บริษัท อิทธิฤทธิ์ ไนซ์ คอร์ปอเรชั่น จำกัด (มหาชน)

นโยบาย (MANAGEMENT POLICY)

เรื่อง

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

รหัสเอกสาร	:	MP-IT-01
แก้ไขครั้งที่	:	08
วันที่มีผลบังคับใช้ :	:	01 กันยายน 2565

ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัทครั้งที่ 3/2565 วันที่ 9 สิงหาคม 2565

ผู้จัดทำ	**ผู้ทบทวน**	**ผู้อนุมัติ**
เลอศักดิ์		
.....	.....	.....
(นายเลอศักดิ์ แสงธนู)	(นางสาวธัณย์สิตา อัครบุญญาพัฒน์)	(นายธนเสฏฐ์ อัครบุญญาพัฒน์)
01/09/2565	01/09/2565	01/09/2565

สารบัญ

หน้า

ประวัติการแก้ไขเอกสาร

แก้ไขครั้งที่	วันที่	รายการแก้ไข	DAR NO.
02	01/06/2564	ข้อ 3 สินค้าคงเหลือ ราคาทุนของสินค้าคำนวณโดยวิธี **FIFO เป็นวิธี Moving** Average Method	
01	21/07/63	เปลี่ยนชื่อบริษัทและแก้ไขรหัสเอกสารและคำผิดพลาดอื่นๆ	
02	18/11/63	ปรับปรุงแก้ไขหัวข้อและรายละเอียด	
03	27/02/64	ปรับปรุงแก้ไขหัวข้อและรายละเอียด	
04	01/11/64	ปรับปรุงแก้ไขหัวข้อและรายละเอียด	
05	01/03/65	ส่วนที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก แก้ไขเป็น การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้ให้บริการภายนอก	62
06	01/05/65	ส่วนที่ 3.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน -ข้อ 7 เพิ่มข้อ 7.7 ผู้ใช้งานที่ต้องใช้บัญชีและรหัสผ่านร่วมกัน 7.8 สิทธิการใช้งานระบบสารสนเทศขั้นพื้นฐาน	16
		ปรับปรุงแก้ไขส่วนที่ 3.4 การบริหารจัดการสินทรัพย์สารสนเทศ	20
07	20/08/65	-ปรับปรุงแก้ไขส่วนที่ 11 การบริหารจัดการผู้ให้บริการภายนอก -ปรับปรุงแก้ไขส่วนที่ 12 การใช้งานจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ -ปรับปรุงแก้ไขส่วนที่ 13 การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ	61 64 65
08	01/09/2565	เปลี่ยนแปลงข้อมูลบริษัทเนื่องจากแปรสภาพจาก บริษัทจำกัด เป็น บริษัทมหาชนจำกัด	

นโยบายและแนวทางปฏิบัติการรักษาความปลอดภัยด้านสารสนเทศ บริษัท อิทธิฤทธิ์ ไนซ์ คอร์ปอเรชั่น จำกัด (มหาชน)

หมวดที่ 1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท อิทธิฤทธิ์ ไนซ์ คอร์ปอเรชั่น จำกัด (มหาชน) หรือต่อไปนี้เรียกว่า “บริษัท” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ บริษัทจึงเห็นสมควรกำหนดนโยบายด้านระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และวิธีการปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 การจัดทำนโยบายด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของบริษัท ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

1.3 นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในบริษัทได้รับทราบและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี หรือตามที่ระบุไว้ในเอกสาร “การตรวจสอบประเมินนโยบาย”

หมวดที่ 2. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อที่จะทำให้บริษัทมีมาตร การในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ของบริษัท ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ซึ่งเจ้าหน้าที่ของบริษัทและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

แนวทางปฏิบัติ

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติด้านการใช้งานและการเข้าถึงข้อมูลของระบบสารสนเทศ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. จัดให้มีข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยว ข้องกับสารสนเทศ การพัฒนาและบำรุงรักษาระบบสาสนเทศ และสิ่งใดๆ ที่เกี่ยวข้องกับสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมและเพียงพอ และมีการกำหนดการควบคุมการใช้งานและการเข้าถึงที่อย่างชัดเจนตามความต้องการในการใช้งานที่เหมาะสมและมั่นคงปลอดภัย

3. จัดให้มีข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยว ข้องกับสารสนเทศ การพัฒนาและบำรุงรักษาระบบสาสนเทศ และสิ่งใดๆ ที่เกี่ยวข้องกับสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมและเพียงพอ และมีการกำหนดการควบคุมการใช้งานและการเข้าถึงที่อย่างชัดเจนตามความต้องการในการใช้งานที่เหมาะสมและมั่นคงปลอดภัย
4. จัดให้มีแนวทางปฏิบัติในการพัฒนาการซอฟต์แวร์ ที่ต้องควบคุมการเข้าถึงแบะสิทธิ์ในการใช้ข้อมูลในระบบไปจนกระทั่งการควบคุมการเข้าถึงด้วยระบบปฏิบัติการ ซึ่งรวมถึงการใช้ข้อมูลในส่วนต่างๆ ภายในคอมพิวเตอร์ของผู้ใช้งาน
5. จัดให้มีแนวทางปฏิบัติในการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์อุปกรณ์หลักสารสนเทศ
6. จัดให้มีทางปฏิบัติในการควบคุมการเข้าถึงห้องเครื่องแม่ข่าย หรือศูนย์ข้อมูลบนอินเทอร์เน็ต รวมทั้งอุปกรณ์สารสนเทศให้เข้าได้เฉพาะผู้มีสิทธิ์เท่านั้น
7. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งานข้อมูลและระบบสารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

หมวดที่ 3. คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

คำนิยาม	ความหมาย
บริษัท	บริษัท อิทธิฤทธิ์ ไนซ์ คอร์ปอเรชั่น จำกัด (มหาชน)
ผู้บังคับบัญชา	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของบริษัท
แผนกเทคโนโลยีสารสนเทศ	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในบริษัท
ผู้จัดการแผนกเทคโนโลยีสารสนเทศ	ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร อนุมัติสิทธิ์เข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ อนุมัติกระบวนการควบคุมการเข้าออก แผนกเทคโนโลยีสารสนเทศ
ผู้ดูแลระบบ แผนกเทคโนโลยีสารสนเทศ	เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในแผนกเทคโนโลยีสารสนเทศ ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์เทคโนโลยีสารสนเทศ และสื่อสารให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของทางแผนกเทคโนโลยีสารสนเทศ อย่างเคร่งครัด ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกแผนกเทคโนโลยีสารสนเทศ ต้องติดบัตรผู้ติดต่อ(Visitor) หรือบัตรประจำตัวของบริษัทเท่านั้น
เจ้าหน้าที่	เจ้าหน้าที่บริษัทที่มีสิทธิ์ในการเข้าออกสถานที่ อาคาร ห้อง ภายในบริษัท
การรักษาความมั่นคงปลอดภัย	การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทที่ธำรงไว้ซึ่ง ความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน ของระบบเทคโนโลยีสารสนเทศ
มาตรฐาน (Standard)	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
วิธีการปฏิบัติ (Procedure)	รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้

คำนิยาม	ความหมาย
	กำหนดไว้ตามวัตถุประสงค์
แนวทางปฏิบัติ (Guideline)	แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
ผู้ใช้งาน	บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัท โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท(Role) ที่กำหนดในการเข้าถึงสารสนเทศของบริษัท 1. **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารของบริษัท 2. **เจ้าหน้าที่** หมายถึง พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของบริษัท 3.**บริษัทภายนอก** หมายถึง บริษัทหรือบริษัทภายนอกที่ บริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานหรือทรัพย์สินต่าง ๆ ของบริษัท โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูลบริษัท
สิทธิ์ของการใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของบริษัท
การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ	การอนุญาต การกำหนดสิทธิหรือมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศ โดยที่เจ้าของข้อมูลให้ใช้งานระบบสารสนเทศนั้นได้
ผู้ดูแลระบบ (System Administrator)	เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ทั้งในด้านฮาร์ดแวร์ และซอฟท์แวร์ ซึ่งสามารถเข้าถึงระบบงาน โปรแกรมเครือข่ายคอมพิวเตอร์ รวมถึงระบบจัดการฐานข้อมูลของบริษัทฯ เช่น การกำหนดสิทธิ์ของผู้ใช้ เป็นต้น
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
ระบบคอมพิวเตอร์	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
ระบบเครือข่าย(Network System)	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัทได้ เช่น ระบบ LAN ระบบ Internet เป็นต้น
ระบบ LAN	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในบริษัทเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัท
ระบบ Internet	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของบริษัทเข้า

คำนิยาม	ความหมาย
	กับเครือข่ายอินเทอร์เน็ตทั่วโลก
ระบบเทคโนโลยีสารสนเทศ (Information Technology System)	ระบบงานของบริษัทที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่บริษัทสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace)	พื้นที่ที่บริษัทอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น ○ พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน ○ พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) ○ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) ○ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) ○ พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)
เจ้าของข้อมูล	ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
ผู้ติดต่อจากบริษัทภายนอก	บุคคลจากบริษัทภายนอกที่มาทำการติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของฝ่ายเทคโนโลยีสารสนเทศ
ทรัพย์สิน	ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท เช่น อุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ์ เป็นต้น
จดหมายอิเล็กทรอนิกส์ (e-mail)	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
สื่อบันทึกพกพา (Portable Media)	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ CD , DVD, Flash Drive, External Had Disk
ชื่อผู้ใช้ (Username)	ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้
รหัสผ่าน (Password)	ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
การเข้ารหัส (Encryption)	การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้ จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

คำนิยาม	ความหมาย
การพิสูจน์ยืนยันตัวตน (Authentication)	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้งานระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
ชุดคำสั่งไม่พึงประสงค์	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
สถานการณ์ความเสี่ยง	ความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทสามารถแบ่งเป็นภัยต่างๆ ได้ 4 ประเภท ได้แก่ - ภัยที่เกิดจากเจ้าหน้าที่หรือบุคคลากรของหน่วยาน (Human Error) - ภัยที่เกิดจาก Software - ภัยจากไฟไหม้หรือระบบไฟฟ้า - ภัยจากน้ำท่วม (อุทกภัย)
สื่อสังคมออนไลน์ (Social Network)	สื่อหรือช่องทางในการติดต่อในลักษณะของการสื่อสารแบบสองทางผ่านระบบเครือข่ายอินเทอร์เน็ต เป็นสื่อรูปแบบใหม่ (New Media) ที่บุคคลทั่วไปสามารถนำเสนอและเผยแผพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่างๆ

หมวดที่ 4. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศความมั่นคงปลอดภัยของบริษัท

ส่วนที่ 1 นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

วัตถุประสงค์ เพื่อกำหนดขอบเขต ทิศทาง และให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล และเป็นไปตามหรือ สอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

<u>ส่วนที่ 1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ(Information Security Policy)</u>

<u>วัตถุประสงค์</u> เพื่อกำหนดขอบเขต ทิศทาง และให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล และเป็นไปตามหรือ สอดคล้องกับข้อกำหนดทาง ธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

<u>นโยบาย</u>

1. เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information Security Policy Document)
   1.1 ต้องจัดทำนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร เพื่อให้เกิดความเชื่อมั่น และมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยนโยบายดังกล่าวจะต้องได้รับอนุมัติจากคณะกรรมการบริษัทในการนำไปใช้

1.2 ต้องจัดให้มีการเผยแพร่เอกสารนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศให้กับเจ้าหน้าที่บริษัท หน่วยงานภายนอก และผู้ที่เกี่ยวข้องในขอบเขตรับทราบ

ส่วนที่ 1.2 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

วัตถุประสงค์ เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงาน เพื่อให้มีความมั่นคงปลอดภัย

นโยบาย

1. บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)
   1.1 ผู้จัดการแผนกเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทไว้อย่างชัดเจน
   1.2 ผู้บริหารของบริษัทต้องแต่งตั้งคณะหรือกลุ่มผู้ทำงานหลัก ตลอดจนทรัพยากรที่จำเป็น เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท
2. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)
   ผู้บริหารของบริษัท ต้องแบ่งหน้าที่และกำหนดความรับผิดชอบที่ชัดเจนในการปฏิบัติงาน เพื่อลดโอกาสที่จะทำให้มีการเปลี่ยนแปลงสินทรัพย์ของบริษัท หรือมีการใช้สินทรัพย์ผิดวัตถุประสงค์โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม
3. การมีรายชื่อและข้อมูลสำหรับการติดต่อกับบริษัทอื่น (Contact with Authorities)
   ผู้จัดการแผนกเทคโนโลยีสารสนเทศต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับบริษัทอื่น ๆ เช่น บมจ.ทศท คอร์ปอเรชั่น ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น
4. การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management)
   4.1 ต้องมีการกำหนดระเบียบ ข้อบังคับ กฎเกณฑ์ต่าง ๆ เกี่ยวกับการดำเนินงานและการเข้าถึงข้อมูล เพื่อให้งานโครงการมีความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน
   4.2 กรณีโครงการที่จ้างบริษัทภายนอก โครงการที่บริษัทภายนอกดำเนินการให้ และโครงการที่บริษัทจัดทำเอง ต้องปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การจัดทำโครงการด้านเทคโนโลยีสารสนเทศ (WI-IT-01) เพื่อให้การบริหารจัดการโครงการเกิดความมั่นคงปลอดภัย และลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น

ส่วนที่ 2 นโยบายการรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human Resource Security)

ส่วนที่ 2.1 การจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์ เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างงานบริษัท

นโยบาย

1. การสรรหาบุคลากร (Screening)
   1.1 เจ้าหน้าที่ฝ่ายทรัพยากรมนุษย์ ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคน ก่อนที่จะบรรจุเป็นเจ้าหน้าที่ผู้บริหาร เจ้าหน้าที่ชั่วคราว หรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของบริษัทใดมาก่อน

1.2 เจ้าหน้าที่ฝ่ายทรัพยากรมนุษย์ ต้องจัดให้มีการลงนามในสัญญาระหว่าง“เจ้าหน้าที่” และบริษัท ว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement : NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างเจ้าหน้าที่นั้น ๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

1.3 ปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การบริหารจัดการทรัพยากรบุคคลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Human resources security) (WI-IT-05)

2. ข้อกำหนดและเงื่อนไขของการจ้างงาน (Terms and conditions of employment)

เจ้าหน้าที่ฝ่ายทรัพยากรมนุษย์ ต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ โดยเจ้าหน้าที่ฝ่ายทรัพยากรมนุษย์ ต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่ และลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายบริษัท
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

ส่วนที่ 2.2 การสร้างความมั่นคงปลอดภัยขณะเป็นเจ้าหน้าที่ (During employment)

วัตถุประสงค์ เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท

นโยบาย

1. หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

ผู้จัดการแผนกเทคโนโลยีสารสนเทศ ต้องกำหนดให้เจ้าหน้าที่ ลูกจ้าง และเจ้าหน้าที่บริษัทภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบและปฏิบัติตามนโยบาย กฎระเบียบและขั้นตอนการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทด้วย

2. การสร้างความตระหนัก การให้ความรู้ และการอบรมให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

2.1 พนักงาน ผู้รับจ้างขององค์กรทุกคนต้องได้รับการอบรมให้ความรู้ โดยเนื้อหาที่แต่ละบุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล เพื่อเป็นการสร้างความตระหนัก และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

2.2 ต้องจัดอบรมให้ความรู้แก่พนักงานเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทด้วย

2.3 พนักงานใหม่ทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือได้รับเอกสารนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศฯ ฉบับย่อ และระเบียบปฏิบัติที่เกี่ยวข้องกับบริษัทภายใน 30 วันนับจากเข้าทำงานในบริษัท เพื่อให้พนักงาน หรือผู้ที่เกี่ยวข้องได้ศึกษาและถือปฏิบัติ โดยอาจเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย

2.4 เจ้าหน้าที่ฝ่ายทรัพยากรมนุษย์ และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทให้แก่บุคลากรด้วย

ส่วนที่ 2.3 การสิ้นสุดหรือเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์ เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการจ้างงาน

