บริษัท เอส.เจ.ซี.คอนกรีต จำกัด

นโยบายด้านเทคโนโลยีสารสนเทศ

(Information Technology Policy)

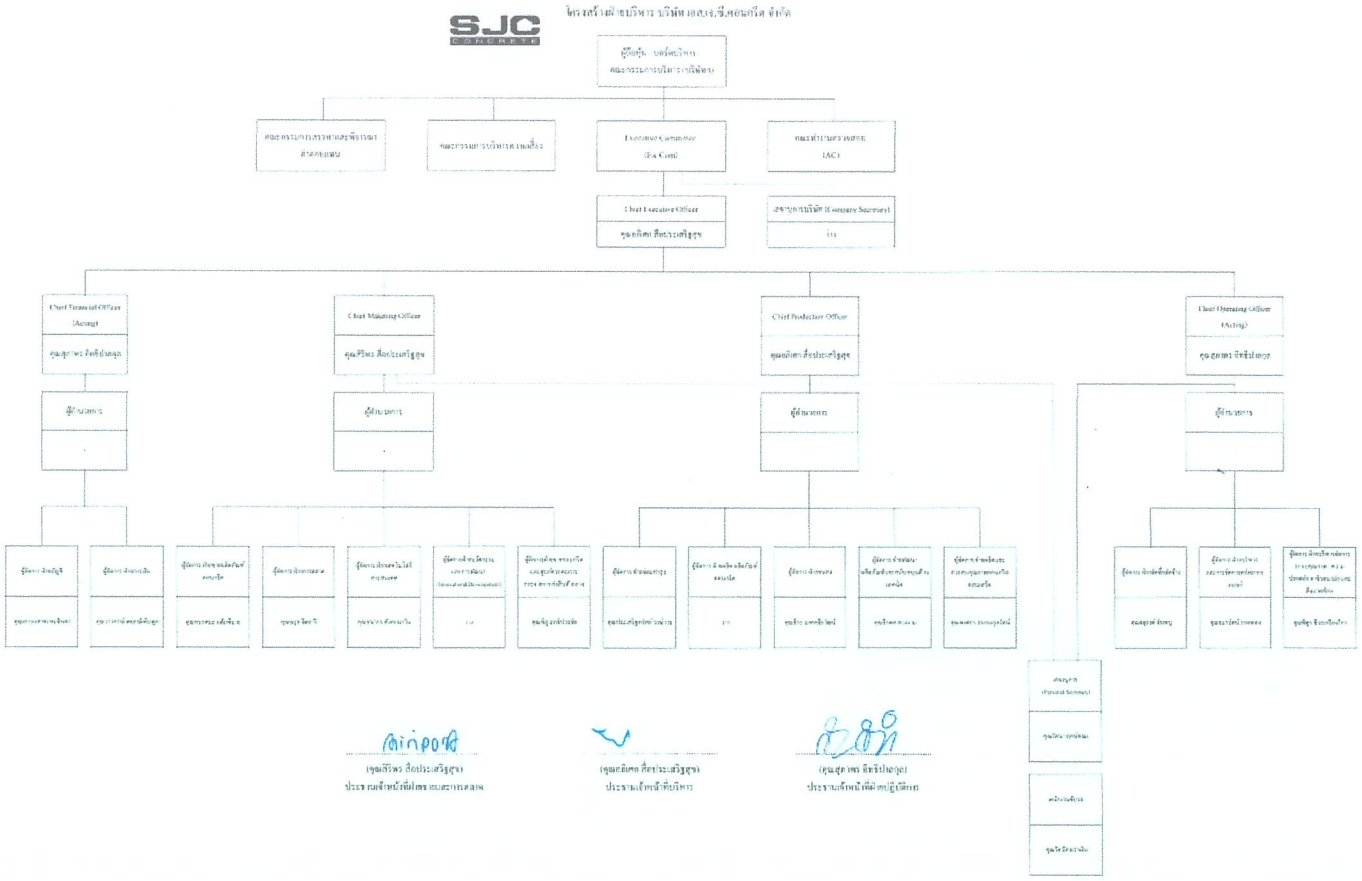
บันทึกรายการแก้ไขเอกสารคู่มือการปฏิบัติงานฝ่ายเทคโนโลยีสารสนเทศ

แผ่นที่	รายละเอียดการแก้ไข	หมายเหตุ

ผู้จัดทำ :	ผู้ตรวจสอบ :	ผู้อนุมัติ :
ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ	ประธานเจ้าหน้าที่ฝ่ายขายและการตลาด	ประธานเจ้าหน้าที่บริหาร

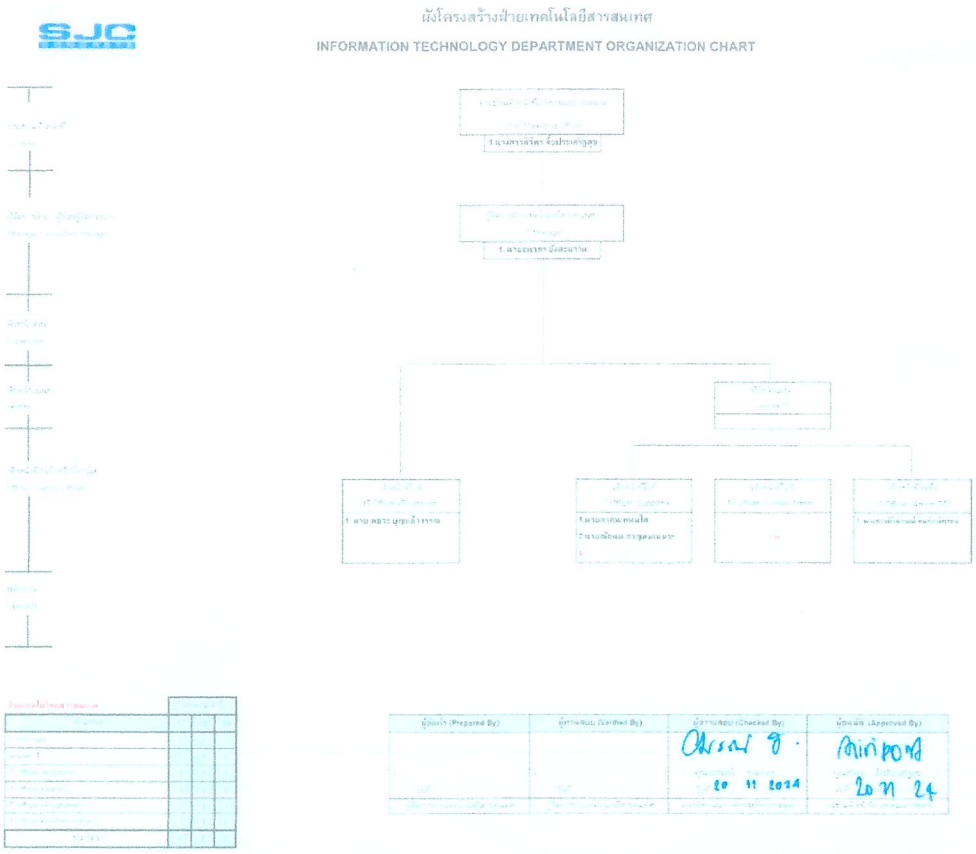
สารบัญ

โครงสร้างการจัดการของบริษัท



อนุมัติ

โครงสร้างการการบริหารงาน – ฝ่ายสารสารสนเทศ



ผู้จัดทำ (Prepared By)	ผู้ทานสอบ (Verified By)	ผู้ตรวจสอบ (Checked By)	ผู้อนุมัติ (Approved By)
		20 11 2024	20 ก.ค. 24

คณนัค

นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Information Technology Security Policy)

1. วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

บริษัทฯ ได้ตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติของพนักงานในองค์กร เพื่อให้พนักงานมีความตระหนักถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศของบริษัท และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา รวมทั้งเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัท ด้านอื่นๆ ที่มุ่งเน้นการปฏิบัติงานภายในบริษัทให้มีความมั่นคงปลอดภัยในการดำเนินกิจการของบริษัท

2. ความมั่นคงปลอดภัยสำหรับสารสนเทศ และแนวทางในการรักษาความปลอดภัย

ความมั่นคงปลอดภัยสำหรับสารสนเทศ หมายถึง การสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศ เพื่อป้องกันความเสียหายที่มีต่อองค์ประกอบทางด้านความมั่นคงปลอดภัย 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) ต่างๆ ขององค์กร
- เครื่องคอมพิวเตอร์ส่วนบุคคล
- เครื่องคอมพิวเตอร์แบบพกพา
- อุปกรณ์เครือข่าย
- ระบบไฟฟ้าสำรอง
- สายสัญญาณเครือข่าย
- ซอฟท์แวร์ระบบ ซอฟท์แวร์จ้างพัฒนา ซอฟท์แวร์พัฒนาเอง ซอฟท์แวร์สำเร็จรูป
- สื่อบันทึกข้อมูล
- เอกสารของบริษัท
- อุปกรณ์สื่อสาร และ แอพพลิเคชั่น ที่อยู่ในอุปกรณ์นั้นๆ

