บริษัท เอสทีซี คอนกรีตโปรดัคท์ จำกัด (มหาชน)
นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

Document Revision History

Version	Date	Created / Modified by	Reviewed by	Changes Made
V1	21/07/2014	Siwapol Osodsit	Amonwan Chaitrakulthong	Initial Document
V2	25/12/2017	Charif Polkerdsuk	Amonwan Chaitrakulthong	Initial Document
V3	20/02/2018	-	Amonwan Chaitrakulthong	Initial Document
V4	04/04/2019	Amonwan Chaitrakulthong	Amonwan Chaitrakulthong	Initial Document
V5	22/04/2020	Amonwan Chaitrakulthong	Amonwan Chaitrakulthong	Initial Document
V6	22/09/2021	Amonwan Chaitrakulthong	Amonwan Chaitrakulthong	Initial Document
V7	24/11/2022	Amonwan Chaitrakulthong	Amonwan Chaitrakulthong	Initial Document
V8	21/12/2023	Amonwan Chaitrakulthong	Amonwan Chaitrakulthong	Initial Document
V9	13/08/2024	Amonwan Chaitrakulthong	Amonwan Chaitrakulthong	Initial Document

สารบัญ

หน้า

1. วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

บริษัทฯ ได้ตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติของพนักงานในองค์กร เพื่อให้พนักงานมีความตระหนักถึงความปลอดภัยของเทคโนโลยี และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศของบริษัท และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา รวมทั้งเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัท ด้านอื่นๆ ที่มุ่งเน้นการปฏิบัติงานภายในบริษัทให้มีความมั่นคงปลอดภัยในการดำเนินกิจการของบริษัท

2. ความมั่นคงปลอดภัยสำหรับสารนสนเทศ และแนวทางในการรักษาความปลอดภัย

ความมั่นคงปลอดภัยสำหรับสารสนเทศ หมายถึง การสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศ เพื่อป้องกันความเสียหายที่มีต่อองค์ประกอบด้านความมั่นคงปลอดภัย 3 ส่วนดังนี้

1. **Confidentiality** ทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงโดยบุคคลที่ได้รับอนุญาตแล้วเท่านั้น
2. **Integrity** ทรัพย์สินสารสนเทศจะต้องมีความถูกต้องและสมบูรณ์
3. **Availability** ทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงได้เมื่อมีความจำเป็นที่ต้องใช้งาน

บริษัทจะต้องกำหนดมาตรการเพื่อรักษาความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศโดยบริษัทจะใช้แนวทางดังนี้ ในการรักษาความมั่นคงปลอดภัย

นโยบายความมั่นคงปลอดภัย (Security Policy) ซึ่งจะประกอบด้วยระเบียบปฏิบัติต่าง ๆ ที่พนักงานต้องปฏิบัติตามโดยเคร่งครัด

ขั้นตอนการปฏิบัติ (Procedure) ระเบียบบางข้ออาจจะมีการอ้างอิงถึงการปฏิบัติงานที่เกี่ยวข้อง

3. ขอบเขตของการสร้างความมั่นคงปลอดภัย

เอกสารฉบับนี้มีขอบเขตครอบคลุมถึงการสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศต่าง ๆ ของบริษัท ดังนี้

- พนักงานและลูกจ้างของบริษัททั้งหมด
- ข้อมูล /สารสนเทศของบริษัท
- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต่าง ๆ ขององค์กร
- เครื่องคอมพิวเตอร์ส่วนบุคคล
- เครื่องคอมพิวเตอร์แบบพกพา
- อุปกรณ์เครือข่าย
- ระบบไฟฟ้าสำรอง
- สายสัญญาณเครือข่าย
- ซอฟแวร์ระบบ ซอฟแวร์จ้างพัฒนา ซอฟแวร์สำเร็จรูป
- สื่อบันทึกข้อมูล
- เอกสารของบริษัท

4. นโยบายความมั่นคงปลอดภัย

นโยบายด้านความมั่นคงปลอดภัยครอบคลุมนโยบาย 8 ด้าน ดังนี้

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และป้องกันความเสียหาย (Physical Security)
4. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
5. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบคอมพิวเตอร์ (Chang Management)
6. การสำรองข้อมูล และระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
7. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)
9. การทำลายสื่อบันทึกข้อมูล (Media Disposal)

สาระสำคัญของนโยบายมีดังต่อไปนี้

1) นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ เพื่อจัดทำนโยบายให้สามารถรองรับความเสี่ยงที่เกิดขึ้นได้ รวมทั้งการประกาศใช้นโยบายให้แก่บุคลากรที่เกี่ยวข้องได้ตระหนักและปฏิบัติตามนโยบายความปลอดภัยของด้านเทคโนโยลีสารสนเทศที่กำหนดไว้

2) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องจัดให้มีการแบ่งแยกหน้าที่การปฏิบัติงานระหว่างบุคลากรภายในแผนกเทคโนโลยีสารสนเทศอย่างเพียงพอ เพื่อช่วยให้มีการสอบยันการปฏิบัติงานอย่างเพียงพอเหมาะสม รวมทั้งการมีขอบเขตการปฏิบัติงานของพนักงานที่ชัดเจนและมีบุคลากรที่เพียงพอต่อการปฏิบัติงานของแผนกเทคโนโลยีสารสนเทศ

3) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) ซึ่งมีสาระสำคัญดังนี้

การควบคุการเข้าออกศูนย์คอมพิวเตอร์อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าศูนย์คอมพิวเตอร์และ ความเสียหายอันจะเกิดจาดอุปกรณ์หรือระบบต่างๆ เช่นระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ซึ่งย่อมมีความเสี่ยงต่ออุปกรณ์และข้อมูลของบริษัท ดังนั้นบริษัทต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงศูนย์คอมพิวเตอร์ได้ และการเข้าถึงดังกล่าวต้องมีการอนุมัติอย่างเพียงพอ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้ระบบป้องกันความเสียหายที่จะเกิดขึ้น

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

บริษัทต้องควบคุมความปลอดภัยของข้อมูลเพื่อป้องกันความเสี่ยงจากการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลของบริษัท ตั้งแต่ระดับข้อมูลข่าวสารทั่วไป จนถึงระดับข้อมูลข่าวสารที่ลับที่สุด และควรจะมีหน่วยงานที่มีหน้าที่ควบคุมหรืออนุมัติกาที่จะเผลแพร่ข้อมูลข่าวสารให้กับหน่วยงานอื่นๆ หรือนำข้อมูลออกไปเผยแพร่ภายนอกองค์การ ซึ่งอาจส่งผลให้เกิดข้อมูลถูกทำลาย หรือนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต ดังนั้นการกำหนดนโยบายการรักษาความปลอดภัยของข้อมูลระบบคอมพิวเตอร์ และระบบเครือข่ายรวมทั้งวิธีการปฏิบัติงานอย่างเพียงพอจะช่วยป้องกันความเสี่ยงที่จะเกิดขึ้นได้

5) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management) ซึ่งมีสาระสำคัญดังนี้

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ เพื่อสร้างความมั่นใจว่าการซื้อหรือการพัฒนามีความเหมาะสม รวมทั้งกระบวนการพัฒนาได้มีการทดสอบอย่างเพียงพอว่าระบบงานที่แก้ไขเปลี่ยนแปลงมีความถูกต้อง และให้ผลลัพธ์ตามที่ได้กำหนดไว้