นโยบาย

1. การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)
   1.1 ต้องมีการกำหนดและสื่อสารให้พนักงานหรือผู้ทำสัญญาได้รับทราบ รวมทั้งมีการควบคุมให้ปฏิบัติตามข้อกำหนดในสัญญา
   1.2 เจ้าหน้าที่ฝ่ายทรัพยากรมนุษย์ มีหน้าที่ดูแลหากมีการแต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงตาแหน่งใด ๆ ที่เกี่ยวข้องกับความรับผิดชอบในบริษัท
   1.3 เจ้าหน้าที่ผู้เกี่ยวข้องเมื่อได้รับเรื่องของผู้ใช้งานที่สิ้นสุดสภาพการจ้างงานหรือเปลี่ยนหน้าที่ความรับผิดชอบจากฝ่ายทรัพยากรมนุษย์ ให้ปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การควบคุมการเข้าถึง (Access Control) (WI-IT-03) เพื่อดำเนินการเพิกถอนสิทธิ์หรือเปลี่ยนแปลงสิทธิ

ส่วนที่ 3 นโยบายการควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ

วัตถุประสงค์ 1.เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงการใช้งานและความมั่นคงปลอดภัย
2.เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจ
3.เพื่อให้ผู้ใช้งานได้รับรู้และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความปลอดภัยของระบบสารสนเทศ

ส่วนที่ 3.1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control)

การควบคุมการเข้าถึงสารสนเทศ หมายถึง การเข้าสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ ห้องเครื่องแม่ข่าย ระบบเครือข่าย อุปกรณ์เทคโนโลยีสารสนเทศ โดยสารสนเทศหมายความรวมถึงสารสนเทศที่อยู่ในรูปแบบของอิเล็คทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

บริษัทฯ มีการควบคุมการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เพื่อกำหนดมาตรการการเข้าถึงข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต ป้องกันการบุกรุกทั้งด้านกายภาพ ผ่านระบบเครือข่ายและจากโปรแกรม ที่จะสร้างความเสียหายแก่ข้อมูลหรือทำให้ระบบหยุดชะงัก และสามารถตรวจสอบติดตามการพิสูจน์ตัวบุคคลที่ใช้งานข้อมูลหรือระบบสารสนเทศขององค์กรได้อย่างถูกต้องโดยยึดหลักดังนี้

1. การรักษาความลับ (Confidentiality) ให้บุคคลผู้มีสิทธิ์เท่านั้น เข้าถึงข้อมูลได้ และมีการควบคุมการเข้าถึงโดยข้อมูลที่เป็นความลับจะได้ไม่ถูกเปิดเผยกับผู้ไม่มีสิทธิ์

2. ความถูกต้องครบถ้วน (Integrity) ให้มีการรักษาความถูกต้องครบถ้วนของข้อมูล และควบคุมความผิดพลาด ไม่ให้ข้อมูลถูกแก้ไข ลบทิ้ง เปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์

3. ความสามารถในการเข้าถึงและใช้งานได้ (Availability) ให้ผู้มีสิทธิ์ใช้ข้อมูลเท่านั้นสามารถที่จะเข้าถึงข้อมูลได้ตามเวลาที่ตกลงไว้ ผู้รับผิดชอบต้องควบคุมไม่ให้ระบบหยุดชะงัก มีสมรรถภาพในการทำงานต่อเนื่อง และมีการป้องกันไม่ให้มีสิ่งใดทำให้ระบบหยุดทำงาน

1.วัตถุประสงค์

1.1 เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้บริษัทฯ ตระหนักถึงความสำคัญของการใช้งานและเข้าถึงข้อมูลและระบบสารสนเทศ

1.2 เพื่อให้การควบคุมบุคคลภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของบริษัทภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากบริษัทภายนอก เป็นต้น

1.3 เพื่อให้ความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ ว่าสามารถเข้าได้เฉพาะผู้มีสิทธิ์ (Confidentiality) มีความครบถ้วนสมบูรณ์ (Integrity) และมีพร้อมใช้งาน (Availability)

1.4 เพื่อให้สามารถตรวจสอบย้อนหลังการเข้าถึงระบบสารสนเทศต่างๆของผู้ใช้งานได้

2.ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

3.กระบวนการหลักในการควบคุมการเข้าถึงระบบ

3.1 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

3.2 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

3.3 ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศ

3.4 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3.5 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

4.การควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ

4.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

4.2 ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามจำเป็นต่อการใช้งาน เท่านั้น

4.3 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงาน

4.4 ป้องกันการเข้าถึงคอมพิวเตอร์ เครือข่าย อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์ต่อพ่วง ไม่ให้เข้าถึงโดยไม่ได้รับอนุญาตโดยการกำหนดขั้นตอนแบบฟอร์มในการขออนุญาติเข้าถึง ประกอบด้วยรายละเอียดอย่างน้อยดังนี้ ชื่อผู้ใช้งาน เหตุผลในการขอใช้ ระยะเวลาในการใช้บริการ

4.5 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์ในการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอดังนี้

4.5.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

4.5.1.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น อ่านอย่างเดียว สร้างข้อมูล ป้อนข้อมูล แก้ไขข้อมูล ลบข้อมูล อนุมัติ ไม่มีสิทธิ์ ฯลฯ

4.5.1.2 กำหนดเกณฑ์การระงับสิทธิ์ มอบหน้าที่ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

4.6 ให้ถือว่าการอนุมัติการเข้าถึงระบบสารสนเทศโดยผู้บังคับบัญชา/เจ้าของข้อมูล/เจ้าของระบบ เป็นการมอบอำนาจของหน่วยงานที่ผู้ใช้งานเข้าถึงระบบสารสนเทศ

4.7 บริษัท กำหนดช่องทางและเวลาสำหรับการเข้าถึงข้อมูล ดังนี้

- ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาทำการ)
- โทรศัพท์ (เข้าถึงได้ในเวลาทำการ)
- โทรสาร (เข้าถึงได้ในเวลาทำการ)
- ระบบเครือข่ายภายใน (เข้าถึงได้ทุกช่วงเวลา)
- ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)
- ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)
- เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา)

4.8 กำหนดให้มีการเข้ารหัสสำหรับข้อมูลสำคัญหรือข้อมูลลับแต่ละประเภท โดยข้อมูลที่ระดับชั้นความลับต้องเข้ารหัสในการจัดเก็บ

4.9 จัดทำข้อตกลงรักษาความลับ (Non-Disclosure Agreement) ระหว่าง บริษัท กับหน่วยงานผู้ที่ได้รับการว่าจ้างหรือผู้ที่จำเป็นต้องเข้าถึงข้อมูล

4.10การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

4.10.1 ข้อมูลภายในบริษัท แบ่งเป็นประเภทต่างๆ ดังนี้

4.10.1.1 ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ นโยบาย ยุทธศาสตร์ ข้อมูลบุคคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

4.10.1.2 ข้อมูลสารสนเทศด้านการดำเนินงาน ได้แก่ กฎหมาย ระเบียบ ผลการดำเนินงาน การใช้จ่ายงบประมาณ เป็นต้น

4.10.1.3 ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลประชาสัมพันธ์ ข้อมูลการตลาด เป็นต้น

4.10.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับคือ

4.10.2.1 ข้อมูลที่มีระดับความสำคัญมาก

4.10.2.2 ข้อมูลที่มีระดับความสำคัญปานกลาง

4.10.2.3 ข้อมูลที่มีระดับความสำคัญน้อย

4.10.3 จัดแบ่งชั้นความลับของข้อมูล ดังนี้

4.10.3.1 ชั้นลับที่สุด เปิดเผยต่อบุคคลภายนอกหรือสาธารณะไม่ได้

4.10.3.2 ชั้นลับมาก เปิดเผยสู่บุคคลภายนอกหรือสาธารณะได้เมื่อได้รับอนุมัติจากผู้บริหารหรือผู้ที่ผู้บริหารมอบหมาย

4.10.3.3 ชั้นลับ เปิดเผยสู่บุคคลภายนอกหรือสาธารณะได้เมื่อร้องขอ

4.10.3.4 ชั้นทั่วไป เปิดเผยสู่สาธารณะได้ตลอดเวลา

4.10.4 จัดแบ่งระดับชั้นการเข้าถึง

4.10.4.1 ระดับชั้นสำหรับผู้บริหาร

4.10.4.2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

4.10.4.3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบมาย

4.10.5 เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4.10.6 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล โดยแบ่งออกเป็นผู้ใช้งานปรกติ ผู้ใช้งานที่มีสิทธิ์สูงและผู้ใช้งานที่ดูแลระบบงานโดยการกำหนดการตั้งชื่อบัญชีผู้ใช้ให้เป็นมาตรฐานพร้อมทั้งจัดทำทะเบียนให้เป็นลายลักษณ์อักษรและปรับปรุงเป็นประจำอย่างสม่ำเสมอ

4.10.7 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส(Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

4.10.8 ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ในเอกสารวิธีการปฏิบัติงาน WI-IT-03 เรื่อง “การควบคุมการเข้าถึง (Access Control)”

4.10.9 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

<u>ส่วนที่ 3.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)</u>

1. จัดให้มีการอบรมการใช้งานระบบเทคโนโลยีสารสนเทศให้กับผู้ใช้งานใหม่ ร่วมกับทางฝ่ายทรัพยากรมนุษย์ และมอบเอกสารสิทธิ์การเข้าถึงแก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์ และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้ผู้ใช้ลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเป็นลายลักษณ์อักษร
2. จัดให้มีมาตรการเชิงป้องกันและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ เช่น ติดตั้งโปรแกรม Antivirus ที่เครื่องผู้ใช้งานทุกเครื่อง มีการติดตั้ง Firewall และ IPS (Intrusion Prevention System) เป็นต้น
3. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งาน (User Registration)
    - จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน โดยต้องระบุข้อมูลพื้นฐานอย่างน้อยดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน ระยะเวลาในการใช้งาน
    - ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานว่าไม่มีการลงทะเบียนผู้ใช้งานมาก่อน
    - ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

- ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

4. กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
    - 4.1 พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน
    - 4.2 จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชีของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าถึงการใช้งานว่าถูกต้องหรือไม่
    - 4.3 ดำเนินการแก้ไขข้อมูล สิทธิ์ต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งจากหน่วยงาน
    - 4.4 กรณีหน่วยงานเป็นผู้ทบทวนสิทธิ์และส่งคำร้องขอมาให้ผู้ดูแลระบบดำเนินการแก้ไข ทบทวนสิทธิ์ตามที่ได้รับคำร้องขอจากหน่วยงาน
5. ผู้ใช้ ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด
6. ตัดผู้ใช้งานออกจากทะเบียนโดยปฏิบัติตามขั้นตอนของการตัดผู้ใช้งาน เมื่อการมีเพิกถอนสิทธิ์ตามกรณีต่อไปนี้
    - สิ้นสุดหน้าที่ตามงานที่รับผิดชอบ เช่นการโอนย้าย การลาออก
    - ผู้บังคับบัญชาแจ้งเป็นลายลักษณ์อักษรว่าให้เพิกถอนสิทธิ์
7. การบริหารจัดการบัญชี และรหัสผ่าน รายชื่อผู้ใช้งานที่รับสิทธิ์สูง (Administrator Account / Privileged Account) และผู้ใช้งานทั่วไป (User account)
    - 7.1 ผู้ดูแลระบบต้องกำหนดระดับสิทธิของเจ้าหน้าที่ ในการเข้าถึงเหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศแต่ระบบ ตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน
        - 7.1.1 บัญชีผู้ใช้งานที่รับสิทธิ์สูง (Administrator Account /Privileged Account) สามารถเข้าถึงไฟล์ ข้อมูล และทรัพยากรต่างๆ ในระบบสารสนเทศ รวมทั้งสามารถ อ่าน สร้างข้อมูล ป้อนข้อมูล แก้ไขข้อมูล ลบข้อมูล อนุมัติและระงับสิทธิ์ผู้ใช้งานอื่นๆ ซึ่งผู้บังคับบัญชาแผนกเทคโนโลยีสารสนเทศเป็นดูแล รับผิดชอบบัญชีผู้ใช้งานที่รับสิทธิ์สูง หากบัญชีผู้ใช้งานที่รับสิทธิ์สูง ถูกนำไปงานในทางที่ผิด จะส่งผลให้เกิดความเสียหายต่อระบบสารสนเทศ จึงได้กำหนดแนวทางปฏิบัติดังนี้
            - 7.1.1.1 ไม่อนุญาตให้ผู้ดูแบบระบบทำการแชร์บัญชีผู้มีสิทธิ์สูง
            - 7.1.1.2 จำกัดจำนวนบัญชีผู้มีสิทธิ์สูงให้น้อยที่สุด ผู้ดูแลระบบแต่ละคนควรมีบัญชีที่มีสิทธิ์สูงบัญชีเดียวสำหรับการทำงานทุกระบบ
            - 7.1.1.3 ในการขอยืมใช้งานบัญชีที่มีสิทธิ์สูงต้องทำตามขั้นตอนการร้องขอและการอนุมัติเอกสาร และเข้าใช้งานได้เฉพาะในช่วงเวลาที่ได้ระบุไว้ การขอยืมใช้ในกรณีดังต่อไปนี้
                - ต้องการลบ หรือ เพิ่ม บัญชีผู้ดูแลระบบ

- เมื่อต้องการแก้ไข Policy และกำหนดกฎเกณฑ์ใหม่สำหรับเครื่องคอมพิวเตอร์
- เมื่อเกิดเหตุฉุกเฉินผู้ใช้งานไม่สามารถเข้าสู่ระบบได้ ต้องมีการยืนตัวตนจากบัญชีที่มีสิทธิ์สูง
- เมื่อมีการปรับเปลี่ยนโครงสร้างโปรแกรมในระบบ หรือมีการอัพเดทระบบงานใหม่

7.1.1.4 ตรวจสอบและเก็บบันทึกกิจการการใช้งานบัญชีผู้มีสิทธิ์สูง เช่นการเข้าออกจากระบบ การดำเนินการอื่นๆ ที่ผู้ใช้งานได้รับสิทธิ์

7.1.2 บัญชีผู้ใช้งานทั่วไป (User Account) กรณีหน่วยงานเป็นผู้ทบทวนสิทธิ์และส่งคำร้องขอมาให้ผู้ดูแลระบบดำเนินการแก้ไข ทบทวนสิทธิ์ตามที่ได้รับคำร้องขอจากหน่วยงาน

7.2 การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม วิธีการปฏิบัติงาน WI-IT-03 เรื่อง “การควบคุมการเข้าถึง (Access Control)” หัวข้อ 3.2 และ 3.5 การยกเลิกสิทธิ์ของผู้ใช้งาน และ การเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน

7.3 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

7.4.1 ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

7.4.2 กรณีจำเป็นต้องมีให้สิทธิ์พิเศษ ต้องควบคุมการใช้งานชื่อผู้ใช้งานที่มีสิทธิ์พิเศษอย่างเข้มงวด จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

7.4.3 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

7.4.4 มีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง โดยกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

7.4.5 กำหนดการตั้งรหัสผ่านตามนโยบายอย่างเคร่งครัด และมีการเปลี่ยนรหัสผ่าน ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

7.4.6 กำหนดให้รหัสผู้ใช้สิทธิ์พิเศษต่างๆจากรหัสผู้ใช้งานตามปกติ

7.5 แบ่งแยกอำนาจหน้าที่ (Segregation of Duties) .ให้มีการสอบยันการปฏิบัติงานระหว่างผู้ใช้งานในฝ่ายเทคโนโลยีสารสนเทศ ดังนี้

7.5.1 ต้องแบ่งแยกบุคคลากรที่ปฏิบัติงานในการพัฒนาระบบงาน (Developer) ออกจากบุคคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment)

7.5.2 ต้องจัดให้มีคำบรรยายลักษณะงาน (Job Description) ซึ่งระบบหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคคลากรแต่ละคนภายในฝ่ายเทคโนโลยีสารสนเทศอย่างชัดเจนเป็นลายลักษณ์อักษร