4. นโยบายความมั่นคงปลอดภัย

นโยบายด้านความมั่นคงปลอดภัยครอบคลุมนโยบาย 10 ด้าน ดังนี้

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
3. การควบคุมการเข้าออกห้องเซิร์ฟเวอร์และการป้องกันความเสียหาย (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)
9. การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ Cloud Computing
10. การบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management)
11. การอนุรักษ์พลังงานในบริษัท
12. การพิจารณาโทษทางวินัยและการเรียกค่าเสียหาย

5. สาระสำคัญของนโยบายมีดังต่อไปนี้

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ เพื่อจัดทำนโยบายให้สามารถรองรับความเสี่ยงที่เกิดขึ้นได้ รวมทั้งการประกาศใช้นโยบายให้แก่บุคคลกรที่เกี่ยวข้องได้ตระหนักและปฏิบัติตามนโยบายความปลอดภัยของด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องจัดให้มีการแบ่งแยกหน้าที่การปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์อย่างเพียงพอ เพื่อช่วยให้มีการสอบยันการปฏิบัติงานและมีการอนุมัติการปฏิบัติงานอย่างเพียงพอและเหมาะสม รวมทั้งการมีขอบเขตการปฏิบัติงานของพนักงานที่ชัดเจนและมีบุคลากรที่เพียงพอต่อการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ

3. การควบคุมการเข้าออกห้องเซิร์ฟเวอร์และการป้องกันความเสียหาย (Physical Security) ซึ่งมีสาระสำคัญดังนี้

การควบคุมการเข้าออกห้องเซิร์ฟเวอร์อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ห้องเซิร์ฟเวอร์ และความเสียหายอันจะเกิดจากอุปกรณ์หรือระบบต่าง ๆ เช่น ระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ซึ่งย่อมมีความเสี่ยงต้องอุปกรณ์และข้อมูลของบริษัท ดังนั้นบริษัทต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงห้องเซิร์ฟเวอร์ได้ และการเข้าถึงดังกล่าวต้องมีการอนุมัติอย่างเพียงพอ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้มีระบบป้องกันความเสียหายที่อาจจะเกิดขึ้น เช่นการป้องกันไฟไหม้ หรือไฟฟ้าขัดข้อง

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

บริษัทต้องควบคุมความปลอดภัยของข้อมูลเพื่อป้องกันความเสี่ยงจากการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลของบริษัท ตั้งแต่ระดับข้อมูลข่าวสารทั่วไป จนถึงระดับข้อมูลข่าวสารที่ลับที่สุด และควรจะมีหน่วยงานที่มีหน้าที่ควบคุมหรืออนุมัติการที่จะเผยแพร่ข้อมูลข่าวสารให้กับหน่วยงานอื่นๆ หรือนำข้อมูลออกไปเผยแพร่ภายนอกองค์การ ซึ่งอาจส่งผลให้เกิดข้อมูลถูกทำลายหรือนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต ดังนั้นการกำหนดนโยบายการรักษาความปลอดภัยของข้อมูลระบบคอมพิวเตอร์ 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 ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงานเพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ และควรมีการจัดทำบันทึกผลการปฏิบัติงานไว้เพื่อให้สามารถตรวจสอบได้ว่ามีการจัดทำอย่างครบถ้วนและเป็นไปตามวิธีการปฏิบัติงานที่กำหนดไว้

8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ซึ่งมีสาระสำคัญดังนี้

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อบริษัท ดังนั้น บริษัทต้องกำหนดนโยบาย การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นเพื่อให้บริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการให้เป็นไปตามที่คาดหวังไว้

9. การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ Cloud Computing ซึ่งมีสาระสำคัญดังนี้

บริษัทได้กำหนดแนวทางการกำกับดูแลและบริหารจัดการการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ตามความต้องการของผู้ใช้งาน หรือ Cloud Computing โดยอ้างอิงกรอบมาตรฐานด้านการบริหารจัดการอันเป็นสากล ที่ครอบคลุมกระบวนการสำคัญตั้งแต่การกำหนดกรอบการกำกับดูแลการใช้งาน Cloud Computing

10. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management) ซึ่งมีสาระสำคัญดังนี้

บริษัทได้กำหนดแนวการใช้งานทรัพย์สิน เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด ป้องกันทรัพยากร และข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

11. การอนุรักษ์พลังงานในบริษัท ซึ่งมีสาระสำคัญดังนี้

บริษัทกำหนดให้ทุกคนในฝ่ายเทคโนโลยีสารสนเทศ ต้องมีส่วนร่วมในการบริหารจัดการพลังงานในบริษัท โดยร่วมรับผิดชอบ และยึดถือปฏิบัติตามมาตรการการอนุรักษ์พลังงาน

ระเบียบปฏิบัติ

นโยบายแต่ละด้านจะประกอบไปด้วยระเบียบปฏิบัติที่พนักงานหรือผู้ที่เกี่ยวข้องต้องปฏิบัติตามโดยเคร่งครัดดังต่อไปนี้

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ความสำคัญ

บริษัทต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยี*สารสนเทศ* โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ เพื่อจัดทำนโยบายให้สามารถรองรับความเสี่ยงที่เกิดขึ้นได้ รวมทั้งการประกาศใช้นโยบายให้แก่บุคคลกรที่เกี่ยวข้องได้ตระหนักและปฏิบัติตามนโยบายความปลอดภัยของด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

ผู้รับผิดชอบหลัก

1. ประธานเจ้าหน้าที่บริหาร
2. ประธานเจ้าหน้าที่ฝ่ายขายและการตลาด

ระเบียบปฏิบัติ

1. จัดให้มีการทำนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศโดยฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายให้จัดทำขึ้น และมีการปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือตามความจำเป็นต่อการใช้งาน และนโยบายดังกล่าวได้รับการอนุมัติจากคณะกรรมการบริษัทหรือผู้มีอำนาจที่ได้รับมอบหมายไว้ และประกาศให้ทราบโดยทั่วกันตามช่องทางการสื่อสารของบริษัท โดยถ้าเป็นการสื่อสารภายในองค์กรจะต้องกำเนินการประสานงานฝ่ายบุคคลเป็นผู้ประกาศให้ ถ้าเป็นการสื่อสารภายนอกองค์กรจะต้องดำเนินการประสานฝ่ายสื่อสารการตลาดเป็นผู้สื่อสารให้
2. จัดทำนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้ง่าย
3. จัดให้มีการสร้างความตระหนักที่เกี่ยวข้องกับภัยคุกคามที่อาจส่งผลกระทบต่อระบบสารสนเทศของบริษัทเพื่อให้พนักงานขององค์กร มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ในระดับหนึ่งอย่างน้อยปีละ 1 ครั้ง

4. จัดให้มีการทำรายงานสรุปปัญหาแนวทางแก้ไขที่มีระดับความสำคัญสูงและความคืบหน้าในการแก้ไข พร้อมทั้งรายงานต่อผู้บริหารระดับสูงรับทราบ โดยรายงานสรุปผลควรจัดทำอย่างน้อยเดือนละ 1 ครั้ง หรือตามความเหมาะสมจัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศขององค์กร ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุงความเสี่ยงหรือปัญหาที่พบ
5. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยปีละ 1 ครั้งและจัดให้มีการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ
6. จัดให้มีการวางแผนกลยุทธ์ด้านสารสนเทศเพื่อให้สอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัท ทั้งแผนระยะสั้นและแผนระยะยาว

2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

วัตถุประสงค์

การแบ่งแยกอำนาจหน้าที่มีวัตถุประสงค์เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์ ซึ่งเป็นการลดความเสี่ยงด้าน Infrastructure risk

ความสำคัญ

บริษัทต้องจัดให้มีการแบ่งแยกหน้าที่การปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์อย่างเพียงพอ เพื่อช่วยให้มีการสอบยันการปฏิบัติงานและมีการอนุมัติการปฏิบัติงานอย่างเพียงพอและเหมาะสม รวมทั้งการมีขอบเขตการปฏิบัติงานของพนักงานที่ชัดเจนและมีบุคลากรที่เพียงพอต่อการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบหลัก

ประธานเจ้าหน้าที่ฝ่ายขายและการตลาด

ระเบียบปฏิบัติ

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

3. การควบคุมการเข้าออกห้องเซิร์ฟเวอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

การควบคุมการเข้าออกห้องเซิร์ฟเวอร์มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk) ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk)

ความสำคัญ

การควบคุมการเข้าออกห้องเซิร์ฟเวอร์อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ห้องเซิร์ฟเวอร์ และความเสียหายอันจะเกิดจากอุปกรณ์หรือระบบต่าง ๆ เช่น ระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ซึ่งย่อมมีความเสี่ยงต่ออุปกรณ์และข้อมูลของบริษัท ดังนั้นบริษัทต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงห้องเซิร์ฟเวอร์ได้ และการเข้าถึงดังกล่าวต้องมีการอนุมัติอย่างเพียงพอ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้มีระบบป้องกันความเสียหายที่อาจจะเกิดขึ้น เช่นการป้องกันไฟไหม้ หรือไฟฟ้าขัดข้อง

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. จัดให้มีการประเมินความเสี่ยงทางกายภาพของพื้นที่จัดเก็บอุปกรณ์ที่สำคัญของระบบเทคโนโลยีสารสนเทศทั้งที่สำนักงานใหญ่ สถานที่สำรองข้อมูล และจัดให้มีการทำแผนเพื่อลดความเสี่ยงหรือแก้ไขปัญหาที่พบ
2. จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในห้องเซิร์ฟเวอร์หรือพื้นที่หวงห้ามซึ่งปิดล็อคตลอดเวลา และต้องกำหนดสิทธิการเข้าออกห้องเซิร์ฟเวอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง
3. ต้องมีระบบเก็บบันทึกการเข้าออกห้องเซิร์ฟเวอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้า+ออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
4. ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องเซิร์ฟเวอร์ ต้องมีการอนุมัติจากผู้มีอำนาจตามคู่มืออำนาจดำเนินการของฝ่ายเทคโนโลยีสารสนเทศก่อน และให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศที่ปฏิบัติงานประจำในห้องเซิร์ฟเวอร์ควบคุมดูแลตลอดเวลาระหว่างที่บุคคลดังกล่าวอยู่ในห้องเซิร์ฟเวอร์
5. ต้องมีการติดตั้งอุปกรณ์เตือนไฟไหม้ เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา และต้องมีการบำรุงรักษาอุปกรณ์ดังกล่าวให้สามารถใช้งานได้อยู่เสมอ

6. ห้องเซิร์ฟเวอร์หลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับห้องเซิร์ฟเวอร์สำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น
7. มีการติดตั้งอุปกรณ์สำรองไฟสำหรับระบบคอมพิวเตอร์ที่สำคัญ เพื่อให้สามารถดำเนินการต่อเนื่องของระบบงานที่สำคัญได้
8. ต้องมีการควบคุมอุณหภูมิและความชื้นให้เหมาะสมที่เหมาะสมกับระบบคอมพิวเตอร์

4. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึงล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง malicious code ต่างๆ มิให้เข้าถึง (access risk) หรือสร้างความเสียหาย (availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ 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 ที่ฝ่ายเทคโนโลยีสารสนเทศให้การสนับสนุนการใช้งาน จัดเป็นข้อมูลที่มีความสำคัญ)
    - ข้อมูลที่ใช้งานในกิจการบริษัท โดยผู้ใช้ กำหนดดูแลโดยผู้มีสิทธิใช้งานที่องค์กรกำหนด
    - ข้อมูลที่อยู่ระหว่างประมวลผล ดูแลโดยฝ่ายเทคโนโลยีสารสนเทศ
    - ข้อมูลที่จัดเก็บสำรองตามข้อปฏิบัติด้านระบบ ดูแลโดยฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

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

    2.1 ข้อมูลทั่วไป

    - ผู้ขอใช้ข้อมูลต้องเป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดกับผู้ดูแลข้อมูล
    - ผู้ขอใช้ข้อมูลหากเป็นพนักงานนอกฝ่ายที่เจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้จัดการฝ่ายผู้ดูแลข้อมูล เมื่อได้รับอนุมัติแจ้งให้เจ้าหน้าที่ผู้ดูแลข้อมูลจัดทำ/ส่งข้อมูลให้

    2.2 ข้อมูลลับ

    - ผู้ขอใช้เป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้บังคับบัญชา (ระดับส่วนขึ้นไป) เมื่อได้รับอนุมัติ แจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่งข้อมูลให้
    - ผู้ขอใช้เป็นพนักงานนอกฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้จัดการฝ่ายของตน และผู้จัดการฝ่ายผู้ดูแลตามลำดับเมื่อ ได้รับอนุมัติ แจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่งข้อมูลให้
    - ผู้ขอใช้เป็นบุคคลภายนอก ให้ขอจากสำนักตรวจสอบ หรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี โดยผู้พิจารณาอนุมัติต้องเป็นผู้บริหารระดับผู้บริหารสาย/ผู้อำนวยฝ่าย/ส่วน ขึ้นไป

2.3 ข้อมูลของบริษัท / ฝ่าย / ส่วน ที่อยู่ในระบบ IT

- ผู้ขอใช้เป็นพนักงานบริษัท แจ้งรายละเอียดเพื่อขออนุมัติ จากผู้บังคับบัญชาของตน (ระดับผู้จัดการฝ่ายขึ้นไป)
- ผู้ขอใช้เป็นบุคคลภายนอก ให้ขอจากสำนักตรวจสอบ หรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี โดยผู้พิจารณาอนุมัติ ต้องเป็นผู้บริหารระดับผู้บริหารสาย/ผู้จัดการฝ่าย/ส่วน ขึ้นไป
- เมื่อต้นสังกัด หรือสำนักตรวจสอบ หรือฝ่าย/ส่วนที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกอนุมัติแล้ว ให้ส่งเรื่องขออนุมัติใช้ข้อมูลไปยังสายงานที่ดูแล IT ผู้ดูแลข้อมูล(ระดับผู้จัดการฝ่ายขึ้นไป)
- เมื่อสายงานที่ดูแล IT ผู้ดูแลข้อมูล พิจารณาอนุมัติให้ใช้ข้อมูลได้ ผู้ดูแลข้อมูลจะสั่งการตามสายงานเพื่อให้เจ้าหน้าที่ผู้ดูแลจัดทำ / ส่ง / เปิดระบบให้ใช้ข้อมูล (ตามแต่วัตถุประสงค์ของผู้ขอ)
- กรณีผู้ขอใช้ เป็นบุคคลภายนอก จะส่งข้อมูลให้สำนักตรวจสอบ หรือฝ่าย/ส่วนที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี เพื่อดำเนินการติดต่อกับผู้ขอใช้(บุคคลภายนอก) ต่อไป
- เมื่อครบระยะเวลาใช้งาน หรือผู้ใช้แจ้งใช้งานเสร็จสิ้น (ก่อนครบกำหนด) ผู้ดูแลข้อมูลปิดระบบการเข้าใช้งาน

3. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (encryption) ทุกครั้ง

4.2 การควบคุมการกำหนดสิทธิและบัญชีรายชื่อผู้ใช้งาน

ผู้รับผิดชอบ

1. พนักงานของฝ่ายเทคโนโลยีสารสนเทศ
2. พนักงานขององค์กรทั้งหมด

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานการเข้ามาใช้งาน

1.1 บริษัทต้องกำหนดสิทธิการเข้าใช้งานของผู้ใช้งานเพื่อยืนยันตัวตนของผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์แยกเป็นรายบุคคล ดังต่อไปนี้

1.1.1 การขอ User name และ Password สำหรับพนักงานเข้าใหม่ ต้องมีการบันทึกการขอและมีการอนุมัติโดยผู้มีอำนาจที่กำหนดไว้

1.1.2 การขอรหัสผ่านใหม่ของพนักงานบริษัท เนื่องจากลืมรหัสผ่าน หรือถูกล็อกรหัสผ่าน จะต้องมีการยืนยันตัวตนของผู้ขอก่อนการให้รหัสผ่านใหม่ทุกครั้ง

1.2 พนักงานต้องเก็บและรักษา Password สำหรับทุกระบบงานที่ได้รับมอบมาให้เป็นความลับ

1.3 พนักงานต้องใช้ User Login และ Password ส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่พนักงานครอบครองใช้งานอยู่ โดย Password ส่วนบุคคลดังกล่าวต้อง

