทุนเพื่อสร้างระบบการรักษาความปลอดภัยที่เหมาะสมให้กับข้อมูลแต่ละประเภทเพื่อลดผลกระทบที่มีต่อการดำเนินธุรกิจ

4.3.1.2. ก่อนที่จะมีการกำหนดสิทธิในการเข้าถึงข้อมูลใดๆต้องมีการตรวจสอบให้แน่ใจว่าผู้ที่จะได้รับสิทธินั้นเป็นผู้ที่สมควรได้รับสิทธิดังกล่าวซึ่งต้องเป็นไปตามความจำเป็นทางธุรกิจ

4.3.1.3. ข้อมูลของบริษัททุกรูปแบบเช่นข้อมูลรูปแบบเอกสารข้อมูลที่จัดเก็บในแผ่นดิสก์และเทปเป็นต้นต้องได้รับการป้องกันตามประเภทของข้อมูลนั้นๆโดยที่สิทธิเข้าถึงข้อมูลนั้นต้องปฏิบัติเช่นเดียวกับการป้องกันข้อมูลไม่ว่าจะเป็นพนักงานคู่สัญญาและผู้ให้บริการระบบ

4.3.1.4. การเปลี่ยนแปลงระดับการป้องกันข้อมูลจำต้องได้รับความเห็นชอบและอนุมัติจากเจ้าของข้อมูลโดยเป็นหน้าที่และความรับผิดชอบของเจ้าของข้อมูลที่ต้องตรวจตราข้อมูลต่างๆภายใต้การดูแลให้มีระดับการป้องกันตามประเภทที่เหมาะสมอย่างต่อเนื่อง

4.4. นโยบายความปลอดภัยด้านบุคลากร (Human resources security)

4.4.1. ข้อกำหนดด้านความปลอดภัยสารสนเทศในเงื่อนไขการจ้างงาน

4.4.1.1. ฝ่ายบริหารทรัพยากรบุคคลมีหน้าที่เน้นย้ำนโยบายด้านการจัดการข้อมูลที่เป็นความลับและต้องการความปลอดภัยแก่พนักงาน โดยเมื่อมีการว่าจ้างพนักงานใหม่ พนักงานใหม่มีหน้าที่ศึกษาทำความเข้าใจนโยบาย

ความปลอดภัยสารสนเทศ และเอกสารต่าง ๆที่เกี่ยวกับความปลอดภัย เพื่อนำไปใช้ประกอบการปฏิบัติงานในแต่ละตำแหน่งหน้าที่งานได้อย่างเหมาะสม

4.4.1.2. พนักงานทุกคนรับทราบ ยอมรับ และยินยอมให้บริษัท สามารถตรวจสอบการทำงานการปฏิบัติงานบนระบบสารสนเทศและระบบเครือข่ายของบริษัท ได้ตลอดเวลา

4.4.1.3. ข้อมูลที่จัดเก็บในอุปกรณ์คอมพิวเตอร์ของบริษัท รวมถึงข้อมูลที่มีการส่งผ่านเครือข่ายของบริษัทและข้อมูลที่อยู่ในระบบจดหมายอิเล็กทรอนิกส์ ถือว่าเป็นข้อมูลของบริษัท ซึ่งบริษัท สามารถตรวจสอบได้ตลอดเวลา

4.4.1.4. ความรับผิดชอบในเรื่องการรักษาความปลอดภัยสารสนเทศบริษัทไม่ได้ครอบคลุมเพียงภายในพื้นที่ของบริษัท เท่านั้น พนักงานมีหน้าที่และความรับผิดชอบในการดูแลรักษาความลับของข้อมูลเมื่อนำข้อมูลไปทำงานภายนอกพื้นที่ของบริษัท หรือนำข้อมูลไปทำงานที่บ้าน รวมถึงการเข้าสู่ระบบของบริษัทจากระยะไกล (Remote Access)

4.4.1.5. การลักลอบอ่านจดหมายอิเล็กทรอนิกส์ โดยผู้ดูแลระบบ ถือว่าเป็นความผิดตามนโยบายของบริษัท ยกเว้นแต่ในกรณีที่ผู้ดูแลระบบได้รับอนุญาตจากผู้บริหารให้เข้าไปตรวจสอบจดหมายอิเล็กทรอนิกส์เป็นรายบุคคลโดยไม่ต้องแจ้งให้พนักงานทราบ ในกรณีที่มีเหตุอันเชื่อได้ว่าพนักงานคนดังกล่าวใช้อุปกรณ์ของบริษัทในทางที่ผิดวัตถุประสงค์การทำงาน

4.4.2. การปลูกฝังความตระหนักการเรียนรู้และการฝึกอบรมด้านความปลอดภัยสารสนเทศ

4.4.2.1. ฝ่ายเทคโนโลยีสารสนเทศมีบทบาทในการส่งเสริมให้พนักงานทุกคนได้ตระหนักถึงความปลอดภัยสารสนเทศอย่างสม่ำเสมอซึ่งฝ่ายบริหารทรัพยากรบุคคลและฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ร่วมกันในการพัฒนาและจัดอบรมพนักงานให้ตระหนักถึงความปลอดภัยสารสนเทศของบริษัท

4.4.2.2. ในกรณีการว่าจ้างหน่วยงานภายนอกบุคคลจากหน่วยงานภายนอกหน่วยงานหรือบุคคลเหล่านั้นต้องทำความเข้าใจรับทราบและยินยอมที่ปฏิบัติตามนโยบายด้านความปลอดภัยสารสนเทศและมาตรฐานของบริษัทในสาระสำคัญต่างๆโดยเฉพาะอย่างยิ่งเรื่องการไม่เปิดเผยข้อมูล

4.4.3. การจัดให้มีความปลอดภัยสารสนเทศเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

4.4.3.1. ฝ่ายบริหารทรัพยากรบุคคลต้องแจ้งหน่วยงานกำกับดูแลระบบเทคโนโลยีสารสนเทศทราบทันทีที่มีการโอนย้าย และการลาออกหรือการสิ้นสุดการเป็นพนักงาน เพื่อดำเนินการยกเลิกสิทธิหรือเปลี่ยนแปลงสิทธิในระบบงานและบัตรพนักงาน รวมทั้งเรียกคืนอุปกรณ์ตามความเหมาะสม

4.4.3.2. พนักงานหรือผู้ที่เกี่ยวข้องกับบริษัททุกคนต้องคืนทรัพย์สินของบริษัทที่อยู่ในความครอบครองของตัวพนักงานกลับคืนสู่บริษัททันทีที่สิ้นสุดสภาพการเป็นพนักงานหรือผู้ที่เกี่ยวข้องของบริษัท

4.4.3.3. สิทธิในการเข้าสู่ระบบของพนักงานและผู้ที่เกี่ยวข้องกับบริษัททุกคนต้องถูกยกเลิกออกจากระบบทันทีที่บุคคลเหล่านั้นสิ้นสุดสภาพการเป็นพนักงานหรือผู้ที่เกี่ยวข้องกับบริษัท

4.5. ความปลอดภัยทางกายภาพและสภาพแวดล้อมการทำงาน (Physical and environmental security)

4.5.1. การกำหนดเขตพื้นที่ควบคุม

4.5.1.1. บริษัทต้องมีการจัดระดับความสำคัญของพื้นที่ในอาคารสำนักงานของบริษัท และกำหนดพื้นที่ควบคุมตามผลประเมินความเสี่ยง โดยควรจัดให้มีมาตรการความปลอดภัยเพิ่มเติมสำหรับพื้นที่ที่มีความสำคัญสูง

4.5.1.2. บริษัทต้องมีการกำหนดเขตพื้นที่ควบคุมในทุกพื้นที่ใช้งานของบริษัท ซึ่งระดับความเข้มงวดของการควบคุมขึ้นอยู่กับผลการประเมินความเสี่ยงและภัยคุกคามทางกายภาพการกำหนดเขตพื้นที่ควบคุมโดยสังเขป ได้แก่

- การกำหนดพื้นที่ควบคุมที่ชัดเจน
- ส่วนประกอบของเขตปลอดภัย (เช่น กำแพง ประตู หน้าต่าง และอื่นๆ) ที่เหมาะสม
- การกำหนดให้มีจุดตรวจสอบบุคคลเข้าออกเพื่อควบคุมการเข้าออกอาคารสำนักงานของบริษัท ณ ทางเข้าออกหลัก และสำหรับทางเข้าออกอื่น ๆ ควรมีการนำอุปกรณ์ควบคุมอื่น ๆ มาใช้ เช่น กล้องวงจรปิด หรืออุปกรณ์ตรวจจับการเข้าออก
- การติดตั้งประตูหนีไฟฉุกเฉินตามมาตรฐานความปลอดภัย