7.5.3 ควรจัดให้มีบุคคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น

7.5.4 กำหนดให้ผู้ที่หน้าที่ในการตรวจสอบประเมินความมั่นคงปลอดภัยของระบบต้องไม่เป็นผู้ดูแลระบบของระบบที่ตนเองตรวจสอบประเมิน

7.6 ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานดังนี้

7.6.1 ทบทวนสิทธิ์การเข้าถึงผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง

7.6.2 ทบทวนสิทธิ์สำหรับผู้ใช้งานในสิทธิ์ในระดับสูง เช่น สิทธิ์ของผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

7.6.3 ทบทวนสิทธิ์ตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

7.6.4 กำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนภายหลัง

7.6.5 ตรวจสอบสิทธิ์และติดตามการใช้งานตามสิทธิ์ที่ได้รับของแต่ละระบบ

7.6.6 กำหนดให้มีการเพิกถอนสิทธิ์หรือระงับการใช้งานของแต่ละสิทธิ์แตกต่างกันไป ตามหน้าที่รับผิดชอบในแต่ละระบบ

7.7 ในกรณีที่ระบบคอมพิวเตอร์หรือระบบสารสนเทศที่มีข้อจำกัดเกี่ยวบัญชีผู้ใช้งาน ทำให้ผู้ใช้งานต้องใช้บัญชีร่วมกันและถือรหัสผ่านผ่านร่วมกัน ให้เจ้าของระบบสารสนเทศเป็นผู้มอบหมายให้ผู้ใช้งานถือรหัสผ่านร่วมกัน

7.8 สิทธิการใช้งานระบบสารสนเทศขั้นพื้นฐาน

ระบบสารสนเทศ	กรรมการบริษัท	พนักงาน	ลูกจ้าง	บุคคลภายนอก
-ระบบ Intranet	/	/		
-ระบบจดหมายอิเล็กทรอนิกส์(E-mail)	/	/		
-เว็บไซต์ www.lighttrio.com www.itthi.co.th	/	/		/
-ระบบ File and print sharing	/	/		
-ระบบ Wi-fi	/	/		/
-ระบบ VPN	/	/		

<u>ส่วนที่ 3.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)</u>

1. **การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติดังนี้**
   1. ผู้ใช้งานมีหน้าที่ป้องกัน ดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username)ของตนเองตามลักษณะงานที่เกี่ยวข้อง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

2. **การบริหารจัดการรหัสผ่าน**
   2.1 กำหนดให้ผู้ใช้งานลงนามหรือยืนยัน ในการป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนเอง เช่นลงนามในเอกสารเพื่อแสดงสิทธิ์และหน้าที่ความรับผิดชอบของผุ้ใช้งานในการเข้าถึงระบบ
   2.2 กำหนดขั้นตอนปฏิบัติ สำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
   2.3 กำหนดกำหนดรหัสผ่านชั่วคราวให้มีความยากต่อการการเดาโดยผู้อื่น และควรกำหนดรหัสผ่านที่แตกต่างกัน
   2.4 เปลี่ยนรหัสโดยทันทีภายหลังจากที่ได้รับหัสผ่านชั่วคราวและควรเปลี่ยนรหัสผ่านให้มีสีความย่อต่อการเดาโดยผู้อื่น

2.5 จัดส่งรหัสผ่านให้ผู้ใช้งานโดยมีการยืนยันการได้รับรหัสผ่านแล้ว หากใช้อีเมลล์ในการส่ง ต้องกำหนดให้ผู้ใช้งานตอบกลับหลังจากได้รับรหัสผ่านแล้ว

2.6 ตรวจสอบยืนยันตัวตน และกำหนดสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Authentication and Authorization) ก่อนการเข้าสู่ระบบงานคอมพิวเตอร์ ที่รัดกุมเพียงพอ โดยให้สอดคล้องกับข้อกำหนดเรื่องการตั้งรหัสและเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยของบริษัท และกำหนดให้ผู้ใช้งานแต่ละรายมีชื่อผู้ใช้งาน (User Account) เป็นของขอบริษัท และกำหนดให้ผู้ใช้งานแต่ละรายมีชื่อผู้ใช้งาน (User Account) เป็นของตนเอง

2.7 เข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่าน เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

2.8 ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบที่มีผลกระทบและมีความสำคัญสูงต่อองค์กรอย่างสม่ำเสมอและดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิ์ใช้งานระบบ แล้ว เช่นบัญชีรายชื่อของบุคคลากรที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ(Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ ได้แก่ การระงับ (Disable) การใช้งาน, ลบออกจากระบบ หรือเปลี่ยนรหัสผ่าน เป็นต้น

ส่วนที่ 3.4 การบริหารจัดการสินทรัพย์ (Assets Management)

1. ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์:
- เพื่อให้สินทรัพย์ของบริษัทได้รับการป้องกันและปกป้องอย่างเหมาะสม
- เพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานอุปกรณ์คอมพิวเตอร์และผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด
  เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของบริษัทให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

นโยบาย

1.1 ทะเบียนสินทรัพย์ (Asset Register)

1) เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำและเก็บทะเบียนสินทรัพย์ ซึ่งรวมถึงสินทรัพย์ข้อมูล และเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ (Software Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ของบริษัท โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงาน เรื่อง ระบบการบริหารจัดการสินทรัพย์ถาวรของบริษัท (Fixed Asset Management) (PM-AC-06)
2) เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ต้องเข้าร่วมการตรวจนับสินทรัพย์ (Physical Check) และจัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภท ตามระยะเวลาที่กำหนดไว้ปีละ 1 ครั้ง
3) เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์เมื่อมีสินทรัพย์ใหม่ หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

1.2 ความเป็นเจ้าของสินทรัพย์ (Ownership for Assets)

เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ จะต้องกำหนดบุคคลหรือบริษัทผู้รับผิดชอบข้อมูลและสินทรัพย์ทั้งหมดด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทอย่างชัดเจน

1.3 การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use for Assets)

1) เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศจะต้องกำหนดแสดงบันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูลและสินทรัพย์จะต้องถูกใช้
2) การอนุญาตให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์ มีดังนี้
   - ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่บริษัทเป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของบริษัท การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่
   - เจ้าหน้าที่ตลอดจนบริษัทภายนอก ที่ได้รับการว่าจ้างโดยบริษัทจะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศของบริษัท
   - ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของบริษัทอย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
   - เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพาทั้งหมดของบริษัท ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งานและต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
   - ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายของบริษัท รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท ก่อนได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ
   - เครื่องคอมพิวเตอร์แบบพกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัท อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์ตามคำแนะนาที่ระบุไว้ใน เอกสารขั้นตอนการปฏิบัติงาน เรื่อง การใช้เครื่องคอมพิวเตอร์แบบพกพาในการปฏิบัติงานนอกสถานที่ (Use of Notebook Computer) (WI-IT-02)
   - อุปกรณ์คอมพิวเตอร์ของบริษัท ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหาร และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด
3) การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์ มีดังนี้
   - ห้ามพนักงานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท
   - ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัท ทั้งที่ได้มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่ หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยบริษัทเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัท
   - ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอเพื่อให้ผู้ใช้งานทั่วไปของบริษัทมีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้
   - รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่า

ซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทเท่านั้น

4) การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้
   - บริษัทจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการทำสืบค้นข้อมูล ความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของบริษัท
   - ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัท และบุคคลผู้ที่เกี่ยวข้องกับบริษัท เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
   - การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ บริษัท ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
   - ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป็อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
   - ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
   - บริษัทไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ดหรือบล็อก) ของพนักงาน ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของพนักงานผู้นั้น

5) การอนุญาตให้ใช้งานอีเมล์มีดังนี้
   - ผู้ใช้งานอีเมล์ทั้งหมดของบริษัท ต้องมี E-mail Account เป็นของตนเอง
   - E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ไปใช้ในทางที่ผิด
   - E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น info@lighttrio.com อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ E-mail Account นั้น
   - E-mail Account ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท ถือเป็นสินทรัพย์ของบริษัท
   - ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบอีเมล์ของบริษัท
   - พื้นที่เก็บอีเมล์บน Google Site ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้ เมื่อปริมาณของอีเมล์มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมล์มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-ส่งอีเมล์ได้ตามปกติอีกต่อไป
   - ขนาดของอีเมล์และไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้

- ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ให้เป็นไปตามขนาดที่บริษัทกำหนด ทั้งนี้ ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงานและอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-mail Account ของบริษัท เพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
- ห้ามใช้ E-mail Account ของบริษัท ในการประกาศข้อมูลใด ๆ ในสื่อสังคมออนไลน์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับบริษัท
- ซอฟต์แวร์สำหรับใช้งานอีเมล์ต้องได้รับการตั้งค่าให้อีเมล์ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อบริษัท บริษัท และเบอร์โทรศัพท์ติดต่อ
- ห้ามผู้ใช้งานทำสำเนาข้อความ หรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนของบริษัท
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม
- ผู้ใช้งานต้องหลีกเลี่ยงการใช้คำสั่ง “Reply with History” ซึ่งเป็นการตอบกลับอีเมล์พร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่จำเป็นต้องใช้งานเท่านั้น อย่างไรก็ตาม เมื่อมีการใช้งานคำสั่ง “Reply with History” ผู้ใช้งานควรทำการลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่งอีเมล์
- ผู้ใช้งานต้องทำการส่งอีเมล์ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้คำสั่ง “Reply All” ถ้าหากอีเมล์ฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน
- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่าง ๆ (Spam Mail) เป็นต้น
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่งอีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติหรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัท
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)
- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

6) การอนุญาตให้ใช้งานโทรศัพท์ เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้
   - ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น
   - ห้ามผู้ใช้งานบันทึกหรือฝากข้อความที่มีข้อมูลลับในเครื่องตอบรับโทรศัพท์อัตโนมัติหรือ ระบบวอยซ์เมล์โดยเด็ดขาด
   - ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลำโพงของเครื่องโทรศัพท์ (Speakerphones) หรือผ่านสื่ออิเล็กทรอนิกส์ใด ๆ เช่น Voice Over IP หรือในระหว่างการประชุมทางไกล เว้นแต่ผู้เข้าร่วมการประชุมทุกฝ่ายได้รับการพิสูจน์ตัวตนแล้วว่า เป็นผู้ที่เกี่ยวข้องและมีสิทธิ์รับทราบข้อมูล
   - ผู้ที่เกี่ยวข้องตรวจสอบจนมั่นใจแล้วว่า ไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลลับที่สนทนาอยู่
   - การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนังและประตูที่เหมาะสมสามารถป้องกันเสียงลอดออกมาได้ เป็นต้น
   - ผู้ใช้งานต้องสนทนาโทรศัพท์ด้วยความระมัดระวัง เพื่อป้องกันข้อมูลลับถูกแอบฟังโดยบุคคลที่ไม่ได้รับอนุญาต
   - ในกรณีที่ต้องมีการเปิดเผยข้อมูลลับใด ๆ ทางโทรศัพท์ ผู้ให้ข้อมูลต้องทำการตรวจสอบให้มั่นใจว่าคู่สนทนานั้น เป็นผู้ได้รับอนุญาตให้รับทราบข้อมูลดังกล่าว ก่อนที่จะเปิดเผยข้อมูล
   - ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือสแกนเอกสารที่มีข้อมูลลับ โดยสำเนาเอกสารนั้นต้องได้รับการปกป้องดูแลในระดับเทียบเท่ากับเอกสารต้นฉบับ
   - เจ้าหน้าที่ต้องไม่เปิดเผยสถานที่ตั้งของห้องเครื่องคอมพิวเตอร์แม่ข่ายต่อบุคคลภายนอกโดยเด็ดขาด เว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อการปฏิบัติงาน

1.4 การคืนสินทรัพย์ (Return on Assets)

พนักงานซึ่งพ้นสภาพจากการจ้างงานต้องคืนสินทรัพย์ทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน โดยปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การส่งคืนทรัพย์สิน (Return of assets) (WI-HR-02)

2. การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification))

วัตถุประสงค์: เพื่อทำให้แน่ใจว่าสารสนเทศของบริษัท ได้รับการปกป้องในระดับที่เหมาะสม

นโยบาย

2.1 การกำหนดชั้นความลับของสารสนเทศ (Classification of Information)

1) สารสนเทศต้องมีการจัดชั้นความลับโดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญและระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
2) พนักงานต้องทำการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม
3) เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลดิจิตอลหรือสารสนเทศดิจิตอลนั้น

2.2 การจัดทำป้ายชื่อของข้อมูล (Labeling of Information)

1) ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์สินทรัพย์สารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร
2) ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้พนักงานต้องปฏิบัติตาม เพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

2.3 การจัดการสินทรัพย์ (Handling of Asset)

1) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น
2) ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม
3) ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน
4) ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร ฯลฯ โดยทันที
5) เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล
6) เจ้าหน้าที่ต้องไม่พูดคุยหรือใช้งานข้อมูลลับของบริษัทในพื้นที่สาธารณะ เช่น ลิฟท์ ร้านอาหาร โถงพักผ่อน ฯลฯ
7) สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น PDA, USB-Drive, CD-ROM เป็นต้น) ที่มีข้อมูลลับของบริษัท บันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

3 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handing)

วัตถุประสงค์: เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของบริษัท โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

นโยบาย

3.1 **การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)**

การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องมีการจัดทำขั้นตอนสำหรับบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้ สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างนี้ที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

1) ให้เจ้าของระบบสารสนเทศเป็นผู้พิจารณาอนุญาตให้ใช้งานสื่อบันทึกข้อมูลแบบถอดแยกได้บนเครื่องคอมพิวเตอร์ที่ตนดูแลรับผิดชอบ
2) ในกรณีที่เจ้าของระบบสารสนเทศอนุญาตให้ใช้งานสื่อบันทึกข้อมูลแบบถอดแยกก่อนการใช้งานสื่อบันทึกข้อมูลแบบถอดแยกต้องได้รับการสแกนไวรัสจากโปรแกรมป้องกันไวรัสที่ได้รับการอัพเดทอยู่เสมอ
3) ห้ามใช้งานสื่อบันทึกข้อมูลแบบถอดแยกได้ที่ไม่สามารถระบุเจ้าของหรือแหล่งที่มาได้และให้ส่งมอบแก่ผู้ดูแลระบบฯ เพื่อทำการตรวจสอบความมั่นคงปลอดภัย

3.2 **การทำลายสื่อบันทึกข้อมูล (Disposal of Media)หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Re-use of Equiment)**

1) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และการทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม
2) ควรทำลายสื่อที่ใช้ในการบันทึกข้อมูล เอกสาร และอุปกรณ์สำนักงานภายใต้สิ่งแวดล้อมที่ได้มีการควบคุม (Controlled Environment)
3) มีมาตรการหรือเทคนิคในการลบหรือเขียนทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้
4) เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล

1) คัดแยกเอกสารบนสื่อบนบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับ และไม่แน่ใจว่าลับหรือไม่ ให้อยู่ในกลุ่มเอกสารลับ

2) กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูลดังนี้

ประเภทสื่อบันทึก	นำสื่อบันทึกกลับมาใช้ใหม่	บันทึกข้อมูลที่มีชั้นความลับและนำสื่อบันทึกกลับมาใช้ใหม่	ไม่นำสื่อบันทึกกลับมาใช้ใหม่
CD/DVD			ใช้การทุบ หรือทำลายให้เสียหาย
สื่อบันทึกข้อมูลแบบมีระบบปฏิบัติการ	ใช้การ Factory Data Reset	-ระบบปฏิบัติ IOS ใช้การ Factory Data Reset -ระบบปฏิบัติการอื่นๆ ใช้การลบและเขียนข้อมูลทับจนเต็มพื้นที่จัดเก็บ	ใช้การทุบ หรือทำลายให้เสียหาย
สื่อบันทึกข้อมูลแบบถอดแยกได้	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบ หรือทำลายให้เสียหาย
เทปบันทึกข้อมูล	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบ หรือทำลายให้เสียหาย
ฮาร์ดไดร์ฟ (Hard Drive)	ใช้วิธีการ Format โดยการเขียนทับข้อมูลเป็นจำนวนหลายๆ รอบ	ใช้การ Format แบบ Zero-filling	ใช้การทุบ หรือทำลายให้เสียหาย
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse	ห้ามนำกลับมาใช้ใหม่ ใช้เครื่องทำลายเอกสารก่อนทิ้ง	ใช้เครื่องทำลายเอกสารก่อนทิ้ง

