การอนุมัติเอกสาร

ประวัติการเปลี่ยนแปลง :

ครั้งที่	วันที่	รายละเอียด	แก้ไขโดย
1	5 เมษายน 2559	ฉบับเริ่มต้น	ธัชกร สุวรรณคล้าย
2	15 มีนาคม 2560	ปรับปรุงรูปแบบตามมาตรฐาน ISO	สุภารัตน์ งามทรัพย์ทวีคูณ
3	5 ตุลาคม 2564	แก้ไข/เพิ่มเติม 4.3 การควบคุมของระบบฐานข้อมูล	ธัชกร สุวรรณคล้าย
4.	15 กรกฎาคม 2567	แก้ไข/เพิ่มเติม 4.2 การควบคุมการกำหนดสิทธิและบัญชีรายชื่อผู้ใช้งาน	ธัชกร สุวรรณคล้าย

การลงนาม :

ผู้จัดทำ	ผู้ตรวจทาน	ผู้อนุมัติ
ธัชกร สุวรรณคล้าย	สุภารัตน์ งามทรัพย์ทวีคูณ	บุญ ชุน เกียรติ
VP Information Technology	SVP Legal and Compliance	Managing Director
15 กรกฎาคม 2567	15 กรกฎาคม 2567	15 กรกฎาคม 2567

สารบัญ

1. วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

บริษัทฯ ได้ตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติของพนักงานในองค์กร เพื่อให้พนักงานมีความตระหนักถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศของบริษัท และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา รวมทั้งเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัท ด้านอื่นๆ ที่มุ่งเน้นการปฏิบัติงานภายในบริษัทให้มีความมั่นคงปลอดภัยในการดำเนินกิจการของบริษัท

2. ความมั่นคงปลอดภัยสำหรับสารสนเทศ และแนวทางในการรักษาความปลอดภัย

ความมั่นคงปลอดภัยสำหรับสารสนเทศ หมายถึง การสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศเพื่อป้องกันความเสียหายที่มีต่อองค์ประกอบทางด้านความมั่นคงปลอดภัย 3 ส่วน ดังนี้

1. Confidentiality ทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงได้โดยบุคคลที่ได้รับอนุญาตแล้วเท่านั้น

2. Integrity ทรัพย์สินสารสนเทศจะต้องมีความถูกต้องและสมบูรณ์

3. Availability ทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงได้เมื่อมีความจำเป็นที่ต้องใช้งาน

บริษัทจะต้องกำหนดมาตรการเพื่อรักษาความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศโดยบริษัทจะใช้แนวทาง ดังนี้ ในการรักษาความมั่นคงปลอดภัย

- **นโยบายความมั่นคงปลอดภัย** (Security Policy) ซึ่งจะประกอบด้วยระเบียบปฏิบัติต่าง ๆ ที่พนักงานต้องปฏิบัติตามโดยเคร่งครัด
- **ขั้นตอนปฏิบัติ** (Procedure) ระเบียบปฏิบัติบางข้ออาจจะมีการอ้างอิงถึงการปฏิบัติงานที่เกี่ยวข้อง เช่น ระเบียบปฏิบัติของการใช้ข้อมูลอ้างอิงถึง ขั้นตอนปฏิบัติสำหรับความมั่นคงปลอดภัยของข้อมูลข่าวสาร

3. ขอบเขตของการสร้างความมั่นคงปลอดภัย

เอกสารฉบับนี้มีขอบเขตคลอบคลุมถึงการสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศต่าง ๆ ของบริษัท ดังนี้

- พนักงานและลูกจ้างของบริษัททั้งหมด
- ข้อมูล /สารสนเทศของบริษัท
- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต่าง ๆ ขององค์กร
- เครื่องคอมพิวเตอร์ส่วนบุคคล
- เครื่องคอมพิวเตอร์แบบพกพา
- อุปกรณ์เครือข่าย
- ระบบไฟฟ้าสำรอง
- สายสัญญาณเครือข่าย
- ซอฟท์แวร์ระบบ ซอฟท์แวร์จ้างพัฒนา ซอฟท์แวร์พัฒนาเอง ซอฟท์แวร์สำเร็จรูป
- สื่อบันทึกข้อมูล
- เอกสารของบริษัท

4. นโยบายความมั่นคงปลอดภัย

นโยบายด้านความมั่นคงปลอดภัยครอบคลุมนโยบาย 8 ด้าน ดังนี้

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
4. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
5. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
6. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
7. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

สาระสำคัญของนโยบาย

1) นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ เพื่อจัดทำนโยบายให้สามารถรองรับความเสี่ยงที่เกิดขึ้นได้ รวมทั้งการประกาศใช้นโยบายให้แก่บุคคลกรที่เกี่ยวข้องได้ตระหนักและปฏิบัติตามนโยบายความปลอดภัยของด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

2) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องจัดให้มีการแบ่งแยกหน้าที่การปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์อย่างเพียงพอ เพื่อช่วยให้มีการสอบยันการปฏิบัติงานและมีการอนุมัติการปฏิบัติงานอย่างเพียงพอและเหมาะสม รวมทั้งการมีขอบเขตการปฏิบัติงานของพนักงานที่ชัดเจนและมีบุคลากรที่เพียงพอต่อการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ

3) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) ซึ่งมีสาระสำคัญดังนี้

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ศูนย์คอมพิวเตอร์ และความเสี่ยงหายอันจะเกิดจากอุปกรณ์หรือหรือระบบต่าง ๆ เช่น ระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ซึ่งย่อมมีความเสี่ยงต้องอุปกรณ์และข้อมูลของบริษัท ดังนั้นบริษัทต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงศูนย์คอมพิวเตอร์ได้ และการเข้าถึงดังกล่าวต้องมีการอนุมัติอย่างเพียงพอ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้มีระบบป้องกันความเสียหายที่อาจจะเกิดขึ้น เช่นการป้องกันไฟไหม้ หรือไฟฟ้าขัดข้อง

4) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องควบคุมความปลอดภัยของข้อมูลเพื่อป้องกันความเสี่ยงจากการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลของบริษัท ตั้งแต่ระดับข้อมูลข่าวสารทั่วไป จนถึงระดับข้อมูลข่าวสารที่ลับที่สุด และควรจะมีหน่วยงานที่มีหน้าที่ควบคุมหรืออนุมัติการที่จะเผยแพร่ข้อมูลข่าวสารให้กับหน่วยงานอื่นๆ หรือนำข้อมูลออกไปเผยแพร่ภายนอกองค์การ ซึ่งอาจส่งผลให้เกิดข้อมูลถูกทำลายหรือนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต ดังนั้นการกำหนดนโยบายการ

รักษาความปลอดภัยของข้อมูลระบบคอมพิวเตอร์ และระบบเครือข่ายรวมทั้งวิธีการปฏิบัติงานอย่างเพียงพอจะช่วยป้องกันความเสี่ยงที่จะเกิดขึ้นได้

5) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management) ซึ่งมีสาระสำคัญดังนี้

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ เพื่อสร้างความมั่นใจว่าการซื้อหรือการพัฒนามีความสอดคล้องกับแผนงานของบริษัท มีหลักเกณฑ์ในการคัดเลือก พัฒนา มีการจัดลำดับความสำคัญของงาน รวมทั้งกระบวนการพัฒนาได้มีการทดสอบอย่างเพียงพอว่าระบบงานที่แก้ไขเปลี่ยนแปลงมีความถูกต้องและให้ผลลัพธ์ตามที่ได้กำหนดไว้

6) การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) **ซึ่งมีสาระสำคัญดังนี้**

บริษัท ต้องกำหนดวิธีการปฏิบัติในกรณีที่เกิดเหตุการณ์ฉุกเฉินในกรณีต่าง ๆ และกำหนดหน้าที่รับผิดชอบของตัวบุคคล พร้อมทั้งมีการซักซ้อมเป็นระยะ เพื่อให้เกิดผลกระทบต่อการบริการของบริษัทแก่ลูกค้าให้น้อยที่สุด และเพื่อให้การดำเนินการของบริษัท ยังสามารถดำเนินต่อได้โดยไม่ติดขัด

7) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องกำหนดวิธีการปฏิบัติงานประจำด้านคอมพิวเตอร์ไว้เป็นลายลักษณ์อักษร เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ และควรมีการจัดทำบันทึกผลการปฏิบัติงานไว้เพื่อให้สามารถตรวจสอบได้ว่ามีการจัดทำอย่างครบถ้วนและเป็นไปตามวิธีการปฏิบัติงานที่กำหนดไว้

8) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ซึ่งมีสาระสำคัญดังนี้

การกำหนดนโยบาย ระเบียบปฏิบัติ มาตรฐานและแนวทางในการคัดเลือกผู้ให้บริการภายนอกจะช่วยให้การตัดสินใจที่จะได้รับประสิทธิผลที่ดีขึ้น ซึ่งจะส่งผลต่อค่าใช้จ่ายที่เหมาะสมในการเลือกใช้บริการ และผลของการให้บริการเป็นไปตามที่คาดหวังไว้

5. ระเบียบปฏิบัติ

นโยบายแต่ละด้านจะประกอบไปด้วยระเบียบปฏิบัติที่พนักงานหรือผู้ที่เกี่ยวข้องต้องปฏิบัติตามโดยเคร่งครัดดังต่อไปนี้

1) นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ความสำคัญ

บริษัทต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ เพื่อจัดทำนโยบายให้สามารถรองรับความเสี่ยงที่เกิดขึ้นได้ รวมทั้งการประกาศใช้นโยบายให้แก่บุคคลกรที่เกี่ยวข้องได้ตระหนักและปฏิบัติตามนโยบายความปลอดภัยของด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

ผู้รับผิดชอบหลัก

ผู้บริหารระดับสูง

ผู้บริหารระดับผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. จัดให้มีการทำนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศและมีการปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือตามความจำเป็นต่อการใช้งาน และนโยบายดังกล่าวได้รับการอนุมัติจากคณะกรรมการบริษัทหรือผู้มีอำนาจที่ได้รับมอบหมายไว้
2. จัดทำนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้ง่าย
3. จัดให้มีการสร้างความตระหนักที่เกี่ยวข้องกับภัยคุกคามทางอินเทอร์เน็ตใหม่ ๆ เพื่อให้พนักงานขององค์กร มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ในระดับหนึ่งอย่างน้อยปีละ 1 ครั้ง
4. จัดให้มีการทำรายงานสรุปปัญหาและแนวทางแก้ไขที่มีระดับความสำคัญสูง เช่น ปัญหาการใช้เครือข่าย การติดไวรัส โครงการพัฒนาระบบงาน ปัญหาจากผู้ใช้งานและเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ และปัญหาอื่นๆ ที่เกี่ยวข้อง โดยประมาณเดือนละ 1 ครั้งหรือตามความเหมาะสม
5. จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศขององค์กร ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุงความเสี่ยงหรือปัญหาที่พบ
6. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยปีละ 1 ครั้งและจัดให้มีการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ

7. จัดให้มีการวางแผนกลยุทธ์ด้านสารสนเทศเพื่อให้สอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัท ทั้งแผนระยะสั้นและแผนระยะยาว

2) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

วัตถุประสงค์

การแบ่งแยกอำนาจหน้าที่มีวัตถุประสงค์เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์ ซึ่งเป็นการลดความเสี่ยงด้าน infrastructure risk

ความสำคัญ

บริษัทต้องจัดให้มีการแบ่งแยกหน้าที่การปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์อย่างเพียงพอ เพื่อช่วยให้มีการสอบยันการปฏิบัติงานและมีการอนุมัติการปฏิบัติงานอย่างเพียงพอและเหมาะสม รวมทั้งการมีขอบเขตการปฏิบัติงานของพนักงานที่ชัดเจนและมีบุคลากรที่เพียงพอต่อการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบหลัก

ผู้บริหารระดับผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. จัดให้มีการแบ่งแยกหน้าที่ของบุคลากรในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System administrator) ซึ่งปฏิบัติงานอยู่บนส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง
2. ต้องจัดให้มีใบกำหนดหน้าที่งานของแต่ละตำแหน่งงานไว้อย่างชัดเจน ซึ่งตำแหน่งงานที่กำหนดไว้เป็นไปตามหลักการแบ่งแยกหน้าที่งานตามข้อที่ 1 และพนักงานได้รับทราบถึงขอบเขตและหน้าที่การปฏิบัติงานของตนตามที่ได้กำหนดไว้
3. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่พอเพียง ต่อการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับในแต่ละปีงบประมาณ
4. จัดให้มีการอบรมเพิ่มพูนความรู้ความสามารถของพนักงานฝ่ายเทคโนโลยีสารสนเทศให้เหมาะสม รวมทั้งจัดให้มีการเก็บข้อมูลการฝึกอบรมเหล่านั้น และจัดให้มีการประเมินผลการอบรม

3) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk) ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk)

ความสำคัญ

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ศูนย์คอมพิวเตอร์ และความเสี่ยงหายอันจะเกิดจากอุปกรณ์หรือหรือระบบต่าง ๆ เช่น ระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ซึ่งย่อมมีความเสี่ยงต้องอุปกรณ์และข้อมูลของบริษัท ดังนั้นบริษัทต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงศูนย์คอมพิวเตอร์ได้ และการเข้าถึงดังกล่าวต้องมีการอนุมัติอย่างเพียงพอ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้มีระบบป้องกันความเสียหายที่อาจจะเกิดขึ้น เช่นการป้องกันไฟไหม้ หรือไฟฟ้าขัดข้อง

ผู้รับผิดชอบหลัก

พนักงานของส่วนสนับสนุนเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. จัดให้มีการประเมินความเสี่ยงทางกายภาพของพื้นที่จัดเก็บอุปกรณ์ที่สำคัญของระบบเทคโนโลยีสารสนเทศทั้งที่สำนักงานใหญ่ สถานที่สำรองข้อมูล และจัดให้มีการทำแผนเพื่อปรับปรุงความเสี่ยงหรือปัญหาที่พบ
2. จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้ามซึ่งปิดล็อคตลอดเวลา และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง
3. ต้องมีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
4. ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ ต้องมีการอนุมัติจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศก่อน และให้มีเจ้าหน้าที่ของฝ่ายสารสนเทศที่ปฏิบัติงานประจำในศูนย์คอมพิวเตอร์ควบคุมดูแลตลอดเวลาระหว่างที่บุคคลดังกล่าวอยู่ในศูนย์คอมพิวเตอร์
5. ต้องมีการติดตั้งอุปกรณ์เตือนไฟไหม้ เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา และต้องมีการบำรุงรักษาอุปกรณ์ดังกล่าวให้สามารถใช้งานได้อยู่เสมอ