4.5.1.3. ห้องเครื่องอุปกรณ์คอมพิวเตอร์และห้องจัดเก็บอุปกรณ์การสื่อสารต้องไม่ตั้งอยู่ในหรือใกล้สถานที่ที่มีความเสี่ยงสูง และต้องตั้งอยู่บนชั้น 2 ของอาคารขึ้นไปเพื่อเป็นการลดโอกาสการถูกโจรกรรมและอุทกภัย

4.5.2. การควบคุมการผ่าน

4.5.2.1. ห้องคอมพิวเตอร์ที่สำคัญต้องมีการควบคุมอย่างเข้มงวดโดยประตูเข้าออกของห้องดังกล่าวต้องถูกปิดล็อคตลอดเวลาบุคคลที่จะเข้าไปใช้งานได้ต้องเป็นบุคคลที่ได้รับอนุญาตและมีกุญแจผ่านหรือรหัสผ่านเพื่อเข้าไปใช้งานได้เท่านั้น

4.5.3. การป้องกันความปลอดภัยของสถานที่ทำงานและอุปกรณ์

4.5.3.1. บริษัทต้องจัดให้มีการติดตามดูแลห้องคอมพิวเตอร์หรือศูนย์ข้อมูลคอมพิวเตอร์ตลอด 24ชั่วโมงการควบคุมเหล่านี้สามารถทำได้โดยการใช้กล้องวงจรปิดการติดสัญญาณเตือนที่ประตูและหน้าต่างการจัดให้มีคนเฝ้าตลอดเวลาหรือใช้หลายวิธีดังกล่าวประกอบกันเพื่อป้องกันการผ่านเข้าออกหรือเข้าถึงข้อมูลอุปกรณ์ที่สำคัญโดยไม่ได้รับอนุญาต

4.5.4. การป้องกันภัยคุกคามจากบุคคลภายนอกและสาธารณภัย

4.5.4.1. บริษัทต้องพิจารณากำหนดขั้นตอนและความรับผิดชอบเกี่ยวกับการใช้สัญญาณเตือนภัยสำหรับระบบที่ต้องการความปลอดภัยสูงเพื่อช่วยลดความเสี่ยงอันเนื่องมาจากการคุกคามจากบุคคลภายนอกหรือภัยอันตรายอื่นๆ

4.5.4.2. อุปกรณ์คอมพิวเตอร์ในห้องเครื่องคอมพิวเตอร์ต้องทำงานอยู่ในสถานที่ที่มีการควบคุมอากาศตลอดเวลาและมีแผนการสำรองการระบายอากาศกรณีที่เครื่องปรับอากาศเกิดชำรุดเสียหายและต้องมีการตรวจจับและป้องกันไฟ (Fire Detector) ภายในสถานที่ที่มีการใช้งานอุปกรณ์คอมพิวเตอร์และมีการกำหนดมาตรการป้องกันที่ดี รวมถึงต้องจัดให้มีอุปกรณ์ดับเพลิงในจุดที่สามารถเข้าถึงได้ง่าย

4.5.4.3. บริษัทต้องจัดเก็บอุปกรณ์และสื่อที่ใช้เก็บสำรองข้อมูลไว้ในสถานที่ที่ห่างจากอุปกรณ์เก็บข้อมูลหลักในระยะที่สามารถป้องกันความเสียหายเมื่อมีเหตุเกิดขึ้นกับสถานที่จัดเก็บอุปกรณ์หลัก

4.5.5. ความปลอดภัยของอุปกรณ์

4.5.5.1. บริษัทต้องจัดให้มีระบบการจ่ายไฟที่เหมาะสมเพื่อป้องกันการหยุดทำงานของระบบเนื่องจากการเกิดปัญหาไฟฟ้าขัดข้องกับอุปกรณ์ที่สำคัญบางส่วนและต้องมีการพิจารณาใช้เครื่องกำเนิดไฟสำรอง (Power Generator) ตามความสำคัญของธุรกิจ

4.5.5.2. บริษัทต้องจัดให้มีการตรวจสอบและบำรุงรักษาอุปกรณ์ทั้งหมดตามวิธีที่ถูกต้องของผู้ผลิตเพื่อให้มีความพร้อมใช้การรักษาความลับและความถูกต้องครบถ้วนของข้อมูลที่อยู่ในอุปกรณ์โดยบริษัทต้องจัดให้มีมาตรการควบคุมที่เหมาะสมสำหรับผู้ที่ได้รับอนุญาตในการบำรุงรักษาซ่อมแซมเท่านั้นรวมทั้งมีการบันทึก

แก้ไขดังกล่าวไว้เป็นหลักฐาน และหากมีความจำเป็นต้องส่งอุปกรณ์ต่างๆ ไปซ่อมแซมภายนอกบริษัทต้องมีการควบคุมที่เหมาะสมเพื่อรักษาความลับและความถูกต้องครบถ้วนของข้อมูลที่อยู่ในอุปกรณ์เหล่านั้น

4.5.5.3. มาตรฐานความปลอดภัยของบริษัทมีผลบังคับใช้กับอุปกรณ์และข้อมูลของบริษัททั้งในและนอกสถานที่

4.5.5.4. พนักงานของบริษัทที่นำเครื่องคอมพิวเตอร์แบบพกพา (Laptop) หรืออุปกรณ์และข้อมูลของ บริษัทไปใช้งานนอกสถานที่ต้องมีความระมัดระวังโดยการพกติดตัวตลอดเวลาหรือต้องมีการควบคุมที่เหมาะสมเมื่อไม่มีคนดูแล

4.5.5.5. อุปกรณ์สำหรับการประมวลผลของบริษัทที่จะทำลายหรือที่จะนำกลับมาใช้ต้องผ่านกระบวนการลบข้อมูล โดยกระบวนการดังกล่าวต้องประกอบไปด้วยการลบข้อมูลที่อยู่ภายในอุปกรณ์และการตรวจสอบหรือทดสอบว่าไม่มีข้อมูลใดๆหลงเหลืออยู่ในอุปกรณ์เหล่านั้นที่สามารถกู้หรือนำกลับมาใช้งานใหม่ได้

4.6. การสื่อสารและการปฏิบัติงาน (Communications and operations)

4.6.1. ระเบียบปฏิบัติในการปฏิบัติงานด้านระบบข้อมูล

4.6.1.1. บริษัทต้องมีการจัดทำและปรับปรุงเอกสารระเบียบปฏิบัติในการปฏิบัติงานด้านระบบข้อมูล เช่น ขั้นตอนการเปิดและปิดระบบ ขั้นตอนการปฏิบัติในกรณีที่พบความล้มเหลวหรือผิดพลาดที่เกิดขึ้นกับระบบขั้นตอนและรูปแบบการสำรองข้อมูลรวมถึงขั้นตอนการกู้คืนระบบเมื่อเกิดความผิดพลาดขึ้นเป็นต้น

4.6.2. การบริหารจัดการการเปลี่ยนแปลง

4.6.2.1. บริษัทต้องมีระเบียบปฏิบัติในการบริหารการเปลี่ยนแปลงทั้งหมดที่เกี่ยวข้องกับระบบประมวลข้อมูลเช่น โปรแกรมที่พัฒนาโดยบริษัท โปรแกรมที่พัฒนาโดยบุคคลภายนอก โปรแกรมที่มีการดัดแปลงโปรแกรมที่ใช้สำหรับการปรับปรุงให้ทันสมัยระบบปฏิบัติการเครือข่ายและอุปกรณ์คอมพิวเตอร์โครงสร้างและรูปแบบของแฟ้มหรือฐานข้อมูล เป็นต้น

4.6.2.2. การขอเปลี่ยนแปลงต้องได้รับการอนุมัติจากผู้จัดการฝ่ายของผู้ขอและหน่วยงานดูแลข้อมูลที่เกี่ยวข้อง

4.6.3. การแบ่งแยกหน้าที่รับผิดชอบ

4.6.3.1. บริษัทต้องกำหนดการแบ่งแยกหน้าที่การทำงานด้านเทคโนโลยีสารสนเทศที่เหมาะสม รวมถึงการแยกสภาพแวดล้อมสำหรับการพัฒนาระบบ (Development) การทดสอบเพื่อการรับรองความถูกต้องของผู้ใช้ (User Acceptance Test) และการใช้งานระบบจริง (Production) ในกรณีที่ไม่สามารถแยกสภาพแวดล้อมสำหรับการทดสอบได้ต้องมีการสร้างสภาพแวดล้อมสำหรับการทดสอบแยกจากสภาพแวดล้อมในการพัฒนาระบบเป็นอย่างน้อย และต้องมั่นใจว่าสภาพแวดล้อมนั้นมีการป้องกันมิให้โปรแกรมเมอร์สามารถทำการแก้ไขระบบได้