5) เจ้าของข้อมูลต้องจัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูล และสื่อบันทึกข้อมูลสำคัญและมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ
6) เจ้าของข้อมูลต้องจัดทำบันทึกรายละเอียดการปฏิบัติงานในการทำลายสื่อบันทึกข้อมูลเพื่อให้สามารถตรวจสอบได้ภายหลัง

ส่วนที่ 3.5 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

1.การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

1.1 ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของบริษัท ต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงานและได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับการมอบหมาย

1.2 การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงานและได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับการมอบหมาย โดยจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น

1.3 ห้ามผู้ใดกระทำเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาต

1.4 ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่บริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพดังนี้

1.4.1 ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

1.4.2 ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

1.4.3 ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยงเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

1.4.4 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกบริษัท ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware)ด้วย

1.4.5 การป้องกันมิให้หน่วยงานภายที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

1.4.6 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

1.4.7 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

1.4.8 การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดต้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องกำหนดสิทธิ์การเข้าใช้งาน และระยะเวลาในการเชื่อมต่อ ภายหลังได้รับอนุญาตผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP ของทั้งต้นทางและปลายทางได้
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

1.5 การป้องกันมิให้หน่วยงานภายที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

1.6 การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงานและได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับการมอบหมาย โดยจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น

1.7 ห้ามผู้ใดกระทำเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาต

1.8 ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอร์ฟแวร์ระบบ (Systems Software

1.9 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุญาตจากผู้ดูแลระบบ และให้ติดตั้งก่อนดำเนินการ

2.การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

2.1 ควรกำหนดบุคคลที่รับผิดรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

2.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

2.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

2.4 ควรดำเนินการติดตั้งอัพเดทระบบซอฟท์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ

2.5 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

2.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ เท่านั้น

3.การบริหารจัดการการบันทึกและการตรวจสอบ

3.1 ควรกำหนดให้มีการบันทึกการทำงานระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

3.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

3.2 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

4.การควบคุมการเข้าใช้งานระบบจากภายนอก

ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในบริษัทเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัตดังนี้

4.1 การเข้าสู้ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของบริษัท ก่อให้เกิดช่องทาง

ที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของบริษัท การควบคุมบุคคลที่เข้าสู่ระบบของบริษัทจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

4.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

4.3 ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับบริษัทอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

4.4 ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้าบริษัทนั้นต้องดูและการจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

4.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

5.การพิสูจน์ตัวตนสำหรับผู้ใช้ภายนอก

5.1 ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบของบริษัท สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

5.1.1 การแสดงตัวตน(Identification) คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)

5.1.2 การพิสูจน์ยืนยันตัวตน(Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน(Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB token ที่มีความสามารถ PKI เป็นต้น

5.2 การเข้าสู่ระบบสารสนเทศของบริษัทนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1วิธี

5.3 การเข้าสู่ระบบสารสนเทศของบริษัทจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

5.4 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

6.การใช้งานโปรแกรมอรรถประโยชน์

6.1 การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

6.2 ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับ

อนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

7.การควบคุมบริษัภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third party Access Control

7.1 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยบริษัทภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

7.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่สารของบริษัทภายนอก

7.2.1 บุคคลบุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทจะต้องทำเรื่องขออนุญาตเพื่อขออนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

7.2.2 บริษัทภายนอก ที่ทำงานให้กับบริษัททุกบริษัท ไม่ว่าจะทำงานอยู่ภายในบริษัทหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาไม่เปิดเผยข้อมูลของบริษัทโดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

7.2.3 บริษัท ควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของบริษัทภายนอกทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

7.2.4 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยบริษัทภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้บริษัทภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

7.2.5 สำหรับโครงการขนาดใหญ่ บริษัทภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของบริษัทผู้ดูแลระบบต้องควบคุมการปฏิบัติการนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

7.2.6 บริษัทมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจว่า บริษัทสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

7.2.7 ควรดำเนินการให้ผู้ให้บริการบริษัทภายนอกจัดทำแผนการดำเนินงาน คู่มือปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

7.2.8 ควรมีการเก็บ Log ในการใช้งานระบบเพื่อให้สามารถตรวจสอบได้ในภายหลัง และควรยกเลิกสิทธิ์เมื่อใช้งานเสร็จสิ้นทันที

<u>ส่วนที่ 3.6 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)</u>

1. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามxxxxxxx)ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อxxxxxxxx) การลาออก หรือการเปลี่ยนตำแหน่งงานภายในบริษัท ในการกรณีที่เป็น เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อเข้ากับระบบโดเมน (Join Domain)
2. กำหนดขั้นตอนการปฏิบัติเพื่อใช้งาน (โดยปฏิบัติตาม WI-IT)
3. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้แสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง
4. การเข้าใช้งานโปรแกรมยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งาน โปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลักเลี่ยงมาตรการป้องกัน

ทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตราการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่ ให้ดำเนินการดังนี้

4.1 การใช้งานโปรแกรมยูทิลิตี้ ผู้ใช้งานต้องปฏิบัติให้สอดคล้องกับประกาศของบริษัท เรื่องนโยบายและแนวปฏิบัติการใช้งานคอมพิวเตอร์ที่ถูกต้องตามกฎหมาย หากมีการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

4.2 ต้องยกเลิกหรือลบทิ้งโปรแกรมยุทิลิตี้และซอฟต์แวร์ที่ไม่มีความจำเป็นในการใช้งานรวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

5. การกำหนดเวลาใช้งานระบบสารสนเทศ (Secsion time-out) (โดยปฏิบัติตาม WI-IT-03
6. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time) (โดยปฏิบัติตามWI-IT-03

<u>ส่วนที่ 3.7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)</u>

1. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติงานสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในบริษัท (โดยปฏิบัติตาม WI-IT-03 วิธีปฏิบัติงาน เรื่อง การควบคุมการเข้าถึง Access Control ข้อ 3.2)
2. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wrireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องสิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
3. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน xx นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง (วิธีปฏิบัติงาน เรื่อง การควบคุมการเข้าถึง Access Control ข้อxxxxx)
4. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคคลากร (โดยปฏิบัติตาม xxxxxxxxx)
5. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ (โดยปฏิบัติตาม xxxxxx)
6. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

   6.1 แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่นๆ

   6.2 มีการควบคุมภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

   6.3 มีการกำหนดสิทธิ์ให้เฉพาะผู้มีสิทธิ์ใช้งานระบบเท่านั้น

7. การใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องปฏิบัติดังนี้

   7.1 ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่สภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

   7.2 ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

7.3 เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

7.4 หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ 3.8 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

1. ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบของบริษัท สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ
   1.1 การแสดงตัวตน(Identification) คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)
   1.2 การพิสูจน์ยืนยันตัวตน(Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน(Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB token ที่มีความสามารถ PKI เป็นต้น

2.. การเข้าสู่ระบบสารสนเทศของบริษัทนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี
3. การเข้าสู่ระบบสารสนเทศของบริษัทจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย
4. การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ส่วนที่ 3.9 การควบคุมการให้ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN)

1. ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของบริษัท จะต้องได้รับการพิจารณาอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
2. ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
3. ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น
4. ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน
5. ผู้ดูแลระบบต้องกำหนดค่าใช้ Web หรือ WPA,WPA2 ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น
6. ผู้ดูแลระบบควรจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในบริษัท
7. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี
8. ผู้ดูแลระบบ ควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

9. ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมไม่ได้
10. ผู้ดูแลระบบ ควรทำเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันที ที่นำ AP มาใช้งาน
11. ผู้ดูแลระบบต้องกำหนดค่าใช้ Web หรือ WPA,WPA2 ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และAP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น
12. ผู้ผู้ดูแลระบบควรมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในบริษัท
13. ผู้ดูแลระบบควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Privat Network)เพื่อช่วยป้องกันการโจมตี
14. ผู้ดูแลระบบ ควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

<u>ส่วนที่ 3.10 การควบคุมการใช้คอมพิวเตอร์ส่วนบุคคล</u>

วัตถุประสงค์ ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของบริษัท ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

นโยบาย

1. การใช้งานทั่วไป
   - 1.1 เครื่องคอมพิวเตอร์ที่บริษัทอนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินของบริษัท ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของบริษัท
   - 1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท ต้องเป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
   - 1.3 ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัท
   - 1.4 การตั้งชื่อเครื่องคอมพิวเตอร์(Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ของบริษัทเท่านั้น
   - 1.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เท่านั้น
   - 1.6 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
   - 1.7 ไม่ควรเก็บข้อมูลสำคัญของบริษัทไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่
   - 1.8 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของบริษัท
   - 1.9 ผู้ใช้ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้
     - 1.9.1 ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
     - 1.9.2 ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

2. การควบคุมการเข้าถึงระบบปฏิบัติการ
   - 2.1 ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ
   - 2.2 ผู้ใช้ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน
   - 2.3 ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Log-out ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver
3. แนวทางปฏิบัติการใช้รหัสผ่าน
   - 3.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน
4. การป้องกันจากโปรกแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)
   - 4.1 ผู้ดูแลระบบ ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability)ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ
   - 4.2 ผู้ใช้ ควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ External Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
   - 4.3 ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน
   - 4.4 ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
5. การสำรองและการกู้คืน
   - 4.1 ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
   - 4.2 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของบริษัท

ส่วนที่ 3.11 การควบคุมการใช้คอมพิวเตอร์แบบพกพา

วัตถุประสงค์ เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกบริษัท เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ของบริษัทให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

นโยบาย

1. การใช้งานทั่วไป
   - 1.1 เครื่องคอมพิวเตอร์แบบพกพาที่บริษัทอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของบริษัท ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานของบริษัท
   - 1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของบริษัทต้องเป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.3 การตั้งชื่อเครื่องคอมพิวเตอร์ (computer name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ เท่านั้น

1.4 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

1.5 ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

1.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

1.7 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

1.8 ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสียงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

1.9 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

1.10 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

1.11 ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

1.12 การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

1.13 ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

1.14 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

1.15 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

1.16 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

1.17 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

1.18 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

2. ความปลอดภัยด้านกายภาพ

2.1 ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2.2 ผู้ใช้ ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

2.3 ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

3. การควบคุมการเข้าถึงระบบปฏิบัติการ
   - 3.1 ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
   - 3.2 ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
   - 3.3 ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน
   - 3.4 ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
4. แนวทางปฏิบัติในการใช้รหัสผ่าน
   - 4.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)
   - 5.1 ผู้ใช้ ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
   - 5.2 ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา
   - 5.3 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้
6. การสำรองข้อมูลและการกู้คืน
   - 6.1 ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล
   - 6.2 ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
   - 6.3 แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

ส่วนที่ 3.12 การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Use Of Electronic Mail)

วัตถุประสงค์ เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัท ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

2. ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท
3. สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์
4. การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่เทคโนโลยีสารสนเทศได้กำหนดไว้
5. รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ O ในการพิมพ์แต่ละตัวอักษร
6. ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 3 ครั้ง
7. ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ Logout ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
8. ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 6 เดือน
10. ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัทหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท
11. ข้อห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์(e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
12. ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อการทำงานของบริษัทเท่านั้น
13. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
14. ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น
15. ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
16. ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัทผ่านทางจดหมายอิเล็กทรอนิกส์
17. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
18. ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
19. ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์
20. ข้อควรระวัง ผู้ใช้ไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

<u>ส่วนที่ 3.13 การใช้งานระบบอินเตอร์เน็ต (Use of the Internet)</u>

เมื่อเครือข่ายอินเทอร์เน็ตเชื่อมโยงเครือข่ายทั่วโลกให้สามารถติดต่อถึงกันได้หมดจนกลายเป็นเครือข่ายของโลก ดังนั้นจึงมีผู้ใช้งานบนเครือข่ายนี้จำนวนมาก การใช้งานเหล่านี้เป็นสิ่งที่กำลังได้รับการกล่าวถึงกันทั่วไป เพราะการเชื่อมโยงเครือข่าย

อินเทอร์เน็ตทำให้โลกไร้พรมแดน ข้อมูลข่าวสารต่างๆ สามารถสื่อสารถึงกันได้อย่างรวดเร็ว ตัวอย่างการใช้งานบนอินเทอร์เน็ตที่จะกล่าวต่อไปนี้เป็นเพียงตัวอย่างที่แพร่หลายและใช้กันมากเท่านั้น ยังมีการประยุกต์งานอื่นที่ได้รับการพัฒนาขึ้นมาใหม่ตลอดเวลา

1. ไปรษณีย์อิเล็กทรอนิกส์ (Electronic Mail : E-mail) เป็นการส่งข้อความติดต่อกันระหว่างบุคคลกับบุคคลหรือกลุ่มบุคคลก็ได้ หากเปรียบเทียบไปรษณีย์อิเล็กทรอนิกส์กับไปรษณีย์ธรรมดาจะพบว่าโดยหลักการนั้นไม่แตกต่างกันมากนัก ไปรษณีย์อิเล็กทรอนิกส์เปลี่ยนบุรุษไปรษณีย์ให้เป็นโปรแกรม เปลี่ยนเส้นทางเป็นระบบเครือข่าย และเปลี่ยนรูปแบบการจ่าหน้าซองจดหมายให้เป็นการจ่าหน้าแบบอ้างอิงระบบอิเล็กทรอนิกส์โดยใช้ที่อยู่ของไปรษณีย์อิเล็กทรอนิกส์ (email address) การส่งจดหมายอิเล็กทรอนิกส์นั้นมีรูปแบบที่ง่าย สะดวก และรวดเร็ว

หากต้องการส่งข้อความถึงใครก็สามารถเขียนเป็นเอกสาร แล้วจ่าหน้าซองที่อยู่ของผู้รับ ระบบจะนำส่งให้ทันทีอย่างรวดเร็ว ลักษณะของที่อยู่จะเป็นชื่อรหัสผู้ใช้และชื่อเครื่องประกอบกันเช่น sombat@ipst.ac.th การติดต่อบนอินเทอร์เน็ตนี้ระบบจะหาตำแหน่งให้เองโดยอัตโนมัติ และนำส่งไปยังปลายทางได้อย่างถูกต้อง การรับส่งไปรษณีย์อิเล็กทรอนิกส์กำลังเป็นที่นิยมกันอย่างแพร่หลาย