6. ศูนย์คอมพิวเตอร์หลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับศูนย์คอมพิวเตอร์สำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น
7. มีการติดตั้งอุปกรณ์สำรองไฟสำหรับระบบคอมพิวเตอร์ที่สำคัญ เพื่อให้สามารถดำเนินการต่อเนื่องของระบบงานที่สำคัญได้
8. ต้องมีการควบคุมอุณหภูมิและความชื้นให้เหมาะสมที่เหมาะสมกับระบบคอมพิวเตอร์

4) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง malicious code ต่างๆ มิให้เข้าถึง (access risk) หรือสร้างความเสียหาย (availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

ความสำคัญ

บริษัทต้องควบคุมความปลอดภัยของข้อมูลเพื่อป้องกันความเสี่ยงจากการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลของบริษัท ตั้งแต่ระดับข้อมูลข่าวสารทั่วไป จนถึงระดับข้อมูลข่าวสารที่ลับที่สุด และควรจะมีหน่วยงานที่มีหน้าที่ควบคุมหรืออนุมัติการที่จะเผยแพร่ข้อมูลข่าวสารให้กับหน่วยงานอื่นๆ หรือนำข้อมูลออกไปเผยแพร่ภายนอกองค์การ ซึ่งอาจส่งผลให้เกิดข้อมูลถูกทำลายหรือนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต ดังนั้นการกำหนดนโยบายการรักษาความปลอดภัยของข้อมูลระบบคอมพิวเตอร์ และระบบเครือข่ายรวมทั้งวิธีการปฏิบัติงานอย่างเพียงพอจะช่วยป้องกันความเสี่ยงที่จะเกิดขึ้นได้

4.1 ความปลอดภัยของข้อมูล

ผู้รับผิดชอบหลัก

- ข้อมูลด้าน IT (ข้อมูลด้านการจัดการ IT จัดการโครงการ งบประมาณการพัฒนา/บำรุงรักษาระบบ)

- ข้อมูลทั่วไป ดูแลโดย ส่วนงาน / ผู้ที่ได้รับมอบหมาย ใช้งานหรือดูแล ข้อมูลนั้นๆ
- ข้อมูลลับ ดูแลโดย ส่วนงาน ที่มีหน้าที่รับผิดชอบงานและหน้าที่กำหนดในโครงสร้างของฝ่าย หรือผู้ที่ได้รับมอบหมาย ให้ปฏิบัติงานในเรื่องนั้นๆ

- ข้อมูลของบริษัท / ฝ่าย / สำนัก ที่อยู่ในระบบ IT (ข้อมูลที่องค์กรใช้ในกิจการบริษัท ทั้งด้านการให้บริการธุรกรรมต่างๆ และข้อมูลเพื่อการบริหารจัดการที่อยู่ในระบบ IT ที่ฝ่ายเทคโนโลยีสารสนเทศให้การสนับสนุนการใช้งานจัดเป็นข้อมูลที่มีความสำคัญ)
  - ข้อมูลที่ใช้งานในกิจการบริษัท โดยผู้ใช้องค์ กำหนด ดูแลโดย ผู้มีสิทธิใช้งาน ที่องค์กรกำหนด
  - ข้อมูลที่อยู่ระหว่างประมวลผล ดูแลโดยฝ่ายเทคโนโลยีสารสนเทศ
  - ข้อมูลที่จัดเก็บสำรองตามข้อปฏิบัติด้านระบบ ดูแลโดยฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. การขอใช้ข้อมูลทุกประเภท ต้องระบุผู้ขอ วัตถุประสงค์ และระยะเวลา ในการใช้งาน ที่ชัดเจน การคืน (ถ้ามี) ให้นำมาคืนเมื่อเสร็จหรือเมื่อกำหนด การยกเลิก (ปิด) สิทธิการใช้ข้อมูลให้ยกเลิกเมื่อเสร็จ หรือเมื่อครบกำหนด ห้ามทำสำเนาข้อมูลที่ระบุไว้ว่า “ห้ามทำสำเนา” โดยมิได้รับอนุญาตจากเจ้าของข้อมูล ผู้ขอข้อมูลต้องปฏิบัติตามขั้นตอนการขอใช้ข้อมูล ที่กำหนดแตกต่างกันตามประเภทข้อมูล และกลุ่มผู้ขอ
2. กำหนดชั้นความลับของข้อมูลเป็นข้อมูลทั่วไป และข้อมูลลับและกำหนดวิธีการขอใช้ข้อมูลไว้ดังนี้

   2.1 ข้อมูลทั่วไป

   - ผู้ขอใช้ข้อมูลต้องเป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดกับผู้ดูแลข้อมูล
   - ผู้ขอใช้ข้อมูลหากเป็นพนักงานนอกฝ่ายที่เจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้อำนวยการฝ่ายผู้ดูแลข้อมูล เมื่อได้รับอนุมัติแจ้งให้เจ้าหน้าที่ผู้ดูแลข้อมูลจัดทำ/ส่งข้อมูลให้

   2.2 ข้อมูลลับ

   - ผู้ขอใช้เป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้บังคับบัญชา (ระดับส่วนขึ้นไป) เมื่อได้รับอนุมัติ แจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่งข้อมูลให้

- ผู้ขอใช้เป็นพนักงานนอกฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้อำนวยการฝ่ายของตน และผู้อำนวยการฝ่ายผู้ดูแลตามลำดับเมื่อ ได้รับอนุมัติ แจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่ง ข้อมูลให้
- ผู้ขอใช้เป็นบุคคลภายนอก ให้ขอจากสำนักตรวจสอบ หรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี โดยผู้พิจารณาอนุมัติต้องเป็นผู้บริหารระดับผู้บริหารสาย/ผู้อำนวยฝ่าย/สำนัก ขึ้นไป

2.3 ข้อมูลของบริษัท / ฝ่าย / สำนัก ที่อยู่ในระบบ IT

- ผู้ขอใช้เป็นพนักงานบริษัท แจ้งรายละเอียดเพื่อขออนุมัติ จากผู้บังคับบัญชาของตน (ระดับผู้อำนวยการฝ่ายขึ้นไป / หรือผู้บังคับบัญชาในส่วนงาน)
- ผู้ขอใช้เป็นบุคคลภายนอก ให้ขอจากสำนักตรวจสอบ หรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี โดยผู้พิจารณาอนุมัติ ต้องเป็นผู้บริหารระดับผู้บริหารสาย/ผู้อำนวยการฝ่าย/สำนัก ขึ้นไป
- เมื่อต้นสังกัด หรือสำนักตรวจสอบ หรือฝ่าย/สำนักที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกอนุมัติแล้ว ให้ส่งเรื่องขออนุมัติใช้ข้อมูลไปยังสายงานที่ดูแล IT ผู้ดูแลข้อมูล(ระดับผู้อำนวยการฝ่ายขึ้นไป)
- เมื่อสายงานที่ดูแล IT ผู้ดูแลข้อมูล พิจารณาอนุมัติให้ใช้ข้อมูลได้ ผู้ดูแลข้อมูลจะสั่งการตามสายงานเพื่อให้เจ้าหน้าที่ผู้ดูแลจัดทำ / ส่ง / เปิดระบบให้ใช้ข้อมูล (ตามแต่วัตถุประสงค์ของผู้ขอ)
- กรณีผู้ขอใช้ เป็นบุคคลภายนอก จะส่งข้อมูลให้สำนักตรวจสอบ หรือฝ่าย/สำนักที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี เพื่อดำเนินการติดต่อกับผู้ขอใช้ (บุคคลภายนอก) ต่อไป
- เมื่อครบระยะเวลาใช้งาน หรือผู้ใช้แจ้งใช้งานเสร็จสิ้น (ก่อนครบกำหนด) ผู้ดูแลข้อมูลปิดระบบการเข้าใช้งาน

3. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (encryption) ทุกครั้ง

4.2 การควบคุมการกำหนดสิทธิและบัญชีรายชื่อผู้ใช้งาน

ผู้รับผิดชอบ

พนักงานขององค์กรทั้งหมด

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานการเข้ามาใช้งาน

1.1 บริษัทต้องกำหนดสิทธิการเข้าใช้งานของผู้ใช้งานเพื่อยืนยันตัวตนของผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์แยกเป็นรายบุคคล

1.2 พนักงานต้องเก็บและรักษา Password สำหรับทุกระบบงานที่ได้รับมอบมาให้เป็นความลับ

1.3 พนักงานต้องใช้ User Login และ Password ส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่พนักงานครอบครองใช้งานอยู่ โดย Password ส่วนบุคคลดังกล่าวต้อง

- การตั้งชื่อ User Login จะต้องมีอย่างน้อย 6 ตัวอักษร
- มีความยาวไม่น้อยกว่า 8 ตัวอักษร
- มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและอักขระพิเศษเข้าด้วยกัน
- จะต้องมีการกำหนดวันหมดอายุการใช้งานของ Password เช่น ต้องเปลี่ยนทุก 90 วัน และเมื่อครบ 90 วัน ต้องมีการบังคับให้เปลี่ยน (Force Change)
- Password เก็บประวัติห้ามซ้ำกัน ย้อนหลัง 3 ครั้ง รวมที่ใช้ปัจจุบันเป็น 4 ครั้ง
- ไม่กำหนด Password ส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
- ไม่กำหนด Password ส่วนบุคคลจากคำศัพท์ที่ใช้ในพจนานุกรม
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

1.4 พนักงานต้องกำหนด Password สำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายขององค์กร

1.5 พนักงานต้องไม่ใช้โปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำ Password ส่วนบุคคลของตนโดยอัตโนมัติ (Save Password)

1.6 พนักงานต้องไม่จดหรือบันทึก Password ส่วนบุคคลไว้ในสถานที่ที่งานต่อการสังเกตเห็นของบุคคลอื่น

1.7 กรณีที่มีความจำเป็นที่จะต้องบอก Password แก่ผู้อื่น เนื่องจากความจำเป็นของงานหลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยน Password ทันที

1.8 บริษัทต้องมีการสอบทานสิทธิการเข้าใช้งานโดยผู้มีอำนาจอนุมัติสิทธิการใช้งานว่าสิทธิดังกล่าวยังมีความเหมาะสมอยู่หรือไม่ โดยควรมีการสอบทานสิทธิอย่างน้อยทุก ๆ 6 เดือน หรือ 1 ครั้งต่อปี

2. กำหนดระเบียบในการ Login เข้ามาใช้งานในระบบคอมพิวเตอร์

2.1 การ Login เข้าใช้งาน Application ขององค์กร ผู้ใช้งานจะต้อง Login เข้าระบบด้วยตนเองห้ามมิให้ผู้อื่นดำเนินการให้

2.2 ไม่อนุญาตให้บุคคลอื่นใช้งานบัญชีผู้ใช้ของตนเอง

2.3 ไม่อนุญาตให้นำ Users ของตนเอง Login เข้าสู่ระบบแล้วให้ผู้อื่นใช้งาน

2.4 ให้ Logout ระบบเมื่อใช้งานแล้วเสร็จหรือมิได้อยู่ที่หน้าเครื่องคอมพิวเตอร์เป็นเวลานาน

2.5 อนุญาตให้ผู้ใช้งานใส่รหัสผิดไม่เกิน 5 ครั้ง ซึ่งระบบจะทำการล็อก ชื่อผู้ใช้งานดังกล่าวทันที โดยจะปลดล็อกเมื่อเวลาผ่านไป 30 นาที

4.3 การควบคุมของระบบฐานข้อมูล

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานการติดตั้งระบบฐานข้อมูล

1.1 ผู้ติดตั้งระบบฐานข้อมูล จะต้องเป็นพนักงานในส่วนสนับสนุนสารสนเทศ หรือพนักงานของบริษัท ซึ่งบริษัทได้มอบหมายให้ทำหน้าที่ดังกล่าว แต่ทั้งนี้จะต้องมีพนักงานในส่วนสนับสนุนสารสนเทศร่วมดำเนินการด้วย

1.2 ผู้ติดตั้งระบบฐานข้อมูลจะต้องใช้ซอฟท์แวร์ที่มีลิขสิทธิ์การใช้งานตามกฎหมาย

1.3 ส่วนสนับสนุนสารสนเทศ หรือพนักงานของบริษัท ที่ได้รับมอบหมาย ให้เป็นผู้ติดตั้ง Patch ของระบบฐานข้อมูลจะต้องคำนึงถึง

- ผลกระทบของการติดตั้งต่อผู้ใช้งานหรือต่อระบบงานที่เกี่ยวข้อง

- การประเมินความเสี่ยงของการติดตั้ง Patch ดังกล่าว
- การแจ้งให้ส่วนที่เกี่ยวข้องได้รับทราบ
- การเตรียมการเพื่อย้อนกลับมาสู่ระบบเดิมหากการติดตั้งไม่สำเร็จ รวมทั้งรายงานผลการติดตั้งให้กับผู้บังคับบัญชาได้รับทราบ

2. กำหนดมาตรฐานของผู้ใช้งาน (User Identification) และการอนุมัติการใช้งาน (Authorization)

2.1 กำหนดมาตรฐานของผู้ใช้งาน ต้องมีการกำหนดกลุ่มใช้งาน ดังนี้

- OS User ได้แก่ Super User, Developer, Operation, DBA, Audit
- Database User ได้แก่ DB Super User (Oracle, SQL Administrator) ,DB Owner Tables, DB Users ,Audit User
- Application User ได้แก่ Read Only Users, Update Users, Admin Users, Audit Users

หากมีความจำเป็นต้องเพิ่มกลุ่มผู้ใช้งานใหม่ ต้องขออนุมัติอย่างเป็นลายลักษณ์อักษรกับผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

2.2 มาตรฐานการอนุมัติการใช้งาน (Authorization)

- เมื่อผู้ใช้งานได้รับความเห็นชอบจากหัวหน้างานและผู้อำนวยการฝ่ายต้นสังกัด ตามลำดับขั้นในการขอใช้งานระบบฐานข้อมูล ผู้ดูแลระบบฐานข้อมูล ต้องจัดทำทะเบียนผู้ใช้งานให้สอดคล้องกับกลุ่มของผู้ใช้งานตามข้อ 2.1