4.6.3.2. ผู้ใช้ต้องใช้สภาพแวดล้อมส่วนบุคคล (User Profile) คนละชุดกันสำหรับสภาพแวดล้อมในการพัฒนาระบบ สภาพแวดล้อมสำหรับการทดสอบและในสภาพแวดล้อมในการใช้งานจริง

4.6.3.3. บริษัทต้องไม่มีการคัดลอกข้อมูลที่มีความสำคัญมาไว้ในสภาพแวดล้อมในการพัฒนาระบบหรือสภาพแวดล้อมสำหรับการทดสอบ

4.6.4. การบริหารจัดการการให้บริการจากหน่วยงานภายนอก

4.6.4.1. บริษัทต้องพิจารณาประเมินกระบวนการปฏิบัติงานทั้งหมดที่ทำโดยบุคคลหรือหน่วยงานภายนอกในเรื่องความเสี่ยงและการเปิดเผยข้อมูลด้านความปลอดภัย (Security Exposure) รวมทั้งพัฒนาแนวทางการปฏิบัติงาน

เพื่อจัดการให้ครอบคลุมความเสี่ยงทั้งหมดโดยต้องครอบคลุมหัวข้อทั้งหมดแต่ไม่จำกัดเฉพาะเรื่องที่ระบุดังต่อไปนี้

- การสนับสนุนและความเห็นชอบจากผู้บริหารของหน่วยงานทางธุรกิจ
- การพิจารณาว่ามีข้อมูลที่มีความสำคัญของข้อมูลจะถูกประมวลผลหรือเปิดเผยให้กับบุคคลหรือสถานที่ภายนอกหรือไม่
- การพิจารณามาตรการควบคุมความปลอดภัยที่จัดให้มีโดยบุคคลหรือสถานที่ภายนอก
- การตอบสนองและการจัดการเหตุการณ์เกี่ยวกับความปลอดภัย
- ผลกระทบต่อบริษัทที่เกี่ยวข้องกับแผนรองรับเหตุการณ์ฉุกเฉินหรือแผนความต่อเนื่องทางธุรกิจ

4.6.4.2. การให้บริการโดยบุคคลภายนอก ต้องคำนึงถึงการดำเนินการด้านความปลอดภัยสารสนเทศ คำนิยามของการให้บริการ และการบริหารจัดการการให้บริการ

4.6.4.3. บริษัทต้องจัดให้มีการตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่นการดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ ที่กำหนดให้บันทึกไว้เป็นต้น

4.6.5. การวางแผนและการรับรองระบบ

4.6.5.1. ระบบข้อมูลทุกระบบต้องสามารถรองรับความต้องการด้านสมรรถภาพที่คาดการณ์ไว้ได้ โดยที่หน่วยงานเทคโนโลยีสารสนเทศที่มีหน้าที่รับผิดชอบในการพิจารณาความต้องการทางด้านฮาร์ดแวร์และพื้นที่บนดิสก์สำหรับจัดเก็บข้อมูล รวมทั้งระบบเฝ้าสังเกตผลการปฏิบัติงานด้านสมรรถภาพของระบบ

4.6.5.2. เจ้าของโปรแกรมฝ่ายงานที่เกี่ยวข้องและหน่วยงานเทคโนโลยีสารสนเทศมีหน้าที่ในการกำหนดเกณฑ์การทดสอบเพื่อรับรองความถูกต้องของระบบใหม่ให้มีความชัดเจนและเป็นที่ยอมรับซึ่งมาตรการควบคุมและปัจจัยต่างๆซึ่งควรรวมการพิจารณาในเรื่องดังต่อไปนี้

- ความต้องการด้านประสิทธิภาพการทำงานและความสามารถของระบบ
- แผนรองรับเหตุการณ์ฉุกเฉิน
- เอกสารระเบียบปฏิบัติงานและมาตรการควบคุมด้านความปลอดภัย
- คู่มือการปฏิบัติงาน
- การพิจารณาถึงผลกระทบต่อภาพรวมด้านความปลอดภัยและโครงสร้างทางเทคนิค
- ความต้องการในการฝึกอบรมของเจ้าหน้าที่ด้านปฏิบัติงานและการสนับสนุนผู้ใช้ที่เกี่ยวข้อง
- ความสะดวกในการใช้งาน
- การปฏิบัติตามมาตรฐานการพัฒนาและบำรุงรักษาระบบ

4.6.5.3. ฝ่ายงานที่ร่วมทำการทดสอบต้องมีการลงนามเห็นชอบ (Sign-off) เพื่อรองรับความถูกต้องของโปรแกรมที่ทดสอบก่อนนำไปใช้งานจริง

4.6.6. มาตรการควบคุมซอฟต์แวร์อันตราย

4.6.6.1. หน่วยงานเทคโนโลยีสารสนเทศที่เกี่ยวข้องต้องให้มีมาตรการป้องกันและใช้ความพยายามในการหาต้นเหตุของการแพร่กระจายไวรัสที่พบ รวมทั้งตรวจหาว่ามีเครื่องคอมพิวเตอร์ของบริษัท อื่นที่อาจติดไวรัสหรือไม่ เพื่อให้มั่นใจว่าปัญหาไวรัสทั้งหมดได้รับการจัดการแก้ไข และเครื่องคอมพิวเตอร์ไม่ติดไวรัสอีกอย่างต่อเนื่อง

4.6.6.2. เครื่องคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์ ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชั่นล่าสุดในระดับระบบปฏิบัติการในกรณีที่เป็นไปได้เครื่องเซิร์ฟเวอร์ทุกตัวที่ให้บริการโปรแกรมประยุกต์ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส เพื่อป้องกันไวรัสเข้ามายังเครือข่ายภายในของบริษัท

4.6.7. การสำรองระบบ

4.6.7.1. อุปกรณ์ที่สำคัญในระบบการประมวลผลข้อมูลต้องมีความสามารถในการทำงานอย่างต่อเนื่อง (Fault Tolerance) เพื่อป้องกันการหยุดการให้บริการของธุรกิจอันเนื่องมาจากการทำงานล้มเหลวเพียงจุดใดจุดหนึ่ง (single point of failure)

4.6.7.2. เจ้าของข้อมูลต้องมั่นใจว่าข้อมูลทั้งหมดที่เกี่ยวข้องกับธุรกิจของตนเองที่อยู่บนระบบการประมวลผลของบริษัท ได้มีการทำสำรองข้อมูลเป็นประจำ โดยเจ้าของข้อมูลมีความรับผิดชอบในการร่วมมือกับหน่วยงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าข้อมูลของตนเองทั้งหมดได้รับการสำรองไว้แล้ว และพร้อมจะกู้กลับคืนได้ในกรณีฉุกเฉิน

4.6.7.3. บริษัทต้องจัดให้มีการทดสอบการกู้ข้อมูลสำรองของระบบที่มีความสำคัญทุกระบบ โดยต้องมีการทดสอบอย่างน้อยปีละครั้ง การทดสอบดังกล่าวต้องใช้ข้อมูลที่สำรองจากระบบที่ใช้จริง แต่ทดสอบบนระบบสำรองของบริษัท การสำรองข้อมูลและเก็บรักษาต้องดำเนินการตามแนวทางการปฏิบัติทางการเก็บรักษาข้อมูลของบริษัทโดยมีการกำหนดระยะเวลาในการเก็บรักษาสำหรับข้อมูลทางธุรกิจที่สำคัญ

4.6.7.4. ข้อมูลอิเล็กทรอนิกส์ของบริษัทต้องได้รับการสำรองข้อมูลและเก็บรักษาไว้ตามแนวทางการปฏิบัติทางการเก็บรักษาข้อมูลของบริษัทเช่นเดียวกับข้อมูลอื่นของบริษัททั้งหมดทั้งนี้บริษัทต้องมีการพิจารณากำหนดระยะเวลาในการเก็บรักษาข้อมูลทางธุรกิจที่สำคัญไว้เป็นลายลักษณ์อักษร

4.6.8. การทำลายข้อมูล

4.6.8.1. บริษัทต้องลบข้อมูลภายในหรือทำลายสื่อทางกายภาพของอุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการจัดเก็บข้อมูลที่สำคัญของบริษัทเช่น ฮาร์ดดิสก์ เทป แผ่นดิสก์ ซีดี เป็นต้น ก่อนที่จะทิ้งสื่อดังกล่าวหรือนำไปใช้งานใหม่