2. การโอนย้ายแฟ้มข้อมูลระหว่างกัน (File Transfer Protocol : FTP) เป็นระบบที่ทำให้ ผู้ใช้สามารถรับส่งแฟ้มข้อมูลระหว่างกันหรือมีสถานีให้บริการเก็บแฟ้มข้อมูลที่อยู่ในที่ต่างๆ และให้บริการ ผู้ใช้สามารถเข้าไปคัดเลือกนำแฟ้มข้อมูลมาใช้ประโยชน์ได้ เช่น โปรแกรม cuteFTP โปรแกรม wsFTP เป็นต้น
3. การใช้เครื่องคอมพิวเตอร์ในที่ห่างไกล (telnet) การเชื่อมโยงคอมพิวเตอร์เข้ากับเครือข่าย ทำให้เราสามารถติดต่อเครื่องคอมพิวเตอร์ที่เป็นสถานีบริการในที่ห่างไกลได้ถ้าสถานีบริการนั้นยินยอม ทำให้ผู้ใช้สามารถนำข้อมูลไปประมวลผลยังเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายเช่นนักเรียนในประเทศไทยส่งโปรแกรมไปประมวลผลที่เครื่องคอมพิวเตอร์ที่ตั้งอยู่ที่บริษัทในประเทศญี่ปุ่นผ่านทางระบบเครือข่ายโดยไม่ต้องเดินทางไปเอง
4. การเรียกค้นข้อมูลข่าวสาร (search engine) ปัจจุบันมีฐานข้อมูลข่าวสารที่เก็บไว้ให้ใช้งานจำนวนมาก ฐานข้อมูลบางแห่งเก็บข้อมูลในรูปสิ่งพิมพ์อิเล็กทรอนิกส์ที่ผู้ใช้สามารถเรียกอ่าน หรือนำมาพิมพ์ ฐานข้อมูลนี้จึงมีลักษณะเหมือนเป็นห้องสมุดขนาดใหญ่อยู่ภายในเครือข่ายที่สามารถค้นหาข้อมูลใดๆ ก็ได้ ฐานข้อมูลในลักษณะนี้เรียกว่าเวิลด์ไวด์เว็บ (World Wide Web : WWW) ซึ่งเป็นฐานข้อมูลที่เชื่อมโยงกันทั่วโลก
5. การอ่านจากกลุ่มข่าว (usenet) ภายในอินเทอร์เน็ตมีกลุ่มข่าวเป็นกลุ่มๆ แยกตามความสนใจ แต่ละกลุ่มข่าวอนุญาตให้ผู้ใช้อินเทอร์เน็ตส่งข้อความไปได้ และหากผู้ใดต้องการเขียน โต้ตอบก็สามารถเขียนตอบได้ กลุ่มข่าวนี้จึงแพร่หลายและกระจายข่าวได้รวดเร็ว
6. การสนทนาบนเครือข่าย (chat) เมื่อเครือข่ายอินเทอร์เน็ตเชื่อมต่อถึงกันได้ทั่วโลก ผู้ใช้จึงสามารถใช้เครือข่ายอินเทอร์เน็ตเป็นตัวกลางในการติดต่อสนทนากันได้ ในยุคแรกใช้วิธีการสนทนากันด้วยตัวหนังสือ เพื่อโต้ตอบกันแบบทันทีทันใดบนจอภาพ ต่อมามีผู้พัฒนาให้ใช้เสียงได้ จนถึงปัจจุบัน ถ้าระบบสื่อสารข้อมูลมีความเร็วพอ ก็สามารถสนทนาโดยที่เห็นหน้ากันและกันบนจอภาพได้
7. การบริการสถานีวิทยุและโทรทัศน์บนเครือข่าย เป็นการประยุกต์เพื่อให้เห็นว่าเป็นสิ่งที่เกิดขึ้นได้ ปัจจุบันมีผู้ตั้งสถานีวิทยุบนเครือข่ายอินเทอร์เน็ตหลายร้อยสถานี ผู้ใช้สามารถเลือกสถานีที่ต้องการและได้ยินเสียงเหมือนการเปิดฟังวิทยุ ขณะเดียวกันก็มีการส่งกระจายภาพวีดิทัศน์บนเครือข่ายด้วย แต่ปัญหายังอยู่ที่ความเร็วของเครือข่ายที่ยังไม่สามารถรองรับการส่งข้อมูลจำนวนมาก ทำให้คุณภาพของภาพวีดิทัศน์ยังไม่ดีเท่าที่ควร

ส่วนที่ 3.14 การตรวจจับการบุกรุก (Intrusion Detection System)

1. บริษัท ควรติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยจองเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง
2. ต้องมีการตรวสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเคือข่ายเป็นประจำโดยผู้ดูแลระบบ
3. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุกการโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบทันทีที่ตรวจพบ
4. พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ จะต้องมีการรายงานให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบ ภายใน 1 ชั่วโมงที่ตรวจพบ
5. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน
6. บริษัทมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤตกรรมเสี่ยงต่อการบุกรุก โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า
7. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของบริษัทการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ 3.15 การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

1. การปรับปรุงระบบปฏิบัติการ (Operatiing System Update)
   - 1.1 ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน
   - 1.2 กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งานระบบ
   - 1.3 กำหนดชื่อเครื่อง (Computer Name) และตั้งค่า IP Address ตามความจำเป็นของการใช้งาน
   - 1.4 ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ
   - 1.5 กรณีที่ระบบปฏิบัติการที่มี ServicePatch Update ให้ตรววสอบหรือปรับปรุงการกำหนดค่าต่างๆ โดยเฉพาะระดับความปลอดภัยของระบบปฏิบัติการ
2. การบริหารจัดการบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)
   - 2.1 กำหนดชื่อและรหัสผ่าน ดูแลระบบ(System Adminstrator)
   - 2.2 กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)
   - 2.3 บันทึกบัญชีผู้ใช้งานและทบทวนสิทธิ์การเข้าใช้ระบบให้เป็นปัจจุบันและสอดคล้องกับหน้าที่ความรับผิดชอบระบบรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการปรับปรุงการป้องกันไวรัส (System Security & antivirus Update)
3. การติดตั้งโปรแกรม Antivirus และปรับปรุงฐานข้อมูลไวรัส (Virus definitition)ให้ทันสมัยอยู่เสมอ และกำหนดค่าการตวจสอบระบบบการสแกนและปรับปรุงโปรแกรม
   - 3.1 ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเวตอร์ เป็นประจำ

3.2 ตรวจสอบ เฝ้าระวัง และติดตาม การทำงานของระบบคอมพิวเตอร์

3.3 ตรวจสอบประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ จากระบบรักษาความปลอดภัยที่ติดตั้ง

3.4 ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา

4. การดำเนินการบริหารจัดการฐานข้อมูล (Database Administrator)

4.1 ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่บริษัทใช้

4.2 กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนด

4.3 สร้างรายชื่อผู้ดูแลระบบฐานข้อมูล (Database Administrator) ชื่อผู้ใช้งาน (User)อื่น และกำหนดสิทธิ์การเข้าใช้งาน

4.4 ปรับปรุง และกำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

5. การติดตั้งฐานข้อมูลโปรแกรมระบบงานต่างๆ กำหนดค่าระบบของโปรกแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการหรือเข้าถึงฐานมูล

5.1 ติดตั้งโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

5.2 กำหนดค่าโปรแกรม หรือตั้งค่า Services ต่างๆ ให้ทำงานร่วมกันกับระบบปฏิบัติการอย่างถูกต้องและมีประสิทธิภาพ

5.3 ติดตั้งฐานข้อมูล เชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามที่ระบบงานกำหนดระบบและฐานข้อมูลตามที่กำหนดไว้

5.4 กำหนดเกณฑ์การสำรอง สำเนา และทดสอบกู้คืน (Restore Test)

5.5 บันทึกข้อกำหนด ค่าติดติ้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้างหรือปรับปรุง

<u>ส่วนที่ 3.16 การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log)</u>

1. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลคลที่เข้าสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง
2. ห้ามแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้
3. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่นบันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพ่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
4. ต้องมีวิธีการป้องกันแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

<u>ส่วนที่ 3.17 การเข้ารหัสข้อมูล (Cryptography)</u>

<u>วัตถุประสงค์</u> เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องกันความลับ การปลอดแปลง หรือความถูกต้องของสารสนเทศ

1. มีนโยบายการควบคุมการเข้ารหัสข้อมูล
   เข้ารหัสข้อมูลโดยใช้รหัสกุญแจ สำหรับข้อมูลที่เป็นความลับอย่างยิ่ง โดยใช้โปรแกรมการเข้ารหัสข้อมูล
2. มีการบริหารจัดการกุญแจในการเข้ารหัสข้อมูล

นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ ต้องมีการจัดทำและปฏิบัติตาม โดยเจ้าของข้อมูลเป็นผู้ดูแลรับผิดชอบรหัสกุญแจที่ใช้งาน

ส่วนที่ 4 นโยบายการรักษาความปลอดภัยฐานข้อมูลและระบบสำรองข้อมูล

วัตถุประสงค์ 1.เพื่อให้ระบบสารสนเทศของบริษัทสามารถให้บริการได้อย่างต่อเนื่อง

2.เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับบริษัทอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

3.เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ.

<u>ส่วนที่ 4.1 การรักษาความปลอดภัยฐานข้อมูล</u>

1. กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล
   - 1.1 จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน
   - 1.2 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงงานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้
     - 1.2.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่ ดูข้อมูล สร้างข้อมูล แก้ไขข้อมูล ลบข้อมูล นำเข้าข้อมูล ส่งออกข้อมูล เป็นต้น
     - 1.2.2 กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้
     - 1.2.3 ผู้ใช้งานที่ต้องการใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย
2. ขั้นตอนปฏิบัติเพื่อจัดเก็บข้อมูล
   - 2.1 จัดแบ่งประเภทของข้อมูล
     - 2.1.1 ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ นโยบาย ยุทธศาสตร์ ข้อมูลบุคคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
     - 2.1.2 ข้อมูลสารสนเทศด้านการดำเนินงาน ได้แก่ กฎหมาย ระเบียบ ผลการดำเนินงาน การใช้จ่ายงบประมาณ เป็นต้น
     - 2.1.3 ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลประชาสัมพันธ์ ข้อมูลการตลาด เป็นต้น
   - 2.2 จัดแบ่งระดับความสำคัญของข้อมูล
     - 2.2.1 ข้อมูลที่มีระบบดับความสำคัญมาก
     - 2.2.2 ข้อมูลที่มีระดับความสำคัญปานกลาง
     - 2.2.3 ข้อมูลที่มีระดับความสำคัญน้อย
   - 2.3 จัดแบ่งชั้นความลับของข้อมูล ดังนี้
     - 2.3.1 ชั้นลับที่สุด เปิดเผยต่อบุคคลภายนอกหรือสาธารณะไม่ได้
     - 2.3.2 ชั้นลับมาก เปิดเผยสู่บุคคลภายนอกหรือสาธารณะได้เมื่อได้รับอนุมัติจากผู้บริหารหรือผู้ที่ผู้บริหารมอบหมาย

2.3.3 ชั้นลับ เปิดเผยสู่บุคคลภายนอกหรือสาธารณะได้เมื่อร้องขอ

2.3.4 ชั้นทั่วไป เปิดเผยสู่สาธารณะได้ตลอดเวลา

2.4 จัดแบ่งระดับชั้นการเข้าถึง

2.4.1 ระดับชั้นสำหรับผู้บริหาร

2.4.2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

2.4.3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบมาย

2.5 การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้ ได้แก่ Intranet หรือ Internet

3. ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่นๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย
4. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใดๆ กับข้อมูลนี้ได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File ได้แก่ ชื่อบัญชีผู้ใช้งาน ฟังก์ชั่นงาน หมายเลขไอดีแอดเดรส วันเดือนปีเวลาที่กระทำการ เป็นต้น) การใช้งานสำหรับฐานข้อมูลตามความจำเป็นเพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งาน

<u>ส่วนที่ 4.2 การสำรองข้อมูล</u>

วัตถุประสงค์ เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น ภัยธรรมชาติ ระบบเสียหาย

นโยบาย

1. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย และจัดทำบัญชีระบบบสารสนเทศที่มีความสำคัญทั้งหมดของบริษัท พร้อมกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง
2. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล
3. การสำรองข้อมูล

3.1 ต้องกำหนดความถี่ในการทำการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบโดยปฏิบัติตามเอกสารวิธีการปฏิบัติงาน เรื่อง การจัดการการสำรองข้อมูลสารสนเทศ (Backup & Restore Procedure) (WI-IT-09)

3.2 ต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ สามารถใช้งานได้ตลอดเวลา

3.3 ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

3.4 ต้องกำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง

3.5 ต้องมีกระบวนการสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องมีการทำเอกสาร และมีการตรวจสอบเป็นระยะ ๆ

3.6 ควรจัดเก็บข้อมูลสำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีเกิดภัยพิบัติกับหน่วยงาน

3.7 ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง

3.8 ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

3.9 ต้องลงบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูล ต้องได้รับการตรวจสอบเป็นประจำทุกปี

3.10 กระบวนการในการเก็บข้อมูลระหว่างสถานที่ระบบคอมพิวเตอร์และสถานที่เก็บข้อมูลต้องได้รับ การตรวจสอบอย่างน้อยปีละ 1 ครั้ง

3.11 สื่อที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- ชื่อระบบ
- วันสร้าง
- ระดับความสำคัญของข้อมูล
- รายละเอียดติดต่อผู้ดูแลข้อมูล

4. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางดังนี้

4.1 มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในการ?ไม่สามารถดำเนการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดดังนี้

2.2.1 มีการกำหนดหน้าที่และความรับผิดชอบของผู้เกี่ยวข้องทั้งหมด

2.2.2 มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาต รการเพื่อลดความเสี่ยงเหล่านั้น เช่นไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้าใช้งานระบบงานได้

2.2.3 มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

2.2.4 มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

2.2.5 มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่นผู้ให้บริการเครือข่าย ฮาร์ดแวร์ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

2.2.6 การสร้างความตระหนัก หรือให้ความรู้แก้เจ้าหน้าที่ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ทำเมื่อเกิดเหตุเร่งด่วน

4.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ปีละ 1 ครั้ง

4.3 ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

5. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ 1 ครั้ง

6. มีการทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงานในบริษัท ปีละ 1 ครั้ง

<u>ส่วนที่ 4.3 การกู้คืนระบบ</u>

1. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข รายงานผลการบันทึกการแก้ไขพร้อมทั้งบันทึก และรายงานสรุปผลการปฏิบัติงานต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
2. ให้ใช้ข้อมูลทันสมัยที่สุด (Lated Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์
4. ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ -5 แผนเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์ 1.เพื่อลดความเสียหายที่จะเกิดขึ้นแก่ระบบเทคโนโลยีสารสนเทศของบริษัท
2.เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท สามารถดำเนินการได้อย่างต่อเนื่อง
3.เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของบริษัท

แนวปฏิบัติ.

<u>ส่วนที่ 5.1 แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (Contingency Plan)</u>

1. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
2. มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญ และกำหนดมาตรการ เพื่อลดความเสี่ยง เช่นไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำไม่สามารถเข้าใช้ระบบงานได้
3. มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
4. มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
5. มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือขายฮาร์ดแวร์ ซอฟต์แวร์ เมื่อมีเหตุจำเป็นที่จะต้องติดต่อ
6. การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ทำเมื่อเกิดเหตุเร่งด่วน
7. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ปีละ 1 ครั้ง

<u>ส่วนที่ 5.2 -ข้อควรปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ</u>

1. กรณีเครื่องลูกข่าย
   - 1.1 ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าที่ฝ่ายเทคโนโลยีสารสนเทศทราบ หรือกรณีมีเหตุอันทำให้ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ฝ่ายเทคโนโลยีสารสนเทศจะต้องประกาศให้ทุกหน่วยงานในบริษัททราบ
   - 1.2 เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว
   - 1.3 ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในบริษัทภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด
   - 1.4 ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด
   - 1.5 ขยย้ายเครื่องไปไว้ในที่ปลอดภัย
   - 1.6 ให้เจ้าหน้าที่ฝ่ายเทคโนโลยีแจ้งเหตุขัดข้องนั้นให้ผู้จัดการฝ่ายเทคโนโลยีทราบโดยเร็วที่สุด
2. กรณีเครื่องบริการ (Server) และอุปกรณ์เครือข่าย
   - 2.1 ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็วแล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

2.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพของเครื่องสำรองไฟฟ้า

2.3 ตัดระบบจ่ายไฟในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

2.4 รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

2.5 ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรองมาเปลี่ยนโดยเร็วที่สุด

2.6 ผู้ดูแลระบบต้องรีบแจ้งให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบโดยเร็ว

3. แผนดำเนินการเพื่อให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)

เพื่อให้ระบบงานของบริษัทสามารถดำเนินงานได้ต่อเนื่องในช่วงการเกิดภัยคุกคามครอบคลุมสถานการณ์ฉุกเฉิน โดยการจัดหาระบบเทคโนโลยีสารสนเทศการสนับสนันการบริหารจัดการ การปฏิบัติงาน และการให้บริการ ให้สามารถดำเนินการได้อย่างต่อเนื่อง ตลอดจนบริหารจัดการความเสี่ยงด้านระบบสารสนเทศที่อาจส่งผลต่อการปฏิบัติงาน และการให้บริการของบริษัทอยู่ในวิสัยที่ยอมรับหรือควบคุมได้

