บริษัท เอไอ เอนเนอร์จี จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยสารสนเทศ

บริษัท เอไอ เอนเนอร์จี จำกัด (มหาชน)

AI Energy Public Company Limited

บันทึกประวัติการแก้ไข

เรื่อง : **นโยบายความมั่นคงปลอดภัยสารสนเทศ**

ฉบับที่/ แก้ไขครั้งที่	วันที่	ส่วนที่แก้ไข	เหตุผลที่แก้ไข
01/00	05/01/2560	จัดทำใหม่	
02/00	05/01/2561	การทบทวนนโยบาย	เพื่อให้นโยบายมีการแก้ไขและเปลี่ยนแปลงตามความเหมาะสม
03/00	12/05/2565	แก้ไขในส่วนของนโยบายและเพิ่มนโยบายเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ	แก้ไขให้อยู่ในขอบเขตของระบบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)
04/00	12/05/2566	ปรับปรุงในส่วนของโยบายความมั่นคงปลอดภัยสารสนเทศในทุกหัวข้อ	ปรับปรุงให้สอดคล้องกับมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)
05/00	02/02/2567	ปรับปรุงในส่วนของนโยบายความมั่นคงปลอดภัยสารสนเทศในหัวข้อที่ - 7.1 แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ - 11.2 การบริหารจัดการบัญชีผู้ใช้งาน (User access management)	ปรับปรุงให้สอดคล้องกับระเบียบปฏิบัติของระบบเทคโนโลยีสารสนเทศของบริษัทฯ

นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

1. หลักการและเหตุผล

บริษัท เอไอ เอนเนอร์จี จำกัด (มหาชน) (“บริษัทฯ”) และบริษัทในกลุ่มตระหนักถึงความสำคัญของการนำเทคโนโลยีสารสนเทศ และการสื่อสารซึ่งเป็นปัจจัยที่ช่วยส่งเสริมการดำเนินธุรกิจ และเพิ่มประสิทธิภาพการทำงานให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ เพื่อให้สอดคล้องกับหลักการกำกับดูแลกิจการที่ดี ตลอดจนกฎหมายอื่นที่เกี่ยวข้องเพื่อให้เหมาะสมกับบริบทการดำเนินธุรกิจ

บริษัทฯ จึงกำหนดนโยบายและแนวทางปฏิบัติเพื่อเป็นกรอบการกำกับดูแลและการบริหารแนวทางการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศของบริษัทฯ (Information Technology Security Policy) ทั้งนี้นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (นโยบายฯ) ฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัทฯทุกท่าน อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติจากพนักงานและบุคคลภายนอก

2. วัตถุประสงค์

เพื่อให้มั่นใจได้ว่าระบบเทคโนโลยีสารสนเทศของบริษัทฯ มีการดูแลด้านการบริหารจัดการอย่างมีประสิทธิภาพและเสถียรภาพ สอดคล้องและเหมาะสมกับการดำเนินและพัฒนาธุรกิจ การบริหารความเสี่ยง เพื่อให้บริษัทฯสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของบริษัทฯได้ โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลที่ดี และเป็นกรอบเพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรเพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

3. ขอบเขตการบังคับใช้

นโยบายฉบับนี้มีผลบังคับใช้กับพนักงาน ผู้บริหาร และกรรมการบริษัท ของบริษัท เอไอ เอนเนอร์จี จำกัด (มหาชน) และบริษัทในกลุ่ม รวมถึงผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศภายในบริษัทฯและตอบสนองต่อ พันธกิจและนโยบายของบริษัทฯ โดยอ้างอิงมาตรฐาน ISO/IEC 27001:2013 บริษัทฯทำการเผยแพร่ให้ผู้บริหาร พนักงานทุกระดับและบุคคลภายนอกที่ปฏิบัติงานในบริษัทฯรับทราบและปฏิบัติตามอย่างเคร่งครัดและกำหนดแนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือ ฝ่าฝืนนโยบายฯ อีกทั้งมีการติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง เน้นกำกับดูแลบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศพร้อมใช้งานอยู่เสมอ และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

4. คำนิยาม

บริษัทฯ	หมายถึง	บริษัท เอไอ เอนเนอร์จี จำกัด (มหาชน)
ผู้บริหาร	หมายถึง	ผู้บริหารของบริษัทฯ ตำแหน่งผู้จัดการฝ่ายขึ้นไป
บุคลากรของบริษัท	หมายถึง	กรรมการ ผู้บริหาร และพนักงานทุกระดับ
ผู้ใช้งาน	หมายถึง	พนักงานประจำ พนักงานตามสัญญาจ้าง ผู้รับจ้าง ผู้ให้บริการภายนอก คู่ค้า หรือลูกค้า
ผู้ให้บริการภายนอก	หมายถึง	บุคคลจากภายนอกบริษัทซึ่งบริษัทฯว่าจ้างเพื่อให้บริการที่เกี่ยวข้องกับระบบสารสนเทศ

ระบบเทคโนโลยีสารสนเทศ หรือ ระบบ IT หรือ ระบบสารสนเทศ หรือ เทคโนโลยีสารสนเทศ หมายถึง ระบบสารสนเทศ ระบบฐานข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบการรักษาความปลอดภัยทางสารสนเทศ (Information Security) ระบบงาน (ซอฟต์แวร์สำเร็จรูป ซอฟต์แวร์ประยุกต์) และระบบสื่อสารของบริษัทฯ ทั้งนี้ไม่ว่าระบบดังกล่าวจะเกี่ยวข้องกับข้อมูลส่วนบุคคลหรือไม่ก็ตาม และหมายรวมถึง “ระบบเครือข่ายและคอมพิวเตอร์”

สารสนเทศ หรือข้อมูลสารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความหรือกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆได้ รวมถึงข้อมูลส่วนบุคคล

ข้อมูล	หมายถึง	ข้อมูล ข้อความ สารสนเทศ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย
ข้อมูลส่วนบุคคล	หมายถึง	มีความหมายตามที่กำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลและตามที่ระบุใน “นโยบายคุ้มครองข้อมูลส่วนบุคคล ของบริษัทฯ”
สินทรัพย์	หมายถึง	ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของส่วนงานเทคโนโลยีสารสนเทศรวมถึงทรัพย์สินสารสนเทศของบริษัทฯ
ทรัพย์สินสารสนเทศ	หมายถึง	1) ทรัพย์สินสารสนเทศประเภทระบบงาน ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ 2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

		3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูล สารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์ และหมายรวมถึงข้อมูลส่วนบุคคลที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์หรือ ข้อมูลคอมพิวเตอร์ด้วย 4) ทรัพย์สินสารสนเทศประเภทลิขสิทธิ์ คือ ทรัพย์สินที่เกิดจากการพัฒนาหรือสิทธิ์ในการใช้จากเจ้าของผลิตภัณฑ์
ระบบสารสนเทศ	หมายถึง	ระบบงานของบริษัทฯที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการทำงานของบริษัทฯ
ระบบเครือข่าย	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัทฯได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบ Internet และระบบการสื่อสารอื่นๆ

5. บทบาทหน้าที่และความรับผิดชอบ

ส่วนงานเทคโนโลยีสารสนเทศ

1. กำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติที่เกี่ยวข้องกับนโยบาย
2. กำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติเฉพาะเรื่องที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์
3. ติดตามดูแลให้ผู้ใช้งานปฏิบัติตามนโยบาย หลักเกณฑ์ระเบียบปฏิบัติของบริษัทฯที่เกี่ยวข้องอย่างถูกต้องเหมาะสม และหากมีการปฏิบัติที่ไม่ถูกต้องให้รายงานต่อคณะกรรมการบริหารทราบ
4. สื่อสารนโยบายให้แก่ผู้ใช้งาน ผู้ประกอบธุรกิจที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง

ผู้ใช้งาน

1. ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ โดยเคร่งครัด
2. ให้ความร่วมมือกับบริษัทฯ อย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์ และข้อมูลสารสนเทศ ของบริษัทฯ สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัทฯ ให้มีความปลอดภัย
3. รายงานต่อบริษัทฯทันที เมื่อพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรม สารสนเทศ รวมถึง ระบบสารสนเทศ ที่อาจสร้างความเสียหายต่อบริษัทฯ