4.6.8.2. พนักงานทุกคนมีความรับผิดชอบในการดูแลการทำลายข้อมูลที่อยู่ในรูปเอกสารในครอบครองอย่างเหมาะสม เอกสารที่จะทำลายต้องดำเนินการโดยการเข้าเครื่องย่อยกระดาษ ใช้วิธีเผาทำลาย หรือด้วยวิธีการอื่นที่จะไม่สามารถกู้ข้อมูลที่สำคัญนั้นกลับมาได้

4.6.9. การแลกเปลี่ยนข้อมูล

4.6.9.1. บริษัทต้องกำหนดการปฏิบัติงาน และมาตรการควบคุมรองรับ เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร โดยผ่านทางช่องทางการสื่อสารทุกชนิด ตัวอย่างเช่น แนวทางปฏิบัติเกี่ยวกับการใช้งานอุปกรณ์สื่อสารข้อมูลอิเล็กทรอนิกส์มาตรการควบคุมหรือข้อบังคับเกี่ยวกับการส่งต่อข้อมูลสำหรับอุปกรณ์สื่อสาร เป็นต้น

4.6.9.2. พนักงานต้องระมัดระวังการเปิดเผยข้อมูลเช่น ไม่ใช้โทรศัพท์มือถือในการสนทนาข้อมูลที่เป็นความลับในที่ที่มีคนอยู่ใกล้ไม่สนทนาเกี่ยวกับข้อมูลที่เป็นความลับในที่สาธารณะไม่วางเอกสารที่เป็นความลับประเภททิ้งไว้บนเครื่องถ่ายสำเนา เป็นต้น

4.6.9.3. บริษัทต้องมีข้อตกลงการแลกเปลี่ยนข้อมูลและซอฟต์แวร์ระหว่างบริษัทกับภายนอก โดยต้องครอบคลุมไปถึงรายละเอียด เช่น ความรับผิดชอบ การส่งมอบและการรับระบบ เป็นต้น

4.6.9.4. ข้อความในจดหมายอิเล็กทรอนิกส์ (E-mail) ถือว่าเป็นเอกสารของบริษัท ซึ่งผู้บริหารสามารถตรวจสอบได้ การเขียนจดหมายอิเล็กทรอนิกส์ต้องปฏิบัติตามแนวทางปฏิบัติของบริษัทในการใช้ข้อความที่เหมาะสม

4.6.9.5. ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทต้องไม่ใช้ในการดำเนินงานของที่ไม่เกี่ยวข้องกับธุรกิจบริษัท เช่นการส่งจดหมายลูกโซ่การสนับสนุนทางการเมืองการกระทำที่ผิดกฎหมายหรือผิดศีลธรรม เป็นต้น

4.6.9.6. บัญชีจดหมายอิเล็กทรอนิกส์ (E-mail Account) เป็นสมบัติเฉพาะบุคคล ห้ามมิให้พนักงานใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นในการรับส่งจดหมายอิเล็กทรอนิกส์ เว้นแต่ได้รับมอบหมายจากเจ้าของรหัสผู้ใช้ อย่างไรก็ตามเจ้าของบัญชีต้องรับผิดชอบในความเสียหายที่เกิดขึ้นจากการให้ใช้งานนั้น

4.6.9.7. ในกรณีที่มีระบบการใช้โทรศัพท์ในการรับส่งหรือเก็บข้อมูลที่สำคัญของบริษัท เช่น การประชุมผ่านโทรศัพท์หรือการคุยโทรศัพท์ ที่สำคัญที่มีการบันทึกเสียง ต้องมีการควบคุมการเข้าถึงสื่อที่ใช้เก็บข้อมูล

4.6.9.8. พนักงานต้องหลีกเลี่ยงการใช้งานเชื่อมต่ออินเทอร์เน็ตที่ไม่เกี่ยวข้องกับธุรกิจ เช่น เกมส์ การสนทนาผ่านอินเทอร์เน็ต หรือทำกิจกรรมส่วนตัวเป็นต้น รวมถึงต้องหลีกเลี่ยงการติดต่อกับเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม เช่น เว็บที่มีภาพลามกอนาจารและต้องไม่ดาวน์โหลดข้อมูลดังกล่าว

4.6.9.9. พนักงานต้องไม่ส่งข้อมูลหรือโปรแกรมที่ไม่เหมาะสมหรือที่อาจรบกวนการดำเนินงานของบริษัท หรือหน่วยงานภายนอก รวมทั้งข้อความที่อาจส่งผลเสียต่อภาพพจน์ของบริษัท

4.6.9.10. พนักงานจะต้องห้ามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (พรบ. คอมพิวเตอร์) ทั้งนี้ บริษัท จะไม่มีส่วนรับผิดชอบต่อการกระทำผิดของพนักงาน

4.6.10. การเฝ้าระวังความปลอดภัยสารสนเทศ

4.6.10.1. คอมพิวเตอร์และระบบการสื่อสารที่จัดการเกี่ยวกับข้อมูลที่มีความสำคัญของบริษัท ต้องมีการบันทึกทุกเหตุการณ์ที่มีส่วนเกี่ยวข้องกับความปลอดภัย เช่น การพยายามคาดเดารหัสผ่านการพยายามที่จะใช้สิทธิพิเศษที่ไม่ได้รับอนุญาตการเปลี่ยนแปลงสิทธิของผู้ใช้ เป็นต้น

4.6.10.2. บันทึกเหตุการณ์ต้องได้รับการป้องกันจากการถูกเปลี่ยนแปลงแก้ไขและลบทำลายโดยไม่ได้รับอนุญาต

4.6.10.3. บริษัทต้องมีการสอบทานบันทึกการทำงานที่ผิดพลาดของระบบอย่างสม่ำเสมอและแก้ไขตามบันทึกนั้นอย่างทันท่วงทีรวมถึงตรวจสอบว่ามาตรการควบคุมต่างๆยังคงมีประสิทธิภาพ

4.7. การควบคุมการเข้าถึง (Access control)

4.7.1. การบริหารการเข้าถึงของผู้ใช้

4.7.1.1. การอนุญาตเข้าถึงระบบข้อมูลต้องมีการทำบันทึกเป็นลายลักษณ์อักษร โดยจัดทำเป็นเอกสารการขออนุญาตเข้าถึงระบบข้อมูล ซึ่งเอกสารนี้จะถูกเก็บไว้เพื่อเป็นประวัติข้อมูลของการจดทะเบียน การอนุมัติ และการเลิกใช้งานของผู้ใช้

4.7.1.2. เจ้าของข้อมูลเป็นผู้กำหนดรูปแบบสิทธิที่เหมาะสมในการเข้าถึงระบบข้อมูลหรือฐานข้อมูลโดยการให้สิทธิต่างๆนั้นจะขึ้นอยู่กับเหตุผลความจำเป็นทางด้านธุรกิจและพื้นฐานของความจำเป็นที่ต้องรู้ตามหน้าที่การทำงาน

4.7.1.3. เจ้าของข้อมูลต้องมีการตรวจทานสิทธิการเข้าถึงของผู้ใช้ให้สอดคล้องตรงกับสิทธิที่ได้ร้องขอและอนุมัติ

4.7.1.4. รหัสผู้ใช้ต้องเป็นรหัสเฉพาะส่วนบุคคลของผู้ที่ร้องขอในกรณีที่พนักงานลาออกจากบริษัทต้องไม่นำรหัสผู้ใช้รายนั้นกลับมาใช้ใหม่เพื่อลดความเสี่ยงในการได้รับการถ่ายทอดสิทธิไปยังผู้ใช้รายใหม่โดยไม่ได้ตั้งใจ

4.7.1.5. ผู้บังคับบัญชาของสายงานมีหน้าที่ในการอนุมัติสิทธิการเข้าถึงระบบ และแจ้งการเปลี่ยนแปลง (เพิ่ม ย้าย เพิก ถอน) ของพนักงานภายใต้บังคับบัญชาไปยังหน่วยงานที่เกี่ยวข้อง รวมทั้งต้องแน่ใจว่าสิทธิในการเข้าถึงข้อมูลนั้นต้องสอดคล้องกับหน้าที่ความรับผิดชอบของบุคคลนั้นๆ

4.7.1.6. บริษัทต้องจัดสรรสิทธิพิเศษใด ๆ ที่กำหนดให้แก่ผู้ใช้บนระบบต่าง ๆ เช่น ผู้บริหารระบบปฏิบัติการ ฐานข้อมูล หรือโปรแกรมประยุกต์หรือผู้ใช้ที่สามารถลบล้าง (Override) การควบคุมระบบหรือโปรแกรมประยุกต์บนพื้นฐานของหน้าที่ความรับผิดชอบและความจำเป็นของงาน เพื่อการสนับสนุนทางเทคนิคหรือการประมวลผลเท่านั้น