- มีความยาวไม่น้อยกว่า 8 ตัวอักษร
- มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและอักขระพิเศษเข้าด้วยกัน
- จะต้องมีการกำหนดวันหมดอายุการใช้งานของ Password เช่น ต้องเปลี่ยนทุก 90 วัน เป็นต้น และเมื่อครบกำหนดอายุการใช้งาน ต้องมีการบังคับให้เปลี่ยนรหัสผ่าน (Force Change)
- Password เก็บประวัติห้ามซ้ำกัน ย้อนหลัง 3 ครั้ง รวมที่ใช้ปัจจุบันเป็น 4 ครั้ง
- ไม่กำหนด Password ส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
- ไม่กำหนด Password ส่วนบุคคลจากคำศัพท์ที่ใช้ในพจนานุกรม
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรบังคับเปลี่ยนรหัสผ่านนั้นโดยทันที

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 โดยควรมีการสอบทานสิทธิอย่างน้อยทุกๆ 1 ปี

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 ระบบเมื่อใช้งานแล้วเสร็จ หรือเมื่อมิได้อยู่ที่หน้าเครื่องคอมพิวเตอร์หรือไม่ใช้งานเป็นเวลา 15 นาที ระบบจะ Logout อัตโนมัติ

2.5 อนุญาตให้ผู้ใช้งานใส่รหัสผิดไม่เกิน 5 ครั้ง ซึ่งระบบจะทำการล็อก ชื่อผู้ใช้งานดังกล่าวทันที โดยจะปลดล็อคเมื่อเวลาผ่านไป 30 นาที

3. กำหนดการควบคุมการใช้ User Root หรือ Administrator และขั้นตอนการเบิกใช้

3.1 บัญชีผู้ใช้งานในระดับพิเศษ เช่น Root หรือ Administrator ของระบบงานสารสนเทศทุกระบบ ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และมีการกำหนดระยะเวลาการเข้าถึงอย่างเหมาะสมกับการทำงานนั้น

3.2 บัญชีผู้ใช้งานในระดับพิเศษ เช่น Root หรือ Administrator สำหรับเข้าถึง Server, Database, Cloud, Co-location ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และมีการกำหนดระยะเวลาการเข้าถึงอย่างเหมาะสมกับการทำงานนั้น

3.3 บัญชีผู้ใช้งานสำหรับเข้าถึง Database ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น

4.3 การควบคุมของระบบฐานข้อมูล

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานการติดตั้งระบบฐานข้อมูล

1.1 ผู้ติดตั้งระบบฐานข้อมูล จะต้องเป็นพนักงานในฝ่ายเทคโนโลยีสารสนเทศ หรือพนักงานของบริษัท ซึ่งบริษัทได้มอบหมายให้ทำหน้าที่ดังกล่าว แต่ทั้งนี้จะต้องมีพนักงานในฝ่ายเทคโนโลยีสารสนเทศร่วมดำเนินการด้วย

1.2 ผู้ติดตั้งระบบฐานข้อมูลจะต้องใช้ซอฟท์แวร์ที่มีลิขสิทธิ์การใช้งานตามกฎหมาย

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

หากมีความจำเป็นต้องเพิ่มกลุ่มผู้ใช้งานใหม่ ต้องขออนุมัติอย่างเป็นลายลักษณ์อักษรกับผู้ช่วยกรรมการผู้จัดการสายงานสนับสนุน

2.2 มาตรฐานการอนุมัติการใช้งาน (Authorization)

- เมื่อผู้ใช้งานได้รับความเห็นชอบจากหัวหน้างานและผู้จัดการฝ่ายต้นสังกัด 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)
- 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 ฝ่ายเทคโนโลยีสารสนเทศ 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 ฝ่ายเทคโนโลยีสารสนเทศ ต้องพิจารณาจัดหา Media ทีมีประสิทธิภาพเพื่อใช้ในการสำรองข้อมูล
   6.2 ฝ่ายเทคโนโลยีสารสนเทศ และฝ่าย/ส่วนงานที่เกี่ยวข้อง ต้องร่วมกันพิจารณาถึงวิธีสำรอง และ ติดตั้งข้อมูลของแต่ละระบบงาน
   6.3 ฝ่ายเทคโนโลยีสารสนเทศ ต้องตรวจสอบการสำรองข้อมูลว่าทำสำเร็จหรือไม่ และหากไม่สำเร็จต้องดำเนินการแก้ไข
   6.4 การ Restore Data สามารถกระทำได้เฉพาะผู้ที่ได้รับมอบหมาย และได้รับการสั่งจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศเท่านั้น
   6.5 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดเก็บ Media ที่ใช้ในการสำรองข้อมูลไว้ในสภาพแวดล้อมที่เหมาะสมและมีระบบรักษาความปลอดภัยที่ดี
   6.6 ฝ่ายเทคโนโลยีสารสนเทศ ต้องตรวจสอบสภาพ Media และข้อมูลที่อยู่ใน Media อย่างสม่ำเสมอว่ายังอยู่ในสภาพที่ใช้งานได้ดีหรือไม่ หากพบปัญหาให้รีบดำเนินการแก้ไข

4.4 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

ผู้รับผิดชอบ

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. การติดตั้งเครื่องคอมพิวเตอร์ Server ต้องมีการจัดแบ่งหมวดหมู่ตามที่ฝ่ายเทคโนโลยีสารสนเทศได้กำหนดไว้
2. การติดตั้งเครื่องคอมพิวเตอร์ Server ต่างๆ ต้องมีการจัดทำแบบแปลนการติดตั้งอุปกรณ์บนตู้ Rack แสดงตำแหน่งต่างๆ ของอุปกรณ์บนตู้ Rack ในรูปแบบที่บริษัทระบุไว้ โดยจัดเก็บไว้ในฝ่ายเทคโนโลยีสารสนเทศ

3. การติดตั้งอุปกรณ์สื่อสารข้อมูล และอุปกรณ์รักษาความปลอดภัยต่าง ๆ ต้องมีการจัดทำแบบแปลนการติดตั้งบนตู้ Rack แสดงตำแหน่งต่างๆ ของอุปกรณ์บนตู้ Rack ในรูปแบบที่บริษัทระบุไว้ โดยจัดเก็บไว้ที่ฝ่ายเทคโนโลยีสารสนเทศ
4. การติดตั้งอุปกรณ์สื่อสารข้อมูลทุกชนิดกับระบบงานต่างๆ ของบริษัท ให้อยู่ในความควบคุมดูแลของส่วนงานสนับสนุนเทคโนโลยีสารสนเทศ
5. การติดตั้งอุปกรณ์ดับเพลิงอัตโนมัติ ระบบเครื่องปรับอากาศ และระบบเครื่องจ่ายไฟสำรองฉุกเฉิน จะต้องมีมาตรฐานตามที่องค์กร หรือผู้ผลิตกำหนดไว้

4.5 การรักษาความปลอดภัยระบบคอมพิวเตอร์เครือข่าย

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานในการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กรผ่านทางเครือข่าย

   1.1 ทำการติดตั้ง Service Pack ตลอดจน Patch ต่าง ๆ ให้ทันสมัยรวมทั้ง Software Antivirus ตามที่องค์กรกำหนด
2. กำหนดมาตรฐานในการติดต่อเข้า – ออกองค์กร โดยใช้ระบบเครือข่ายผ่าน VPN

   2.1 สำหรับเครื่องคอมพิวเตอร์ที่อนุญาตให้ติดตั้ง Client VPN สำหรับ Link Dial Up ผ่านทางระบบ Internet จากผู้มีอำนาจตามคู่มือ อำนาจดำเนินการของฝ่ายเทคโนโลยีสารสนเทศ ให้ทำการติดตั้ง Software Personal Firewall ด้วย
3. กำหนดมาตรฐานของระบบรักษาความปลอดภัยบนระบบเครือข่าย

   3.1 ต้องมีระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก

   3.2 ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

   - ความพยายามในการบุกรุกผ่านระบบเครือข่าย
   - การใช้งานในลักษณะที่ผิดปกติ
   - การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

   3.3 จัดหาอุปกรณ์รักษาความปลอดภัยที่ทันต่อความเปลี่ยนแปลงของภัยคุกคามทางด้านเครือข่าย โดยจัดให้มีการทบทวนภาพรวมของการรักษาความปลอดภัยบนเครือข่ายในทุกๆ 1 ปี เพื่อดำเนินการจัดหาอุปกรณ์ป้องกันต่อไป

   3.4 จัดเก็บทะเบียนเลขหมายประจำเครื่องคอมพิวเตอร์ (IP Address) ที่มีการควบคุมการใช้งาน