หัวหน้าส่วน / หัวหน้าหน่วยงาน

1. ชี้แจงและส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และตักเตือนลงโทษทางวินัยกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

6. นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

บริษัทฯ กำหนดให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และครอบคลุมในเรื่อง ดังต่อไปนี้

6.1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ผู้จัดการส่วนงานเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือ แนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่แล้ว นำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

6.2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)

- ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้องมีการควบคุมการเข้า-ออกและการใช้งาน การตรวจสอบระบบต่างๆ เช่น ระบบเตือนอุณหภูมิภายในห้อง ระบบเตือนอัคคีภัย เป็นต้น
- ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัย เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจมีชุดคำสั่งไม่พึงประสงค์ ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะ มัลแวร์ เช่น ไวรัส คอมพิวเตอร์ เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น
- ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ต้องมีการตรวจสอบ และเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต ตรวจสอบและเฝ้าระวังช่องโหว่ เชื่อมต่อเครือข่ายภายนอก โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกัน ชุดคำสั่งไม่พึงประสงค์ การกรองข้อมูลรับส่งอีเมล เป็นต้น
- ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานและการเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่างๆ ข้อมูลและข้อมูลส่วนบุคคล ให้เป็นไปตามสิทธิ์ที่พึงมีเพื่อป้องกันการเข้าถึง ใช้แก้ไขเปลี่ยนแปลง ข้อมูลและข้อมูลส่วนบุคคลโดยมิชอบหรือโดยปราศจากอำนาจ

6.3. การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้นเพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้

6.3.1. ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี

6.3.2. ความเสี่ยงจากผู้ปฏิบัติงานหรือความเสี่ยงด้านบุคคล ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลโดยมิชอบหรือปราศจากหรือนอกเหนืออำนาจหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้

6.3.3. ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้ง สถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น

6.3.4. ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่มีอยู่หรือการนำนโยบายไปปฏิบัติ หรือการปฏิบัติงานซึ่งอาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

6.4. การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทฯ ยอมรับได้ จัดทำตารางลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

6.5. กำหนดตัวชี้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหาร และจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

7. นโยบายการกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

7.1. แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

- ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรม อันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น
- ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้งานหรือรหัสผ่าน หรือข้อมูลยืนยันตัวตนของผู้อื่นทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
- ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีมาตรการป้องกันการเข้าถึงของผู้อื่น หรือมาตรการป้องกันการเข้าถึงที่บริษัทฯ กำหนดไว้เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอกหรือ กระทำการอื่นใดที่โดยปราศจากอำนาจหรือเกินขอบอำนาจ
- ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน หรือข้อมูลส่วนบุคคลใดๆ โดยไม่ได้รับอนุญาต
- ห้ามรบกวน ขัดขวาง หรือกระทำด้วยประการใดๆ ให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทฯ เกิดความเสียหายหรือถูกทำลายหรือไม่สามารถใช้การได้ตามปกติ เช่น การส่งชุดคำสั่งไม่พึงประสงค์ใดๆ การป่อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรือ อุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น
- ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัทฯ และของผู้อื่นที่อยู่ ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
- ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาชุดคำสั่งไม่พึงประสงค์ เช่น ไวรัส ผ่านโปรแกรมป้องกันไวรัสก่อนทุกครั้ง
- ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตนซึ่งบริษัทฯกำหนดสิทธิ์ให้ใช้เฉพาะบุคคลเท่านั้น
- **ผู้ใช้ต้องปฏิบัติตามมาตราการการควบคุมการใช้งานระบบอินเตอร์เน็ตภายในบริษัทฯ**

8. การจัดโครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

8.1. การจัดโครงสร้างภายในองค์กร (Internal organization)

วัตถุประสงค์

เพื่อควบคุมการเข้าระบบเครือข่าย ระบบคอมพิวเตอร์ และการเข้าถึงข้อมูลตามประเภทชั้นความลับและระดับตำแหน่งบทบาทหน้าที่ของผู้ใช้งาน โดยมีผู้ดูแลระบบทำหน้าที่บริหารการจัดการเข้าถึงข้อมูลตามประเภทชั้นความลับ เพื่อป้องกันความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ และป้องกันมิให้ข้อมูลทางด้านสารสนเทศได้รับความเสียหาย โดยมีการบริหารจัดการ การเข้าถึงระบบเครือข่ายและบริการเครือข่ายและการเข้าใช้งานฐานข้อมูลกลาง โดยให้เป็นไปตามขั้นตอนและระเบียบบริษัทฯ และเพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับระบบสารสนเทศขององค์กร

แนวทางปฏิบัติ

กรรมการบริหาร

กรรมการบริหาร ต้องกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติ

ผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กร

ผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กร ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในส่วนงานเทคโนโลยีสารสนเทศ ในการรับผิดชอบการดูแลระบบสารสนเทศของบริษัทฯ ให้มั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศบริษัทฯ

หัวหน้าส่วนส่วนงานเทคโนโลยีสารสนเทศ

หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator ในระบบสารสนเทศจะต้องทำหน้าที่ปรับปรุงดูแลระบบความปลอดภัยในการใช้งานระบบ และเมื่อมีเหตุการณ์กระทบต่อความมั่นคงปลอดภัยสารสนเทศให้ทำการปรับปรุงแก้ไขและรายงานต่อผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กร โดยให้ทันต่อเหตุการณ์ในช่วงเวลาที่เหมาะสม

เจ้าหน้าที่เทคโนโลยีสารสนเทศ

เจ้าหน้าที่เทคโนโลยีสารสนเทศ ทำหน้าที่ดูแลและตรวจสอบระบบความปลอดภัยในการใช้งานระบบ ควบคุมผู้ปฏิบัติงานในการใช้งานให้เป็นไปตามนโยบายและแนวทางปฏิบัติ และเมื่อมีเหตุการณ์กระทบต่อความมั่นคงปลอดภัยสารสนเทศให้ทำการแก้ไขและรายงานต่อหัวหน้าส่วนงานเทคโนโลยีสารสนเทศให้ทันต่อเหตุการณ์ในช่วงเวลาที่เหมาะสม

ผู้ใช้งาน

ผู้ใช้งาน ต้องตระหนักและปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด โดยผู้ใช้งานสามารถร้องขอสิทธิ์ในการเข้าถึงกระบวนการสารสนเทศภายในบริษัทฯ ได้ด้วยการร้องขอมายังส่วนงานเทคโนโลยีสารสนเทศและต้องได้รับการเห็นชอบจากผู้บังคับบัญชา

8.2. การใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล(Mobile devices and teleworking)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

แนวทางปฏิบัติ

- กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์ประเภทพกพาโดยระบุ ยี่ห้อ รุ่น ระบบปฏิบัติการ เพื่อให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของระบบสารสนเทศ
- บริษัทฯมีนโยบายกำหนดให้ต้องใช้อุปกรณ์พกพาเฉพาะที่เป็นของบริษัทฯ ในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทฯเท่านั้น หากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงต้องได้รับการอนุมัติจากทางผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กร
- บริษัทฯกำหนดการใช้งานระยะไกล(VPN) ให้เฉพาะผู้จัดการของแต่ละส่วนงานเท่านั้น และกำหนดให้ใช้งานต้องมีการเข้ารหัสผ่านก่อนทุกครั้ง ในกรณีที่ผู้ใช้งานจำเป็นต้องใช้ ต้องขออนุมัติจากทางผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กร และจะเมื่อเลิกการใช้งานจะปิดการใช้งานทันที

9. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของบริษัทฯและคัดสรรบุคคลก่อนที่จะเข้ามาทำงาน เพื่อลดความเสี่ยงจากความผิดพลาด และการนำไปใช้ในทางที่ไม่เหมาะสมของพนักงานอันเกิดจากปฏิบัติงานกับระบบสารสนเทศและทรัพยากรสารสนเทศอื่นๆ ขององค์กร

แนวทางปฏิบัติ

ก่อนจ้างงาน (Prior to employment)