4.7.1.7. การอนุญาตให้มีสิทธิพิเศษเพื่อการเข้าถึงข้อมูลใด ๆต้องได้รับความยินยอมจากเจ้าของข้อมูลนั้นๆ

4.7.1.8. บริษัทต้องมีการพัฒนาระบบหรือมีวิธีการทางเทคนิคเพื่อป้องกันหรือควบคุมการให้สิทธิพิเศษโดยไม่จำเป็น

4.7.1.9. ผู้ใช้ที่มีสิทธิในการเข้าถึงระบบข้อมูลใดๆของบริษัทมีหน้าที่ความรับผิดชอบในการเก็บรักษารหัสผ่านเป็นความลับเฉพาะบุคคลโดยต้องให้ผู้ใช้ลงนามรับทราบและปฏิบัติตามเงื่อนไขในการรักษาความลับรหัสผ่าน

4.7.1.10. บริษัทต้องจัดทำเอกสารเกี่ยวกับขั้นตอนการตรวจทานสิทธิการใช้งานของผู้ใช้และต้องมีการตรวจทานสิทธิในการเข้าถึงเป็นประจำอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการปรับโครงสร้างองค์กรหรือปรับเปลี่ยนสิทธิของพนักงานเมื่อผู้ใช้งานได้ปรับเปลี่ยนตำแหน่งงาน

4.7.2. ความรับผิดชอบของผู้ใช้

4.7.2.1. พนักงานต้องตรวจทานว่าได้รับสิทธิการเข้าสู่ระบบเหมาะสมกับหน้าที่ความรับผิดชอบ ในกรณีที่สิทธิที่ได้รับไม่เหมาะสมต้องแจ้งผู้บังคับบัญชาทราบ

4.7.2.2. ผู้ใช้ต้องรับผิดชอบเกี่ยวกับการเปลี่ยนรหัสผ่านของตนเองเป็นประจำสม่ำเสมอ ไม่ว่าระบบมีการบังคับให้เปลี่ยนแปลงรหัสผ่านหรือไม่ก็ตาม

4.7.2.3. ผู้ใช้ควรตั้งรหัสผ่านที่หลากหลายตามมาตรฐานรหัสผ่านและไม่ควรเป็นคำในพจนานุกรมทั้งคำรวมทั้งผู้ใช้ต้องไม่ตั้งรหัสผ่านซ้ำหรือคล้ายคลึงของเดิม เช่น ไม่เพิ่มตัวเลขต่อท้ายรหัสผ่านเดิมเพื่อใช้งานต่อ

4.7.2.4. ผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสผ่านของตนให้บุคคลอื่นไม่ว่าจะโดยจงใจหรือประมาทเลินเล่อเว้นแต่รหัสผ่านดังกล่าวได้ล่วงรู้ถึงบุคคลอื่นอันเนื่องมาจากความบกพร่องของระบบข้อมูลหรือการกระทำของบุคคลอื่นซึ่งมิได้เกิดจากความผิดของผู้ใช้

4.7.2.5. บุคคลที่ทำงานในบริษัท ต้องจัดเก็บเอกสารและสื่อต่าง ๆ ประเภทที่เป็นความลับไว้ในตู้เก็บเอกสารที่มีการล็อคหรือห้องจัดเก็บเอกสารที่มีการรักษาความปลอดภัยทุกครั้งหลังการใช้งาน เมื่อข้อมูลเหล่านั้นไม่มีความจำเป็นที่จะใช้งานอีกต่อไปต้องทำลายจนไม่สามารถนำกลับมาใช้งานได้อีก

4.7.3. การควบคุมการเข้าถึงเครือข่าย

4.7.3.1. บริษัทต้องจัดให้มีควบคุมช่องทางในการเข้าถึงระบบข้อมูลโดยการกำหนดไว้ล่วงหน้า ซึ่งต้องจัดเก็บเป็นเอกสารอ้างอิง และปรับปรุงให้ทันสมัยอยู่เสมอ ตัวอย่างของการควบคุมเหล่านี้ ได้แก่

- การกำหนดสายสัญญาณและหมายเลขโทรศัพท์

- การกำหนดการให้บริการด้านเครือข่ายหรือพอร์ต (port) ที่อนุญาตและที่ไม่อนุญาตให้ใช้งาน
- การจัดช่องทาง (Port) เฉพาะให้กับโปรแกรมประยุกต์และระบบ
- การใช้งานไฟร์วอลล์ (Firewall) หรือเกตเวย์ (Gateway)
- การใช้งาน Virtual Private Networking (VPN)

4.7.3.2. บริษัทต้องไม่อนุญาตให้ทำการเชื่อมโยงไปยังระบบคอมพิวเตอร์ภายนอก ยกเว้นกรณีที่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศและเจ้าของระบบงาน

4.7.3.3. บริษัทต้องมีการแบ่งแยกเครือข่ายออกเป็นโดเมนเครือข่ายย่อยตามกลุ่มบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ หรือกลุ่มของระบบสารสนเทศ เพื่อที่จะสามารถควบคุมในแต่ละเครือข่ายย่อยได้อย่างเหมาะสม โดยในแต่ละโดเมนต้องมีการกำหนดขอบเขตความปลอดภัย ซึ่งสามารถกระทำได้โดยการใช้ไฟร์วอลล์ (Firewall) หรือเกตเวย์ (Gateway) ในการควบคุมการเข้าถึงและการผ่านเข้าออกข้อมูลของโดเมนนั้น

4.7.4. การควบคุมการเข้าถึงระบบปฏิบัติการ

4.7.4.1. บริษัทต้องมีกระบวนการการพิสูจน์ตัวตนผู้ใช้ในระบบปฏิบัติการ โดยพิจารณาใช้มาตรฐานทางเทคนิคที่ทันสมัยของการพิสูจน์ผู้ใช้ และต้องวิเคราะห์ต้นทุนที่ใช้ต่อประโยชน์ที่ได้รับ ก่อนจะนำวิธีการพิสูจน์ตัวตนดังกล่าวมาใช้

4.7.4.2. ผู้ใช้ต้องมีรหัสเฉพาะส่วนบุคคลที่ไม่ซ้ำซ้อนกัน เพื่อที่จะสามารถระบุและติดตามการใช้งานของผู้ใช้แต่ละคนได้ การอนุญาตให้ใช้รหัสผู้ใช้ร่วมกันต้องขึ้นอยู่กับเหตุผลความจำเป็นทางด้านธุรกิจซึ่งต้องมีการควบคุมเพิ่มเติมเพื่อที่จะสามารถระบุและติดตามการใช้งานของผู้ใช้แต่ละคนได้

4.7.5. การบริหารรหัสผ่าน

4.7.5.1. บริษัทต้องจัดให้มีระบบการบริหารจัดการรหัสผ่านเพื่อควบคุมให้การกำหนดรหัสผ่านมีคุณภาพ

4.7.5.2. ผู้ใช้คอมพิวเตอร์ต้องกำหนดรหัสผ่านที่มีความยาวของรหัสไม่ต่ำกว่า 6 ตัวอักษรซึ่งรหัสดังกล่าวต้องประกอบไปด้วยตัวอักษรตัวเลขและอักขระพิเศษเพื่อลดโอกาสของความสำเร็จในการคาดเดารหัสผ่าน

4.7.5.3. ผู้ใช้ทุกคนต้องทำการเปลี่ยนรหัสผ่านทุกๆ 90 วันโดยที่ผู้บริหารระบบต้องกำหนดอายุของรหัสผ่านเข้าไปในระบบซึ่งหากเป็นไปได้ต้องมีการกำหนดให้ระบบระงับการใช้งานของรหัสผู้ใช้ที่ไม่มีการใช้งานนานเกิน 120 วันโดยอัตโนมัติ ตามที่แต่ระบบได้กำหนดไว้ (ยกเว้นรหัสผู้ใช้ที่มีสิทธิพิเศษ)

4.7.6. การใช้คอมพิวเตอร์แบบเคลื่อนที่และการเชื่อมโยงเครือข่ายระยะไกล

4.7.6.1. การใช้คอมพิวเตอร์และอุปกรณ์สื่อสารแบบพกพาของบริษัท ต้องมีกระบวนการป้องกัน การรั่วไหลของข้อมูลโดยเฉพาะอย่างยิ่งข้อมูลที่เป็นความลับจากกรณีสูญหาย หรือถูกโจรกรรมตัวอย่างเช่นการมีมาตรการควบคุมทางกายภาพการเข้ารหัสข้อมูลที่อยู่ในคอมพิวเตอร์และอุปกรณ์สื่อสารแบบพกพาการสำรองข้อมูลเก็บเอาไว้เป็นประจำตามระยะเวลาที่เหมาะสม เป็นต้น