3. กำหนดมาตรฐานในการเข้ามาใช้งาน (Login) และการเข้าถึงข้อมูล (Access Control) ในระบบฐานข้อมูล

3.1 กำหนดมาตรฐานการเข้ามาใช้งาน (Login)

- การตั้งชื่อ User Login จะต้องมีอย่างน้อย 6 ตัวอักษร
- มีความยาวไม่น้อยกว่า 8 ตัวอักษร (Super User ไม่ต่ำกว่า 12 ตัวอักษร)
- มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและอักขระพิเศษเข้าด้วยกัน
- จะต้องมีการกำหนดวันหมดอายุการใช้งานของ Password เช่น ต้องเปลี่ยนทุก 90 วัน และเมื่อครบ 90 วัน ต้องมีการบังคับให้เปลี่ยน (Force Change)
  หรือข้อยกเว้นกรณีมีผลกระทบต่อระบบงานในการเปลี่ยนแปลงรหัสผ่านให้กำหนดรหัสผ่านที่ยากแก่การจดจำ
- Password เก็บประวัติห้ามซ้ำกัน ย้อนหลัง 3 ครั้ง รวมที่ใช้ปัจจุบันเป็น 4 ครั้ง

- ไม่กำหนด Password ส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
- ไม่กำหนด Password ส่วนบุคคลจากคำศัพท์ที่ใช้ในพจนานุกรม
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

3.2 กำหนดมาตรฐานการเข้าถึงข้อมูล (Access Control)

- กำหนดวิธีการเข้าถึงข้อมูลให้สอดคล้องกับกลุ่มของผู้ใช้งานระบบ

Super User = ALL

DBA User = Tables (Create/Drop/Read/write/Insert/delete), Grant Privilege

Developer = Read /Write ขึ้นกับความจำเป็นของระบบงาน

Operator User = Read (For Backup)

Audit User = Read

- กำหนดมาตรฐานการตั้งชื่อกลุ่มผู้ใช้งานระบบฐานข้อมูล (DB Roles) โดยให้ขึ้นต้นด้วยตัวย่อของระบบงานและให้มีความยาวไม่เกิน 3 ตัวอักษรและตามด้วยเครื่องหมาย '_' และชื่อกลุ่ม Users

4. กำหนดมาตรฐานในการส่งข้อมูลผ่านระบบเครือข่าย (Data Exchange)

4.1 ส่วนสนับสนุนสารสนเทศ จะเป็นผู้ Setup Permission ของ Patch ที่ใช้เก็บ Data ในการ Interface เพื่อใช้ในการแลกเปลี่ยนข้อมูลผ่านระบบเครือข่าย

5. กำหนดมาตรฐานของการตรวจสอบการเข้าใช้งาน (Audit Trail) และความถูกต้องของข้อมูล (Data Integrity) ในระบบฐานข้อมูล

5.1 ตรวจสอบการเข้าใช้ระบบฐานข้อมูลโดยผู้ใช้งานและรายงานสรุปให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

5.2 ตรวจสอบความถูกต้องของข้อมูล (Data Integrity) ร่วมกับฝ่ายตรวจสอบภายในและจัดทำรายงานผลการตรวจสอบให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

6. กำหนดมาตรฐานการสำรองข้อมูลและการนำกลับมาใช้ เพื่อป้องกันข้อมูลเสียหาย

6.1 ส่วนสนับสนุนสารสนเทศ ต้องพิจารณาจัดหา Media ที่มีประสิทธิภาพเพื่อใช้ในการสำรองข้อมูล

6.2 ส่วนสนับสนุนสารสนเทศ และฝ่าย/ส่วนงานที่เกี่ยวข้อง ต้องร่วมกันพิจารณาถึงวิธีสำรอง และ ติดตั้งข้อมูลของแต่ละระบบงาน

6.3 ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบการสำรองข้อมูลว่าทำสำเร็จหรือไม่ และหากไม่สำเร็จต้องดำเนินการแก้ไข

6.4 การ Restore Data สามารถกระทำได้เฉพาะผู้ที่ได้รับมอบหมาย และได้รับการสั่งจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

6.5 ส่วนสนับสนุนสารสนเทศ ต้องจัดเก็บ Media ที่ใช้ในการสำรองข้อมูลไว้ในสภาพแวดล้อมที่เหมาะสม และมีระบบรักษาความปลอดภัยที่ดี

6.6 ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบสภาพ Media และข้อมูลที่อยู่ใน Media อย่างสม่ำเสมอว่ายังอยู่ในสภาพที่ใช้งานได้ดีหรือไม่ หากพบปัญหาให้รีบดำเนินการแก้ไข

4.4 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

ระเบียบปฏิบัติ

1. การติดตั้งเครื่องคอมพิวเตอร์ Server ต้องมีการจัดแบ่งหมวดหมู่ตามที่ส่วนสนับสนุนสารสนเทศได้กำหนดไว้
2. การติดตั้งเครื่องคอมพิวเตอร์ Server ต่าง ๆ ต้องมีการจัดทำแบบแปลนการติดตั้งอุปกรณ์บนตู้ Rack แสดงตำแหน่งต่าง ๆ ของอุปกรณ์บนตู้ Rack ในรูปแบบที่บริษัทระบุไว้ โดยจัดเก็บไว้ในส่วนสนับสนุนสารสนเทศ
3. การติดตั้งอุปกรณ์สื่อสารข้อมูล และอุปกรณ์รักษาความปลอดภัยต่าง ๆ ต้องมีการจัดทำแบบแปลนการติดตั้งบนตู้ Rack แสดงตำแหน่งต่าง ๆ ของอุปกรณ์บนตู้ Rack ในรูปแบบที่บริษัทระบุไว้ โดยจัดเก็บไว้ที่ส่วนสนับสนุนสารสนเทศ
4. การติดตั้งอุปกรณ์สื่อสารข้อมูลทุกชนิดกับระบบงานต่าง ๆ ของบริษัท ให้อยู่ในความควบคุมดูแลของส่วนงานสนับสนุนสารสนเทศ
5. การติดตั้งอุปกรณ์ดับเพลิงอัตโนมัติ ระบบเครื่องปรับอากาศ และระบบเครื่องจ่ายไฟสำรองฉุกเฉิน จะต้องมีมาตรฐานตามที่องค์กร หรือผู้ผลิตกำหนดไว้

4.5 การรักษาความปลอดภัยระบบคอมพิวเตอร์เครือข่าย

ผู้รับผิดชอบหลัก

พนักงานของสนับสนุนสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานในการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร ผ่านทางเครือข่าย
   1.1 ทำการติดตั้ง Service Pack ตลอดจน Patch ต่าง ๆ ให้ทันสมัยรวมทั้ง Software Antivirus ตามที่องค์กรกำหนด
2. กำหนดมาตรฐานในการติดต่อเข้า – ออกองค์กร โดยใช้ระบบเครือข่ายผ่านทางโทรศัพท์

2.1 สำหรับเครื่องคอมพิวเตอร์ที่อนุญาตให้ติดตั้ง Modem สำหรับ Link Dial Up ผ่านทางระบบโทรศัพท์จากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ให้ทำการติดตั้ง Software Personal Firewall ด้วย