ทรัพยากร	กลยุทธ์ความต่อเนื่องในการดำเนินการ
สถานที่ปฏิบัติงานหลัก	กำหนดพื้นที่ปฏิบัติงานสำรองไว้มากกว่า 1 แห่ง โดยมีการสำรวจความเหมาะสมของสถานที่ การประสานงาน และการเตรียมความพร้อมกับส่วนงานเจ้าของพื้นที่
วัสดุ/อุปกรณ์ที่สำคัญ	1. กำหนดให้มีการจัดอุปกรณ์คอมพิวเตอร์สำรอง ที่มีคุณลักษณะเหมาะสมกับการใช้งาน พร้อมอุปกรณ์ที่สามารถเชื่อมโยงผ่านระบบเครือข่ายสื่อสารของบริษัทได้ 2. กำหนดให้จัดหาคอมพิวเตอร์แบบพกพาให้กับบุคลากรใช้งานเป็นการชั่วคราว โดยพิจารณ่าถึงลำดับความสำคัญ ความจำเป็นเหมาะสมในการใช้งาน
ระบบสารสนเทศและข้อมูลที่สำคัญ	1. กำหนดให้ศูนย์เทคโนโลยีสารสนเทศจัดระบบเทค เทคโนโลยีสำรอง และฐานข้อมูลกลาง เพื่อรับประกันความมั่นคงปลอดภัยของระบบและข้อมูลคัญ 2. กำหนดให้มีการเก็บข้อมูลส่วนกลางสำรองไว้ในสถานที่อื่นเพื่อป้องกันการสูญหายของข้อมูลในระหว่างเกิดวาวะวิกฤตและสามารถดึงข้อมูลจากฐานข้อมูลสำรองได้ 3. กำหนดให้บันทึกข้อมูลด้วยระบบมือสำหรับฐานข้อมูลที่ไม่สามารถดึงข้อมูลจากฐานข้อมูลสำรองได้
o บุคลากรหลัก	1. พัฒนาบุคลกรอื่นนอกบริษัท ให้สามารถทำหน้าที่ร่วมหรือทำหน้าที่แทนบุคลากรหลัก กรณีบุคลกรไม่เพียงพอ

4. แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)

เพื่อให้ระบบอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้ จำเป็นต้องกู้คืนระบบคืนให้ได้เร็วที่สุดเท่าที่จะทำได้ การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจาย

สัญญาณจำเป็นต้องทำอย่างรวดเร็วเพื่อให้ได้ใช้งานอย่างรวดเร็วที่สุด โดยแผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และแฟ้มข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน

4.1 จัดหาอุปกรณ์ชิ้นส่วนใหม่ทดแทน

4.2 เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

4.3 ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง

4.4 ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

4.5 นำ BACKUP TAPE /HARDDISK ที่ได้สำรองข้อมูลไว้ นำกลับมาRestoreใช้

4.6 ทีมกู้ระบบ (ผู้ดูแลระบบ) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง

4.7 ทำการตรวจสอบระบบปฏิบัติการระบบฐานข้อมุลตรวจสอบความถูกต้องของข้อมูลและระบบ

4.8 อื่นๆ ที่เกี่ยวข้อง

5. การจัดการองค์กรปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน

กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง ในการวางระบบรักษาความปลอดภัย (Security) และระบบการบริหารความเสี่ยงของระบบสารสนเทศ เพื่อเตรียมพร้อมในการแก้ไขสถานการณ์ฉุกเฉินได้อย่างรวดเร็ว ต่อเนื่อง และมีประสิทธิภาพ ดังนี้

5.1 การจัดหน่วยปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน

5.1.1 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

5.1.1.1 กำหนดนโยบายให้ฝ่ายเทคโนโลยีสารสนเทศ

5.1.1.2 เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศ

5.1.1.3 มีอำนาจสั่งการให้ทุกหน่วยงาน ปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศ

5.1.1.4 มีอำนาจสั่งทำลายกุญแจพื้นที่เก็บวัตถุอันตรายเพื่อระงับเหตุฉุกเฉิน

5.1.1.5 ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

5.1.1.6 กำหนดอัตรากำลังพล วัสดุอุปกรณ์และเครื่องมือจำเป็นต้องขอเพิ่มเติมในอนาคต

5.1.1.7 ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

5.1.2 เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

5.1.2.1 แจ้งเหตุฉุกเฉินและเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดโดยเร็ว

5.1.2.2 ให้ข้อมูลเกี่ยวสถานที่เกิดเหตุแก่ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และวิเคราะห์สถานการณ์ที่เกิดเหตุ เพื่อประสานงานในการรักษาความปลอดภัยระบบสารสนเทศ

5.1.2.3 มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่าผู้จัดการฝ่ายเทคโนโลยีสารสนเทศจะมาถึงที่เกิดเหตุ

5.1.2.4 สั่งการให้ผู้ที่เกี่ยวข้องปฏิบัติตามแผนฯ

5.1.2.5 ทำหน้าที่แทนผู้จัดการฝ่ายเทคโนโลยีสารสนเทศตามที่ได้รับหมาย

5.1.2.6 ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่นช่างไฟฟ้า ยานพาหนะ และหน่วยดับเพลิง

5.1.2.7 รายงานให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

5.1.2.8 นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพและสอบทานบัญชีทรัพย์สิน

ที่จัดทำขึ้นมาและทำรายงานเสนอต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

5.1.3 ผู้ดูแลระบบเครือข่าย

5.1.3.1 กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

5.1.3.2 พิจารณาแจ้งสถานีดับเพลิงหรือหน่วยงานภายนอกอื่นๆ มาช่วย

5.1.3.3 ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่เกิดเหตุฉุกเฉิน

5.1.3.4 ป้องกันชีวิตทรัพย์สินและสิ่งแวดล้อมให้ได้รับความเสียหายน้อยที่สุด

5.1.3.5 หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหาย รายงานให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบ อุปกรณ์ที่ต้องตรวจสอบได้แก่

5.1.3.1 ทำการตรวจสอบระบบ Firewall

5.1.3.2 ทำการตรวจสอบ Virus, Worm, Spyware

5.1.3.2 ทำการตรวจสอบ UPS

5.1.3.4 ทำการตรวจสอบ Transaction Log files

5.1.3.5 ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ

5.1.3.6 ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ

5.1.3.7 ทำการครวจสอบความถูกต้องของไฟล์ข้อมูล

5.1.3.8 ทำการตรวจสอบค่า Configurationของระบบ

5.1.3.6 เตรียมเครื่องมืออุปกรณ์ทั้งทางด้านHardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

5.1.3.7 ทำการสำรองข้อมูลในส่วนของข้อมูล และสำรองข้อมูลทั้งระบบ

5.1.3.8 ทำการเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัยโดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบโปรแกรม และแฟ้มข้อมูล Tape Backup รายชื่อโปรแกรม เอกสารที่เกี่ยกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์ สำเนาคู่มือต่างๆ

5.1.3.9 นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

ส่วนที่ -6 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์ 1.เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

2.เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับร่ะบบสารสนเทศ

3.เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ.

<u>ส่วนที่ 6.1 การตรวจสอบความเสี่ยง</u>

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ตรวจสอบโดยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง เพื่อให้บริษัทได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัย โดยมีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึง ดังนี้

1. จัดลำดับความสำคัญของความเสี่ยง
2. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

3. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
4. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้
5. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

<u>ส่วนที่ 6.2 ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ</u>

จากการติดติดตรวจสอบความเสี่ยงต่างๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกภัยต่างๆ ได้ 5 ประเภทดังนี้

1. ภัยที่เกิดขึ้นจากเจ้าหน้าที่หรือบุคลกรของบริษัท (Human Error)
   เช่น เจ้าหน้าที่หรือบุคลากรของบริษัทขาดความรู้ความเข้าใจ และความตระหนัก ในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardward และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ ไม่สามารถใช้งานร่ะบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยประชาสัมพันธ์หลักสูตรอบรมหรือสื่อมัลติมีเดียแก่เจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในในด้าน กฎหมายคอมพิวเตอร์ Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น
2. ภัยที่เกิดจาก Software
   2.1 Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ทำระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ประกอบด้วย
      2.1.1 ไวรัสคอมพิวเตอร์ (Computor Virus)
      2.1.2 หนอนอินเทอร์เน็ต (Internet Worm)
      2.1.3 ม้าโทจัน (Trojan Horse)
      2.1.4 Ransomware
      2.1.5 ข่าวไวรัสหลอกลวง (Hoax)
   2.2 กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้
      2.1.1 ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก
      2.1.2 ติดตั้งซอฟ์ตแวร์ Anti Virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์
3. ภัยจากไฟไหม้ หรือระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้
   3.1 ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย
   3.2 ควรติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่XXXXXXXXXXX และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

4. ภัยจากธรรมชาติ จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้
   - 4.1 เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา
   - 4.2 ตรวจสอบการสำรองข้อมูล พร้อมทั้งการกู้คืน ตามแนวทาง ส่วนที่ 2.2 การสำรองข้อมูล
   - 4.3 ตรวจสอบระบบฟ้าในห้องควบคุมเครือข่ายสำหรับการติดตั้งเครื่องคอมพิวเตอร์ แม่ข่าย และอุปกรณ์เครือข่าย
   - 4.4 ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายหรือไม่
   - 4.5 เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามาถให้บริการข้อมุลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องกับ เพื่อเข้ามาใช้บริการได้ตามปกติ
5. ภัยทางด้านการพัฒนา Software และฐานข้อมูล ไม่ตรงตามมาตรฐาน ใช้ระบบเทคโนโลยีที่ล้าสมัยทั้งด้าน Hardware และ Software ส่งผลต่อความเสี่ยงในการถูกโจมตีจากผู้ไม่ประสงค์ดี ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้
   - 5.1 ให้จัดแผนทดแทนอุปกรณ์คอมพิวเตอร์ที่ล้าสมัย มีการใช้งานเกิน Xxปี หรือมีอายุการใช้งานตามที่บริษัทกำหนดไว้นโยบายการบัญชี หลักเกณฑ์การคำนวณค่าเสื่อมราคาสินทรัพย์ถาวร
   - 5.2 จัดทำแผนปรับปรุงระบบงานสนเทศที่ใช้เทคโนโลยีที่ล้าสมัย มีความเสี่ยงต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี
   - 5.3 ให้ผู้ดูแลระบบ ติดตามข่าวสารการใหการสนับสนุนทางเทคนิคจากเจ้าของผลิตภัณฑ์ Software ที่เกี่ยวข้องและดำเนินการจัดหาทดแทนเมื่อมีความล้าสมัย
6. ภัยทางด้านโรคระบาดที่ส่งผลต่อการปฏิบัติงานจากภายในบริษัท ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้
   - 6.1 กำหนดพื้นที่เข้า-ออก .ให้สามารถควบคุมและตรวจสอบบุคลกรที่เข้าไปในสถานที่ปฏิบัติงานที่มีความจำเป็นเท่านั้น ผู้ไม่มีหน้าที่เกี่ยวข้องไม่สามารถเข้า-ออกได้
   - 6.2 ปฏิบัติตามขั้นตอนตามประกาศของศูนย์ปฏิบัติการภาวะฉุกเฉินในกรณีเกิดโรคระบา
   - 6.3 ให้เจ้าหน้าที่ที่ไม่มีความจำเป็นในการควบคุมดูแลระบบ กำหนดนโยบายให้ปฏิบัติงานที่พัก โดยปรับระบบการทำงานให้สามารถพร้อมทำงานจากที่พักได้
   - 6.4 ในกรณีที่มีความจำเป็นเร่งด่วนที่จะต้องเข้าพื้นที่ปฏิบัติงานให้แจ้งกับผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบถึงเหตุจำเป็น

ส่วนที่ 7 นโยบายการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์ 1.เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และบริษัทภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

2.เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้แก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของบริษัท โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคลต่าง ๆ ที่มีความ

จำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

แนวปฏิบัติ.

<u>การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย</u>

1. ภายในบริษัท ควรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวังควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้
2. ผู้บริหาร ควรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น
3. ผู้บริหาร ต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่จำกัดเฉพาะผู้ที่ได้รับอนุมัติเท่านั้น จึงจะสามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยมีอุปกรณ์รักษาความปลอดภัยเช่นการใช้ลายนิ้วมือในการสแกนผ่านการเข้าออก การล็อคกุญแจห้อง เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย
   - 3.1 จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” สำหรับการผ่านเข้าออกของผู้ดูแลระบบและเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ
   - 3.2 ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”
   - 3.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง
   - 3.4 จัดการสภาพแวดล้อมทางกายภาพภายในศูนย์คอมพิวเตอร์ รวมถึงอุปกรณ์รักษาความปลอดภัยต่างๆให้เหมาะสมได้แก่ ความสะอาด ความชื้น และอุณหภูมิของศูนย์คอมพิวเตอร์รวมถึงจัดให้มีอุปกรณ์เพื่อป้องกันและแจ้งเตือนภัยกรณีเกิดไฟไหม้เช่น อุปกรณ์ตรวจจับควันและความร้อนเพื่อลดผลกระทบที่ได้รับตลอดจนการรักษาความสะอาดภายในศูนย์คอมพิวเตอร์ให้สะอาดอยู่เสมอ ควรควบคุมการเข้าถึงศูนย์ข้อมูลโดยจัดทำทะเบียนบันทึกผู้เข้าเยี่ยมชมที่มีการลงนามและเหตุผลของการเข้าชม สำหรับบุคคลภายนอก รวมถึงผู้รับผิดชอบติดตามเข้าไปต้องทำการลงนาม และบันทึกระยะเวลาเยี่ยมชม และจัดให้ระบบการติดตาม เช่นมีกล้องวงจรปิดเพื่อใช้เป็นหลักฐานอ้างอิงที่ชัดเจน หากมีผู้บุกรุกเข้าศูนย์คอมพิวเตอร์โดยไม่ได้รับอนุญาต

<u>ส่วนที่ 7.1 การควบคุมการเข้าออก อาคาร สถานที่</u>

1. จัดทำเอกสารระบุสิทธิ์ของผู้ใช้ และ “บริษัทภายนอก” ในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้
   - 1.1 บริษัทต้องกำหนดสิทธิ์ ผู้ใช้ ที่มีสิทธิ์ผ่านเข้าออกและช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน
   - 1.2 การเข้าถึงอาคารของบริษัท ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น และทำการลงบันทึกข้อมูลบัตในสมุดบันทึก และรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)
   - 1.3 บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจน ตลอดเวลาที่อยู่ในบริษัท
   - 1.4 เจ้าหน้าที่ ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกได้

ถูกต้อง

1.5 บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และรปภ.ต้องตรวจสอบผู้ติดต่ออุปกรณ์พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

2.6 ผู้ใช้จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

2.7 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้ ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า บริษัทเจ้าของพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่บริษัทออกให้โดยบริษัทเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

<u>ส่วนที่ 7.2 การควบคุมการเข้าออกห้องศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (Data Center Entry Control)</u>

1. ผู้ดูแลระบบ ฝ่ายเทคโนโลยีสารสนเทศ และเจ้าหน้าที่บริษัท มีแนวทางปฏิบัติ ดังนี้

1.1 ผู้ดูแลระบบ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย(Server Zone) ส่วนเครื่องพิมพ์ (Printer Zone) เป็นต้น เพื่อสะดวกในกาปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

1.2 ฝ่ายเทคโนโลยีสารสนเทศ ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกฝ่ายเทคโนโลยีสารสนเทศโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

1.3 การเข้าถึงห้องคอมพิวเตอร์ Server ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” พร้อมโดยเหตุผลของการเข้าและระยะเวลาการเข้า รวมถึงผู้รับผิดชอบติดตาม

1.4 เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว

1.5 ผู้ติดต่อจากบริษัทภายนอก มีแนวทางปฏิบัติดังนี้

1.5.1 ผู้ติดต่อจากบริษัทภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

1.5.2 ผู้ติดต่อจากบริษัทภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในฝ่ายเทคโนโลยีสารสนเทศ

1.5.3 ผู้ติดต่อจากบริษัทภายนอก สามารถเข้าออกฝ่ายเทคโนโลยีสารสนเทศ ได้ด้วยบัตรผู้ติดต่อ “Visitor” โดยสิทธิ์จะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงานภายในฝ่ายเทคโนโลยีสารสนเทศ