6) การสำรองข้อมูล และระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องมีการสำรองข้อมูลและกำหนดหน้าที่รับผิดชอบของตัวบุคคล เพื่อให้เกิดผลกระทบต่อการบริการของบริษัทแก่ลูกค้าให้น้อยที่สุด และเพื่อให้การดำเนินการของบริษัท ยังสามารถดำเนินต่อได้โดยไม่ติดขัด

7) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องกำหนดวิธีการปฏิบัติงานประจำด้านคอมพิวเตอร์ไว้เป็นลายลักษณ์อักษร เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ และควรมีการจดบันทึกผลการจัดทำบันทึกผลการปฏิบัติงานไว้เพื่อให้สามารถตรวจสอบได้ว่ามีการจัดทำอย่างครบถ้วนและเป็นไปตามวิธีการปฏิบัติงานที่กำหนดไว้

8) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ซึ่งมีสาระสำคัญดังนี้

การกำหนดนโยบาย ระเบียบปฏิบัติ มาตรฐานและแนวทางในการคัดเลือกผู้ให้บริการภายนอกจะช่วยในการตัดสินใจที่จะได้รับประสิทธิผลที่ดีขึ้น ซึ่งจะส่งผลต่อค่าใช้จ่ายที่เหมาะสมในการเลือกใช้บริการและผลของการให้บริการเป็นไปตามที่คาดหวังไว้

9) การทำลายสื่อบันทึกข้อมูล (Media Disposal) ซึ่งมีสาระสำคัญดังนี้

การกำหนดนโยบาย ระเบียบปฏิบัติในการทำลายสื่อบันทึกข้อมูลเพื่อกำหนดแนวทางการทำงานให้แก่ผู้ปฏิบัติงานของเจ้าหน้าที่และเพื่อป้องกันไม่ให้ข้อมูลสารสนเทศที่สำคัญของบริษัทฯ รั่วไหลสู่ภายนอก

5. ระเบียบปฏิบัติ

นโยบายแต่ละด้านจะประกอบไปด้วยระเบียบปฏิบัติที่พนักงานหรือผู้ที่เกี่ยวข้องต้องปฏิบัติตามโดยเคร่งครัด ดังต่อไปนี้

1) นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ความสำคัญ

บริษัทต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ เพื่อจัดทำนโยบายให้สามารถรองรับความเสี่ยงที่เกิดขึ้นได้ รวมทั้งการประกาศใช้นโยบายให้แก่บุคลากรที่เกี่ยวข้องได้ตระหนักและ ปฏิบัติตามนโยบายความปลอดภัยของด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

ผู้รับผิดชอบหลัก

ผู้บริหารระดับสูง
ผู้อำนวยการฝ่ายบัญชีและการเงิน

ระเบียบปฏิบัติ

1. จัดให้มีการทำนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศและมีการปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือตามความจำเป็นต่อการใช้งาน และนโยบายดังกล่าวได้รับการอนุมัติจากคณะกรรมการบริษัท หรือผู้มีอำนาจที่ได้รับมอบหมายไว้
2. นโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้ง่าย
3. จัดให้มีการสร้างความตระหนักที่เกี่ยวข้องกับภัยคุกคามทางอินเตอร์เน็ตใหม่ๆ เพื่อให้พนักงานขององค์กร มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ในระดับหนึ่งอย่างน้อยปีละ 1 ครั้ง
4. จัดให้มีการทำรายงานสรุปปัญหาและแนวทางแก้ไขที่มีระดับความสำคัญสูง เช่น ปัญหาการใช้เครือข่าย การติดไวรัส โครงการพัฒนาระบบงาน ปัญหาจากผู้ใช้งานและเจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศ และปัญหาอื่นๆ ที่เกี่ยวข้อง โดยประมาณไตรมาสละ 1 ครั้งหรือตามความเหมาะสม
5. จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศขององค์กร ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุงความเสี่ยงหรือปัญหาที่พบ

6. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ

2) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

วัตถุประสงค์

การแบ่งแยกอำนาจหน้าที่มีวัตถุประสงค์เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในแผนกเทคโนโลยีสารสนเทศ

ความสำคัญ

บริษัทต้องจัดให้มีการแบ่งแยกหน้าที่การปฏิบัติงานระหว่างบุคลากรภายในแผนกเทคโนโลยีสารสนเทศอย่างเพียงพอ เพื่อช่วยให้มีการสอบยันการปฏิบัติงานและมีการอนุมัติการปฏิบัติงานอย่างเพียงพอและเหมาะสม รวมทั้งการมีขอบเขตการปฏิบัติงานของพนักงานที่ชัดเจนและมีบุคลากรที่เพียงพอต่อการปฏิบัติงานของแผนกเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบหลัก

ผู้อำนวยการฝ่ายบัญชีและการเงิน

ระเบียบปฏิบัติ

1. จัดให้มีการแบ่งแยกหน้าที่ของบุคลากรในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง
2. ต้องให้มีใบกำหนดหน้าที่งานของแต่ละตำแหน่งไว้อย่างชัดเจน ซึ่งตำแหน่งที่กำหนดไว้เป็นไปตามหลักการแบ่งแยกหน้าที่งานตามข้อที่ 1 และพนักงานได้รับทราบถึงขอบเขตและหน้าที่การปฏิบัติงานของตนตามที่ได้กำหนดไว้
3. จัดให้มีการอบรมเพิ่มพูนความรู้ความสามารถของพนักงานแผนกเทคโนโลยีสารสนเทศให้เหมาะสมรวมทั้งจัดให้มีการเก็บข้อมูลการฝึกอบรมเหล่านั้น และจัดให้มีการประเมินผลการอบรม

3) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์มีวัตถุประสงค์เพื่อประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง เข้าถึง แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ

ความสำคัญ

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ศูนย์คอมพิวเตอร์ และความเสี่ยงหายอันจะเกิดจากอุปกรณ์หรือระบบต่างๆ เช่นระบบไฟฟ้า ซึ่งย่อมมีความเสี่ยงต่ออุปกรณ์และข้อมูลของบริษัท ดังนั้นบริษัทต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงศูนย์คอมพิวเตอร์ได้ และการเข้าถึงดังกล่าวต้องมีการอนุมัติอย่างเพียงพอ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้มีระบบป้องกันความเสียหายที่อาจจะเกิดขึ้น เช่นการป้องกันไฟไหม้หรือไฟฟ้าขัดข้อง

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. จัดให้มีการประเมินความเสี่ยงทางกายภาพของพื้นที่จัดเก็บอุปกรณ์ที่สำคัญของระบบเทคโนโลยีสารสนเทศทั้งที่สำนักงานใหญ่ สถานที่สำรองข้อมูล และจัดให้มีการทำแผนเพื่อปรับปรุงความเสี่ยงหรือปัญหาที่พบ
2. จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้ามซึ่งปิดล็อคตลอดเวลา และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง
3. ต้องมีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
4. ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ ต้องมีการอนุมัติจากผู้อำนวยการฝ่ายบัญชีและการเงินก่อน และให้มีเจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศที่ปฏิบัติงานประจำศูนย์คอมพิวเตอร์ควบคุมดูแลตลอดเวลาระหว่างที่บุคคลดังกล่าวอยู่ในศูนย์คอมพิวเตอร์
5. ศูนย์คอมพิวเตอร์ต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น
6. มีการติดตั้งอุปกรณ์สำรองไฟสำหรับระบบคอมพิวเตอร์ที่สำคัญ เพื่อให้สามารถดำเนินการต่อเนื่องของระบบงานที่สำคัญได้

4) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคลไวรัส รวมทั้ง malicious code ต่างๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

ความสำคัญ

บริษัทต้องควบคุมความปลอดภัยของข้อมูลเพื่อป้องกันความเสี่ยงจากการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลของบริษัท ตั้งแต่ระดับข้อมูลข่าวสารทั่วไป จนถึงระดับข้อมูลข่าวสารที่ลับที่สุด และควรจะมีหน่วยงานที่มีหน้าที่ควบคุมหืออนุมัติการที่จะเผยแพร่ข้อมูลข่าวสารให้กับหน่วยงานต่างๆ หรือนำข้อมูลออกไปเผยแพร่ภายนอกองค์การ ซึ่งอาจส่งผลให้เกิดข้อมูลถูกทำลายหรือนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต ดังนั้นการกำหนดนโยบายการรักษาความปลอดภัยของข้อมูลระบบคอมพิวเตอร์ และระบบเครือข่าย รวมทั้งวิธีการปฏิบัติงานอย่างเพียงพอจะช่วยป้องกันความเสี่ยงที่จะเกิดขึ้นได้

4.1 ความปลอดภัยของข้อมูล

ผู้รับผิดชอบหลัก

- ข้อมูลทั่วไป ดูแลโดย ส่วนงาน / ผู้ที่ได้รับมอบหมาย ใช้งานหรือดูแล ข้อมูลนั้นๆ
- ข้อมูลลับ ดูแลโดย ส่วนงาน ที่มีหน้าที่รับผิดชอบงาน และหน้าที่กำหนดในโครงสร้างของแผนก หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติงาน ให้ปฏิบัติในเรื่องนั้น ๆ
- ข้อมูลที่อยู่ระหว่างประมวลผล ดูแลโดยแผนกเทคโนโลยีสารสนเทศ
- ข้อมูลที่จัดเก็บสำรองตามข้อปฏิบัติด้านระบบ ดูแลโดยแผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. การขอใช้ข้อมูลทุกประเภท ต้องระบุผู้ขอ วัตถุประสงค์ และระยะเวลา ในการใช้งานที่ชัดเจน การคืน (ถ้ามี) ให้นำมาคืนเมื่อเสร็จหรือเมื่อกำหนด การยกเลิก (ปิด) สิทธิการใช้ข้อมูลยกเลิกเมื่อเสร็จหรือเมื่อครบกำหนด ห้ามทำสำเนาข้อมูลที่ระบุไว้ว่า “ห้ามทำสำเนา” โดยมิได้รับอนุญาตจากเจ้าของข้อมูล ผู้ขอข้อมูลต้องปฏิบัติตามขั้นตอนการขอใช้ข้อมูล ที่กำหนดแตกต่างกันตามประเภทข้อมูล และกลุ่มผู้ขอ
2. กำหนดชั้นความลับของข้อมูลเป็นข้อมูลทั่วไป และข้อมูลลับและกำหนดวิธีการขอใช้มูลไว้ดังนี้

2.1 ข้อมูลทั่วไป

- ผู้ขอใช้ข้อมูลต้องเป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดกับผู้ดูแลข้อมูล
- ผู้ขอใช้ข้อมูลหากเป็นพนักงานนอกฝ่ายที่เจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่ออนุมัติจากผู้อำนวยการฝ่ายผู้ดูแลข้อมูล เมื่อได้รับอนุมัติแจ้งให้เจ้าหน้าที่ผู้ดูแลข้อมูลจัดทำ / ส่งข้อมูลให้

2.2 ข้อมูลลับ

- ผู้ขอใช้เป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้บังคับบัญชา (ระดับผู้อำนวยการขึ้นไป) เมื่อได้รับอนุมัติ แจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ / ส่งข้อมูลให้
- ผู้ขอใช้เป็นพนักงานนอกฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้อำนวยการฝ่ายของตน และผู้อำนวยการฝ่ายผู้ดูแลตามลำดับเมื่อ ได้รับอนุมัติ แจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่ง ข้อมูลให้
- ผู้ขอใช้เป็นบุคคลภายนอก ให้ขอจากสำนักตรวจสอบ หรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี โดยผู้พิจารณาอนุมัติต้องเป็นผู้บริหารระดับผู้อำนวยการขึ้นไป

4.2 การควบคุมการกำหนดสิทธิ และบัญชีรายชื่อผู้ใช้งาน

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

พนักงานขององค์กรทั้งหมด

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานการเข้ามาใช้งาน
   1.1 บริษัทต้องกำหนดสิทธิการใช้งานของผู้ใช้งานเพื่อยืนยันตัวตนของผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์แยกเป็นรายบุคคล
   1.2 พนักงานต้องเก็บและรักษา Password สำหรับทุกระบบงานที่ไดรับมอบมาให้เป็นความลับ
   1.3 พนักงานต้องใช้ User Account และ Password ส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่พนักงานอยู่
   - การตั้งชื่อ User Account และ Password จะต้องใช้ตัวอักษรภาษาอังกฤษ
   - การตั้ง User Account จะต้องประกอบด้วย ชื่อ.นามสกุลตัวแรก 2 ตัว
   - การตั้ง Password มีความยาวไม่น้อยกว่า 8 ตัวอักษร

- มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและอักขระพิเศษเข้าด้วยกัน
- จะต้องมีการกำหนดวันหมดอายุการใช้งานของ Password เช่น ต้องเปลี่ยนทุก 90 วัน และเมื่อครบ 90 วัน ต้องมีการบังคับให้เปลี่ยน (Force Change)
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
- การกำหนดรหัสผ่านต้องห้ามซ้ำอย่างน้อย 10 ครั้ง

1.4 พนักงานต้องกำหนด Password สำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายขององค์กร

1.5 พนักงานต้องไม่ใช้โปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำ Password ส่วนบุคคลของตนโดยอัตโนมัติ (Save Password)

1.6 พนักงานต้องมีบัญชีผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น ห้ามเผยแพร่ แจกจ่าย จดหรือบันทึก Password ส่วนบุคคลไว้ในสถานที่ที่ทำงานต่อการสังเกตุเห็นของบุคคลอื่นหรือให้ผู้อื่นล่วงรู้รหัสผ่าน

1.7 พนักงานต้องเปลี่ยนรหัสผ่านทุกครั้งที่ได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

1.8 บริษัทต้องมีการทานสิทธิการเข้าใช้งานตามหน้าที่งาน โดยผู้มีอำนาจอนุมัติสิทธิการใช้งานว่าสิทธิดังกล่าวยังมีความเหมาะสมอยู่หรือไม่ โดยมีการสอบทานสิทธิอย่างน้อยปีละ 1 ครั้งในระดับ Active Directory และ Application