2.2 เครื่องคอมพิวเตอร์ และเครื่องคอมพิวเตอร์แม่ขาย (Server) ที่อยู่ใน Zone ของ Server Segment ไม่อนุญาตให้มีการติดตั้ง Modem Dial Up ผ่านระบบโทรศัพท์โดยเด็ดขาด แต่หากมีความจำเป็นต้องใช้งานจะต้องขออนุมัติผ่านความเห็นชอบร่วมกันจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ช่วยกรรมการผู้จัดการที่ดูแลฝ่ายเทคโนโลยีสารสนเทศก่อนที่จะมีการติดตั้ง และต้องการกำหนดวันเริ่มต้นและวันสิ้นสุดการใช้งานอย่างชัดเจน และให้ผู้ดูแล Server ดังกล่าวต้องดูแลอย่างใกล้ชิดในระหว่างที่มีการใช้งานนั้น

3. กำหนดมาตรฐานของระบบรักษาความปลอดภัยบนระบบเครือข่าย

3.1 กำหนดให้มีอุปกรณ์ Firewall อย่างน้อย 2 ชุด สำหรับเครือข่ายขององค์กร ภายในกับเครือข่ายภายนอก รวมทั้งกำหนดให้มี Firewall ที่ทำหน้าเป็น Redundant ของ Firewall ทั้ง 2 ชุดนั้น

3.2 จัดหาอุปกรณ์รักษาความปลอดภัยที่ทันต่อความเปลี่ยนแปลงของภัยคุกคามทางด้านเครือข่าย โดยจัดให้มีการทบทวนภาพรวมของการรักษาความปลอดภัยบนเครือข่ายในทุก ๆ 1 ปี เพื่อดำเนินการจัดหาอุปกรณ์ป้องกันต่อไป

3.3 จัดเก็บทะเบียนเลขหมายประจำเครื่องคอมพิวเตอร์ (IP Address) ที่มีการควบคุมการใช้งาน

3.4 จัดทำและปรับปรุง Configuration ของระบบเครือข่ายให้มีความทันสมัยและปลอดภัยอยู่เสมอ

3.5 ทำการ Backup Configuration ของอุปกรณ์สื่อสารข้อมูลเป็นประจำทุก 6 เดือน หรือทุกครั้งที่มีการเปลี่ยนแปลง

3.6 จัดการเปลี่ยน Password ของอุปกรณ์สื่อสารขององค์กรทุกชุดทุก 4 เดือนและให้พิมพ์รายละเอียดของอุปกรณ์ Password ใส่ซองปิดผนึก และให้หัวหน้าส่วนสนับสนุนสารสนเทศ เซ็นกำกับ และส่งต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ หรือ ผู้อำนวยการแผนก ควบคุมภายใน เพื่อเก็บรักษาไว้รวมทั้งทำลายซอง Password เดิมทันทีหลังจากได้รับซอง Password ชุดใหม่

3.7 ห้ามใช้ Community Name ของอุปกรณ์สื่อสารข้อมูลทุกชนิดหรือ อุปกรณ์อื่นที่ใช้ Protocol SNMP ที่ถูกกำหนดชื่อมาโดยผู้ผลิตอุปกรณ์เมื่อเริ่มใช้งานกับระบบงานขององค์กร ให้ดำเนินการเปลี่ยนชื่อนั้นโดยทันที

3.8 สำหรับ Server ที่จะทำการติดตั้งเข้ากันเครือข่ายขององค์กร ส่วนสนับสนุนสารสนเทศ หรือพนักงานองค์กรหรือบริษัท ผู้ดูแลการติดตั้ง Server ดังกล่าวต้องส่งรายละเอียดของระบบปฏิบัติการ (Operating System) และ Service Pack หรืออื่น ๆ ที่จำเป็นสำหรับการติดตั้งให้กับส่วนสนับสนุนสารสนเทศ รับทราบข้อมูลก่อนหลังจากนั้นจึงจะจ่าย IP Address ให้และให้ทำการ Monitor Port ที่จ่ายให้กับ Server ดังกล่าวไม่น้อยกว่า 1 สัปดาห์อย่างใกล้ชิดพร้อมกันรายงานผลต่อหัวหน้าหรือผู้อำนวยการฝ่าย

3.9 ให้ส่วนสนับสนุนสารสนเทศ เป็นผู้ถือกุญแจห้องอุปกรณ์สื่อสาร/ห้อง Server ขององค์กร

4. กำหนดมาตรฐานในการเชื่อมต่อกับเครือข่ายภายนอกองค์กร

4.1 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายขององค์กรต้องผ่านความเห็นชอบจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทุกกรณี

4.2 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายขององค์กรต้องเชื่อมต่อโดยมีอุปกรณ์ Firewall ป้องกันทุกระบบ

4.3 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากันระบบเครือข่ายขององค์กรให้ใช้วงจรที่เป็นวงจร Permanent เท่านั้น ไม่อนุญาตให้ทำในลักษณะ Link Dial Up

5. กำหนดให้มีการจัดทำแผนผังเครือข่ายขององค์กร

5.1 ให้มีการจัดทำแผนผังเครือข่ายขององค์กร และต้องปรับปรุงแผนผังดังกล่าวให้มีความทันสมัยอยู่เสมอ รวมทั้งจัดเก็บไว้ในสถานที่ที่มีความปลอดภัย

4.6 การป้องกันไวรัสคอมพิวเตอร์ /มัลแวร์

ผู้รับผิดชอบหลัก

พนักงานของส่วนสนับสนุนสารสนเทศ

พนักงานของส่วนพัฒนาระบบสารสนเทศ

ระเบียบปฏิบัติ

1. ติดตั้งและตรวจสอบเครื่องมือในการกำจัดไวรัสคอมพิวเตอร์/สมัลแวร์

1.1 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์สำหรับเครื่องแม่ข่ายให้บริการจดหมายอิเล็กทรอนิกส์ที่ Gate way (SMTP Gateway) เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้ง ต้องจัดให้มีการอัพเดต จากเจ้าของผลิตภัณฑ์นั้นๆทุก 24 ชั่วโมง

1.2 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/ มัลแวร์สำหรับ HTTP เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้งต้องจัดให้มีการอัพเดต จากเจ้าของผลิตภัณฑ์นั้นๆ ทุก 24 ชั่วโมง

1.3 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์สำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Server Protect and Office Scan) เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้ง ต้องจัดให้มีการอัพเดตจากเจ้าของผลิตภัณฑ์นั้นๆทุก 24 ชั่วโมง

1.4 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ บน เครื่องแม่ข่ายที่ให้บริการ E-mail (Scan Mail) เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้ง ต้องจัดให้มีการอับเดตจากเจ้าของผลิตภัณฑ์นั้นๆ ทุก 24 ชั่วโมง

1.5 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ให้กับ PC ขององค์กรทุกเครื่อง เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้งต้องจัดให้มีการอัพเดตจากเจ้าของผลิตภัณฑ์นั้นๆทุก 24 ชั่วโมง

2. กำหนดหน้าที่และความรับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์

2.1 กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการตรวจจับ และทำลายไวรัสคอมพิวเตอร์/มัลแวร์บนเครื่องคอมพิวเตอร์ส่วนบุคคล ไม่ให้แพร่กระจายทำความเสียหายกับข้อมูลขององค์กร

2.2 กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ ต้องมีการแจ้งข่าวเกี่ยวกับไวรัสคอมพิวเตอร์/มัลแวร์ทันที หากมีการระบาดของไวรัสคอมพิวเตอร์/มัลแวร์ตัวใหม่