3.5 จัดทำและปรับปรุง Configuration ของระบบเครือข่ายให้มีความทันสมัยและปลอดภัยอยู่เสมอ

3.6 ทำการ Backup Configuration ของอุปกรณ์สื่อสารข้อมูลเป็นประจำทุก 6 เดือน หรือทุกครั้งที่มีการเปลี่ยนแปลง

3.7 จัดการเปลี่ยน Password ของอุปกรณ์สื่อสารขององค์กรทุกชุดทุก 3 เดือนและให้พิมพ์รายละเอียดของอุปกรณ์ Password ใส่ซองปิดผนึก และให้ผู้จัดการฝ่ายเทคโนโลยีเซ็นต์กำกับ และส่งต่อ Chief Executive Officer เพื่อเก็บรักษาไว้ รวมทั้งทำลายซอง Password เดิมทันทีหลังจากได้รับซอง Password ชุดใหม่

3.8 ห้ามใช้ Community Name ของอุปกรณ์สื่อสารข้อมูลทุกชนิดหรือ อุปกรณ์อื่นที่ใช้ Protocol SNMP ที่ถูกกำหนดชื่อมาโดยผู้ผลิตอุปกรณ์เมื่อเริ่มใช้งานกับระบบงานขององค์กร ให้ดำเนินการเปลี่ยนชื่อนั้นโดยทันที

3.9 สำหรับ Server ที่จะทำการติดตั้งเข้ากันเครือข่ายขององค์กร ฝ่ายเทคโนโลยีสารสนเทศ หรือพนักงานองค์กรหรือบริษัท ผู้ดูแลการติดตั้ง Server ดังกล่าวต้องส่งรายละเอียดของระบบปฏิบัติการ (Operating System) และ Service Pack หรืออื่น ๆ ที่จำเป็นสำหรับการติดตั้งให้กับฝ่ายเทคโนโลยีสารสนเทศรับทราบข้อมูลก่อน-หลัง จากนั้นจึงจะจ่าย IP Address ให้และให้ทำการ Monitor Port ที่จ่ายให้กับ Server ดังกล่าวไม่น้อยกว่า 1 สัปดาห์อย่างใกล้ชิดพร้อมกันรายงานผลต่อหัวหน้าหรือผู้จัดการฝ่าย

3.10 ให้ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้ถือกุญแจห้องอุปกรณ์สื่อสาร/ห้อง Server ขององค์กร

4. กำหนดมาตรฐานในการเชื่อมต่อกับเครือข่ายภายนอกองค์กร

4.1 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายขององค์กรต้องผ่านความเห็นชอบจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทุกกรณี

4.2 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายขององค์กรต้องเชื่อมต่อโดยต้องมีระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น

4.3 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากันระบบเครือข่ายขององค์กรให้ใช้วงจรที่เป็นวงจร Permanent (Leased Line, MPLS, VPN Client to Site, VPN Site-to-Site) เท่านั้น ไม่อนุญาตให้ทำในลักษณะ Link Dial Up

5. กำหนดให้มีการจัดทำแผนผังเครือข่ายขององค์กร

5.1 ให้มีการจัดทำแผนผังเครือข่ายขององค์กร และต้องปรับปรุงแผนผังดังกล่าวให้มีความทันสมัยอยู่เสมอ รวมทั้งจัดเก็บไว้ในสถานที่ที่มีความปลอดภัย

4.6 การป้องกันไวรัสคอมพิวเตอร์/ มัลแวร์

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. ติดตั้งและตรวจสอบเครื่องมือในการกำจัดไวรัสคอมพิวเตอร์/มัลแวร์

   1.1 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ สำหรับเครื่องแม่ข่ายให้บริการจดหมายอิเล็กทรอนิกส์ที่ Gateway (SMTP Gateway) เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้ง ต้องจัดให้มีการอัปเดต จากเจ้าของผลิตภัณฑ์นั้นๆ ทุก 24 ชั่วโมง

   1.2 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/ มัลแวร์สำหรับ HTTP เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้งต้องจัดให้มีการอัปเดตจากเจ้าของผลิตภัณฑ์นั้นๆ ทุก 24 ชั่วโมง

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

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

   1.5 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ให้กับ PC ขององค์กรทุกเครื่อง เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้งต้องจัดให้มีการอัปเดตจากเจ้าของผลิตภัณฑ์นั้นๆ ทุก 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/ มัลแวร์ขององค์กรอย่างน้อยเดือนละ 1 ครั้งต่อ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

5. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity risk

ความสำคัญ

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ เพื่อสร้างความมั่นใจว่าการซื้อหรือการพัฒนามีความสอดคล้องกับแผนงานของบริษัท มีหลักเกณฑ์ในการคัดเลือก พัฒนา มีการจัดลำดับความสำคัญของงาน รวมทั้งกระบวนการพัฒนาได้มีการทดสอบอย่างเพียงพอว่าระบบงานที่แก้ไขเปลี่ยนแปลงมีความถูกต้องและให้ผลลัพธ์ตามที่ได้กำหนดไว้

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

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

2. กำหนดให้จัดทำเอกสาร สิ่งส่งมอบขั้นต่ำ ตามที่แสดงไว้ในตารางด้านล่าง

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 - เอกสารหน้าจอสำหรับผู้ใช้งานเพื่อสามารถเปรียบเทียบกับความต้องการการใช้งานที่กำหนดไว้ในกระบวนการที่ 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 ต้องนำไปเก็บไว้กับผู้ที่ได้รับมอบหมายให้ดูแลรักษา

6. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

ความสำคัญ

บริษัท ต้องกำหนดวิธีการปฏิบัติในกรณีที่เกิดเหตุการณ์ฉุกเฉินในกรณีต่าง ๆ และกำหนดหน้าที่รับผิดชอบของตัวบุคคล พร้อมทั้งมีการซักซ้อมเป็นระยะ เพื่อให้เกิดผลกระทบต่อการบริการของบริษัทแก่ลูกค้าให้น้อยที่สุด และเพื่อให้การดำเนินการของบริษัท ยังสามารถดำเนินต่อได้โดยไม่ติดขัด

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดหน้าที่ความรับผิดชอบ
   - 1.1 ติดตั้งอุปกรณ์ Hardware ติดตั้งโปรแกรม OS และทดสอบการใช้งานให้มีความพร้อมในกรณีที่เกิดเหตุการณ์ฉุกเฉิน โดยฝ่ายเทคโนโลยีสารสนเทศ และส่วนพัฒนาระบบสารสนเทศ
   - 1.2 ติดตั้งอุปกรณ์เครือข่ายให้สามารถใช้งานได้ โดยส่วนเครือข่าย
   - 1.3 จัดหาอุปกรณ์อำนวยความสะดวก (Facility) ให้มีความพร้อมในการใช้งานโดยฝ่ายเทคโนโลยีสารสนเทศ
   - 1.4 นำข้อมูลสำรองชุดล่าสุดมาลงในระบบเพื่อใช้งาน โดยฝ่ายเทคโนโลยีสารสนเทศ
   - 1.5 ทดสอบการใช้งานเพื่อเตรียมความพร้อมอย่างสม่ำเสมอ โดยฝ่ายเทคโนโลยีสารสนเทศ และพัฒนาระบบสารสนเทศ
   - 1.6 กำหนดหน้าที่ความรับผิดชอบของพนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉิน
     - 1.6.1 พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉินต้องเข้ารับอบรมหรือสร้างความตระหนักเพื่อให้รู้หรือทราบวิธีปฏิบัติในกรณีที่เกิดเหตุฉุกเฉินในกรณีต่าง ๆ
     - 1.6.2 พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉินต้องร่วมซ้อมการใช้งานแผนสำรองฉุกเฉิน ซึ่งจะจัดขึ้นปีละ 1 ครั้ง

2. กำหนดมาตรฐานสำหรับห้องเซิร์ฟเวอร์สำรอง
   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 ในทุกๆ 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 พร้อมทั้งสำเนาขั้นตอนหรือวิธีการปฏิบัติงานต่างๆ 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

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. จัดทำขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer operator) และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ
2. กำหนดมาตรฐานการ Login เข้าใช้งานระบบ
   2.1 กำหนดให้มีระบบการตรวจสอบการ Login เข้ามาใช้งาน โดยต้องบันทึกข้อมูลที่เกี่ยวข้องกับการ Login นั้นไว้ และให้บันทึกทั้งการ Login ที่ทำได้สำเร็จ และไม่สำเร็จเพื่อใช้ในการตรวจสอบภายหลัง
3. ควรกำหนดให้มีการบันทึก (Log book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้
   - ผู้ปฏิบัติงาน
   - เวลาปฏิบัติงาน
   - รายละเอียดการปฏิบัติงาน
   - ปัญหาที่เกิดขึ้นและการแก้ไข
   - สถานะของระบบ
   - ผู้ตรวจทานการปฏิบัติงาน