- หัวหน้าส่วนทรัพยากรมนุษย์ทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเข้ารับการทำงานภายในบริษัทฯ โดยต้องไม่พบประวัติในการ บุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วนงานใดมาก่อน
- กำหนดให้ลงนามในสัญญาระหว่างผู้ปฏิบัติงาน ว่าจะไม่เปิดเผยความลับของบริษัทฯ (Non-Disclosure Agreement: NDA) ซึ่งรวมถึงการไม่เปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความควบคุม โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้าง ผู้ปฏิบัติงานนั้นๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลา ไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

ระหว่างการจ้างงาน (During employment)

- ผู้ดูแลต้องกำกับดูแลและกำหนดแนวทางการปฏิบัติ ให้ผู้ใช้งานมีความตระหนักและมีความรับผิดชอบในหน้าที่ของตนเกี่ยวกับความปลอดภัยระบบเทคโนโลยีสารสนเทศ

- กำหนดบทลงโทษทางวินัย โดยกำหนดอย่างเป็นทางการและสื่อสารให้พนักงานรับทราบ เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยของบริษัทฯ
- ผู้ปฏิบัติงานใหม่ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ

การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

- เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด หัวหน้าส่วนงานทรัพยากรมนุษย์แจ้งให้หัวหน้าส่วนงานเทคโนโลยีสารสนเทศทราบทันที ลาออกจากงาน หรือมีการโยกย้ายสายงาน
- พนักงานที่สิ้นสุดการเป็นพนักงานของบริษัทฯ ต้องคืนสินทรัพย์ของบริษัทฯ เช่น Notebook จากนั้นผู้ดูแลระบบจะระงับสิทธิ์การเข้าถึงระบบสารสนเทศภายในช่วงเวลาที่กำหนด
- กรณีหากมีการโยกย้ายส่วนงาน ผู้ดูแลจะทำการทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศให้เหมาะสมกับภาระหน้าที่และความรับผิดชอบ

10. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

10.1. หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (Responsibility for assets)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และ อุปกรณ์คอมพิวเตอร์ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทฯ ให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

- ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
- ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ เพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
- ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของบริษัทฯ เว้นแต่ได้รับอนุมัติตามระเบียบปฏิบัติงาน โดยส่วนงานเทคโนโลยีสารสนเทศจะเป็นผู้ติดตั้งหรือแก้ไขโปรแกรมเท่านั้น
- ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพวงให้มีสภาพเดิม
- ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
- ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน

- หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้งานที่พ้นสภาพต้องคืนเครื่องคอมพิวเตอร์ และอุปกรณ์ คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อส่วนงานเทคโนโลยีสารสนเทศในสภาพที่พร้อมใช้งาน
- การเคลื่อนย้ายเครื่องหรืออุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกาหนดการนำทรัพย์สินของบริษัทฯ ออกนอกบริษัทฯ รวมทั้งต้องปฏิบัติตามข้อกำหนด หรือระเบียบหรือแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องหรืออุปกรณ์ คอมพิวเตอร์ทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย
- เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดขององค์กรต้องได้รับการปกป้องด้วยการยืนยันตัวตน(Authentication) โดยจำเป็นต้องใช้ชื่อผู้เข้าใช้งาน(Username) และรหัสผ่านของผู้เข้าใช้งาน(Password) ในแต่ละบุคคลที่ได้รับจากผู้ดูแลระบบ ในการเข้าใช้งานระบบสารสนเทศทุกครั้งเมื่อต้องการใช้งาน โดยต้องมีการจัดทำ Screen Saver และทำการ Log Off อุปกรณ์ทุกครั้งไม่ได้ใช้งานอุปกรณ์
- บริษัทฯกำหนดให้ไม่อนุญาตให้ผู้ใช้งานนำอุปกรณ์ที่ไม่ใช้อุปกรณ์ที่ทางบริษัทฯจัดหาให้ (BYOD : Bring Your Own Devices) เข้ามาใช้งานภายในบริษัทฯ หากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงต้องได้รับการอนุมัติจากทางผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กร
- กำหนดให้มีการทำลายทรัพย์สินที่ไม่ต้องใช้งานแล้วอย่างเหมาะสม เช่น กระดาษ ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร, แผ่น CD/DVD ใช้การหักหรือใช้เครื่องหั่นทำลายเอกสาร และยกเลิก หรือทำลายข้อมูลสารสนเทศภายในสื่อบันทึกข้อมูลโดยการฟอร์แมตโดย Low Level Format เช่น ฮาร์ดดิสก์ไดรฟ์ (Hard Disk Drive) โซลิดสเตตไดรฟ์ (Solid State Drive) หรือ USB แฟลชไดรฟ์(USB Flash Drive)
- กำหนดให้ตั้งรหัสผ่านสำหรับสื่อบันทึกข้อมูลเพื่อป้องกันการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึก และมีการตั้งให้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถทำการขนย้ายสื่อบันทึกข้อมูลได้ เพื่อความมั่นคงปลอดภัยของสื่อบันทึกข้อมูลสารสนเทศ

10.1.1. การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจการใช้โปรแกรมที่ถูกต้องตามกฎหมายลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

แนวทางปฏิบัติ

ผู้ดูแลระบบ

- มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ ตามสิทธิ์การใช้งานที่กำหนด
- มีหน้าที่รับผิดชอบในการติดตั้ง และอัพเกรดโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวัน เวลาที่นัดหมาย
- ทำการถอดและยกเลิกสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อมีอนุมัติแจ้งยกเลิกและ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์

ผู้ใช้งาน

- ต้องใช้โปรแกรมคอมพิวเตอร์ อย่างเช่น วิญญูชนพึงจะใช้ทรัพย์สินของตนเอง โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัทฯ
- โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน
- ห้ามคัดลอก จำหน่าย เผยแพร่ โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย
- ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์อย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทฯกำหนดมาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว นอกจากนี้ หากโปรแกรมที่ไม่ชอบด้วยกฎหมายดังกล่าวส่งผลกระทบให้เกิดการสูญหาย แก้ไขเปลี่ยนแปลง ข้อมูลส่วนบุคคล ผู้ใช้งานอาจต้องมีความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอีกด้วย

10.1.2. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์

แนวทางปฏิบัติ

ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ ข้อมูลสารสนเทศ รวมถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบสารสนเทศอยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์หรือผู้ใช้งานที่ทำการเกินขอบอำนาจหน้าที่ และควบคุมไม่ให้มีการเข้าถึงในขณะที่ไม่มีผู้ใช้อุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

- ออกจากระบบสารสนเทศ(Log out) โดยทันทีเมื่อเสร็จสิ้นงาน
- มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

- ต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญต่อสายงานส่วนงานหรือหน่วยงานไว้ในที่ที่ปลอดภัยการจัดเก็บข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ใน Shared File ซึ่งมีการกำหนดสิทธิ์การเข้าใช้งานของแต่ละ Folder
- ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 2 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้น เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
- การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 15 นาที
- ระมัดระวังและดูแลทรัพย์สินสารสนเทศและทรัพย์สินอื่นใดของบริษัทฯ ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

10.1.3. การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สามารถสนับสนุนการปฏิบัติงานและเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมาย ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของบริษัทฯ ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์ หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

แนวทางปฏิบัติ

- ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูลสารสนเทศ อยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์หรือผู้ใช้งานที่ทำการเกินขอบเขตอำนาจหน้าที่ และควบคุมไม่ให้มีการเข้าถึงในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน
- ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศหรือนโยบายอื่นใด ที่กำหนดไว้
- ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัทฯ จะต้องใช้จดหมายอิเล็กทรอนิกส์เพื่อผลประโยชน์ของบริษัทฯภายใต้ขอบเขตสิทธิ์การใช้งานที่บริษัทฯกำหนดเท่านั้น