4.7.6.2. คอมพิวเตอร์และอุปกรณ์สื่อสารแบบพกพาบางชนิดที่สามารถใช้งานเครือข่ายไร้สายได้ อาจถูกนำมาใช้งานเครือข่ายไร้สายอย่างไม่ถูกต้องหรือเป็นต้นเหตุของการนำภัยคุกคามเข้ามาสู่ระบบของบริษัทได้ เช่น นำไวรัสเข้ามากระจาย บริษัทจะต้องมีมาตรการควบคุมการเข้าถึงระบบเครือข่ายไร้สายอย่างเหมาะสม ตัวอย่างเช่น

- โปรโตคอลสำหรับการสื่อสารแบบไร้สายที่ปลอดภัย

- การปรับแต่งค่าอุปกรณ์ให้ปลอดภัย

4.8. การจัดหา การพัฒนา และบำรุงรักษาระบบงาน (Information systems acquisition, development and maintenance)

4.8.1. ความต้องการด้านความปลอดภัยของระบบ

4.8.1.1. การจัดหาระบบงานใหม่ การพัฒนาระบบงานใหม่ การปรับปรุงระบบงานเดิมที่มีอยู่ของบริษัทการพัฒนาระบบภายในบริษัท การใช้โปรแกรมสำเร็จรูป หรือการใช้บริการจากผู้ให้บริการจากภายนอก ต้องมีการพิจารณาและกำหนดความต้องการด้านความปลอดภัยในทุกขั้นตอนของวงจรการพัฒนาระบบข้อมูลตั้งแต่ขั้นตอนการออกแบบระบบ การพัฒนาสถาปัตยกรรมของระบบและการนำระบบไปใช้งาน รวมถึงต้องมีการประเมินความเสี่ยง เพื่อช่วยในการวิเคราะห์ความต้องการด้านความปลอดภัยและการจำแนกการควบคุมในการจัดหาและการพัฒนาระบบงานใหม่ซึ่งต้องสัมพันธ์กับมูลค่าทางธุรกิจของทรัพย์สินด้านข้อมูลที่เกี่ยวข้องและความเสียหายทางธุรกิจที่เป็นไปได้

4.8.1.2. เจ้าของข้อมูล หน่วยงานดูแลข้อมูล และฝ่ายเทคโนโลยีสารสนเทศ ต้องมีส่วนร่วมในการกำหนดการควบคุมสภาพแวดล้อมของระบบงานประยุกต์ โดยมีหัวข้อในการพิจารณาดังต่อไปนี้

- การควบคุมการเข้าถึง
- การพิสูจน์ตัวตนและการได้รับอนุญาต
- การแบ่งแยกหน้าที่
- การควบคุมการนำเข้า การควบคุมการประมวลผล และการควบคุมผลลัพธ์
- การสำรองข้อมูลและการฟื้นคืนระบบ
- ร่องรอยการตรวจสอบ (Audit Trail) หรือรายการบันทึกของกิจกรรมต่างๆ(Activity Log)

4.8.2. การประมวลผลสารสนเทศในระบบงานประยุกต์ (Applications)

4.8.2.1. โปรแกรมประยุกต์ของบริษัท ที่มีการป้อนข้อมูลต้องมีการตรวจสอบความถูกต้องของข้อมูลที่ทำการป้อนเข้าสู่ระบบ โดยครอบคลุมถึง

- การตรวจจับความผิดพลาดของการนำเข้าข้อมูล เช่น ตรวจข้อมูลที่ขาดหายไป
- ตรวจเช็คตัวอักขระและข้อมูลที่ไม่ถูกต้องหรือการป้อนข้อมูลที่มีความขัดแย้งกัน เช่น การป้อนข้อมูลที่เป็นตัวอักษรในช่องตัวเลข
- การตรวจสอบความผิดพลาดทางตรรกะ เช่น การป้อนข้อมูลวันที่ที่เป็นไปไม่ได้

4.8.2.2. บริษัทต้องผนวกการตรวจสอบความถูกต้องเข้ากับระบบงานประยุกต์เพื่อป้องกันการทุจริตบนข้อมูลที่เกิดจากการประมวลผลผิดพลาดหรือจากผู้ประสงค์ร้าย เช่นการสร้างเงื่อนไขของการควบคุมเซสชั่น (Session) หรือแบ็ช (Batch) เพื่อป้องกันการทำงานแบ็ชต่อไปโดยอัตโนมัติหลังจากเกิดความผิดพลาดการควบคุมยอด (Balance Control) เพื่อให้มั่นใจว่ายอดรวมได้มีการเปลี่ยนแปลงอย่างถูกต้อง เป็นต้น

4.8.2.3. บริษัทต้องจัดให้มีการตรวจสอบและป้องกันการส่งข้อมูลภายในระบบงานประยุกต์เพื่อให้มั่นใจถึงความถูกต้องของข้อมูล โดยครอบคลุมถึงประเด็นต่างๆ ดังนี้

- การควบคุมระบบงานประยุกต์ที่เหมาะสมและเชื่อถือได้เพื่อให้มั่นใจได้ว่าข้อมูลที่ส่งผ่านมีความถูกต้อง

- การควบคุมในระบบงานประยุกต์ต้องสามารถป้องกันการเปลี่ยนแปลงข้อมูลที่ไม่ได้รับอนุญาตหรือการสร้างความเสียหายให้กับข้อมูลในระหว่างส่งข้อมูล

4.8.3. การรักษาความปลอดภัยของแฟ้มข้อมูลระบบ

4.8.3.1. บริษัทต้องมีการควบคุมการเข้าถึงไลบรารี/ไดเร็กทอรีที่เก็บซอร์สโค้ดของโปรแกรมประยุกต์และซอฟต์แวร์ที่ใช้ในการปฏิบัติงานที่อยู่ในระบบงานจริง โดยอนุญาตเฉพาะผู้ดูแลไลบรารี (Librarian) เท่านั้นที่มีสิทธิในการเข้าถึงแบบอ่านและเขียนได้

4.8.3.2. การอัพเดทซอร์สโค้ดและการส่งโปรแกรมต้นฉบับให้กับผู้พัฒนาระบบเพื่อแก้ไข ต้องดำเนินการโดยผู้ดูแลไลบรารีที่รับผิดชอบเกี่ยวกับโปรแกรมประยุกต์นั้นๆ เท่านั้น

4.8.3.3. ก่อนมีการอัพเดทเวอร์ชั่นใหม่ของซอฟต์แวร์ที่ใช้ในการปฏิบัติงานในระบบที่ใช้งานจริง บริษัทต้องได้รับเอกสารการอนุมัติการใช้โปรแกรมเวอร์ชั่นใหม่ และหลักฐานประกอบ อื่นๆ เช่น ผ่านการทดสอบเพื่อการรับรองความถูกต้องของผู้ใช้ และซอร์สโค้ดในไลบรารีต้องได้รับการปรับเปลี่ยนให้สอดคล้องกัน เป็นต้น

4.8.3.4. ในกรณีที่มีการทำสำเนาข้อมูลจากระบบงานจริงเพื่อใช้ในการทดสอบ ต้องดำเนินการควบคุมเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง การควบคุมต่าง ๆ ต้องประกอบด้วย

- ต้องได้รับอนุญาตก่อนการทำสำเนาข้อมูลจริงไปยังระบบงานทดสอบในแต่ละครั้ง
- มีการควบคุมการเข้าถึงข้อมูลที่ใช้ในการทดสอบระบบ
- มีการดัดแปลงข้อมูลจริงบางส่วนก่อนนำมาใช้ในการทดสอบ
- ทำการลบข้อมูลทดสอบออกจากระบบทันทีที่ได้เสร็จสิ้นการทดสอบ
- มีการจัดเก็บบันทึก (Audit Log) เพื่อตรวจสอบของกิจกรรมการทดสอบ

4.8.4. การรักษาความปลอดภัยในกระบวนการพัฒนาระบบและการสนับสนุน

4.8.4.1. บริษัทต้องมีการควบคุมเพื่อมิให้ผู้พัฒนาระบบเข้าไปแก้ไขโปรแกรมที่อยู่ในระบบทดสอบสำหรับผู้ใช้ (User Acceptance Test) ควรมีการใช้ซอฟต์แวร์เครื่องมือที่ช่วยในการควบคุมการเปลี่ยนแปลง (Change Control Software Tools) เพื่อให้มั่นใจว่ามีการจำกัดสิทธิไม่ให้ผู้พัฒนาระบบเข้าถึงระบบใช้งานจริงและระบบทดสอบ