2.3 กำหนดให้ส่วนเทคนิคปฏิบัติการส่วนเครือข่าย มีหน้าที่รับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์อย่างสม่ำเสมอบน Servers และอุปกรณ์เครือข่าย เพื่อป้องกันความเสียหายกับข้อมูลขององค์กร

2.4 กำหนดให้ส่วนเทคนิคปฏิบัติการทำการรายงานสถิติการติดไวรัสคอมพิวเตอร์/มัลแวร์ของเครื่องคอมพิวเตอร์ส่วนบุคคลที่แสดงอยู่บนเซิร์ฟเวอร์แม่ข่ายสำหรับป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ขององค์กร อย่างน้อยเดือนละ 1 ครั้งต่อ ผู้อำนายการฝ่ายสนับสนุนสารสนเทศ

5) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk

ความสำคัญ

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ เพื่อสร้างความมั่นใจว่าการซื้อหรือการพัฒนามีความสอดคล้องกับแผนงานของบริษัท มีหลักเกณฑ์ในการคัดเลือก พัฒนา มีการจัดลำดับความสำคัญของงาน รวมทั้งกระบวนการพัฒนาได้มีการทดสอบอย่างเพียงพอว่าระบบงานที่แก้ไขเปลี่ยนแปลงมีความถูกต้องและให้ผลลัพธ์ตามที่ได้กำหนดไว้

ผู้รับผิดชอบหลัก

พนักงานของส่วนสนับสนุนสารสนเทศ

พนักงานของส่วนพัฒนาระบบสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดให้ปฏิบัติตามขั้นตอนดังนี้ในการพัฒนาซอฟต์แวร์

- การเริ่มต้นโครงการ (Initiation)
- การวิเคราะห์ระบบ (Analysis)
- การออกแบบระบบ (Design)
- การพัฒนาและทดสอบระบบ (Build and Test)
- การติดตั้งและใช้งานระบบ (Deployment)

2. กำหนดให้จัดทำเอกสาร สิ่งส่งมอบ ขั้นต่ำตามที่แสดงไว้ในตารางด้านล่าง

ที่	ขั้นตอน	สิ่งที่ต้องส่งมอบ
1	การเริ่มต้นโครงการ (Initiation)	- ปัญหา - เหตุผลความจำเป็น - ความต้องการของผู้ใช้งานระบบ (User requirement) - ความเป็นไปได้ทางเทคนิค - ความต้องการทางด้านความปลอดภัยที่จำเป็น (security requirement)
2	การวิเคราะห์ระบบ (Analysis)	- เอกสาร System flow diagram - เอกสาร data flow diagram level 1-2 - เอกสาร entity relationship diagram - เอกสารหน้าจอสำหรับผู้ใช้งานเพื่อสามารถเปรียบเทียบกับความต้องการ การใช้งาน ที่กำหนดไว้ในกระบวนการที่ 1 - เอกสารการวางแผนการทดสอบระบบซึ่งรวมถึงการทดสอบ security requirement ด้วย
3	การออกแบบ (Design)	- เอกสารการกำหนดฮาร์ดแวร์และซอฟต์แวร์ที่จำเป็นต้องใช้ - เอกสารการกำหนด program specification - เอกสาร test case ที่ใช้ในการทดสอบ
4	การพัฒนาและทดสอบ (Build and Test)	- คู่มือการใช้งานสำหรับผู้ใช้งาน - คู่มือการใช้งานำหรับผู้ปฏิบัติงาน (operator) - คู่มือการใช้งานสำหรับผู้ดูแลระบบ - Source code ของระบบ - เอกสารผลการทดสอบตาม Test case - เอกสาร user acceptance test เช่น ทดสอบตาม user requirement ที่กำหนดไว้ เป็นต้น
5	การติดตั้งและใช้งาน (Deployment)	- เอกสารการลงนามยอมรับการใช้งาน (user acceptance) - Source code ที่เป็นเวอร์ชั่นที่จะนำขึ้นสู่ Production ต้องนำไปเก็บไว้กับ ผู้ที่ได้รับมอบหมายให้ดูแลรักษา

6) การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

ความสำคัญ

บริษัท ต้องกำหนดวิธีการปฏิบัติในกรณีที่เกิดเหตุการณ์ฉุกเฉินในกรณีต่าง ๆ และกำหนดหน้าที่รับผิดชอบของตัวบุคคล พร้อมทั้งมีการซักซ้อมเป็นระยะ เพื่อให้เกิดผลกระทบต่อการบริการของบริษัทแก่ลูกค้าให้น้อยที่สุด และเพื่อให้การดำเนินการของบริษัท ยังสามารถดำเนินต่อได้โดยไม่ติดขัด

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดหน้าที่ความรับผิดชอบ
   - 1.1 ติดตั้งอุปกรณ์ Hardware ติดตั้งโปรแกรม OS และทดสอบการใช้งานให้มีความพร้อมในกรณีที่เกิดเหตุการณ์ฉุกเฉิน โดยส่วนสนับสนุนสารสนเทศ และส่วนพัฒนาระบบสารสนเทศ
   - 1.2 ติดตั้งอุปกรณ์เครือข่ายให้สามารถใช้งานได้ โดยส่วนเครือข่าย
   - 1.3 จัดหาอุปกรณ์อำนวยความสะดวก (Facility) ให้มีความพร้อมในการใช้งานโดยส่วนสนับสนุนสารสนเทศ
   - 1.4 นำข้อมูลสำรองชุดล่าสุดมาลงในระบบเพื่อใช้งาน โดยส่วนสนับสนุนสารสนเทศ
   - 1.5 ทดสอบการใช้งานเพื่อเตรียมความพร้อมอย่างสม่ำเสมอ โดยส่วนสนับสนุนสารสนเทศ และพัฒนาระบบสารสนเทศ
   - 1.6 กำหนดหน้าที่ความรับผิดชอบของพนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉิน

1.6.1 พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉินต้องเข้ารับอบรมหรือสร้างความตระหนักเพื่อให้รู้หรือทราบวิธีปฏิบัติในกรณีที่เกิดเหตุฉุกเฉินในกรณีต่าง ๆ

1.6.2 พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉินต้องร่วมซ้อมการใช้งานแผนสำรองฉุกเฉิน ซึ่งจะจัดขึ้นปีละ 1 ครั้ง

2. กำหนดมาตรฐานสำหรับศูนย์คอมพิวเตอร์สำรอง

2.1 ติดตั้งและดูแลระบบคอมพิวเตอร์สำรองอย่างสม่ำเสมอเพื่อให้สามารถให้บริการทดแทนระบบคอมพิวเตอร์หลักได้

2.2 ติดตั้งข้อมูลระบบ Facility ให้พร้อมสำหรับการใช้งานอย่างสม่ำเสมอ

2.3 นำข้อมูลที่สำรองไว้มา Update ให้มีความทันสมัยอยู่ตลอดเวลา

2.4 ทดสอบการใช้งานระบบคอมพิวเตอร์ เครือข่าย และระบบ Facility อย่างสม่ำเสมอเพื่อให้สามารถใช้งานได้โดยไม่ติดขัด

2.5 สรุปรายงานผลการปฏิบัติตั้งแต่ข้อ 2.1 -2.4 ในทุก ๆ ไตรมาส และนำเสนอต่อผู้ช่วยกรรมการผู้จัดการ