- ผู้ใช้งานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ปฏิบัติงานที่ได้รับแจ้งมาจากส่วนงานใต้บังคับบัญชา
- ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์(Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อมูลเว้นแต่ จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
- การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
- การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามธุรกิจของบริษัทฯ หรือติดต่อกับหน่วยงานหรือบุคคลอื่นใดที่เกี่ยวข้องกับการปฏิบัติงานผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น
- การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่นยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคลโดยอ้างว่า เป็นความเห็นของบริษัทฯ หรือก่อให้เกิดความเสียหายต่อกลุ่มธุรกิจ
- ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมายหมิ่นต่อสถาบันพระมหากษัตริย์ กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ หรือกระทบต่อการดำเนินงานของกลุ่มธุรกิจตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัทฯ
- ห้ามผู้ใช้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีการกระทำดังกล่าวให้ถือว่าเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์ หรือเจ้าของบัญชีใช้งานสื่อสังคมออนไลน์เป็นผู้รับผิดชอบการกระทำดังกล่าวแต่ผู้เดียว
- ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่(Chain mail) การส่งจดหมายจำนวนมาก(Spam mail) การส่งจดหมายต่อเนื่อง(Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายโปรแกรมไม่พึงประสงค์ เช่น ไวรัสคอมพิวเตอร์ เป็นต้น
- ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทฯ ให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัทฯ
- ในกรณีบริษัทฯ ได้รับการร้องเรียนหรือร้องขอหรือตรวจสอบพบการกระทำหรือเหตุการณ์ใดที่เกี่ยวข้องกับการใช้ระบบจดหมายอิเล็กทรอนิกส์อันมีความเสี่ยงต่อความไม่ปลอดภัยต่อระบบเครือข่ายและคอมพิวเตอร์ หรือ ความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล หรือ ความเสี่ยงต่อการกระทำใดๆ อันฝ่าฝืนกฎหมาย บริษัทฯ มีสิทธิ์ยกเลิกหรือระงับการบริการชั่วคราวแก่ผู้ใช้งานหรือปฏิบัติงานที่เกี่ยวข้องเพื่อสอบสวนและตรวจสอบสาเหตุ
- หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด หรือความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลใดๆ เกิดขึ้นให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัทฯ

- การกระทำใดๆ ที่เกี่ยวข้องกับการเผยแพร่ หรือส่งต่อหรือนำเข้าสู่ระบบ ซึ่งข้อมูล ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการเท่านั้น ผู้ดูแลระบบและบริษัทฯไม่มีส่วนเกี่ยวข้องใดๆ

10.2. การจัดชั้นความลับของสารสนเทศ (Information classification)

วัตถุประสงค์

เพื่อให้ข้อมูลสารสนเทศได้รับการป้องกันที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศที่มีต่อองค์กร การจัดระดับชั้นความลับต้องพิจารณาถึงข้อกำหนดทางด้านกฎหมาย คุณค่าระดับความสำคัญ และระดับความอ่อนไหวเพื่อป้องกันมิให้ข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่รับการอนุญาต โดยให้ปฏิบัติอย่างเหมาะสมตามระดับชั้นความลับข้อมูล

แนวทางปฏิบัติ

ผู้จัดการฝ่ายทรัพยากรมนุษย์และงานสนับสนุนองค์กรกำหนดประเภทของข้อมูล ระดับความสำคัญ ลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง และช่องทางการเข้าถึง เป็นลายลักษณ์อักษรและมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ

แนวทางในการจัดแบ่งระดับชั้นการเข้าถึง

ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดเพียงบางส่วนจะก่อให้เกิดความเสียหาย

ข้อมูลใช้ภายใน หมายถึง ข้อมูลที่ใช้เฉพาะภายในสำนักงานเท่านั้น

ข้อมูลสาธารณะ หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่แก่สาธารณะได้

จัดแบ่งระดับชั้นการเข้าถึง

- การเข้าถึงและการใช้งานข้อมูลลับที่สุด บริษัทฯกำหนดสิทธิ์ในการเข้าถึงและใช้งานข้อมูล โดยผ่านการอนุมัติเพื่อสำหรับจัดเก็บข้อมูล เป็นลายลักษณ์อักษรจากผู้บริหารและต้องมีการลงนามไปให้เอกสารข้อตกลงการไม่เปิดเผยข้อมูล เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรองรับ
- การเข้าถึงและการใช้งานข้อมูลลับมาก บริษัทฯกำหนดสิทธิ์ในการเข้าถึงและการใช้งานข้อมูลสำหรับเจ้าของข้อมูลโดยแยกออกเป็น สายงาน/ส่วนงาน/หน่วยงาน หรือ บุคคล โดยผ่านการพิจารณาและอนุมัติจากผู้จัดการฝ่ายทรัพยากรมนุษย์และงานสนับสนุนองค์กร
- การเข้าถึงและการใช้งานกลุ่มข้อมูลใช้ภายใน บริษัทฯกำหนดให้ผู้ใช้งานทั้งหมดของสำนักงานสามารถเข้าถึงและใช้งานข้อมูลได้
- การเข้าถึงและการใช้งานข้อมูลสาธารณะ ไม่มีข้อบังคับพิเศษสามารถเปิดเผยต่อสาธารณะได้

10.3. การจัดการสื่อบันทึกข้อมูล (Media Handling)

วัตถุประสงค์

เพื่อป้องกันการเปิดเผยโดยไม่ได้รับการอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

แนวทางปฏิบัติ

10.3.1. การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)

- ข้อมูลที่มีชั้นความลับ บริษัทฯกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว
- ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจากสำนักงาน ต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก
- บริษัทฯกำหนดให้มีการสื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูล
- ห้ามไม่ให้นำสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ไปใช้เพื่อกิจการอื่นซึ่งไม่เกี่ยวกับภารกิจของบริษัทฯ

10.3.2. การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

ในกรณีสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งาน ทางบริษัทฯกำหนดให้ต้องทำลายสื่อบันทึกข้อมูลนั้น และต้องมั่นใจว่าสื่อบันทึกข้อมูลไม่สามารถกู้คืนกลับมาใช้ใหม่ได้ เช่น หากเป็นเอกสารให้ทำการฉีกหรือย่อยทำลาย เทป ฮาร์ดดิส แฟลชไดร์ฟ ให้ทำการทุบทำลาย

10.3.3. การส่งสื่อบันทึกข้อมูลออกไปภายนอกสำนักงาน (Physical Media Transfer)

- บรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการส่งโดยเป็นไปตามความเหมาะสม
- ส่งโดยเจ้าหน้าที่ของบริษัทฯเพื่อความปลอดภัยของข้อมูล
- หากต้องมีการขนย้ายออกต้องมีการล๊อกรหัสการเข้าถึงเพื่อป้องกันการเข้าใช้งานโดยไม่ได้รับอนุญาต

11. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

11.1. การควบคุมการเข้าถึงตามข้อกำหนดทางธุรกิจ (Business requirements of access control)

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของบริษัทฯ และการถึงข้อมูลตามประเภทชั้นความลับ และระดับตำแหน่งหน้าที่ของผู้ใช้งาน โดยมีผู้ดูแลระบบทำหน้าที่บริหารการจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ โดยกำหนดให้มีการยืนยันตัวตน(Authentication) ในการเข้าถึงระบบเครือข่ายและระบบข้อมูลของบริษัทฯ และเพื่อให้ผู้ใช้งานมีความตระหนักในการเข้าใช้งานเว็บไซต์ต่างๆ ผ่านระบบเครือข่ายของบริษัทฯ

แนวทางปฏิบัติ

กำหนดสิทธิ์การเข้าถึงข้อมูลของแต่ละสายงาน/ส่วนงาน/หน่วยงานอย่างเหมาะสม รวมทั้งมีการทบทวนความต้องการภายในหน่วยงานและความต้องการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมเก็บบันทึกข้อมูลการขอเข้าถึงสิทธิ์การใช้งาน และยกเลิกสิทธิ์การใช้งานหรือการเปลี่ยนแปลงต่างๆ ของผู้ใช้งานทั้งที่ได้รับอนุมัติและไม่ได้รับอนุมัติ เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น หากได้รับการอนุมัติจะถูกอัพเดทในไฟล์ เอกสารควบคุมการเข้าถึงและสิทธิ์ในการเข้าถึงระบบ(Access Control and Permission Control List)

11.2. การบริหารจัดการบัญชีผู้ใช้งาน (User access management)

วัตถุประสงค์

เพื่อให้มีการควบคุมสิทธิ์การใช้งานระบบสารสนเทศอย่างเหมาะสมและป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งาน