1.6 พื้นที่ที่ผู้ติดต่อจากบริษัทภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้าออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

1.7 ผู้ติดต่อจากบริษัทภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้าออกว่ามีเจ้าหน้าที่ลงนาม

อนุญาตแล้วทุกครั้ง

ส่วนที่ 8 นโยบายความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

ส่วนที่ 8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

วัตถุประสงค์ เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

1. การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)
   - 1.1 ต้องจัดทำคู่มือ และ/หรือ ขั้นตอนการปฏิบัติงานสารสนเทศในบริษัท เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ (PM-IT-01) ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติและเจ้าหน้าที่หรือบริษัทผู้รับผิดชอบ
   - 1.2 คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนและผู้รับผิดชอบการปฏิบัติงานนั้น ๆ โดยคู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง
   - 1.3 มีการกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด
2. การจัดการการเปลี่ยนแปลง (Change Management)
   - 2.1 ต้องมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ทุกครั้งโดยปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การจัดการการเปลี่ยนแปลงสารสนเทศ (Change Management) (WI-IT-07)
   - 2.2 เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ เช่น ระบบปรับอากาศ น้ำ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ ฯลฯ เจ้าหน้าที่ต้องประสานงานหรือรายงานกับผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
   - 2.3 เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการในการร้องขอการเปลี่ยนแปลงทุกครั้ง
   - 2.4 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการประชุมเป็นประจำเพื่อตรวจสอบคำร้องขอการเปลี่ยนแปลง (Change Request) และพิจารณาตรวจสอบ การเปลี่ยนแปลงต่าง ๆ ให้เป็นที่พอใจและยอมรับได้
   - 2.5 ตาราง และ/หรือ แผนการเปลี่ยนแปลงทุกครั้งต้องได้รับความเห็นชอบจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อนจะทำการเปลี่ยนแปลง
   - 2.6 บันทึกการเปลี่ยนแปลงทุกครั้งจะต้องแจ้งให้บริษัทที่เกี่ยวข้องได้รับทราบโดยบันทึกฯ ต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
     - วันที่รับเรื่อง และวันที่ทำการเปลี่ยนแปลง
     - เจ้าของข้อมูล และผู้ดูแลระบบ
     - วิธีการเปลี่ยนแปลง
     - ผลของการเปลี่ยนแปลง (สำเร็จ หรือ ล้มเหลว)
3. การจัดการขีดความสามารถ (Capacity Management)
   - 3.1 ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันอย่างสม่าเสมอ ตามความเหมาะสมของทรัพยากรชนิดต่าง ๆ
   - 3.2 ต้องมีการวางแผนจัดการขีดความสามารถของระบบอย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากความต้องการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนาคต (อาทิ ความต้องการใน 1 ปี ที่จะถึง เช่น

CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น เป็นต้น) สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี

3.3 แผนการจัดการขีดความสามารถของระบบต้องประกอบด้วยวิธีการจัดการขีดความสามารถ อาทิการ Tuning การจัดหาเพิ่มเติม

3.4 การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบและสภาพแวดล้อมในการปฏิบัติงาน (Separation of Development, Testing and Operational Environment)

3.4.1 ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบออกจากกับเครื่องที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริงด้วย

<u>ส่วนที่ 8.2</u> การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์ เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

นโยบาย

1. การมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control against Malware)

1.1 เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง โดยปฏิบัติตามเอกสารวิธีการปฏิบัติงาน เรื่อง การจัดการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls against Malicious Code Procedure) (WI-IT-08)

1.2 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊คทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส

1.3 เอกสารการติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก 6 เดือน และต้องจัดทำเอกสาร Checklist ประกอบการตรวจสอบด้วย

1.4 ห้ามพนักงานทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต เว้นแต่กรณีถ้าต้องการใช้งานเป็นเฉพาะกรณี ต้องแจ้งมายังเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศให้ดำเนินการ

1.5 ไฟล์ทุกไฟล์ที่ดาวน์โหลดในฝ่ายเป็นไฟล์แนบของอีเมล์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส

1.6 ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใด ๆ ตัวอย่างเช่น ไวรัส หนอนอินเทอร์เน็ตโปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ของบริษัท

1.7 ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

1.8 ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้น ที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านระบบเครือข่ายของบริษัทได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จัก และจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสของบริษัทก่อนเปิดใช้งานเสมอ

1.9 เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชั่นการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

ส่วนที่ 8.3 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software)

วัตถุประสงค์ เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้องนโยบาย

1. การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

1.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

1.1.1 ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

ส่วนที่ 8.4 การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)

วัตถุประสงค์ เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

นโยบาย

1. การวางแผนการตรวจสอบระบบสารสนเทศทั้งหมด (Information System Audit Controls)

1.1 ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่ โดยปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การควบคุมระบบสารสนเทศที่ใช้ในการปฏิบัติงาน (Control of operational software) (WI-IT-10)

ส่วนที่ 8.5 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์ เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

นโยบาย

1. การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

1.1 ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

1.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

1.2.1 บริษัท ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่บริษัทจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

1.2.2 บริษัท ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่ตามคู่มือการปฏิบัติงาน เรื่อง การตรวจสอบการใช้ซอฟต์แวร์ที่ละเมิดสินทรัพย์ทางปัญญา (Monitoring of illegal Software Usage Procedure) (PM-IT-03)

1.2.3 ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท โดยเด็ดขาด

1.2.4 เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่บริษัท มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัท เพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตจาก ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และในขณะเดียวกัน เจ้าหน้าที่บริษัท ไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับการอนุญาต ทั้งนี้ เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

1.2.5 บริษัท กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง เพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าบริษัท มีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็น บริษัทอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

ส่วนที่ 8.6 การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)

วัตถุประสงค์ เพื่อให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงานของบริษัท

นโยบาย

1. การวางแผนการตรวจสอบระบบสารสนเทศทั้งหมด (Information System Audit Controls)
   1.1 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ต้องวางแผนการตรวจสอบระบบ โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของบริษัทน้อยที่สุด

ส่วนที่ 9 นโยบายความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

ส่วนที่ 9.1 การการจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

วัตถุประสงค์ เพื่อป้องกันข้อมูลในระบบเครือข่าย และปูองกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัท

1. การควบคุมการเข้าถึงเครือข่าย (Network Control)
   1.1 ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด
   1.2 การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในบริษัท ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย
   1.3 ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่บริษัทนั้นรับผิดชอบ
   1.4 ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้บริษัทอื่นๆ ที่เกี่ยวข้องทราบกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

1.5 บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทด้วย

2. การความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

2.1 ระบบเครือข่ายทั้งหมดของบริษัท ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

2.2 ต้องจำกัดจานวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของบริษัท ทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้บริษัทภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายบริษัทได้

2.3 ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัทโดยไม่ได้รับอนุญาตจากผู้บริหาร

2.4 ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัทโดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

2.5 ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่ายตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด

2.6 ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัท ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอกผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัท โดยเด็ดขาด

3. การจัดแบ่งเครือข่ายภายในบริษัท (Segregation in Network)

3.1 ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และ โซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

3.2 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ส่วนที่ 9.2 การถ่ายโอนข้อมูล (Information Transfer)

วัตถุประสงค์ เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในองค์กรและถ่ายโอนข้อมูลกับภายนอกบริษัท

1. นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures)

1.1 ต้องมีการจัดทำนโยบาย ขั้นตอนปฏิบัติ หรือมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการและมีการปฏิบัติตามเพื่อปูองกันสารสนเทศที่มีการถ่ายโอนกับบริษัทภายนอก

1.2 ต้องมีการดำเนินการแลกเปลี่ยนสารสนเทศ โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการแลกเปลี่ยนสารสนเทศ (Information Exchange Procedure) (P IT CO 04)

2. ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer)

2.1 ต้องมีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูล โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการแลกเปลี่ยนสารสนเทศ (Information Exchange Procedure) (P IT CO 04)

3. การรักษาความมั่นคงปลอดภัยการส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging)

3.1 ต้องมีการกำหนดวิธีการปูองกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

4. การรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreement)

4.1 ต้องมีการจัดทำข้อตกลง หรือสัญญาการรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) ซึ่งเป็นไปตามความต้องการด้านการปูองกันข้อมูลของบริษัท และมีการทบทวนอย่างสม่าเสมอ

4.2 พนักงาน บุคคล หรือผู้ติดต่อจากบริษัทอื่น ที่มีส่วนต้องเข้าถึงสารสนเทศของ บริษัท ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และ “ผู้ติดต่อ” ว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA)

<u>ส่วนที่ 10 นโยบายการจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquistion Development and aintenance)</u>

<u>ส่วนที่ 10.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements Of Information Systems)</u>

วัตถุประสงค์ เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะการควบคุมการเข้าถึงเครือข่าย (Network Control)

1. การกำหนดความต้องการด้านความมั่นคงปลอดภัย(Information Security Requirements Analysis and Specification) ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน

1.1 ฝ่ายเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

-มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย เช่น การสำรองข้อมูล ระบบเครือข่ายสำรอง เป็นต้น

- มาตรการปฏิบัติหลังจากเกิดความเสียหาย เช่น แผนการกู้คืนข้อมู ระยะเวลาในการกู้คืนข้อมูล

1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

1.2.1 สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับการป้องกันและการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

1.3.1 สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการปูองกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

<u>ส่วนที่ 10.2 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)</u>

วัตถุประสงค์ เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ (development lifecycle)

นโยบาย

1. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

1.1 ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามนโยบายหรือข้อกำหนดที่องค์กรกำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคานึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนาตรวจพบช่วงโหว่ และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้

1.2 กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

1.2.1 ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น

- คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์
- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
- ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

โดยปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การจัดการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Work Instruction) (WI-IT-07)

1.3 การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications after Operating Platform Changes)

1.3.1 เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบซอฟต์แวร์ต่าง ๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

1.4 การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สาเร็จรูป (Restrictions on Changes to Software Packages)

1.4.1 เมื่อมีการใช้งานซอฟต์แวร์สาเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนามาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

1.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

1.5.1 เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบ ต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ

1.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

1.6.1 บริษัท ต้องมีการจัดทำหรือปูองกันสภาพแวดล้อมในการทำงานต่าง ๆ ให้มีความเหมาะสมและปลอดภัย ทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

1.7 การจ้างบริษัทภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development)

1.7.1 ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัท ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

1.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

1.8.1 โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา

1.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

1.9.1 มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่ และระบบที่ปรับปรุง

1.9.2 ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และให้มีการเซ็นชื่อเจ้าหน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ โดยปฏิบัติตามเอกสารวิธีการปฏิบัติงาน เรื่อง การจัดการการยอมรับระบบ (System Acceptance) (WI-IT07)

ส่วนที่ 10.3 ข้อมูลสำหรับการทดสอบ (Test Data)

วัตถุประสงค์ เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

นโยบาย

1. การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

1.1 ข้อมูลจริงที่จะนาไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นาข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และฝ่ายที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

ส่วนที่ 11 การบริหารจัดการผู้ให้บริการภายนอก (Third Party Manament)

ส่วนที่ 11.1 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Outsourec Access Control)

วัตถุประสงค์ เพื่อให้มีการป้องกันสินทรัพย์ขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

นโยบาย

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน ให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก ควรประกอบด้วย

1. บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย
2. หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหน่วยงาน หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ
3. สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงาน ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล(Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
4. ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และ

เอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

แนวปฏิบัติ

1. ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร
2. หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรจะต้อง ทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากประธานเจ้าหน้าที่บริหารสายสนับสนุน
3. จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้
   - เหตุผลในการขอใช้
   - ระยะเวลาในการใช้
   - การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
   - การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
   - กำหนดข้อตกลงการใช้งานข้อมูล เพื่อเป็นการป้องกันการเปิดเผยข้อมูล
4. หน่วยงานภายนอก ที่ทำงานให้กับหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ
5. หน่วยงานภายนอก ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล
6. สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้านคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity)และการรักษาความพร้อมที่จะให้บริการ (Availability)
7. องค์กรมีสิทธิในการตรวจสอบตามสัญญา หรือข้อตกลงการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น
8. ต้องกำหนดให้หน่วยงานภายนอก หรือผู้ให้บริการจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของหน่วยงานภายนอก หรือผู้ให้บริการ เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดหรือตกลงไว้

<u>ส่วนที่ 11.2</u> ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

วัตถุประสงค์ เพื่อให้มีการป้องกันสินทรัพย์ขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

นโยบาย

1. นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

   1.1 บริษัทจะต้องกำหนดให้มีการจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างบริษัทกับผู้ให้บริการภายนอก และต้องจัดทำเป็นลายลักษณ์อักษร โดยปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การให้บริการของบริษัทภายนอก (Third Party Service Delivery Management) (W IT CO 01)

1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing security within supplier agreements)

1.2.1 เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ต้องระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่างบริษัทกับผู้ให้บริการภายนอก ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การให้บริการของบริษัทภายนอก (Third Party Service Delivery Management) (W IT CO 01) เมื่อมีความจำเป็นต้องให้ผู้ให้บริการภายนอกนั้น เข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศของบริษัท และก่อนที่จะอนุญาตให้สามารถเข้าถึงได้ ผู้ให้บริการภายนอกต้องปฏิบัติตามวิธีการปฏิบัติงาน เรื่องการลงทะเบียนใช้งานระบบสารสนเทศ (W IT AC 02)

1.3 ห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

1.3.1 ข้อตกลงกับผู้ให้บริการภายนอก ต้องรวมถึงความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร โดยผู้ให้บริการภายนอกต้องปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การให้บริการของบริษัทภายนอก (Third Party Service Delivery Management)

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายในการควบคุมดูแลผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศของผู้ประกอบธุรกิจอย่างไม่เหมาะสม ทั้งนี้ นโยบาย ดังกล่าวต้องมีเนื้อหาขั้นต่ าครอบคลุมประเด็นดังต่อไปนี้
   (1) กำหนดข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและกระบวนการควบคุม อย่างเป็นลายลักษณ์อักษร และมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและผู้ให้บริการภายนอก
   (2) กำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอก
   (3) ระบุประเภทข้อมูลสารสนเทศที่อนุญาตให้ผู้บริการภายนอกเข้าถึง เพื่อให้การกำหนดมาตรการ ควบคุมและติดตามการเข้าถึงข้อมูลเป็นไปอย่างเหมาะสม ภายใต้หลักความจ าเป็นในการรู้ข้อมูล (need-to-know basis)
   (4) จัดให้มีขั้นตอนและกระบวนการติดตามควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม
   (5) มีการควบคุมความครบถ้วนถูกต้องของข้อมูลและการประมวลผลข้อมูลที่ได้รับจาก ผู้ให้บริการภายนอก
   (6) กำหนดกระบวนการควบคุมอย่างเป็นมาตรฐานเพื่อติดตามการท างานของผู้ให้บริการภายนอก
   (7) ผู้ให้บริการภายนอกต้องกำหนดแผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคง ปลอดภัยของระบบสารสนเทศ (incident response policy) ให้สอดคล้องกับแผนของผู้ประกอบธุรกิจ รวมทั้งกำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการกู้คืนระบบงานให้เป็นไปตาม ข้อตกลงที่ได้กำหนดไว้ เพื่อให้ข้อมูลและการประมวลผลข้อมูลอยู่ในสภาพที่พร้อมใช้งานเสมอ
   (8) มีการจัดอบรมให้กับบุคคลที่เกี่ยวข้องกับการจัดหาผู้ให้บริการภายนอก เพื่อให้ทราบถึงนโยบาย ขั้นตอน และกระบวนการ
   (9) มีการรักษาความมั่นคงปลอดภัยในกรณีที่มีการเคลื่อนย้ายหรือถ่ายโอนข้อมูลสารสนเทศ 32
2. ข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องมีเนื้อหาขั้นต่ าดังนี้
   (1) รายละเอียดของข้อมูลที่จำเป็นต้องใช้หรือเข้าถึงโดยผู้ให้บริการภายนอกรวมทั้งวิธีการเข้าถึงข้อมูล ดังกล่าว