4.8.4.2. การกำหนดค่าระบบโดยปริยาย (System Default Setting) ต้องมีการทบทวนก่อนที่จะทำ การติดตั้งระบบเพื่อค้นหาข้อบกพร่องด้านความปลอดภัยที่เป็นไปได้ และเมื่อพบการกำหนดค่าที่มีความเสี่ยงด้านความปลอดภัย ต้องดำเนินการกำหนดใหม่ก่อนที่จะนำไปใช้งานจริง

4.8.4.3. เมื่อมีการเปลี่ยนแปลงในโปรแกรมประยุกต์ ต้องดำเนินการทดสอบเพื่อการรับรองความถูกต้องของผู้ใช้ (User Acceptance Test) โดยผู้ใช้ที่ทำการขอให้มีการเปลี่ยนแปลงและฝ่ายงานที่เกี่ยวข้องต้องเข้าร่วมการทดสอบ และก่อนที่จะนำซอฟต์แวร์ไปติดตั้งใช้งานจริง ต้องระบุขั้นตอนการทดสอบไว้ในเอกสารการขอเปลี่ยนแปลง

4.8.4.4. ในกรณีที่มีการเปลี่ยนแปลงที่สำคัญในระบบงานหลักต้องดำเนินการประมวลผลระบบงานใหม่ควบคู่กับระบบงานเดิม (Parallel Run) ไประยะหนึ่งก่อนที่จะใช้ระบบงานใหม่

4.8.4.5. ระหว่างขั้นตอนการทดสอบเพื่อการรับรองความถูกต้องของผู้ใช้ ต้องจำกัดการเข้าถึงเพื่อมั่นใจว่าผู้พัฒนาระบบไม่สามารถเข้าถึงโปรแกรมที่ทำการทดสอบ และการแก้ไขซอร์สโค้ดของโปรแกรมที่กำลังทำการตรวจสอบ จะดำเนินการได้ต้องได้รับความยินยอมจากผู้ใช้เป็นลายลักษณ์อักษรก่อน

4.8.4.6. บริษัทควรมีการใช้งานซอฟต์แวร์สำเร็จรูปโดยปราศจากการแก้ไขซอฟต์แวร์ ถ้ามีความจำเป็นในการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูปต้องมีการพิจารณาการควบคุมต่าง ๆ ดังนี้

- การประเมินระบบการควบคุมที่มาพร้อมกับซอฟต์แวร์สำเร็จรูป
- การได้รับความยินยอมในการแก้ไขจากผู้จำหน่ายซอฟต์แวร์
- การดูแลรักษาและการเปลี่ยนเวอร์ชั่นซอฟต์แวร์ซึ่งได้มีการเปลี่ยนแปลง
- การเปลี่ยนแปลงต้องได้รับการทดสอบทั้งหมดและจัดทำเอกสารอย่างชัดเจน

4.8.4.7. บริษัทต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศของบริษัท หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป เช่น ตรวจสอบข้อมูลก่อนออกจากบริษัท เฝ้าตรวจสอบกิจกรรมต่างๆ ของบุคลากรและของระบบตามที่กฎหมายอนุญาตให้ทำได้ เฝ้าตรวจสอบการใช้งานทรัพยากรระบบคอมพิวเตอร์ของบริษัท เป็นต้น

4.8.4.8. บริษัทต้องดำเนินการควบคุมเพื่อป้องกันรหัสโทรจันที่อาจแอบแฝงมากับซอฟต์แวร์สำเร็จรูปซึ่งต้องพิจารณาการควบคุมดังต่อไปนี้

- ซื้อซอฟต์แวร์จากแหล่งที่เชื่อถือได้เท่านั้น
- ทำการทดสอบก่อนที่จะนำไปติดตั้งในระบบงานจริง
- ถ้าเป็นไปได้ให้นำซอร์สโค้ดมาตรวจสอบก่อนนำมาใช้งานจริง
- มีการควบคุมการเข้าถึงซอร์สโค้ดเพื่อป้องกันการแก้ไขโดยไม่รับอนุญาต

4.8.4.9. บริษัทต้องจัดให้มีมาตรการควบคุมการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอกดังต่อไปนี้

- การจัดเตรียมสัญญาที่ระบุถึงความเป็นเจ้าของทรัพย์สินทางปัญญาของทั้ง
- ซอร์สโค้ดและซอฟต์แวร์ที่ใช้ในการปฏิบัติงานนั้น
- การรับรองคุณภาพและความถูกต้องภายหลังจากได้พัฒนาเรียบร้อยแล้ว
- การทำสัญญาในการเก็บรักษาซอร์สโค้ดไว้กับบุคคลที่สาม
- สิทธิและขอบเขตของอำนาจหน้าที่ในการเข้าไปตรวจสอบคุณภาพและความถูกต้องของงานที่ได้ พัฒนาเรียบร้อยแล้ว
- ข้อตกลงที่ครอบคลุมถึงความต้องการด้านคุณภาพและการรองรับการรักษาความปลอดภัยที่จำเป็นต่อการดำเนินงานของบริษัท
- การทดสอบก่อนการติดตั้งเพื่อตรวจสอบชุดคำสั่งที่ไม่ประสงค์ดีหรือโทรจันที่อาจแอบแฝงมาพร้อมกับตัวโปรแกรม

4.9. การบริหารจัดการเหตุการณ์ที่กระทบต่อความปลอดภัยสารสนเทศ (Information security incident management)

4.9.1. การรายงานเหตุการณ์ที่กระทบต่อความปลอดภัยสารสนเทศและจุดอ่อนด้านความปลอดภัย

4.9.1.1. บริษัทต้องจัดให้มีทีมงานจัดการเหตุการณ์ที่กระทบต่อความปลอดภัยสารสนเทศ ซึ่งมีความรับผิดชอบในการตรวจสอบเหตุการณ์ที่กระทบต่อความปลอดภัยสารสนเทศ โดยมีหน่วยงานที่ทำหน้าที่ดูแลและเผยแพร่ข้อมูลที่ใช้ในการติดต่อระหว่างสมาชิกในทีม เช่น หมายเลขโทรศัพท์ และเรียกประชุมทีมงานเมื่อได้รับการรายงานถึงความผิดปกติที่เกิดขึ้น ทีมงานจัดการเหตุการณ์ผิดปกติด้านความปลอดภัยคอมพิวเตอร์ควรประกอบด้วย

บุคคลที่ปฏิบัติงาน ณ เวลาที่เกิดเหตุการณ์ ผู้ดูแลระบบ และตัวแทนจากกลุ่มงานเทคโนโลยีสารสนเทศ และสายงานธุรกิจที่เกี่ยวข้อง

4.9.1.2. หากพนักงานสงสัยว่าอาจเกิดเหตุการณ์ที่กระทบต่อความปลอดภัยสารสนเทศ พนักงานต้องรีบแจ้งหน่วยงานที่ดูแล หรือฝ่ายความปลอดภัยและกำกับดูแลระบบเทคโนโลยีสารสนเทศทราบโดยทันที

4.9.1.3. หากพนักงานสงสัยว่ามีเหตุการณ์ที่กระทบต่อความปลอดภัยสารสนเทศเกิดขึ้นในระบบ พนักงานต้องออกจากระบบเครือข่ายของบริษัทโดยทันที และรีบแจ้งให้หน่วยงานที่ดูแลทราบเพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น รวมทั้งแจ้งฝ่ายที่ดูแลระบบเทคโนโลยีสารสนเทศทราบ เป็นหน้าที่ของผู้ใช้งานระบบทุกคนที่ต้องตรวจตราให้มั่นใจว่าเหตุการณ์ที่กระทบต่อความปลอดภัยสารสนเทศดังกล่าวได้รับการแก้ไขแล้ว ก่อนที่จะใช้งานระบบอีกครั้งหนึ่ง

4.9.1.4. ทีมที่รับผิดชอบต้องแก้ปัญหาได้ในเวลาอันเหมาะสม มีการปรึกษาหารือร่วมกันกับผู้เกี่ยวข้อง เช่นผู้ให้บริการ เจ้าของผลิตภัณฑ์ หรือหน่วยงานภายนอก เกี่ยวกับเหตุการณ์ที่กระทบต่อความปลอดภัยสารเทศ