แนวทางปฏิบัติ

- กำหนดให้ต้องร้องขอใช้งาน บัญชีผู้ใช้งานระบบสารสนเทศและยกเลิกบัญชีผู้ใช้งานโดยทันที เมื่อบุคคลที่ได้รับสิทธิ์ลาออก เลิกสัญญาว่าจ้าง หรือเปลี่ยนแปลงหน้าที่ปฏิบัติงานเพื่อควบคุมการให้สิทธิ์และการยกเลิกสิทธิ์ในการเข้าถึงหน้าที่ความรับผิดชอบของผู้ใช้งาน
- ผู้ดูแลระบบกำหนดให้มีการพิสูจน์ตัวตนและการระบุตัวตน(Identification and Authentication) ทุกครั้งก่อนเข้าสู่ระบบสารสนเทศของบริษัทฯ เช่น การกำหนดรหัสผ่านให้มีความซับซ้อน (Complexity) เป็นต้น เพื่อเป็นการยืนยันตัวผู้ใช้งานทุกครั้ง โดยแต่ละผู้ใช้งานจะมีบัญชีผู้ใช้ (User Account) เป็นของตนเองโดยทางผู้ดูแลระบบจะเป็นคนส่งมอบให้
- **กำหนดจำนวนครั้งที่ยินยอมให้ผู้ใช้งานใส่รหัสผ่านผิด (Logon Attempt - Retires) หากการใส่รหัสผ่าน (Password) ผิดเกินจำนวนครั้งที่กำหนดไว้** จะมีการระงับการเข้าใช้งานและทางผู้ดูแลระบบ จะเข้าตรวจสอบและจัดทำรายงาน และยกเลิกการระงับการเข้าใช้งาน ในส่วนของระบบ ERP เช่น SAP จะเป็นของผู้จัดการฝ่ายสายงานการเงินและบัญชีในการบริหารการจัดการบัญชีผู้ใช้งาน(Username) รหัสผ่าน(Password) และสิทธิ์ในการเข้าถึงต่างๆ ของระบบ SAP
- กำหนดให้ผู้ดูแลระบบ สอบทานการใช้ระบบงานสารสนเทศของบริษัทฯ โดยจะมีการสอบทานบัญชีผู้ใช้งาน (Username) สำหรับการระบุตัวตนการเข้าใช้งานฐานข้อมูลกลางของบริษัทฯปีละ 2 ครั้ง และสอบทานสิทธิ์การเข้าใช้ระบบ VPN (Virtual Private Network) ปีละ 1 ครั้ง

11.2.1. การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

- บริษัทฯ กำหนดให้บัญชีที่มีสิทธิ์สูง (HPID: High Privilege User ID) ให้กับกรรมการบริหาร 1 ท่านและผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กรอีก 1 ท่าน ในส่วนของระบบ ERP จะมีกรรมการบริหาร 1 ท่านที่มีสิทธิ์ HPID ที่ใช้ในการควบคุมแก้ไขปรับปรุง
- ในกรณีที่ผู้ดูแลระบบต้องการใช้บัญชีที่มีสิทธิ์สูง (HPID: High Privilege User ID) ต้องมีการควบคุมการใช้งานอย่างรัดกุม โดยผู้ดูแลระบบจำเป็นจะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาที่มีอำนาจอนุมัติและเหตุผลในการใช้งานบัญชีที่มีสิทธิ์สูง

- ต้องควบคุมการเข้าถึงข้อมูล ข้อมูลสำคัญ ข้อมูลส่วนบุคคล และอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์พนักงานหรือบุคคลใดให้เป็นผู้ใช้งานที่มีหน้าที่รับผิดชอบและมีสิทธิ์เข้าถึงข้อมูลสำคัญและข้อมูลส่วนบุคคล รวมทั้งดำเนินการเพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- ต้องกำหนดสิทธิ์การใช้ข้อมูล ข้อมูลสำคัญ ข้อมูลส่วนบุคคล และระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ตระบบฐานข้อมูล เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
- ในกรณีมีความจำเป็นต้องใช้ ผู้ใช้งาน หรือ User ที่มีสิทธิ์พิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น บริษัทฯจะใช้ปัจจัยประกอบการพิจารณาในภาพรวมดังต่อไปนี้
  - ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
  - ควรควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิ์พิเศษอยางเข้มงวด เช่น จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
  - ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

11.3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูล ส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

แนวทางปฏิบัติ

- ผู้ใช้งานต้องเก็บชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในระบบสารสนเทศของบริษัทให้เป็นความลับและไม่ควรนำไปเผยแพร่ให้กับผู้อื่น เช่น การให้ผู้อื่นเข้าใช้งานบัญชีของตนเอง การติดรหัสผ่านในระบบสารสนเทศของบริษัทฯ ไว้ที่โต๊ะปฏิบัติงานหรือหน้าจอมอนิเตอร์
- ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่อง หรืออุปกรณ์คอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์
- ในกรณีผู้ใช้งานหรือผู้ปฏิบัติงานได้รับอนุญาตในการให้สิทธิ์ผู้ใช้งานหรือผู้ปฏิบัติงานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูล ในความรับผิดชอบของตนในกรณีจำเป็นดังกล่าวข้างต้น เช่น การ

Share Files ผู้ใช้งานจะต้องให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ์ดังกล่าวทันทีเมื่อสิ้นสุดเหตุความจำเป็น ตามที่ได้รับอนุญาต รวมทั้งต้องบันทึกหลักฐานการให้สิทธิ์ดังกล่าวเพื่อการตรวจสอบด้วย

- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับและความลับทางการค้าของ กลุ่มธุรกิจยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัทฯ
- ห้ามผู้ใช้งานเปิดเผยหรือโอนหรือส่งต่อข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของบริษัทฯ เว้นแต่เป็นการดำเนินการตามขอบเขตของสิทธิ์และหน้าที่ภายใต้เงื่อนไขของนโยบายนี้ และนโยบายคุ้มครองข้อมูลส่วนบุคคลของกลุ่มธุรกิจ
- ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดสิทธิ์ของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อกลุ่มธุรกิจ รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทฯ ในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติหรือข้อกำหนดหรือระเบียบที่กำหนดไว้อย่างเคร่งครัด
- ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัทฯ เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น

11.4. การควบคุมการเข้าถึงระบบสารสนเทศและแอพพลิเคชั่น (System and application access control)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงระบบสารสนเทศและแอพพลิเคชั่นโดยไม่ได้รับอนุญาต

แนวทางปฏิบัติ

บริษัทฯกำหนดให้มีการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งานข้อมูล เช่น เขียน อ่าน ลบ และ ในกรณีมีบุคคลภายนอกเข้ามาปฏิบัติงานภายในบริษัทฯ ต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัย และผู้ดูแลระบบต้องกำกับดูแลความเรียบร้อย

12. การเข้ารหัสข้อมูล (Cryptography)

12.1. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

วัตถุประสงค์

เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ

แนวทางปฏิบัติ

บริษัทฯ กำหนดให้มีการควบคุมการเข้ารหัสข้อมูล ที่คำนึงชนิด และขั้นตอนวิธีการเข้ารหัสข้อมูล (Algorithm) ที่สอดคล้องและเหมาะสม รวมทั้งกำหนดให้มีการบริหารจัดการกุญแจ(Key Management) โดยผู้ดูแลระบบ

13. ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

13.1. พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure areas)

วัตถุประสงค์

เพื่อเป็นมาตราฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์ของบริษัทฯ

แนวทางปฏิบัติ

13.1.1. การเข้าใช้งานห้องคอมพิวเตอร์แม่ข่าย(Server Room)