1.9 แผนกบุคคลเป็นผู้แจ้งต่อแผนกสารสนเทศเมื่อมีพนักงานเข้า-ออก หรือโยกย้ายตำแหน่งโดยทำการร้องขอร่วมกับผู้จัดการแผนกต้นสังกัด ผู้อำนวยการฝ่ายบัญชีและการเงินเป็นผู้พิจารณาอนุมัติผ่านเอกสาร User Request Form และจัดให้มีทะเบียนคุม

2. กำหนดระเบียบในการ Login เข้ามาใช้งานในระบบคอมพิวเตอร์

2.1 การ Login เข้าใช้งาน Application ขององค์กร ผู้ใช้งานจะต้อง Login เข้าระบบด้วยตนเองห้ามมิให้ผู้อื่นดำเนินการให้

2.2 ไม่อนุญาตให้ผู้อื่นใช้งานบัญชีผู้ใช้ของตนเอง

2.3 ไม่อนุญาตให้นำ Users ของตนเอง Login เข้าสู่ระบบแล้วให้ผู้อื่นใช้งาน

2.4 ให้ Logout ระบบเมื่อใช้งานเสร็จแล้วหรือมิได้อยู่ที่หน้าเครื่องคอมพิวเตอร์เป็นเวลานาน

2.5 อนุญาตให้ผู้ใช้งานใส่รหัสผ่านผิดไม่เกิน 5 ครั้ง ซึ่งระบบจะทำการล็อคชื่อผู้ใช้งานดังกล่าวทันทีโดยจะปลดล็อคเมื่อเวลาผ่านไป 60 นาที

3. กำหนดระเบียบการใช้ User “ Administrator”

3.1 ห้ามมิให้ผู้ใดล่วงรู้รหัสผ่านโดยรหัสผ่านจะต้องถูกเก็บใส่ซองปิดผนึกมิดชิด เก็บรักษาไว้ที่ผู้อำนวยการฝ่ายบัญชีและการเงิน

3.2 หากมีการเบิกใช้งานจะต้องทำการจดบันทึกการเบิกใช้งาน

3.3 เปลี่ยนรหัสผ่านทุกครั้งหลังเลิกใช้งาน

4. กำหนดมาตรฐานของการตรวจสอบการเข้าใช้งาน (Audit Trail)
   4.1 ตรวจสอบการเข้าใช้งานโดยผู้ใช้งานและรายงานสรุปให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมออย่างน้อยไตรมาสละ 1 ครั้ง

4.3 การควบคุมของระบบฐานข้อมูล

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานการติดตั้งระบบฐานข้อมูล
   1.1 ผู้ติดตั้งระบบฐานข้อมูล จะต้องเป็นพนักงานแผนกเทคโนโลยีสารสนเทศ หรือ พนักงานของบริษัท ซึ่งบริษัทได้มอบหมายให้ทำหน้าที่ดังกล่าว แต่ทั้งนี้ต้องมีพนักงานในแผนกเทคโนโลยีสารสนเทศร่วมดำเนินการด้วย
   1.2 ผู้ติดตั้งระบบฐานข้อมูลจะต้องใช้ซอฟท์แวร์ที่มีลิขสิทธิ์การใช้งานตามกฎหมาย
   1.3 แผนกเทคโนโลยีสารสนเทศหรือพนักงานของบริษัท ที่ได้รับมอบหมาย ให้เป็นผู้ติดตั้ง Patch ของระบบฐานข้อมูลต้องคำนึงถึง
      - ผลกระทบของการติดตั้งต่อผู้ใช้งานหรือต่อระบบงานที่เกี่ยวข้อง
      - การประเมินความเสี่ยงของการติดตั้ง Patch ดังกล่าว
      - การแจ้งให้ส่วนที่เกี่ยวข้องได้ทราบ
      - การเตรียมการเพื่อย้อนกับสู่ระบบเดิมหากการติดตั้งไม่สำเร็จ รวมทั้งรายงานผลการติดตั้งให้กับผู้บังคับบัญชาได้ทราบ
2. กำหนดมาตรฐานข้อมูลการใช้งาน (User Identification) และการอนุมัติการใช้งาน (Authorization)
   2.1 กำหนดมาตรฐานข้อมูลการใช้งาน

   พนักงานไม่สามารถเข้าใช้งานระบบฐานข้อมูลโดยตรงได้ต้องเข้าผ่าน Application เท่านั้น นอกจากกลุ่มผู้ดูแลระบบที่ได้รับอนุมัติโดยผู้อำนวยการฝ่ายบัญชีและการเงิน

   2.2 มาตรฐานการอนุมัติการใช้งาน (Authorization)

   เมื่อผู้ใช้งานได้รับความเห็นชอบจากหัวหน้างานและผู้อำนวยการฝ่ายต้นสังกัดตามลำดับขั้นในการขอใช้งานระบบฐานข้อมูล
3. กำหนดมาตรฐานในการเข้ามาใช้งาน (Login) และเข้าถึงข้อมูล (Access Control) ในระบบฐานข้อมูล

ผู้ใช้งานที่สามารถเข้ามาใช้งานระบบฐานข้อมูลจะต้องเป็นผู้ใช้งานที่มีรายชื่ออยู่ใน Active Directory ของบริษัท และต้องปฏิบัติตามระเบียบ ข้อ 4.2 การควบคุมการกำหนดสิทธิ และบัญชีรายชื่อผู้ใช้งาน

4. กำหนดมาตรฐานของการตรวจสอบการเข้าใช้งาน (Audit Trail) และความถูกต้องของข้อมูล (Data Integrity) ในระบบฐานข้อมูล
   4.1 ตรวจสอบการเข้าใช้ระบบฐานข้อมูลโดยผู้ใช้งานและรายงานสรุปให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมออย่างน้อยไตรมาสละ 1 ครั้ง
5. กำหนดมาตรฐานการสำรองข้อมูลและการนำกลับมาใช้ เพื่อป้องกันข้อมูลเสียหาย
   5.1 ส่วนสนับสนุนสารสนเทศ ต้องพิจารณาจัดหา Media ที่มีประสิทธิภาพเพื่อใช้ในการสำรองข้อมูล
   5.2 ส่วนสนับสนุนสารสนเทศ และฝ่าย/ส่วนงานที่เกี่ยวข้อง ต้องร่วมกันพิจารณาถึงวิธีสำรอง และติดตั้งข้อมูลของแต่ละระบบงาน
   5.3 ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบการสำรองข้อมูลว่าทำสำเร็จหรือไม่ และหากไม่สำเร็จต้องดำเนินการแก้ไข
   5.4 การ Restore Data สามารถกระทำได้เฉพาะผู้ที่ได้รับมอบหมาย และได้รับการสั่งจากผู้อำนวยการฝ่ายบัญชีและการเงิน หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการฝ่ายบัญชีและการเงินเท่านั้น
   5.5 ส่วนสนับสนุนสารสนเทศ ต้องจัดเก็บ Media ที่ใช้ในการสำรองข้อมูลไว้ในสภาพแวดล้อมที่เหมาะสมและมีระบบรักษาความปลอดภัยที่ดี
   5.6 ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบสภาพ Media และข้อมูลที่อยู่ใน Media อย่างสม่ำเสมอว่ายังอยู่ในสภาพที่ใช้งานได้ดีหรือไม่ หากพบปัญหาให้รีบดำเนินการแก้ไข