4.9.1.5. หากพบว่าซอฟต์แวร์มีข้อบกพร่องในการทำงานหรือมีความผิดพลาดขณะปฏิบัติงาน ผู้ใช้งานต้องแจ้งให้หน่วยงานให้ความช่วยเหลือด้านสารสนเทศทราบ โดยผู้ใช้งานควรบันทึกถึงลักษณะการบกพร่องที่พบ ข้อความที่บ่งบอกข้อผิดพลาด และในกรณีที่เชื่อได้ว่าข้อบกพร่องดังกล่าวมีผลกระทบต่อความปลอดภัย หน่วยงานให้ความช่วยเหลือด้านสารสนเทศต้องแจ้งให้กับฝ่ายที่กำกับดูแลระบบเทคโนโลยีสารสนเทศทราบ

4.9.1.6. ในกรณีที่มีเหตุการณ์ที่กระทบความปลอดภัยที่มีสาเหตุจากภายนอกบริษัท ต้องมีการดำเนินการ เพื่อรักษาความถูกต้องด้านหลักฐาน ในกรณีที่จำเป็นต้องมีการดำเนินการทางกฎหมายจะต้องมีตัวแทนผู้บริหารที่ได้รับมอบหมายของบริษัท โดยผ่านความร่วมมือจากสายงานกฎหมายในการให้ข้อมูลกับเจ้าหน้าที่รักษากฎหมายของรัฐตามระเบียบปฏิบัติทางด้านอาชญากรรม

4.10. การจัดการเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ (Business continuity management)

4.10.1. การบริหารจัดการเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ

4.10.1.1.บริษัทต้องมีระบบการจัดการที่เหมาะเพื่อรักษาความต่อเนื่องทางธุรกิจของบริษัท ซึ่ง ประกอบด้วย

- การวิเคราะห์และการประเมินความเสี่ยงของบริษัทที่เกิดขึ้น โดยพิจารณาในแง่ของผลกระทบต่อธุรกิจและระบบงานข้อมูลหลัก
- การประเมินราคาและหาแนวทางของกลยุทธ์ที่ใช้ในการป้องกัน การลด หรือการโอนความเสี่ยง เช่น การทำการประกันให้ครอบคลุมผลเสียหายที่อาจเกิดขึ้น เป็นต้น
- การประเมินทรัพยากรทางด้านการเงิน บุคคล เทคนิค และอื่นๆ ที่จำเป็นต้องใช้ในการเตรียมการเพื่อพัฒนาแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ
- การพัฒนาและการจัดทำเอกสารของกลยุทธ์ของแผนการเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจให้สอดคล้องกับรูปแบบการประกอบธุรกิจและกลยุทธ์ทางด้านความปลอดภัยของบริษัทโดยรวม
- การทดสอบอย่างสม่ำเสมอ การตรวจทาน และการปรับปรุงขั้นตอนวิธีการซึ่งเกี่ยวกับแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจให้ทันสมัยอยู่เสมอ

4.10.1.2.เมื่อมีการประเมินความเสี่ยงแล้วบริษัทจะต้องมีการกำหนดกลยุทธ์ด้านความต่อเนื่องทางธุรกิจที่ครอบคลุมกับความเสี่ยงที่สำคัญทั้งหมดซึ่งเมื่อได้มีการวางกลยุทธ์แล้วจะต้องมีการอนุมัติจากผู้บริหารและนำแผนกลยุทธ์ดังกล่าวไปใช้ต่อไป

4.10.1.3.ในแต่ละแผนงานต้องมีการกำหนดเจ้าของแผนงานและแนวทางปฏิบัติ ซึ่งเจ้าของแผนฯ ต้องรับผิดชอบในการบำรุงรักษาและทดสอบ พัฒนาหลักเกณฑ์ความต้องการและเงื่อนไขสำหรับการนำแผนฯ ไปใช้

4.10.1.4.ผู้บริหารของบริษัทต้องอนุมัติแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจทุกแผนก่อนนำไปปฏิบัติโดยแผนฯ ดังกล่าวต้องสอดคล้องกับกรอบมาตรฐานของแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจของบริษัทตลอดจนมีการจัดทำเอกสารคู่มือประกอบโดยได้รับการอนุมัติจากเจ้าของหน่วยงานที่ได้รับผลกระทบซึ่งครอบคลุมถึงความต้องการที่กำหนดขึ้นโดยฝ่ายบริหาร

4.10.1.5.บริษัทต้องจัดทำตารางการทดสอบแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจต่างๆซึ่งแผนฯที่มีความสำคัญต่อระบบการดำเนินธุรกิจต้องได้รับการทดสอบเป็นประจำอย่างน้อยปีละหนึ่งครั้งตามกำหนดเวลาการทดสอบของฝ่ายบริหารหน่วยงานตรวจสอบภายในและเจ้าของแผนฯ

4.11. การกำกับดูแลการปฏิบัติตามข้อกำหนด (Compliance)

4.11.1. การปฏิบัติตามกฎหมาย

4.11.1.1.ฝ่ายกฎหมาย ต้องรวบรวมและจัดทำเอกสารที่ระบุถึงกฎหมายกฎระเบียบ พระราชบัญญัติ หรือข้อบังคับตามสัญญาต่าง ๆ ที่มีผลบังคับกับบริษัททั้งหมดไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ ซึ่งหน้าที่ความรับผิดชอบในการกำกับดูแลเพื่อให้มีการปฏิบัติเป็นไปตามกฎหมายกฎระเบียบ หรือข้อบังคับที่เกี่ยวข้องเฉพาะด้านเป็นหน้าที่ของหน่วยงานที่เกี่ยวข้องตาม พรบ.คอมพิวเตอร์

4.11.1.2.ซอฟต์แวร์ที่พัฒนาโดยบริษัทหรือเพื่อบริษัท ถือเป็นทรัพย์สินของบริษัท

4.11.1.3.ระบบประมวลข้อมูลของบริษัท ใช้เพื่อประโยชน์ทางธุรกิจเท่านั้น ห้ามนำไปใช้เพื่อวัตถุประสงค์อื่น หากมีการฝ่าฝืนต้องมีการรายงานให้ผู้บริหารทราบ

4.11.1.4.เจ้าของข้อมูลและฝ่ายที่กำกับดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้มีอำนาจในการอนุมัติการนำแชร์แวร์และฟรีแวร์มาใช้กับทรัพยากรทางคอมพิวเตอร์ของบริษัท

4.11.1.5.แชร์แวร์ที่ได้รับอนุญาตให้นำมาใช้และต้องการใช้ต่อหลังจากสิ้นสุดระยะเวลาการทดลองใช้ ต้องมีการลงทะเบียนขอสิทธิในการใช้อย่างถูกต้อง และผู้ใช้ซอฟต์แวร์ดังกล่าวต้องปฏิบัติตามกฎหมายลิขสิทธิ์และรายละเอียดข้อบังคับต่าง ๆ ของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

4.11.1.6.บริษัทต้องจัดซื้อหรือใช้ซอฟต์แวร์ของผู้ขายที่เชื่อถือได้ เพื่อให้มั่นใจว่าลิขสิทธิ์ ซอฟต์แวร์ที่ได้มานั้นถูกต้องและต้องปฏิบัติให้สอดคล้องกับข้อตกลงด้านลิขสิทธิ์ ห้ามนำซอฟต์แวร์ที่ซื้อไปติดตั้งที่คอมพิวเตอร์เครื่องอื่นนอกเหนือจากเครื่องที่ได้มีการติดตั้งแล้วตามข้อตกลงเรื่องลิขสิทธิ์ซอฟต์แวร์

4.11.1.7.บริษัทต้องมีการตรวจสอบการใช้งานคอมพิวเตอร์ประเภทส่วนบุคคลหรือคอมพิวเตอร์ประเภทพกพาของบริษัทอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าการใช้งานอุปกรณ์คอมพิวเตอร์ทุกชนิดเป็นไปตามข้อตกลงด้านลิขสิทธิ์ซอฟต์แวร์ และเมื่อมีการพบซอฟต์แวร์ที่ฝ่าฝืนนโยบายต้องนำซอฟต์แวร์ดังกล่าวออกจากระบบคอมพิวเตอร์ทันที

5. บทลงโทษ

พนักงานฝ่าฝืนการปฏิบัติตามนโยบายฉบับนี้จะถูกลงโทษทางวินัยตามกฎข้อบังคับของบริษัท และอาจมีความผิดตามกฎหมาย กฎเกณฑ์ หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้อง

6. เริ่มมีผลบังคับใช้

นโยบายนี้ให้เริ่มบังคับใช้ตั้งแต่วันที่ 1 เดือน มกราคม พ.ศ. 2568

ประกาศ ณ วันที่ 1 มกราคม พ.ศ. 2568

.....

(นายณัฐพงษ์ รัตนสุวรรณทวี)

กรรมการผู้จัดการ กลุ่มบริษัท เอสซี