- บริษัทฯ กำหนดสิทธิ์เฉพาะผู้ดูแลระบบ และบุคคลตามที่บริษัทฯ กำหนดเข้าใช้งานห้องคอมพิวเตอร์แม่ข่าย(Server Room) ได้เท่านั้นเพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าถึง ล่วงรู้ แก้ไขการเปลี่ยนแปลงหรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ภายในบริษัทฯ
- บริษัทฯ กำหนดให้เพียงกรรมการบริหาร 1 ท่าน ผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กร และผู้ดูแลระบบ (พนักงาน/หัวหน้าส่วน ส่วนงานเทคโนโลยีสารสนเทศ) เป็นผู้มีสิทธิ์เข้าใช้งานห้อง Server ได้เท่านั้น
- กำหนดการทบทวนสิทธิ์การเข้าถึงห้องคอมพิวเตอร์แม่ข่าย (Server Room) ตามแผนผังโครงสร้างส่วนงานเทคโนโลยีสารสนเทศ
- พนักงานภายในบริษัทฯ หรือบุคคลภายนอกที่มีความประสงค์เข้าดำเนินงานต่างๆ ภายในห้องคอมพิวเตอร์แม่ข่าย (Server Room) จะต้องมีการร้องขอผ่านทางผู้ดูแลระบบและต้องได้รับความเห็นชอบจากผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กรโดยต้องมีการระบุเหตุผล ช่วงเวลาในการเข้าดำเนินงานต่างๆ โดยผู้ดูแลระบบจะเข้าควบคุมการดำเนินงานต่างๆ เพื่อไม่ให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศภายในบริษัทฯ

13.1.2. การป้องกันความเสียหาย

- ระบบป้องกันอัคคีภัยภายในห้องคอมพิวเตอร์แม่ข่าย (Server Room)

  ภายในห้องคอมพิวเตอร์แม่ข่าย(Server Room) ติดตั้งเครื่องดับเพลิงแบบอัตโนมัติ (Automatic fire extinguisher) และ เครื่องตรวจจับควัน(Smoke Detector) เพื่อใช้สำหรับป้องกันอัคคีภัยเบื้องต้น และมีหน่วยงานความปลอดภัยในการรับผิดชอบตรวจสอบการใช้งาน

- อุปกรณ์สำรองไฟฟ้า (Uninterruptible Power Supply)

  ภายในห้องคอมพิวเตอร์แม่ข่าย(Server Room) ติดตั้งอุปกรณ์สำรองไฟฟ้าที่สามารถป้องกันความเสียหายที่เกิดจากความผิดปกติของพลังงานไฟฟ้า เช่น ไฟฟ้าดับ ไว้สำหรับสำรองไฟฟ้าให้กับระบบคอมพิวเตอร์แม่ข่ายและระบบกล้องวงจรปิด CCTV เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง

- การควบคุมอุณหภูมิและความชื้น(Temperature and humidity sensor)

  ภายในห้องคอมพิวเตอร์แม่ข่าย(Server Room) ติดตั้งเครื่องปรับอากาศไว้ และตั้งอุณหภูมิให้มีความเหมาะสมกับสภาพห้อง รวมถึงมีอุปกรณ์วัดอุณหภูมิและความชื้น (Temperature and humidity sensor) ติดตั้งภายในห้องคอมพิวเตอร์แม่ข่าย(Server Room) โดยจะมีการบอกสถานะอุณหภูมิและความชื้นภายในห้องคอมพิวเตอร์แม่ข่ายให้กับผู้ดูแลระบบ
- ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security) โดยจัดทำป้ายกำกับ (Labels)ให้กับสายสัญญาณและสายสื่อสาร

13.2. อุปกรณ์ (Equipment)

- การบำรุงรักษาอุปกรณ์ (Equipment maintenance)
  - ผู้ดูแลระบบมีหน้าที่บำรุงรักษาอุปกรณ์สารสนเทศให้ได้รับการบำรุงรักษาอย่างถูกต้องเพื่อให้พร้อมต่อการใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง
  - ผู้ดูแลระบบมีการจัดทำและจัดจ้างการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) และการบริการดูแลและบำรุงรักษา (Maintenance Agreement)โดยจัดจ้างให้ผู้บริการภายนอกดูแลในส่วนอะไหล่หรือการซ่อมแซมชิ้นส่วนต่างๆ ของเครื่องคอมพิวเตอร์แม่ข่าย(Server) เครื่องสำรองไฟฟ้า (UPS) ระบบกล้องวงจรปิด CCTV และตลอดจนระบบโปรแกรมใช้งานเฉพาะทางด้านต่างๆ (Application Software) ให้อยู่สถานะพร้อมใช้งานตลอดเวลา
- การนำทรัพย์สินของบริษัทฯ ออกนอกบริษัทฯ (Removal of assets)

  บริษัทฯ ได้กำหนดให้ระดับผู้จัดการฝ่ายในแต่ละ สายงาน/ส่วนงาน/หน่วยงาน ขึ้นไปสามารถทำทรัพย์สินสารสนเทศออกนอกบริษัทฯ ได้เท่านั้น โดยจะมีการเข้ารหัสข้อมูลทุกครั้งในการเข้าใช้งาน

14. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

14.1. ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational procedures and responsibilities)

ผู้ดูแลระบบ มีการจัดทำขั้นตอนการปฏิบัติงาน (Work Instruction, WI) ที่เป็นลายลักษณ์อักษร เพื่อให้สอดคล้องกับการปฏิบัติงานและหน้าที่ความรับผิดชอบต่อระบบสารสนเทศของบริษัทฯ โดยจะต้องได้รับการอนุมัติจากผู้จัดการฝ่ายสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กรและผู้บริหารสูงสุด

14.2. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

บริษัทฯ มีมาตรการป้องกันโปรแกรมไม่ประสงค์ดีไว้ที่เครื่องคอมพิวเตอร์แม่ข่าย(Server) เครื่องผู้ใช้งาน (Clients) เพื่อเป็นการป้องกันโปรแกรมไม่ประสงค์ดีจากทั้งภายในและภายนอกบริษัทฯ และกำหนดให้มีการตรวจสอบ ปรับปรุง แก้ไขการป้องกันโปรแกรมไม่ประสงค์ดีในทุกเดือน โดยมีการบันทึกผลการตรวจสอบ ปรับปรุง แก้ไขให้กับผู้บังคับบัญชาทราบ

14.3.การสำรองข้อมูล (Backup)

จัดให้มีการกำหนดความถี่ในการสำรองข้อมูล ระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่เชื่อมโยงระบบเครือข่าย รวมถึงระบบข้อมูลของบริษัทฯที่ถูกจัดเก็บไว้ใน NAS (Network Attached Storage) และมีการทำการทดสอบความสมบูรณ์ของข้อมูลของการจัดเก็บการสำรองข้อมูลอย่างน้อยปีละ 1 ครั้ง และควรจัดให้มีการสำรองข้อมูลภายนอกบริษัทฯ

14.4.การบันทึกการดำเนินการและการเฝ้าระวัง (Logging and Monitoring)

บริษัทฯ กำหนดให้มีการบันทึกข้อมูล (Logging Files) เพื่อจัดเก็บรายละเอียดการเข้าใช้งานระบบสารสนเทศ เช่น ระบบเครือข่าย (Firewall Logging) และข้อมูลของบริษัท (NAS Logging) โดยมีการจัดเก็บการบันทึกข้อมูล (Logging Files) แยกระบบออกเป็นอิสระจากภายในระบบเครือข่ายภายในบริษัทฯ เพื่อป้องกันการเข้ามาแก้ไขการบันทึกข้อมูล (Logging Files) โดยไม่ได้รับอนุญาต ให้เป็นไปตามขั้นตอนและขอบเขตของกฎหมายตามแบบปฏิบัติ

บริษัทฯ ได้กำหนดให้ผู้ดูแลระบบมีการจัดการการเฝ้าระวัง (Monitoring) การทำงานของระบบสารสนเทศที่ไม่เป็นไปตามขั้นตอนปกติ ที่เกิดจากความผิดผลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องได้รับการตรวจสอบ ป้องกัน และมีการเปลี่ยนแปลงอยู่สม่ำเสมอ โดยให้เป็นไปตามขั้นตอนการปฏิบัติงานในภาวะปกติ (Normal Working)

14.5.การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control operational software)

บริษัทฯ ได้กำหนดซอฟต์แวร์ของเครื่องคอมพิวเตอร์พื้นฐานสำหรับผู้ใช้งาน โดยมีเพียงผู้ดูแลระบบที่สามารถติดตั้งซอฟต์แวร์เพิ่มเติมให้กับผู้ใช้งาน ในกรณีมีการร้องขอใช้งานซอฟต์แวร์เฉพาะหรือซอฟต์แวร์ที่อยู่นอกเหนือที่ระเบียบปฏิบัติของทางบริษัทฯ ได้กำหนดไว้