4.4 รักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

ผู้รับผิดชอบ

พนักงานแผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. การติดตั้งเครื่องคอมพิวเตอร์ Server ต้องมีการจัดแบ่งหมวดหมู่ตามที่แผนกเทคโนโลยีสารสนเทศได้กำหนดไว้
2. การติดตั้งเครื่องคอมพิวเตอร์ Server ต่างๆต้องมีการจัดแบบแปลนการติดตั้งอุปกรณ์นบตู้ Rack แสดงตำแหน่งต่าง ๆ ของอุปกรณ์บนตู้ Rack ในรูปแบบที่บริษัทระบุไว้ โดยจัดเก็บไว้ในส่วนแผนกเทคโนโลยีสารสนเทศ

3. การติดตั้งอุปกรณ์สื่อสารข้อมูลทุกชนิดกับระบบงานต่าง ๆ ของบริษัท ให้อยู่ในความควบคุมดูแลของแผนกเทคโนโลยีสารสนเทศ
4. การติดตั้งอุปกรณ์ดับเพลิง ระบบเครื่องปรับอากาศ และระบบเครื่องจ่ายไฟสำรองฉุกเฉิน จะต้องมีมาตรฐานตามที่องค์กร หรือผู้ผลิตกำหนดไว้

4.5 การรักษาความปลอดภัยของระบบคอมพิวเตอร์เครือข่าย

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานในการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร ผ่านทางเครือข่าย ทำการติดตั้ง Service Pack ตลอดจน Patch ต่าง ๆ ให้ทันสมัยร่วมทั้ง Software Antivirus ตามที่องค์กรกำหนด
2. กำหนดมาตรฐานในการติดต่อเข้า - องค์กร โดยใช้ระบบเครือข่ายผ่านทางโทรศัพท์ เครื่องคอมพิวเตอร์ และเครื่องคอมพิวเตอร์แม่ขาย (Server) ที่อยู่ใน Zone ของ Server Segment ไม่อนุญาตให้มีการติดตั้ง Modem Dial Up ผ่านระบบโทรศัพท์โดยเด็ดขาด แต่หากมีความจำเป็นต้องใช้งานจะต้องขออนุมัติผ่านความเห็นชอบร่วมกันจากผู้อำนวยการฝ่ายบัญชีและการเงิน หรือผู้ช่วยกรรมการผู้จัดการที่ดูแลแผนกเทคโนโลยีสารสนเทศก่อนที่จะมีการติดตั้งและต้องการกำหนดวันเริ่มต้นและวันสิ้นสุดการใช้งานอย่างชัดเจน และให้ผู้ดูแล Server ดังกล่าวต้องดุแลอย่างใกล้ชิดในระหว่างที่มีการใช้งานนั้น
3. กำหนดมาตรฐานของระบบรักษาความปลอดภัยบนระบบเครือข่าย
   3.1 จัดหาอุปกรณ์รักษาความปลอดภัยที่ทันต่อความเปลี่ยนแปลงของภัยคุกคามทางด้านเครือข่ายอย่างสม่ำเสมอ เพื่อดำเนินการจัดหาอุปกรณ์ป้องกันต่อไป
   3.2 จัดเก็บทะเบียนเลขหมายประจำเครื่องคอมพิวเตอร์ (IP Address) ที่มีการควบคุมการใช้งาน
   3.3 ทำการ Backup Configuration ของอุปกรณ์สื่อสารข้อมูลเป็นประจำอย่างน้อยปีละ 1 ครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลง
   3.4 เปลี่ยน Password ของอุปกรณ์สื่อสารขององค์กรชุดทุก 3 เดือนและให้พิมพ์รายละเอียดของอุปกรณ์ Password ใส่ซองปิดผนึก และให้หัวหน้าส่วนสนับสนุนสารสนเทศ เซ็นกำกับ และส่งต่อผู้อำนวยการฝ่ายบัญชีและการเงิน เพื่อเก็บรักษาไว้
   3.5 ห้ามใช้ Community Name ของอุปกรณ์สื่อสารข้อมูลทุกชนิดหรือ อุปกรณ์อื่นที่ใช้ Protocol SNMP ที่ถูกกำหนดชื่อมาโดยผู้ผลิตอุปกรณ์เมื่อเริ่มใช้งานกับระบบงานขององค์กร ให้ดำเนินเปลี่ยนชื่อโดยทันที

3.6 สำหรับ Server ที่จะทำการติดตั้งเข้ากันเครือข่ายขององค์กร ส่วนสนับสนุนสารสนเทศหรือพนักงานองค์กรหรือบริษัท ผู้ดูแลการติดตั้ง Server ดังกล่าวต้องส่งรายละเอียดของระบบปฏิบัติการ (Operating System) และ Service Pack หรืออื่นๆ ที่จำเป็นสำหรับการติดตั้งให้กับส่วนสนับสนุนสารสนเทศ รับทราบข้อมูลก่อนหลังจากนั้นจึงจะจ่าย IP Address ให้และให้ทำการ Monitor Port ที่จ่ายให้กับ Server ดังกล่าว ไม่น้อยกว่า 1 สัปดาห์อย่างใกล้ชิดพร้อมกันรายงานผลต่อหัวหน้าหรือผู้อำนวยการฝ่าย

3.7 ให้บุคคลที่ได้รับมอบหมายจากผู้อำนวยการฝ่ายบัญชีและการเงินเป็นผู้ถือกุญแจห้องอุปกรณ์สื่อสาร/ห้อง Server ขององค์กร

3.8 บุคคลที่จะเข้าห้อง Server จะต้องลงลายมือชื่อเบิก – คืนกุญแจทุกครั้งพร้อมระบุสาเหตุการเข้า

4. กำหนดมาตรฐานในการเชื่อมต่อกับเครือข่ายภายนอกองค์กร

4.1 การเชื่อต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายขององค์กรต้องผ่านความเห็นชอบจากผู้อำนวยการฝ่ายบัญชีและการเงินทุกกรณี

4.2 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายขององค์กรต้องเชื่อมต่อโดยมีอุปกรณ์ Firewall ป้องกันทุกระบบ

4.3 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายขององค์กรให้ใช้วงจรที่เป็นวงจร Permanent เท่านั้น ไม่อนุญาตให้ทำในลักษณะ Link Dial Up

5. กำหนดให้มีการจัดทำแผงผังเครือข่ายขององค์กร

ให้มีการจัดทำแผงผังเครือข่ายขององค์กร และต้องปรับปรุงแผงผังดังกล่าวให้มีความทันสมัยอยู่เสมอ รวมทั้งจัดเก็บไว้ในสถานที่ที่มีความปลอดภัย

4.6 การป้องกันไวรัสคอมพิวเตอร์ /มัลแวร์

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. ติดตั้งและตรวจสอบเครื่องมือในการกำจัดไวรัสคอมพิวเตอร์ /มัลแวร์

1.1 ติดตั้งและตรวจสอบระบบป้องกันไวรัสคอมพิวเตอร์ /มัลแวร์สำหรับเครื่องแม่ข่ายให้บริการจดหมาย อิเล็กทรอนิกส์ที่ Gate way (SMTP Gateway) เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้องรวมทั้งต้องจัดให้มีการอัพเดต จากเจ้าของผลิตภัณฑ์นั้นๆ ทุก 24 ชั่วโมง