การปฏิบัติงานประจำควรประกอบด้วย

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

8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นมีวัตถุประสงค์เพื่อให้บริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

ความสำคัญ

การกำหนดนโยบาย ระเบียบปฏิบัติ มาตรฐานและแนวทางในการคัดเลือกผู้ให้บริการภายนอกจะช่วยให้การตัดสินใจที่จะได้รับประสิทธิผลที่ดีขึ้น ซึ่งจะส่งผลต่อค่าใช้จ่ายที่เหมาะสมในการเลือกใช้บริการ และผลของการให้บริการเป็นไปตามที่คาดหวังไว้

ผู้รับผิดชอบหลัก

1. ประธานเจ้าหน้าที่บริหาร
2. ประธานเจ้าหน้าที่ฝ่ายขายและการตลาด
3. พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

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 การศึกษาจากรายงานและข้อมูลต่าง ๆ

3.2 ต้องมีการกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือการให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การปรับปรุงเทคโนโลยี ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

9. การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ Cloud Computing

วัตถุประสงค์

เพื่อให้บริษัทมีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่สอดคล้องกับความต้องการของกิจการรวมทั้งดูแลให้มีการนำเทคโนโลยีสารสนเทศในส่วนที่เป็นเทคโนโลยีที่เกี่ยวกับบริการคลาวด์ มาใช้ในการสนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความสี่ยง รวมถึงเพื่อให้กิจการสามารถรรวัตถุประสงค์และเป้าหมายหลักของกิจการ โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลกิจการ

ความสำคัญ

ในปัจจุบันมีการประยุกต์ใช้งานเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งในการสนับสนุนและดำเนินกิจกรรมสำคัญ ในการขับเคลื่อนธุรกิจ หนึ่งในเทคโนโลยีที่มีการประยุกต์ใช้อย่างกว้างขวาง คือ การใช้บริการระบบประมวลผลร่วมกันผ่านเครือข่ายตามความต้องการของผู้ใช้งาน (Cloud Computing) ทั้งเพื่อเพิ่มขีดความสามารถในการประมวลผล และเพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการบริหารจัดการต้นทุนด้านเทคโนโลยีอย่างมีนัยสำคัญ การประยุกต์ใช้งาน Cloud Computing เป็นรูปแบบการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อบริหารจัดการความต้องการทรัพยากรในการประมวลผลตามความต้องการของผู้ใช้งาน ซึ่งอาจมีการกำหนดขอบเขตการใช้งานทรัพยากรการประมวลผลดังกล่าวอย่างเฉพาะเจาะจงสำหรับผู้หนึ่งผู้ใด หรืออาจมีการใช้งานร่วมกันของกลุ่มผู้ใช้งานและนิติบุคคล

เพื่อประสิทธิภาพในการใช้บริหารจัดการทรัพยากรและต้นทุนอย่างเหมาะสม การใช้งานทรัพยากรร่วมกันบนเครือข่ายส่งผลให้เกิดความซับซ้อนด้านเทคโนโลยี รวมถึงความเสี่ยงอันอาจจะเกิดขึ้นต่อสารสนเทศที่ถูกจัดเก็บอยู่บนเครือข่ายที่มีการบริหารจัดการโดยบุคคลภายนอก หรือผู้ให้บริการ Cloud Computing

ผู้รับผิดชอบหลัก

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. บริษัทได้กำหนดแนวทางการกำกับดูแลและบริหารจัดการการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ตามความต้องการของผู้ใช้งาน หรือ Cloud Computing ที่ครอบคลุมกระบวนการสำคัญตั้งแต่การกำหนดกรอบการกำกับดูแลการใช้งาน Cloud Computing การกำหนดแนวทางเชิงกลยุทธ์ในการใช้งาน การกำกับผู้ให้บริการ ตลอดจนการยกเลิกหรือสิ้นสุดการใช้งาน
2. ประเภทของ Cloud Computing (Service Models) ที่อนุญาตให้ใช้งาน

2.1. Software-as-a-Service (SaaS) หมายถึง บริการด้านแอปพลิเคชันที่ทำงานบนโครงสร้างพื้นฐานระบบ Cloud Computing ซึ่งผู้ใช้บริการสามารถเข้าใช้งานแอปพลิเคชันผ่านเครือข่ายผ่านโปรแกรมบนอุปกรณ์ของผู้ใช้บริการ เช่น เว็บเบราว์เซอร์ แอปพลิเคชันบนมือถือ เป็นต้น โดยผู้ให้บริการทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งครอบคลุมถึง ความปลอดภัยทางกายภาพระบบปฏิบัติการ ระบบเครือข่าย ระบบจัดเก็บข้อมูล รวมถึงค่าพื้นฐานของแอปพลิเคชัน

2.2. Platform-as-a- Service (PaaS) หมายถึง บริการด้านแฟลตฟอร์มที่ทำงานบนโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งผู้ใช้บริการสามารถเข้าแฟลตฟอร์มในการพัฒนาแอปพลิชั่น โดยผู้ให้บริการทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งครอบคลุมถึง ความปลอดภัยทางกายภาพระบบปฏิบัติการ ระบบเครือข่าย และระบบให้บริการ เช่น เว็บเซอร์วิส ระบบจัดการฐานข้อมูล เป็นต้น อย่างไรก็ตาม การควบคุมที่เกี่ยวกับการบริหารจัดการแอปพลิเคชัน เช่น การแก้ไขเปลี่ยนแปลงโปรแกรม ผู้ใช้บริการจะเป็นผู้ดำเนินการ

2.3. Infrastructure-as-a-Service (IaaS) หมายถึง บริการด้านโครงสร้างพื้นฐานระบบคลาวด์ที่มีการใช้งานทรัพยากรทางด้านระบบสารสนเทศร่วมกัน เช่น ระบบปฏิบัติการ ระบบเครือข่าย หรือระบบจัดเก็บข้อมูลโดยทางผู้ให้บริการทำหน้าที่ดูแลทางกายภาพ และทรัพยากรสารสนเทศที่ใช้ในการสนับสนุนการทำงานของโครงสร้างพื้นฐานระบบคลาวด์

3. รูปแบบของการนำไปใช้งาน (Deployment Models)

3.1. Public Cloud หมายถึงโครงสร้างพื้นฐานระบบคลาวด์ที่เปิดให้ใช้งานผ่านเครือข่ายสาธารณะ

3.2. Private Cloud หมายถึง โครงสร้างพื้นฐานระบบคลาวด์ที่จัดเตรียมไว้สำหรับการใช้งานโดยหน่วยงานภายในองค์กรเดียวกัน

3.3. Hybrid Cloud หมายถึง โครงสร้างพื้นฐานระบบคลาวด์ที่ประกอบด้วยโครงสร้างพื้นฐานระบบคลาวด์ ที่แตกต่างกันตั้งแต่สองรูปแบบขึ้นไป (Public และ Private)

4. การประเมินความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัย ทางไซเบอร์จากการใช้งาน Cloud Computing

5. ประเมินความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัย ทางไซเบอร์จากการใช้งาน Cloud Computing

5.1. ความเสี่ยงด้านกลยุทธ์ เช่น ความเสี่ยงจากการพึ่งพิงผู้ให้บริการภายนอกและความสามารถในการเปลี่ยนแปลงผู้ให้บริการ (vendor locked-in)

5.2. ความเสี่ยงด้านปฏิบัติการ เช่น ระบบประมวลผลผิดพลาดจากระบบให้บริการหรือบุคลากรผู้ให้บริการ การใช้งานเทคโนโลยีร่วมกัน (Share technology risk) การละเมิดข้อกำหนดและข้อตกลงการใช้งาน Cloud Computing หรือความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลหรือการจำกัดการเข้าถึงของข้อมูลจากผู้ให้บริการ

5.3. ความเสี่ยงด้านกฎหมาย เช่น การไม่ปฏิบัติตามกฎหมาย หลักเกณฑ์และข้อกำหนดของทางการ ทั้งภายในประเทศและต่างประเทศ

5.4. ความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น การเรียกใช้โปรแกรม (APIs) หรือช่องทางบริหารจัดการที่ไม่ปลอดภัย

5.5. ความเสี่ยงด้านข้อมูลส่วนบุคคล (data privacy) และการรักษาความปลอดภัยของข้อมูล (data security)