14.6.การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

บริษัทฯ มีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจจะเป็นความเสี่ยงต่อความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทฯ และมีการรายงานเกี่ยวกับช่องโหว่ทางเทคนิคเพื่อเป็นแนวทางการป้องกันการคุกคามช่องโหว่ทางเทคนิคที่เกิดขึ้น เช่นการแจ้งข่าวสารให้ทุกคนรับทราบผ่านทาง Email

14.7.สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information systems audit considerations)

ส่วนงานเทคโนโลยีสารสนเทศต้องวางแผนการตรวจสอบระบบงานสารสนเทศ โดยการตรวจสอบนั้นจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด

การวางแผนการตรวจสอบระบบสารสนเทศต้องสอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

15. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

วัตถุประสงค์

เพื่อเป็นแนวทางปฏิบัติในการป้องกันระบบเครือข่ายสารสนเทศภายในบริษัทฯ จากภายนอกที่จะเข้ามายังระบบเครือข่ายภายใน และเพื่อเป็นแนวทางในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลและระบบสารสนเทศภายในบริษัทฯจากบุคคล ไวรัส(โปรแกรมที่ไม่ประสงค์ดี) รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึงหรือสร้างความเสียหายการทำงานของระบบสารสนเทศ

แนวทางปฏิบัติ

15.1.การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

บริษัทฯ ได้กำหนดมาตรการความมั่นคงปลอดภัยของระบบเครือข่ายโดยมีการติดตั้งระบบ Firewall สำหรับการเชื่อมต่อไปยังระบบเครือข่ายสาธารณะ โดยมีผู้ดูแลระบบกำหนดมาตรการความปลอดภัยในการเชื่อมต่อระบบเครือข่ายสารสนเทศต่างๆ ให้มีความมั่นคงปลอดภัย โดยมีมาตรการดังนี้

- ผู้ดูแลระบบมีหน้าที่บริหารจัดการแบ่งการเชื่อมต่อระหว่างเครือข่ายสาธารณะกับระบบเครือข่ายภายในบริษัทฯ
- ผู้ดูแลระบบมีการบริหารจัดการและควบคุมการเชื่อมต่อกับระบบเครือข่ายไร้สายอย่างรัดกุม โดยการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ของบุคคลภายในและภายนอกออกจากกัน รวมถึงการเปลี่ยนรหัสการเข้าถึงระบบเครือข่ายไร้สายเพื่อให้มีความมั่นคงปลอดภัยของระบบและข้อมูลสารสนเทศภายในบริษัทฯ
- บริษัทฯ มีการจัดเก็บข้อมูล (Logging Files) เพื่อให้มีการตรวจสอบ แก้ไข ปรับปรุง ระบบที่เกี่ยวข้องหรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามขั้นตอนและขอบเขตของกฎหมาย

15.2.การถ่ายโอนสารสนเทศ (Information transfer)

- บริษัทฯ ให้พนักงานและผู้ให้บริการภายนอก มีการจัดทำเงื่อนไขและข้อตกลงหรือสัญญาระหว่างผู้ใช้บริษัทฯและผู้ใช้บริการ
- กำหนดการจัดการและระเบียบปฏิบัติในการโอนถ่ายข้อมูลสารสนเทศผ่านช่องทางประเภทต่างๆ ให้กับผู้ใช้งานภายในและภายนอก บริษัทฯ

16. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อให้ผู้ดูแลระบบมีหน้าที่ทำการพัฒนา ปรับปรุงหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศ ให้เป็นไปสอดคล้องกับการพัฒนาของเทคโนโลยีสารสนเทศที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา โดยยังคงอยู่ในขอบเขตของนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทฯ

แนวทางปฏิบัติ

16.1.ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

บริษัทฯ กำหนดให้ผู้ดูแลระบบมีการพัฒนา ปรับปรุงหรือแก้ไขเปลี่ยนแปลงความมั่นคงปลอดภัยของระบบสารสนเทศภายในบริษัทฯ ให้สอดคล้องกับความมั่นคงปลอดภัยและการเปลี่ยนแปลงของเทคโนโลยีต่างๆ โดยต้องได้รับการเห็นชอบจากผู้บังคับบัญชาหรือผู้จัดการสายงานทรัพยากรมนุษย์และงานสนับสนุนองค์กร อีกทั้งยังต้องกำหนดขั้นตอนและวิธีปฏิบัติในการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และควรมีเหตุผลบันทึกโดยให้ผู้มีอำนาจลงนามทุกครั้ง

16.2.ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

บริษัทฯ กำหนดให้มีมาตรการควบคุมการปรับปรุงซอฟต์แวร์ให้มีความมั่นคงปลอดภัยสำหรับสารสนเทศตลอดจนวงจรชีวิตของการพัฒนาระบบสารสนเทศ โดยผู้ดูแลระบบหรือเจ้าของระบบหรือหน่วยงานที่เกี่ยวข้อง เช่น

- กำหนดขั้นตอนปฏิบัติงานการควบคุมความเปลี่ยนแปลงของระบบ(System change control procedures) บริษัทฯ มีกระบวนการหรือขั้นตอนควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศ
- การพัฒนาระบบสารสนเทศโดยหน่วยงานภายนอก(Outsourced development)โดยบริษัทฯ กำหนดให้หน่วยงานที่เกี่ยวข้องมีการกำกับดูแลและเฝ้าติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ ตามข้อตกลงการให้บริการ

16.3.ข้อมูลสำหรับการทดสอบระบบ (Test data)

บริษัทฯ กำหนดให้ในการใช้ข้อมูลสำหรับการทดสอบระบบของซอฟต์แวร์ประเภท ERP เช่น ระบบ SAP ทางผู้จัดการฝ่ายสายงานการเงินและบัญชีจะเป็นผู้ดูแลในส่วนของการทดสอบระบบ โดยมีการแยกการใช้ข้อมูลของระบบทดสอบออกจากระบบที่ใช้งานจริง

17. ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)

วัตถุประสงค์

เพื่อเป็นการป้องกันสินทรัพย์ของบริษัทฯที่มีการเข้าถึงโดย ผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ (IT Outsourcing) และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

แนวทางปฏิบัติ

17.1.การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริหารภายนอก (Addressing security within supplier agreements)

บริษัทฯ กำหนดข้อตกลงกับผู้ให้บริหารภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึง การจัดเก็บ การสื่อสาร เพื่อให้สอดคล้องกับความต้องการของบริษัทฯและความมั่นคงปลอดภัยของระบบสารสนเทศ

17.2.การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

- บริษัทฯ กำหนดให้ติดตาม ทบทวน และตรวจประเมินการและเยี่ยมชมผู้ให้บริการภายนอก โดยใช้เกณฑ์ที่บริษัทฯกำหนดขึ้นเพื่อให้เป็นตามนโยบายของบริษัทฯและลดความเสี่ยงที่เกิดขึ้นของผู้ให้บริการ
- บริษัทฯ กำหนดข้อปฏิบัติและขั้นตอนการพิจารณาในการคัดเลือกผู้ให้บริการโดยใช้เกณฑ์ที่บริษัทฯ กำหนดขึ้น และประเมินความเสี่ยงที่อาจจะเกิดในกรณีเปลี่ยนผู้ให้บริการภายนอก เพื่อให้ตรงกับความต้องการของบริษัทฯ

18. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

18.1. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์

เพื่อให้มีการบริหารจัดการเหตุการณ์หรืออุบัติการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งกำหนดผู้ที่มีหน้าที่(เจ้าหน้าที่)รับผิดชอบ เหตุการณ์และจุดอ่อนหรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงความปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง และให้มีการรายงานและดำเนินการตามสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ในช่วงเวลาที่เหมาะสม ตามขั้นตอนและเป็นไปตามขอบเขตของกฎหมาย