1.2 ติดตั้งและตรวจสอบระบบป้องกันไวรัสคอมพิวเตอร์ /มัลแวร์สำหรับ HTTP เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้องรวมทั้งต้องจัดให้มีการอัพเดตจากเจ้าของผลิตภัณฑ์นั้นๆทุก 24 ชั่วโมง

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

1.4 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์ /มัลแวร์ ให้กับ PC ขององค์กรทุกเครื่อง เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้องรวมทั้ง ต้องจัดให้มีการอัพเดตจากเจ้าของผลิตภัณฑ์นั้นๆทุก 24 ชั่วโมง

2 กำหนดหน้าที่และความรับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์ /มัลแวร์

2.1 กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์บนเครื่องคอมพิวเตอร์ส่วนบุคคลไม่ให้แพร่กระจายทำความเสียหายกับข้อมูลขององค์กร

2.2 กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ ต้องมีการแจ้งข่าวเกี่ยวกับไวรัสคอมพิวเตอร์/มัลแวร์ทันที หากมีการระบาดของไวรัสคอมพิวเตอร์/มัลแวร์ตัวใหม่

2.3 กำหนดให้ส่วนเทคนิคปฏิบัติการส่วนเครือข่ายมีหน้าที่รับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์อย่างสม่ำเสมอ บน Servers และอุปกรณ์เครือข่าย เพื่อป้องกันความเสียหายกับข้อมูลขององค์กร

2.4 กำหนดให้ส่วนเทคนิคปฏิบัติการทำการรายงานสถิติการติดไวรัสคอมพิวเตอร์/มัลแวร์ของเครื่องคอมพิวเตอร์ส่วนบุคคลที่แสดงอยู่บนเซิร์ฟเวอร์แม่ข่ายสำหรับป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ขององค์กร อย่างน้อยเดือนละ 1 ครั้งต่อ ผู้อำนวยการฝ่ายสนับสนุนสารสนเทศ

4.7 การนำอุปกรณ์ส่วนตัวมาเชื่อมต่อกับบริษัทและการเข้าถึงเครือข่ายของบริษัทจากระยะไกล

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดมาตรฐานการเข้ามาใช้งาน
   - ผู้ใช้ หมายถึง พนักงานแผนกสารสนเทศ, ผู้ให้บริการจากภายนอก (Outsource), ผู้ขาย (Vendors) และตัวแทน (Agent) ที่ต้องการเชื่อมต่อเพื่อปฏิบัติงานจากระยะไกล
   - การเชื่อมต่อระยะไกล หมายถึง การเข้าใช้ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายจากระยะไกล เช่น การเข้าใช้เครื่องคอมพิวเตอร์แม่ข่ายจากนอกบริษัทฯ เป็นต้น

1.1 ผู้ใช้ต้องทำการขออนุญาติในการเข้าถึงระบบจากระยะไกลผ่านเอกสาร ‘แบบฟอร์มการขอใช้บริการอินเตอร์เน็ต บุคคลภายนอก ’ โดยระบุวัตถุประสงค์และระยะเวลาการเข้าใช้งาน

1.2 บริษัทต้องกำหนดสิทธิการใช้งานของผู้ใช้งานเพื่อยืนยันตัวตนของผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์แยกเป็นรายบุคคล

1.3 ผู้ใช้งานต้องเก็บและรักษา Password สำหรับทุกระบบงานที่ได้รับมอบมาให้เป็นความลับ

2. กำหนดให้ต้องมีการจัดเก็บบันทึกการเชื่อมต่อของผู้ใช้งานจากระยะไกลไว้ในอุปกรณ์ firewall หรือ Log Analyzer
3. กำหนดให้เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศต้องทำการยกเลิกการใช้ทุกครั้งเมื่อผู้ใช้งานสิ้นสุดการใช้งาน

5) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk

ความสำคัญ

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ เพื่อสร้างความมั่นใจว่าการซื้อหรือพัฒนามีความสอดคล้องกับแผนงานบริษัท มีหลักเกณฑ์ในการคัดเลือก พัฒนามีการจัดลำดับความสำคัญของงาน รวมทั้งกระบวนการพัฒนาได้มีการทดสอบอย่างเพียงพอว่าระบบงานที่แก้ไขเปลี่ยนแปลงมีความถูกต้องและให้ผลลัพธ์ตามที่ได้กำหนดไว้

ผู้รับผิดชอบหลัก

ผู้อำนวยการฝ่ายบัญชีและการเงิน

ระเบียบปฏิบัติ

5.1 การพัฒนาซอฟแวร์

1. กำหนดให้ปฏิบัติตามขั้นตอนดังนี้ในการพัฒนาซอฟแวร์
   1.1 การเริ่มต้นโครงการ (Initiation)
   1.2 การวิเคราะห์ระบบ (Analysis)
   1.3 การออกแบบระบบ (Design)
   1.4 การพัฒนาและทดสอบระบบ (Build and Test)
   1.5 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 - เอกสารหน้าจอสำหรับผู้ใช้งานเพื่อสามารถเปรียบเทียบกับความต้องการใช้งาน ที่กำหนดไว้ในกระบวนการที่ 1 -เอกสารการวางแผนการทดสอบระบบซึ่งรวมถึงการทดสอบ Security Requirement ด้วย
3	การออกแบบ (Design)	- เอกสารการกำหนดฮาร์ดแวร์และซอฟแวร์ที่จำเป็นต้องใช้ - เอกสารการกำหนด Program Specification - เอกสาร Test Case ที่ใช้ในการทดสอบ
4	การพัฒนาและทดสอบ (Build and Test)	- คู่มือการใช้งานสำหรับผู้ใช้งาน - คู่มือการใช้งานสำหรับผู้ดูแลระบบ - Source Code ของระบบ - เอกสารผลการทดสอบตาม Test Case - เอกสาร User Acceptance Test เช่น ทดสอบตาม User requirement ที่กำหนดไว้เป็นต้น
5	การติดตั้งและใช้งาน (Deployment)	- เอกสารการลงนามยอมรับการใช้งาน (User Acceptance) - Source Code ที่เป็นเวอร์ชั่นที่จะนำขึ้นสู่ Production ต้องนำไปเก็บไว้กับผู้ที่ได้รับมอบหมายให้ดูแลรักษา

5.2 การเปลี่ยนแปลงอื่นๆ

1. การเปลี่ยนแปลง Hardware
2. การเปลี่ยนแปลง Software

3. การเปลี่ยนแปลงระบบปฏิบัติการ
4. การเปลี่ยนแปลงค่ามาตรฐานต่างๆ และรายงานของระบบงาน (Program Configurations and Reports)
5. การเปลี่ยนแปลงโครงสร้างระบบฐานข้อมูล (Database)

การกำหนดหน้าที่และความรับผิดชอบดังนี้

ที่	ขั้นตอน	หน้าที่ความรับผิดชอบ
1	การร้องขอ (Request)	ผู้ร้องขอ : ผู้ใช้งาน ผู้จัดการแผนก ระบุความจำเป็นและรายละเอียดความเปลี่ยนแปลงที่ต้องการ ผู้อนุมัติ : ผู้อำนวยการฝ่ายบัญชีและการเงิน
2	ทดสอบ (Test)	ผู้ทดสอบ : ผู้ร้องขอในข้อ 1 หรือผู้ที่ผู้จัดการแผนกที่ร้องขอมอบหมายให้ทำการทดสอบ ผู้ตรวจสอบและอนุมัติ : ผู้อำนวยการฝ่ายบัญชีและการเงิน
3	การติดตั้งและใช้งาน (Deployment)	ผู้ทำการติดตั้ง : เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ หรือบุคคลที่ได้รับมอบหมายจากผู้อำนวยการแผนกเทคโนโลยีสารสนเทศ ผู้อนุมัติ : ผู้อำนวยการแผนกเทคโนโลยีสารสนเทศ