(2) การจัดแบ่งประเภทข้อมูลโดยต้องสอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัย ของระบบสารสนเทศ

(3) มีมาตรการดำเนินการเพื่อให้มั่นใจได้ว่าข้อมูลที่เป็นความลับหรือมีความสำคัญ ทรัพย์สินทางปัญญา และลิขสิทธิ์ของผู้ประกอบธุรกิจได้รับการคุ้มครองอย่างปลอดภัยตามกฎหมายและหลักเกณฑ์ ของทางการที่เกี่ยวข้อง

(4) กำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการปฏิบัติงานภายใต้การควบคุมต่าง ๆ เช่น กำ หนดเงื่อนไขการเข้าถึงข้อมูลของผู้ใช้บริการ ติดตามตรวจสอบการปฏิบัติงานของ ผู้ให้บริการภายนอกให้เป็นไปตามข้อตกลงของผู้ใช้บริการกำหนดให้ผู้ให้บริการภายนอกรายงาน ผลการปฏิบัติงานให้ผู้ใช้บริการทราบเมื่อร้องขอการแก้ไขปัญหาต่าง ๆ ภายในระยะเวลาที่กำหนด รวมทั้งการปฏิบัติงานให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบ สารสนเทศของผู้ใช้บริการ

(5) แนวทางการใช้งานข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม

(6) แนวทางการแก้ไขปัญหากรณีที่เกิดข้อผิดพลาดจากการปฏิบัติหน้าที่

(7) แผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy)

(8) รายชื่อและช่องทางสำหรับติดต่อบุคคลหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งบุคคล หรือหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(9) สิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้ให้บริการภายนอก รวมทั้งควบคุมให้มี การปฏิบัติงานเป็นไปตามข้อตกลงที่ได้กำหนดไว้ทั้งนี้ ในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจ ในต่างประเทศและมีข้อจากัดในการเข้าตรวจสอบการปฏิบัติงานดังกล่าวผู้ประกอบธุรกิจควรมี มาตรการเพื่อให้มั่นใจได้ว่ามีการควบคุมผู้ให้บริการภายนอกให้ปฏิบัติงานเป็นไปตามข้อตกลง ที่ได้กำหนดไว้อย่างเหมาะสม

(10) ข้อกำหนดเพิ่มเติมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีที่ผู้ให้บริการ ภายนอกมอบหมายการปฏิบัติงานให้กับบุคคลอื่นต่อ(sub-contracting to another supplier)

<u>ส่วนที่ 12</u> การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารเทศ (IT Outsourcing Policy)

วัตถุประสงค์ เพื่อให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing Policy) และเพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องได้แก่ ผู้ให้บริการภายนอก บุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของบริษัท รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

แนวปฏิบัติ

1. การจัดจ้างผู้ให้บริการภายนอกเพื่อเข้ามาดำเนินงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดและตกลงเกี่ยวกับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอกไว้ในเอกสารจัดจ้างหรือสัญญา เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินของบริษัทฯโดยผู้ให้บริการภายนอก
2. มีการระบุความเสี่ยงอันเกิดจากการจ้างช่วงและการสื่อสารโดยผู้ให้บริการภายนอก เช่น การจ้างช่วงต้องมีการแจ้งให้บริษัทฯ ได้รับทราบหากผู้รับจ้างมีการดำเนินการในลักษณะดังกล่าวอย่างเป็นลายลักษณ์อักษรและระบุในสัญญาเกี่ยวกับความรับผิดชอบต่อความเสี่ยงที่เกิดขึ้นจากการจ้างช่วง
3. กำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกให้

สอดคล้องกับระยะเวลาในการจ้างผู้ให้บริการภายนอกรายนั้นๆ ซึ่งการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอกเพื่อทำให้มั่นใจว่าผู้ให้บริการภายนอกยังคงปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศและเงื่อนไขที่ได้ระบุไว้ในข้อตกลง

4. การเปลี่ยนแปลงที่เกี่ยวข้องกับบริการที่ได้รับจากผู้ให้บริการภายนอกทั้งในส่วนที่ร้องขอการเปลี่ยนแปลงโดยบริษัทฯ เองและส่วนที่ร้องขอการเปลี่ยนแปลงโดยผู้ให้บริการภายนอก

ส่วนที่ 13 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

ส่วนที่ 13.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์ เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัท ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

นโยบาย

1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

1.1 แผนกเทคโนโลยีสารสนเทศ กำหนดการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของฝ่ายและขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

2. การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)

2.1 ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ โดยผ่านช่องทางรายงานที่กำหนดไว้ และเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ โดยปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management Procedure) (W IT IM 01)

2.2 ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในบริษัทฯ ต่อผู้บังคับบัญชาหรือฝ่ายจัดการความปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที

2.3 ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ (บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ) ทันที

2.4 ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อ เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ เพื่อบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศทันที

2.5 ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในบริษัทฯ ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา แผนกเทคโนโลยีสารสนเทศ ผู้บริหารและห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้น ด้วยตนเอง

2.6 การกระทำอื่น ๆ ที่ถือเป็นข้อห้ามของบริษัทฯ มีดังนี้

2.6.1 การกระทำใดๆ ที่กฎหมายบัญญัติว่าเป็นความผิด ตลอดจนการกระทำในลักษณะอื่นๆ ที่กล่าวถึงด้านล่างนี้ ถือเป็นข้อห้ามของบริษัทฯ ไม่ยินยอมให้พนักงานดำเนินการโดยเด็ดขาด ทั้งนี้ บริษัทฯ มิได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้ แต่เขียนเพื่อเป็นแนวทางให้แก่ผู้ใช้งานได้รับทราบเท่านั้น

หมายเหตุ: เจ้าหน้าที่บางส่วนอาจได้รับยกเว้นจากข้อห้ามบางข้อที่กล่าวไว้ด้านล่างนี้ (ตราบเท่าที่ไม่ขัดต่อกฎหมาย) หากเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับการเข้าถึงระบบเครือข่ายของอุปกรณ์ใด ๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศ

2.6.2 การใช้งานทรัพยากรของ บริษัท ฯ เพื่อการจัดหาหรือส่งต่อ วัสดุ เอกสาร หรือรูปภาพลามกอนาจาร หรือที่ขัดต่อกฎหมาย

2.6.3 การฉ้อโกงโดยใช้ User ID และรหัสผ่านที่บริษัท ฯ กำหนดให้ เพื่อเสนอขายสินค้าหรือบริการใด ๆ

2.6.4 การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่ายตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย ได้แก่ การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย ได้แก่ Sniffing, Pinged Floods, Pack Spoofing, Denial of Service และ Forged Routing Information ด้วยเจตนามุ่งร้าย เป็นต้น

2.6.5 การใช้งาน Bandwidth จำนวนมากโดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P File Sharing

2.6.7 การทำPort Scanning และ Security Scanning เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย

2.6.7 การดักฟังหรือดักจับข้อมูลที่พนักงานไม่ได้รับอนุญาตให้รับรู้ด้วยวิธีการใด ๆ เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย

2.6.8 การค้นหาจุดบกพร่องของระบบ เพื่อทำการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

2.6.9 การหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ระบบเครือข่ายใด ๆ

2.6.7 การใช้โปรแกรม/สคริปต์/คำสั่ง หรือการส่งข้อความใด ๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบภายใน หรือผ่านระบบเครือข่ายต่าง ๆ

2.6.8 การให้ข้อมูลลับเกี่ยวกับรายชื่อพนักงาน รายชื่อลูกค้า ความลับของบริษัทฯ และข้อมูลลับอื่น ๆ แก่บุคคลภายนอก

2.6.9 การข่มขู่คุกคามทุกรูปแบบผ่านอีเมล์ โทรศัพท์ หรือระบบส่งข้อความ ไม่ว่าจะด้วยภาษาความถี่หรือขนาดของข้อความการแสดงความคิดเห็น หรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจานวนมาก (Newsgroup Spam)

2.6.10 การละเมิดสิทธิ์ส่วนบุคคล ลิขสิทธิ์ของบริษัทฯ ความลับของบริษัทฯ สิทธิบัตร ทรัพย์สินทางปัญญา หรือกฎหมายอื่นใด

1.3 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

1.3.1 เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ ที่สังเกตุพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

1.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

1.4.1 สถานการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องมีการประเมินและต้องมีการตัดสินว่าสถานการณ์นั้นถือเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

1.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

1.5.1 แผนกเทคโนโลยีสารสนเทศ ต้องมีการกำหนดขั้นตอนไว้รองรับกรณีเกิดเหตุการณ์ที่ประเมินแล้วว่าก่อให้เกิดความไม่มั่นคงปลอดภัย

1.5.2 เมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

1.6 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from Information Security Incidents)

1.6.1 เจ้าหน้าที่แผนเทคโนโลยี ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ปริมาณที่เกิดขึ้นและค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้วและเตรียมการปูองกันที่จำเป็นไว้ล่วงหน้า

1.7 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

1.7.1 เจ้าหน้าที่แผนกเทคโนโลยี ต้องรวบรวมและจัดเก็บหลักฐานตามกฎ หรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

แนวปฏิบัติ

1. กำหนดให้มีขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถและประสบการณ์ โดยขั้นต่ำต้องมีการกำหนดขั้นตอนและกระบวนการดังต่อไปนี้

1.1 การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

1.2 การประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

1.3 จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (point of contacl) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป (escalation)

1.4 การคำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่กิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติอย่างรวดเร็ว

1.5 การรวบรวมและจัดเก็บหลักฐานทันทีที่เกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญอย่างมีนัยสำคัญ เช่น ก่อให้เกิดความเสียหายกับข้อมูลหรือทรัพย์สินของลูกค้าโดยคำนึงถึงประเด็นสำคัญต่าง ๆ เช่น มีกระบวนการการจัดเก็บอย่างมั่นคงปลอดภัย การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง การคัดเลือกบุคคลที่มีความรู้ความสามารถหรือมีประสบการณ์ค้านการรวบรวมและจัดเก็บหลักฐาน เพื่อวิเคราะห์ตรวจสอบและ จัดทำเอกสารสรุปนำเสนอต่อบุคคลที่มีหน้าที่รับผิดชอบ เป็นต้น ทั้งนี้ การรวบรวม จัดเก็บและนำเสนอหลักฐานต้องสอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

1.6 การบันทึกและจัดเก็บหลักฐานการบริหารจัดการทุกขั้นตอน

1.7 การตรวจหา ติดตาม วิเคราะห์ และรายงานเหตุการณ์ ทั้งนี้ ให้รวมถึงการวิเคราะห์ภายหลังเหตุการณ์ยุติแล้ว เพื่อระบุถึงสาเหตุของเหตุการณ์และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

2. ผู้ประกอบธุรกิจต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคล หรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์โดยให้ดำเนินการดังนี้

2.1 จัดทำแบบฟอร์มที่เป็นมาตรฐานเพื่อรองรับการรายงานสถานการณ์ และสร้างความเข้าใจให้กับผู้รายงานเกี่ยวกับการดำเนินการต่าง ๆ ที่จำเป็นในกรณีที่เกิดเหตุการณ์ ทั้งนี้ เนื้อหาขั้นต่ำต้องประกอบด้วย วันเวลาเหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไข ผลการแก้ไขระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต

2.2 รายงานคณะผู้บริหารขององค์กรเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยเช่น พบช่องโหว่ในการควบคุมความมั่นคงปลอดภัย (inelfective sccuriy control) เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrily)และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศ ข้อผิดพลาดจากการปฏิบัติงาน(human errors) การบุกรุกด้านกายภาพ (breaches of physical security arrangements) การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (non-complianceswith policies) การเปลี่ยนแปลงระบบปฏิบัติการหรือชุดคำสั่งที่ควบคุมระบบงาน โดยไม่ได้รับอนุญาต (uncontrolled system changes) การทำงานผิดพลาดของโปรแกรมและอุปกรณ์คอมพิวเตอร์(malfunctions of software or hardware) และการเข้าถึงโดยไม่ได้รับอนุญาต (access violations)

2.3 รายงานสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญ ประเภทดังต่อไปนี้

(ก) ระบบหยุดชะงัก (system disruption)

(ข) มีการบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)

(ค) ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (har to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacemen!)โดยให้รายงาน ดังนี้

- รายงานทันทีเมื่อทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์และผลกระทบ ที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ตามความเหมาะสม
- รายงานภายในวันทำการถัดไปหลังทราบเหตุการณ์ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การคำเนินการแก้ไขปัญหาและความคืบหน้าในการแก้ไขปัญหา
- รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเกทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การคำเนินการแก้ไขปัญหาผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต

2.4 แจ้งบุคคลที่กี่ยวข้อง เช่น ลูกค้า ผู้มีส่วนได้ส่วนเสีย รับทราบโดยไม่ชักช้าในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคลดังกล่าว

2.5 จัดให้มีรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการเป็นระยะ และเมื่อเหตุการณ์ยุติแล้ว

ส่วนที่ 14 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของฝ่าย (Compliance)

ส่วนที่ 14.1 การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์: เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่างๆ

นโยบาย

1. การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

1.1 บริษัทฯ ต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของฝ่าย

1.2 เจ้าหน้าที่บริษัทฯ เจ้าหน้าที่บริษัทฯ ทุกคนต้องรับทราบ ทาความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการตรวจสอบกับกฎหมาย IT (W IT CL 02) และมีรายการดังต่อไปนี้เป็นอย่างน้อย

- นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทาธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
- พ.ร.บ. ลิขสิทธิ์

1.3 ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทฯ ถือเป็นสินทรัพย์ของบริษัทฯ (ยกเว้น ข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธ์ของบุคคลภายนอก) ทั้งนี้ บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

1.4 เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของบริษัทกำหนดไว้

1.5 บริษัทฯ ขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตามบริษัทฯ จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใด ๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาลตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

1.6 ห้ามเจ้าหน้าที่บริษัทใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

1.7 การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศ ไม่ขัดต่อข้อกฎหมายใด ๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

2. สินทรัพย์ทางปัญญา (Intellectual Property Rights)

2.1 บริษัทต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่ฝ่ายจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด

2.2 บริษัทต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แว ร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไ ม่ ตามคู่มือการปฏิบัติงาน เรื่อง การตรวจสอบการใช้ซอฟต์แวร์ที่ละเมิดสินทรัพย์ทางปัญญา (Monitoring of illegal Software Usage Procedure) (P IT CL 01)

2.3 ห้ามผู้ใช้งานดำเนินการทำซ้ำ หรือเผยแพร่รูปภาพบท เพลง บทความหนังสือหรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัทโดยเด็ดขาด

2.4 เพื่อที่จะให้เกิดความแน่ใจว่า เจ้าหน้าที่บริษัทมิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัท เพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตจาก ISMR และในขณะเดียวกัน เจ้าหน้าที่บริษัทไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับการอนุญาต ทั้งนี้ เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

2.5 บริษัทกำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 2 ครั้ง เพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าบริษัทมีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็น บริษัทอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

3. การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

3.1 บริษัทต้องจัดเก็บข้อมูล เพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อ - กำหนดทางด้านกฎระเบียบหรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล

4. ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

4.1 บริษัทต้องมีการการปูองกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ สัญญาที่เกี่ยวกับบริษัท

5. การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

5.1 บริษัทต้องมีการควบคุมการเข้ารหัสข้อมูลตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

<u>ส่วนที่ 14.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)</u>

วัตถุประสงค์: เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่างๆ

นโยบาย

1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

1.1 IST ต้องมีการทบทวน วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติขององค์กร เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย วิธีปฏิบัติงานต่าง ๆ ให้ถูกต้องและเป็นปัจจุบันตามรอบระยะเวลาที่กำหนด เช่น ปีละ 1 ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

2 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของฝ่าย (Compliance with Security Policy and Standards)

2.1 IST ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของฝ่ายตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้

2.2 IST ต้องมีการตรวจสอบและทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

3 การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

3.1 IST ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

การทบทวนนโยบาย

หากไม่มีการเปลี่ยนแปลงทบทวนทุก 3 ปี