3. การสำรองข้อมูล

3.1 ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (operating system) โปรแกรมระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

3.2 จัดทำขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้

- ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
- ประเภทสื่อบันทึก (media)
- จำนวนที่ต้องสำรอง (copy)
- ขั้นตอนและวิธีการสำรองโดยละเอียด
- สถานที่และวิธีการเก็บรักษาสื่อบันทึก

3.3 จัดทำบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

3.4 ทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

3.5 จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีการปฏิบัติงานต่าง ๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องมีการควบคุมการเข้าออกและระบบป้องกันความเสียหายที่เป็นมาตรฐาน

3.6 ต้องจัดทำฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อสำรองข้อมูล เพื่อให้สามารถค้นหาได้โดยเร็ว

3.7 การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

7) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

วัตถุประสงค์

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk และ availability risk

ความสำคัญ

บริษัทต้องกำหนดวิธีการปฏิบัติงานประจำด้านคอมพิวเตอร์ไว้เป็นลายลักษณ์อักษร เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ และควรมีการจัดทำบันทึกผลการปฏิบัติงานไว้เพื่อให้สามารถตรวจสอบได้ว่ามีการจัดทำอย่างครบถ้วนและเป็นไปตามวิธีการปฏิบัติงานที่กำหนดไว้

ผู้รับผิดชอบหลัก

พนักงานของส่วนสนับสนุนระบบสารสนเทศ

ระเบียบปฏิบัติ

1. จัดทำขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญ เป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (computer operator) และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบัน อยู่เสมอ
2. กำหนดมาตรฐานการ Login เข้าใช้งานระบบ
   2.1 กำหนดให้มีระบบการตรวจสอบการ Login เข้ามาใช้งาน โดยต้องบันทึกข้อมูลที่เกี่ยวข้องกับการ Login นั้นไว้ และให้บันทึกทั้งการ Login ที่ทำได้สำเร็จ และไม่สำเร็จเพื่อใช้ในการตรวจสอบภายหลัง

2.2 ควรกำหนดให้มีการบันทึก (log book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้

- ผู้ปฏิบัติงาน
- เวลาปฏิบัติงาน
- รายละเอียดการปฏิบัติงาน
- ปัญหาที่เกิดขึ้นและการแก้ไข
- สถานะของระบบ
- ผู้ตรวจทานการปฏิบัติงาน

การปฏิบัติงานประจำควรประกอบด้วย

- การสำรองข้อมูล
- การตรวจสอบความพร้อมของอุปกรณ์คอมพิวเตอร์ในศูนย์คอมพิวเตอร์
- การตรวจสอบซอฟท์แวร์ระบบ ระบบเครือข่าย และระบบป้องกันไวรัส
- การตรวจสอบความพร้อมของอุปกรณ์ป้องกันภัยหรืออุปกรณ์อื่นที่เกี่ยวข้อง เช่น ระบบดับเพลิง ระบบควบคุมอุณหภูมิ
- การตรวจสอบและบำรุงรักษาอุปกรณ์

8) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นมีวัตถุประสงค์เพื่อให้บริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

ความสำคัญ

การกำหนดนโยบาย ระเบียบปฏิบัติ มาตรฐานและแนวทางในการคัดเลือกผู้ให้บริการภายนอกจะช่วยให้การตัดสินใจที่จะได้รับประสิทธิผลที่ดีขึ้น ซึ่งจะส่งผลต่อค่าใช้จ่ายที่เหมาะสมในการเลือกใช้บริการและผลของการให้บริการเป็นไปตามที่คาดหวังไว้

ผู้รับผิดชอบหลัก

ผู้บริหารระดับสูง

ผู้บริหารระดับผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

พนักงานของส่วนพัฒนาระบบสารสนเทศ

ระเบียบปฏิบัติ

1. การคัดเลือกผู้ให้บริการจากภายนอก

การคัดเลือกผู้ให้บริการจากภายนอกให้เป็นไปตามระเบียบวิธีการคัดเลือกตามกระบวนการจัดซื้อจัดจ้าง โดยการพิจารณาคัดเลือกต้องครอบคลุมเรื่องดังต่อไปนี้

1.1 การเปรียบเทียบข้อเสนอกับความต้องการของบริษัท

1.2 การประเมินผลงานที่ผ่านมาของผู้ให้บริการภายนอก

1.3 กำหนดมาตรฐานของอุปกรณ์ที่นำมาติดตั้งใช้งานจะต้องเป็นอุปกรณ์ที่มีคุณภาพและได้มาตรฐาน

1.3.1 อุปกรณ์ที่นำมาติดตั้งต้องมีมาตรฐานรับรองจากบริษัทหรือจากผู้ผลิตโดยตรง

1.3.2 อุปกรณ์ที่นำมาติดตั้งใช้งาน จะต้องมีมาตรฐานที่เป็นสากล (Standard)

2. การควบคุมด้านความมั่นคงปลอดภัย

2.1 กำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ที่บริษัททำสัญญาว่าจ้างให้มาปฏิบัติงานซึ่งสอดคล้องกับนโยบายความมั่นคงปลอดภัยของบริษัทและให้ผู้ปฏิบัติงานนั้นลงนามในเอกสารดังกล่าว

2.2 เมื่อสิ้นสุดการจ้างงานหรือการเปลี่ยนแปลงลักษณะการจ้างงานของหน่วยงานภายนอกจะต้องถอนสิทธิการเข้าถึงระบบสารสนเทศและทรัพย์สินสารสนเทศทันที

3. การควบคุมระหว่างการให้บริการ

3.1 ต้องควบคุมผู้ให้บริการจากภายนอกว่ามีการปฏิบัติตามข้อกำหนดที่จัดทำขึ้นอย่างสม่ำเสมอ เช่น ดูจากการให้บริการ การศึกษาจารายงานและข้อมูลต่าง ๆ

3.2 ต้องมีการกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญจ่อระบบหรือการให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การปรับปรุงเทคโนโลยี ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

6. การพิจารณาโทษทางวินัยและการเรียกค่าเสียหาย

6.1 พนักงานและลูกจ้างที่ฝ่าฝืนข้อกำหนดนโยบายด้านความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศ โดยจงใจหรือประมาณเลินเล่อ และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวิจัยและความรับผิดทางแพ่งและอาญาแก่พนักงานและลูกจ้างนั้น ตามกฎหมาย ข้อบังคับ ระเบียบ หรือประกาศที่เกี่ยวข้อง

ผู้บังคับบัญชาผู้ใด งดเว้น หรือละเว้นการปฏิบัติตามหน้าที่ และเป็นเหตุให้พนักงานหรือลูกจ้างที่อยู่ภายใต้การบังคับบัญชาของตน ฝ่าฝืนข้อกำหนดของนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสานสนเทศนี้ ให้นำบทบัญญัติในวรรคก่อนมาใช้บังคับโดยอนุโลม

6.2 การฝ่าฝืนขอกำหนดใด ๆ ตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ แม้จะไม่ก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใดก็ตาม ถ้าผู้บังคับบัญชาเห็นว่ามีเหตุอันสมควร อาจจะบันทึกในประวัติการปฏิบัติงานและจะใช้เป็นข้อมูลประกอบการพิจารณาต่ออายุสัญญาจ้าง การขึ้นเงินเดือน หรือเลื่อนตำแหน่งด้วยก็ได้