กำหนดให้มีการติดตามสถานะรายงานการเปลี่ยนแปลงอย่างน้อยไตรมาสละ 1 ครั้ง โดยผู้อำนวยการฝ่ายบัญชีและการเงิน

6) การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and It Continuity Plan)

วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์ เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์รวมทั้งการทดสอบและเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและทดสอบแผนฉุกเฉิน

ความสำคัญ

บริษัท ต้องกำหนดวิการปฏิบัติในกรณีที่เกิดเหตุการณ์ฉุกเฉินในกรณีต่างๆ และกำหนดหน้าที่รับผิดชอบของตัวบุคคล พร้อมทั้งมีการซักซ้อมเป็นระยะ เพื่อให้เกิดผลต่อการบริการของบริษัทแก่ลูกค้าให้น้อยที่สุด และเพื่อให้การดำเนินการของบริษัท ยังสามารถดำเนินต่อได้โดยไม่ติดขัด

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. กำหนดหน้าที่ความรับผิดชอบ
   1.1 ทำการสำรองข้อมูลอย่างสม่ำเสมอ โดยแผนกเทคโนโลยีสารสนเทศ
   1.2 นำข้อมูลสำรองชุดล่าสุดมาลงในระบบเพื่อทดสอบการว่าข้อมูลสำรองสามารถใช้งานได้ โดยแผนกเทคโนโลยีสารสนเทศ
   1.3 กำหนดหน้าที่ความรับผิดชอบของพนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉิน
   - พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉินต้องเข้ารับอบรมหรือสร้างความตระหนักเพื่อให้รู้หรือทราบวิธีปฏิบัติในกรณีที่เกิดเหตุฉุกเฉินในกรณีต่างๆ
   - พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉินต้องร่วมซ้อมการใช้งานแผนสำรองฉุกเฉิน ซึ่งจะจัดปีละ 1 ครั้ง
2. กำหนดมาตรฐานสำหรับศูนย์คอมพิวเตอร์สำรอง
   2.1 ติดตั้งและดูแลระบบคอมพิวเตอร์สำรองอย่างสม่ำเสมอเพื่อให้สามารถบริการทดแทนระบบคอมพิวเตอร์หลักได้
   2.2 ติดตั้งข้อมูลระบบ Facility ให้พร้อมสำหรับการใช้งานอย่างสม่ำเสมอ
   2.3 นำข้อมูลที่สำรองไว้มา Update ให้มีความทันสมัยอยู่ตลอดเวลา
   2.4 ทดสอบการใช้งานระบบคอมพิวเตอร์ เครือข่าย และระบบ Facility อย่างสม่ำเสมอเพื่อให้สามารถใช้งานได้โดยไม่ติดขัด
3. การสำรองข้อมูล
   3.1 ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติ (operating system) โปรแกรมระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมทำงานได้อย่างต่อเนื่อง
   3.2 จัดทำขั้นตอนหรือวิธีการปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้
   - ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
   - ประเภทสื่อบันทึก (media)
   - จำนวนที่ต้องสำรอง (copy)
   - ขั้นตอนและวิธีการสำรองโดยละเอียด

- สถานที่และวิธีการเก็บสื่อบันทึก

3.3 จัดทำบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

3.4 ทดสอบข้อมูลสำรองเพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

3.5 จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีการปฏิบัติต่างๆไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โยสถานที่ดังกล่าวต้องมีการควบคุมการเข้าออกและระบบป้องกันความเสียหายที่เป็นมาตรฐาน

3.6 ต้องจัดทำฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อสำรองข้อมูล เพื่อให้สามารถค้นหาได้โดยเร็ว

3.7 การขอใช้งานสื่อสารบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

7) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

วัตถุประสงค์

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาควบคุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ ซึ่ง ได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน

ความสำคัญ

บริษัทต้องกำหนดวิธีการปฏิบัติงานประจำด้านคอมพิวเตอร์ไว้เป็นลายลักษณ์อักษรเพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่และควรมีการจัดทำบันทึกผลการปฏิบัติงานไว้เพื่อให้สามารถตรวจสอบได้ว่ามีการจัดทำอย่างครบถ้วนและเป็นไปตามวิธีการปฏิบัติงานที่กำหนดไว้

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. จัดทำขั้นตอนหรือวิธีการปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆที่สำคัญเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์(computer operator) และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ
2. กำหนดมาตรฐาน Login เข้าใช้งานระบบ

2.1 กำหนดให้มีระบบการตรวจสอบการ Login เข้ามาใช้งาน โดยบันทึกข้อมูลที่เกี่ยวข้องกับการ Login นั้นไว้ และให้บันทึกทั้งการ Login ที่ทำได้สำเร็จ และไม่สำเร็จเพื่อใช้ในการตรวจสอบภายหลัง

3. ควรกำหนดให้มีการบันทึก (log book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้
   - ผู้ปฏิบัติงาน
   - เวลาปฏิบัติงาน
   - รายละเอียดการปฏิบัติงาน
   - ปัญหาที่เกิดขึ้นและการแก้ไข
   - สถานะของระบบ
   - ผู้ตรวจทานการปฏิบัติงาน

การปฏิบัติงานประจำควรประกอบด้วย

- การสำรองข้อมูล
- การตรวจสอบข้อมูลความพร้อมของอุปกรณ์คอมพิวเตอร์ในศูนย์คอมพิวเตอร์
- การตรวจสอบซอฟท์แวร์ระบบ ระบบเครือข่าย และระบบป้องกันไวรัส
- การตรวจสอบข้อมูลความพร้อมของอุปกรณ์ป้องกันภัยหรืออุปกรณ์อื่นเกี่ยวข้อง เช่น ระบบดับเพลิง ระบบควบคุมอุณหภูมิ
- การตรวจสอบและบำรุงรักษา

8) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ใช้บริการรายอื่น(IT Outsourcing)

วัตถุประสงค์

การควบคุมการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ใช้บริการรายอื่นมีวัตถุประสงค์เพื่อให้บริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ใช้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ใช้บริการ

ความสำคัญ

การกำหนดนโยบาย ระเบียบปฏิบัติ มาตรฐานและแนวทางในการคัดเลือกผู้ใช้บริการภายนอกจะช่วยให้ตัดสินใจที่จะได้รับประสิทธิผลที่ดีขึ้น ซึ่งจะส่งผลต่อค่าใช้จ่ายที่เหมาะสมในการคัดเลือกใช้บริการ และผลของการให้บริการเป็นไปตามที่คาดหวังไว้

ผู้รับผิดชอบหลัก

ผู้บริหารระดับสูง

ผู้บริหารระดับผู้อำนวยการฝ่ายบัญชีและการเงิน

ระเบียบปฏิบัติ

1. การคัดเลือกผู้ใช้บริการจากภายนอก

   การคัดเลือกผู้ใช้บริการจากภายนอกให้เป็นไปตามระเบียบวิธีการคัดเลือกตามกระบวนการจัดซื้อจัดจ้าง โดยการพิจารณาคัดเลือกต้องครอบคลุมเรื่องดังต่อไปนี้