5.6. ความเสี่ยงจากการใช้ผู้ให้บริการภายนอกที่มีการใช้ผู้ให้บริการภายนอกอื่นรับช่วงจัดการงาน (sub-contract)

6. จัดเตรียมและพัฒนาองค์ความรู้ด้านการบริหารจัดการ Cloud Computing ให้แก่ผู้ดูแลระบบ (Administrator) และบุคลากรที่เกี่ยวข้องอย่างเพียงพอ

7. กำหนดให้มีการประเมินและคัดเลือกผู้ให้บริการ (Due Diligence) ดังนี้

7.1. ตรวจสอบความพร้อมและพิจารณาความเหมาะสมของผู้ให้บริการเพื่อให้มั่นใจว่าผู้ให้บริการสามารถให้บริการได้อย่างต่อเนื่อง โดยคำนึงถึงปัจจัยสำคัญ ได้แก่ ความรู้ความสามารถ ประสบการณ์ ความสามารถทางการเงินที่สามารถ ในการให้บริการอย่างต่อเนื่อง

7.2. ประเมินมาตรฐานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ได้แก่ การรักษาความลับข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และ ความต่อเนื่องของการให้บริการ (Availability) เช่น ผลการประเมินมาตรฐานความปลอดภัยที่เป็นที่ยอมรับในสากล ได้แก่ ISO27001, ISO27017, PCI/DSS, TIA เป็นต้น

7.3. ประเมินผลรายงานการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ ด้านมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น System and Organization Control (SOC) Report โดยพิจารณาถึงขอบเขตการตรวจสอบ ระยะเวลาที่ครอบคลุมในรายงานการตรวจสอบ ผลการตรวจสอบและประเด็นสำคัญในผลการตรวจสอบ nv

7.4. ประเมินความสอดคล้องกันของแนวทางการรักษาความต่อเนื่องของการให้บริการของผู้ให้บริการระบบ Cloud Computing และผลการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) ของระบบงานที่จะมีการใช้บริการบนระบบ Cloud Computing อันประกอบไปด้วย ระยะเวลาการหยุดชะงักของระบบให้บริการที่ยอมรับได้ (Maximum Tolerable Downtime: MTD) ระยะเวลาที่ยอมรับได้ในการกู้คืนระบบงานและข้อมูล (Recovery Time Objective: RTO) และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective: RPO)

7.5. ประเมินความเสี่ยงและแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และความต่อเนื่องในการให้บริการในกรณีที่ผลการประเมินผู้ให้บริการไม่เป็นไปตามข้อกำหนดหรือมาตรฐานความปลอดภัยที่กำหนดไว้

8. จัดทำสัญญาและข้อตกลงการให้บริการ (Engage) ซึ่งมีรายละเอียดในเรื่องดังต่อไปนี้เป็นอย่างน้อย

8.1. หน้าที่และความรับผิดชอบของผู้ให้บริการ รวมถึงความรับผิดชอบต่อบริษัทในกรณีที่ผู้ให้บริการ ไม่สามารถปฏิบัติตามข้อตกลงได้

8.2. ขอบเขตการให้บริการ ประเภท และเงื่อนไขการให้บริการ

8.3. เงื่อนไขความเป็นเจ้าของข้อมูลของผู้ใช้บริการ สิทธิการใช้และลิขสิทธิ์ที่เกี่ยวข้อง โดยผู้ใช้บริการควรเป็นเจ้าของสิทธิในข้อมูล

8.4. ข้อกำหนดด้านเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามที่กำหนดในข้อตกลง ทั้งนี้ บริษัทควรพิจารณาถึงเงื่อนไขการประเมินความเสียหาย รวมถึงข้อจำกัดในกรณีมีเงื่อนไขการจำกัด ความรับผิดในสัญญาระหว่างผู้ใช้บริการและผู้ให้บริการ

8.5. ข้อกำหนดด้านการเข้าถึงข้อมูลของผู้ให้บริการ ประกอบด้วยสิทธิการเข้าถึงและเงื่อนไขการเปิดเผยข้อมูล โดยผู้ให้บริการจากความยินยอมของผู้ใช้บริการ หรือการเปิดเผยข้อมูลโดยข้อกำหนดทางกฎหมายของประเทศ ที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล ทั้งนี้ ต้องมีการแจ้งให้ผู้ใช้บริการรับทราบ

8.6. ข้อกำหนดด้านการสำรองข้อมูลและการจัดทำแผนสำรองฉุกเฉิน และแผนความต่อเนื่องทางธุรกิจสำหรับ การให้บริการ โดยมีเงื่อนไขที่ชัดเจนทางด้าน

- สถานที่ในการกู้คืนข้อมูล (Location)
- ระยะเวลากู้คืนระบบให้บริการ (Service Restoration)
- ระยะเวลากู้คืนข้อมูล (Recovery Time Objective: RTO)
- ชุดข้อมูลล่าสุดที่กู้คืนได้ (Recovery Point Objective: RPO)

8.7. ข้อกำหนดและเงื่อนไขการส่งมอบข้อมูลเมื่อมีการยกเลิก หรือสิ้นสุดการใช้บริการ

8.8. ข้อกำหนดด้านเงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (Subcontract of the cloud provider)

8.9. ข้อกำหนดและมาตรการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ

8.10. ข้อกำหนดด้านสิทธิในการตรวจสอบ (Rights to Audit)

8.11. ช่องทางติดต่อและผู้รับผิดชอบด้านปัญหาการใช้งาน และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ของผู้ให้บริการ

9. บริษัทฯ กำหนดให้มีการติดตาม และ ประเมินผลด้านประสิทธิภาพและการปฏิบัติตามข้อตกลงการให้บริการ อย่างน้อยปีละ 1 ครั้ง
10. ติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ
11. ต้องพิจารณาความเสี่ยงที่เกี่ยวข้องในการยกเลิกการใช้บริการระบบประมวลผลร่วมกันผ่านเครือข่าย อย่างรอบด้าน เพื่อกำหนดกลยุทธ์และจัดทำแผนการยกเลิกการใช้บริการอย่างเหมาะสม เพื่อป้องกันหรือลดผลกระทบ อันอาจจะเกิดขึ้นจากความเสี่ยง เช่น ความเสี่ยงด้านการหยุดชะงักของระบบให้บริการ ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความลับข้อมูล ความเสี่ยงด้านความถูกต้องของระบบประมวลผล เป็นต้น

10. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ โน้ตบุค โทรศัพท์และอุปกรณ์คอมพิวเตอร์ของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

ความสำคัญ

การควบคุมการใช้งานเครื่องคอมพิวเตอร์ โน้ตบุค โทรศัพท์และอุปกรณ์คอมพิวเตอร์อย่างเพียงพอจะเป็นการป้องกันการสูญเสียทรัพย์สิน เช่น การใช้งานไม่ถูกต้อง ขาดกการบำรุงรักษาอย่างสม่ำเสมอ ดังนั้นบริษัทต้องมีการควบคุมเพื่อให้มีการใช้งานทรัพย์สินสารสนเทศอย่างถูกต้อง และเหมาะสม

ผู้รับผิดชอบหลัก

1. พนักงานของฝ่ายเทคโนโลยีสารสนเทศ
2. ผู้ใช้งานทรัพย์สินสารสนเทศ

ระเบียบปฏิบัติ

1. ผู้ใช้งานเครื่องคอมพิวเตอร์ โน้ตบุค โทรศัพท์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
2. ห้ามใช้เครื่องคอมพิวเตอร์ โน้ตบุค โทรศัพท์ และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้าหรือบริการใด ๆ ที่เป็นของส่วนตัว และไม่เหมาะสม
3. ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ โน้ตบุค โทรศัพท์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน โดยโปรแกรมซอฟแวร์มาตรฐานประกอบไปด้วย

   - โปรแกรมในกลุ่ม Antivirus

   - โปรแกรมจัดการงานเอกสาร ได้แก่ Microsoft Office, Office 365

   - โปรแกรมจัดการเอกสาร PDF ได้แก่ PDF, Adobe Reader

   - โปรแกรม ERP ได้แก่ SAP, SML Account

   - โปรแกรมสำหรับงานผลิต ได้ RMX Express

   - โปรแกรมสำหรับงานจัดส่ง ได้แก่ Terminus, LiveFleet Xsense, DTC

   - โปรแกรมสำหรับงานเขียนแบบที่บริษัทฯ ได้ทำการจัดซื้อแบบถูกลิขสิทธิ์ได้แก่ Auto Cad, Takla