แนวทางปฏิบัติ

- กำหนดเจ้าหน้าที่รับผิดชอบและมีขั้นตอนปฏิบัติเพื่อรับมือป้องกันแก้ไขที่เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทฯ
- ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน
- หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อส่วนเทคโนโลยีสารสนเทศ
- กำหนดให้ผู้ดูแลระบบทำการตรวจสอบ สังเกต ในกรณีพบสิ่งผิดปกติและรายงานต่อผู้จัดการส่วนงานเทคโนโลยีสารสนเทศเพื่อทำการตรวจสอบและแก้ไข
- หากเกิดเหตุการณ์ หรือสิ่งที่คาดว่าเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต้องจัดทำเป็นลายลักษณ์อักษรเพื่อรายงานต่อผู้บริหารระดับสูงเพื่อหาแนวทางในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศ เพื่อนำมาแก้ไข ปรับปรุง ตรวจสอบและป้องกันไม่ให้เกิดความเสียหายกับระบบสารสนเทศของบริษัทฯ
- ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน พร้อมแจ้งเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่เคยเกิดขึ้นให้ผู้ที่เกี่ยวข้องรับทราบ เพื่อช่วยลดความรุนแรงหรือโอกาสเกิดเหตุการณ์ความมั่นคงปลอดภัยเดิมในอนาคต
- ต้องมีการประเมินความเสี่ยง ตรวจสอบ และแจ้งเหตุการณ์ภัยคุกคามหรือความเสี่ยงอันอาจส่งผลกระทบต่อข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ ตามลำดับขั้นและจัดทำรายงานผลกระทบ รวมทั้งแจ้งรายงานตามเงื่อนไขของกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- กำหนดให้ผู้ดูแลระบบเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบรวมถึงเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุกเข้ามาทางระบบเครือข่าย เช่น Firewall, Antivirus เพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตราย

19. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ(Information security aspects of business continuity management)

19.1. ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

วัตถุประสงค์

เพื่อเป็นแนวทางการปฏิบัติการฟื้นฟูระบบเมื่อเกิดเหตุการณ์ฉุกเฉินเพื่อลดการหยุดชะงักของระบบสารสนเทศภายในบริษัทฯ โดยอ้างอิงจากเอกสารภายในบริษัทฯ การวางแผนความต่อเนื่องทางธุรกิจ (Business Continuity Planning) อีกทั้งเพื่อเป็นการเพิ่มความมั่นคงปลอดภัยให้กับข้อมูลสารสนเทศ และระบบสารสนเทศภายในบริษัทฯ และสร้างความต่อเนื่องในระบบสารสนเทศ

แนวทางปฏิบัติ

- ส่วนงานเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ ความไม่แน่นอน และภัยพิบัติ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤต(Crisis Management Plan) เช่น การสำรองข้อมูลระบบสารสนเทศและข้อมูลสารสนเทศ ภายในบริษัทฯ และข้อมูล Logging ของระบบ Firewall เพื่อให้มีความพร้อมสำหรับการใช้งานและการดำเนินการข้อมูลสำรองต่างๆ
- ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง อย่างน้อยปีละ 1 ครั้ง และทำการบันทึกและรายงานผลให้กับผู้บังคับบัญชาทราบ
- บริษัทฯ กำหนดให้มีการประเมินสถานการณ์ความเสี่ยงที่เกิดขึ้นและขนาดของผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (Business Impact Analysis) เพื่อกำหนดระดับเหตุการณ์ฉุกเฉินทางด้านเทคโนโลยีสารสนเทศ และเตรียมอุปกรณ์ทางสารสนเทศพร้อมแผนรองรับและป้องกันในแต่ระดับ ปีละ 1 ครั้ง
    - มีการวางแผนความต่อเนื่องทางธุรกิจ(Business Continuity Planning) และปฏิบัติตามแผนความต่อเนื่องทางธุรกิจ
    - มีการทดสอบและปรับปรุงแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้งและทำการบันทึกและรายงานผลให้กับผู้บังคับบัญชาทราบ
    - มีการกำหนดระดับความรุนแรงและขั้นตอนการแก้ไขในแต่ละสถานการณ์และเตรียมความพร้อมหากเกิดสถานการณ์
    - มีการกำหนดปริมาณข้อมูลเสียหาย (Recovery Point Object) และกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Object) เพื่อนำผลลัพธ์จากการกู้คืนระบบ นำมาปรับปรุงแก้ไขเพิ่มเติมให้กับผู้บังคับบัญชารับทราบ

19.2. การเตรียมอุปกรณ์ประมวลผลสำรอง(Redundancy of information processing facilities)

วัตถุประสงค์

เพื่อเป็นการเตรียมความพร้อมของอุปกรณ์ประมวลผลสำรองให้มีความพร้อมต่อการใช้งานของระบบสารสนเทศ

แนวทางปฏิบัติ

จัดเตรียมระบบสำรองให้เพียงพอต่อการปฏิบัติงานของระบบสารสนเทศ เพื่อไม่ให้ระบบสารสนเทศภายในบริษัทฯ ระบบฐานข้อมูลกลางไม่ได้รับความเสียหายและเพื่อให้ตรงตามสภาพพร้อมใช้ที่กำหนดไว้

20. ความสอดคล้อง (Compliance)

20.1. ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

วัตถุประสงค์

เพื่อป้องกันการละเมิดกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

- การระบุข้อกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements) ระบุข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างอย่างเคร่งคัด โดยระบุอย่างชัดเจนและจำทำเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัย
- การป้องกันข้อมูล(Protection of records) สายงาน/ส่วนงาน/หน่วยงาน ที่ทำสัญญาจ้างกับผู้ให้บริการจากภายนอก ต้องทำสัญญาห้ามนำข้อมูลภายในไปเผยแผ่ ทำหาย หรือทำลาย โดยไม่ได้รับอนุญาต โดยให้สอดคล้องกับกฎหมาย และความต้องการทางธุรกิจ
- ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information) บริษัทฯ ได้มีการจัดเก็บข้อมูลส่วนบุคคลเพื่อนำไปประมวลผลข้อมูล โดยให้เป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคล และเป็นไปตามขั้นตอนของกฎหมาย โดยจะมีการ เก็บรักษาข้อมูลเป็นความลับและป้องกันการเอาถึงข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามกฎหมายและระเบียบข้อบังคับภายในบริษัทฯ
- กำหนดให้ผู้บังคับบัญชาของส่วนงานเทคโนโลยีสารสนเทศ ดำเนินการทบทวนความสอดคล้องของระบบสารสนเทศและขั้นตอนปฏิบัติงานโดยเทียบกับ นโยบาย มาตรฐาน และความต้องการทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

20.2. การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

วัตถุประสงค์

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศเป็นไปตามนโยบายและหลักปฏิบัติของผู้ประกอบธุรกิจ รวมทั้งมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

จัดให้มีการทบทวนและปรับปรุงขั้นตอนและการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและสอดคล้องกับมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

21. <u>การทบทวนนโยบาย</u>

จัดให้มีการทบทวนนโยบายฉบับนี้เป็นประจำอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง เพื่อให้สอด คล้องกับกลยุทธ์และความเสี่ยงของบริษัทฯ และข้อบังคับที่เปลี่ยนแปลงไป และนำเสนอต่อคณะกรรมการบริษัทฯเพื่อพิจารณาอนุมัติ

บริษัทฯเห็นความสำคัญของการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะส่งผลให้การดำเนินกิจการ มีประสิทธิภาพมากยิ่งขึ้น ทั้งยังสามารถสร้างความเชื่อมั่นให้กับคู่ค้า ลูกค้า และผู้ถือหุ้นในแง่ของการเป็นบริษัทฯที่มีการกำกับดูแลกิจการที่ดี ทั้งนี้ บริษัทฯ เชื่อมั่นว่านโยบายความมั่นคงปลอดภัยสารสนเทศจะเป็นส่วนหนึ่งที่ช่วยพัฒนาศักยภาพของบริษัทฯ ให้เจริญเติบโต ก้าวหน้าและมีความมั่นคง

นโยบายความมั่นคงปลอดภัยสารสนเทศฉบับนี้ ผ่านการพิจารณาและได้รับอนุมัติจากที่ประชุมคณะกรรมการบริษัทฯ ครั้งที่ 1/2567 เมื่อวันที่ 20 กุมภาพันธ์ 2567 ทั้งนี้ให้มีผลบังคับใช้ตั้งแต่วันที่ 20 กุมภาพันธ์ 2567 เป็นต้นไป

(นายณรงค์ ธารีรัตนาวิบูลย์)
ประธานกรรมการ
20 กุมภาพันธ์ 2567