   1.1 การเปรียบเทียบข้อเสนอกับความต้องการของบริษัท

   1.2 การประเมินผลงานที่ผ่านมาของผู้ใช้บริการภายนอก

   1.3 การประเมินทักษะและประสบการณ์เกี่ยวกับงาน

   1.4 กำหนดมาตรฐานของอุปกรณ์ที่นำมาติดตั้งใช้งานจะต้องเป็นอุปกรณ์ที่มีคุณภาพและได้มาตรฐาน

   - อุปกรณ์ที่นำมาติดตั้งต้องมีมาตรฐานรับรองจากบริษัทหรือจากผู้ผลิตโดยตรง
   - อุปกรณ์ที่นำมาติดตั้งใช้งานจะต้องมีมาตรฐานที่เป็นสากล (Standard)

2. การควบคุมด้านความมั่นคงปลอดภัย

   2.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ที่บริษัททำสัญญาว่าจ้างให้มาปฏิบัติงานซึ่งสอดคล้องกับนโยบายความมั่นคงปลอดภัยของบริษัทและให้ผู้ปฏิบัติงานนั้นลงนามในเอกสารดังกล่าว

   2.2 เมื่อสิ้นสุดการจ้างงานหรือการเปลี่ยนแปลงลักษณะการจ้างงานของหน่วยงานภายนอกจะต้องถอนสิทธิการเข้าถึงระบบสารสนเทศและทรัพย์สินสารสนเทศทันที

3. การควบคุมระหว่างการให้บริการ

   3.1 ต้องควบคุมผู้ให้บริการจากภายนอกว่ามีการปฏิบัติตามข้อกำหนดที่จัดทำขึ้นอย่างสม่ำเสมอ เช่นดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ

   3.2 ต้องมีการกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือการให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การปรับปรุงเทคโนโลยี ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ใช้บริการจากภายนอก

9) การทำลายสื่อบันทึกข้อมูล (Media Disposal)

วัตถุประสงค์

การทำลายสื่อบันทึกข้อมูลมีวัตถุประสงค์เพื่อป้องกันไม่ให้ข้อมูลสารสนเทศที่สำคัญของบริษัทฯ รั่วไหลสู่ภายนอกโดยสินทรัพย์ข้อมูลที่สำคัญที่จัดเก็บผ่านอุปกรณ์ IT จะต้องได้รับการสำรองคัดลอก และหรือลบออกอย่างเพียงพอก่อนที่จะถูกกำจัด เพื่อให้แน่ใจว่ามีการกำจัดอุปกรณ์ IT ของบริษัทฯ อย่างปลอดภัย

ความสำคัญ

บริษัทต้องกำหนดวิธีการทำลายสื่อบันทึกข้อมูลไว้เป็นลายลักษณ์อักษรเพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่และควรมีการจัดทำบันทึกผลการปฏิบัติงานไว้เพื่อให้สามารถตรวจสอบได้ว่ามีการดำเนินการอย่างครบถ้วนและเป็นไปตามวิธีการปฏิบัติงานที่กำหนดไว้

ผู้รับผิดชอบหลัก

แผนกเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

- สื่อบันทึกข้อมูล หมายถึง อุปกรณ์ที่ใช้ในการเก็บข้อมูลสารสนเทศ, ข้อมูลทั่วไป, ไฟล์ข้อมูล, รูปภาพ, วีดีโอ, ไฟล์เสียง ฯลฯ ของบริษัทไม่ว่าจะเป็น ฮาร์ดดิสก์, แผ่นซีดี, แผ่นดีวีดี, ฟลอปปี้ดิสก์ (Floppy Disk), แฟลชไดรฟ์ (Flash Drive), เอสเอสดี (SSD- Solid State Disk) เครื่องบันทึกเสียง, เมมโมรี่การ์ด (Memory Card),เทปสำรองข้อมูล (Backup Tape) เป็นต้น
- ทำลาย หมายถึง กระบวนการ/วิธี/ขั้นตอน ที่ทำให้เกิดความเสียหาย, พัง, สลาย, สูญเสียสภาพทางกายภาพของวัตถุ ฯลฯ จนทำไม่สามารถนำกลับมาใช้ประโยชน์ได้อีก
- ผู้ทำลาย” หมายถึง เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย หรือบุคคลภายนอกที่ได้รับการอนุมัติให้กระทำการแทนเจ้าหน้าที่ของบริษัท

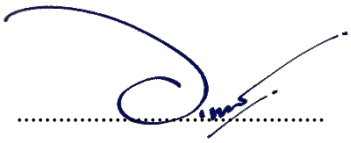
1. พนักงานของแผนกเทคโนโลยีสารสนเทศ จัดทำทะเบียนทรัพย์สินที่ต้องการทำลายข้อมูล (เครื่องเช่า , เครื่องที่เตรียมไปบริจาค , เครื่องที่รอตัดจำหน่าย)
2. ส่งข้อมูลให้ผู้อำนวยการฝ่ายบัญชีและการเงินตรวจสอบ พร้อมลงนามอนุมัติรับทราบ
3. พนักงานของแผนกเทคโนโลยีสารสนเทศ ทำการ Format เครื่อง ตามทะเบียนทรัพย์สินที่ต้องการทำลายข้อมูล
4. ส่งทะเบียนทรัพย์สินที่ทำลายเสร็จให้ผู้อำนวยการฝ่ายบัญชีและการเงินตรวจสอบ หรือผู้ที่ได้รับมอบหมายทำการตรวจสอบพร้อมจัดทำสำเนาแจ้งไปยังแผนกบัญชี ก่อนส่งมอบเครื่องคืนให้บริษัทฯ

6. การพิจารณาโทษทางวินัยและการเรียกค่าเสียหาย

6.1 พนักงานและลูกจ้างที่ฝ่าฝืนข้อกำหนดนโยบายด้านความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศ โดยจงใจหรือประมาณเลินเล่อ และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กรหรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวิจัยและความรับผิดชอบทางแพ่งและอาญาแก่พนักงานและลูกจ้างนั้น ตามกฎหมาย ข้อบังคับ ระเบียบ หรือประกาศที่เกี่ยวข้อง

บังคับบัญชาผู้ใด งดเว้น หรือละเว้นการปฏิบัติตามหน้าที่ และเป็นเหตุให้พนักงานหรือลูกจ้างที่อยู่ภายใต้การบังคับบัญชาของตน ฝ่าฝืนข้อกำหนดของนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ ให้นำบทบัญญัติในวรรคก่อนมาใช้บังคับโดยอนุโลม

6.2 การฝ่าฝืนขอกำหนดใดๆ ตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ แม้จะไม่ก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใดก็ตาม ถ้าผู้บังคับบัญชาเห็นว่ามีเหตุอันสมควร อาจจะบันทึกในประวัติ การปฏิบัติงานและจะใช้เป็นข้อมูลประกอบการพิจารณาต่ออายุสัญญาจ้าง การขึ้นเงินเดือน หรือ เลื่อนตำแหน่งด้วยก็ได้



(นายเอกชัย ชัยตระกูลทอง)
กรรมการผู้จัดการ