   - โปรแกรมสำหรับงานกราฟฟิคดีไซด์ที่บริษัทฯ ได้ทำการจัดซื้อแบบถูกลิขสิทธิ์

4. ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม

5. ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน มีฝุ่นละออง และต้องระวังการตกกระทบในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน

6. ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่

7. ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน

8. บริษัทฯ กำหนดให้มีการติดตาม และ ประเมินผลด้านประสิทธิภาพของคอมพิวเตอร์ โน้ตบุค โทรศัพท์ อย่างน้อย ปีละ 3 ครั้ง

11. การอนุรักษ์พลังงานในบริษัท

วัตถุประสงค์

กำหนดให้ทุกคนมีส่วนร่วมในประหยัดพลังงาน และใช้พลังงานอย่างคุ้มค่าเกิดประโยชน์สูงสุด

ความสำคัญ

ปลูกจิตสำนักการใช้พลังงานแก่พนักงานในบริษัท เพื่อการควบคุมการใช้พนักงานในบริษัทให้เกิดประโยชน์สูงสุด

ผู้รับผิดชอบหลัก

พนักงานของฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

กำหนดให้ทุกคนในฝ่ายเทคโนโลยีสารสนเทศ มีส่วนร่วมในการบริหารจัดการพลังงานในบริษัท โดยต้องร่วมรับผิดชอบ และยึดถือปฏิบัติตามมาตรการการอนุรักษ์พลังงานที่ได้จัดทำขึ้นมาดังนี้

1. ไฟฟ้า และแสงสว่าง
   1.1. ปิดไฟช่วงพักกลางวัน และปิดไฟฟ้าที่ไม่ได้ใช้งาน
   1.2. ปลดหลอดไฟฟ้าบริเวณที่ไม่ใช้งาน หรือไม่จำเป็นออก
   1.3. ทำความสะอาดหลอดไฟอย่างสม่ำเสมอ
   1.4. ใช้แสงธรรมชาติ (Daylight) แทนหลอดไฟ
2. ระบบปรับอากาศ และระบายอากาศ
   2.1. เปิดเครื่องปรับอากาศก่อนเวลาทำงานเพียง 15 นาที หรือน้อยกว่า
   2.2. ปิดเครื่องปรับอากาศก่อนเวลาเลิกงาน 15-30 นาที หรือมากกว่า
   2.3. ปิดเครื่องปรับอากาศช่วงพักกลางวัน และไม่เปิดประตูหรือหน้าต่างทิ้งไว้เพื่อป้องกันความชื้น และความร้อนจากภายนอก
   2.4. ตั้งอุณหภูมิของเครื่องปรับอากาศในฤดูฝน, ฤดูหนาว ตั้งอุณหภูมิที่ 26.00 °C และฤดูร้อนตั้งอุณหภูมิที่ 25.00 °C

2.5. ปิดประตูหน้าต่างบริเวณปรับอากาศตลอดเวลา

2.6. นำสัมภาระ เอกสาร ฯลฯ ที่ไม่ใช้งานนำไปเก็บบริเวณที่ไม่ได้ปรับอากาศ

3. Computer และเครื่อง Printer

3.1. ปิดหน้าจอ Computer ทุกครั้งที่ไม่ใช้งาน

3.2. ปิดสวิตช์เครื่อง Printer เมื่อไม่ใช้งาน

3.3. ดึงปลั๊ก Computer และเครื่อง Printer ออกหลังเลิกงาน

การพิจารณาโทษทางวินัยและการเรียกค่าเสียหาย

1. พนักงานและลูกจ้างที่ฝ่าฝืนข้อกำหนดนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยจงใจหรือประมาทเลินเล่อ และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและความรับผิดทางแพ่งและอาญาแก่พนักงานและลูกจ้างนั้น ตามกฎหมาย ข้อบังคับ ระเบียบ หรือประกาศที่เกี่ยวข้อง ผู้บังคับบัญชาผู้ใด งดเว้น หรือละเว้นการปฏิบัติตามหน้าที่ และเป็นเหตุให้พนักงานหรือลูกจ้างที่อยู่ภายใต้การบังคับบัญชาของตน ฝ่าฝืนข้อกำหนดของนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ ให้นำบทบัญญัติในวรรคก่อนมาใช้บังคับโดยอนุโลม
2. การฝ่าฝืนข้อกำหนดใดๆ ตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ แม้จะไม่ก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใดก็ตาม ถ้าผู้บังคับบัญชาเห็นว่ามีเหตุอันสมควร อาจจะบันทึกในประวัติการปฏิบัติงานและจะใช้เป็นข้อมูลประกอบการพิจารณาต่ออายุสัญญาจ้าง การขึ้นเงินเดือน หรือ เลื่อนตำแหน่งด้วยก็ได้

กิจกรรมการควบคุม

- การกำหนดฝ่ายเทคโนโลยีสารสนเทศ
  บริษัทฯ จัดให้มีฝ่ายเทคโนโลยีสารสนเทศเพื่อรองรับการปฏิบัติงานด้านสารสนเทศ และแผนงานที่เกี่ยวข้องในอนาคต รวมถึงการพัฒนาระบบ ERP ของบริษัท

- การแบ่งแยกหน้าที่ที่สำคัญ
  บริษัทฯ มีการควบคุมการแบ่งแยกหน้าที่ที่สำคัญของระบบงานสารสนเทศ ซึ่งได้แก่ผู้ดูแลระบบและผู้ใช้ระบบ เจ้าหน้าที่ปฏิบัติการ และเจ้าหน้าที่พัฒนาระบบสารสนเทศ ออกจากกัน และกำหนดในผังโครงสร้างองค์กรอย่างชัดเจน

- กำหนดนโยบาย แผนงานด้านสารสนเทศ
  บริษัทฯ มีการกำหนดแผนการปฏิบัติงาน และระยะเวลาที่ชัดเจน เพื่อให้เชื่อมันได้ว่าระบบสารสนเทศของบริษัทจะมีการพัฒนาจนสามารถใช้งานได้เต็มระบบและตอบสนองต่อความต้องการของผู้ใช้งานและเกิดประโยชน์สูงสุดต่อบริษัทฯ

- การจัดทำและการควบคุมงบประมาณ
  มีการกำหนดงบประมาณการจัดซื้อทรัพยากรสารสนเทศไว้อย่างชัดเจน รวมถึงบริษัทฯ มีการกำหนดคุณสมบัติของอุปกรณ์ที่เหมาะสมกับการใช้งานเพื่อเป็นแนวทางในการจัดซื้อ

- การกำหนดระเบียบปฏิบัติของผู้ใช้งานระบบสารสนเทศ
  บริษัทฯ มีการจัดอบรมในเรื่องระเบียบปฏิบัติของผู้ใช้งาน เพื่อใช้เป็นแนวทางในการปฏิบัติงาน

- การควบคุมการเข้าใช้ระบบงาน
  บริษัทฯ มีการควบคุมให้มีการเข้าใช้งานของระบบงานที่สำคัญโดยการกำหนดรหัสผ่าน และกำหนดสิทธิการเข้าถึงข้อมูลตามอำนาจที่ผู้ปฏิบัติงานได้รับ

- การควบคุมเครือข่าย
  มีการควบคุมการเข้าใช้งานเครือข่าย และมีการสอบทานการใช้งานอย่างสม่ำเสมอเพื่อพิจารณารายการผิดปกติ

- การควบคุมทางกายภาพ
  มีการแบ่งแยกห้องเซิร์ฟเวอร์ออกจากพื้นที่ปฏิบัติงานของส่วนงานอื่น ๆ และมีการควบคุมการเข้า - ออกห้องคอมพิวเตอร์ รวมถึงการควบคุมให้มีอุปกรณ์ป้องกันสำหรับเหตุฉุกเฉิน

- การป้องกันการหยุดชะงักของระบบสารสนเทศ
  บริษัทฯ กำหนดให้มีการสำรองข้อมูล รวมถึงการเตรียมความพร้อมในการปฏิบัติงานในกรณีที่มีเหตุฉุกเฉินเพื่อให้ระบบงานสารสนเทศของบริษัทสามารถทำงานต่อไปได้

- การป้องกันและความปลอดภัยของข้อมูล
  มีการใช้โปรแกรมป้องกันไวรัสและมีการปรับปรุงอย่างสม่ำเสมอ

- การควบคุมการจัดเก็บข้อมูลตามข้อกำหนดของหน่วยงานราชการ
  บริษัทฯ มีการกำหนดให้จัดเก็บรายการงานตามที่หน่วยงานราชการกำหนดไว้อย่างครบถ้วน