TRITON

ประกาศที่ 3/2562

เรื่อง นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

โดยมติที่ประชุมคณะกรรมการบริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน) ครั้งที่ 1/2562 เมื่อวันที่ 18 มกราคม 2562 ได้มีมติอนุมัตินโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รายละเอียดตามเอกสารที่แนบมานี้

ฝ่ายบริหารจึงเห็นควรประกาศแจ้งมาเพื่อให้พนักงานในกลุ่มบริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย รับทราบเพื่อนำไปใช้ปฏิบัติให้เป็นแนวทางเดียวกันทั่วทั้งองค์กร ทั้งนี้ ให้มีผลบังคับใช้ ตั้งแต่วันที่ 19 มกราคม 2562 เป็นต้นไป

ประกาศมา ณ วันที่ 1 กุมภาพันธ์ 2562

.....

นายเชิดศักดิ์ กู้เกียรตินันท์

ประธานเจ้าหน้าที่บริหาร

TRITON

นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย

ประจำปี 2562

สารบัญ

หน้า

1. วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่ ความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

บริษัทตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติให้ผู้ใช้งานมีความตระหนักถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศของบริษัท และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา รวมทั้งเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัทด้านอื่น ๆ ที่มุ่งเน้นการปฏิบัติงานภายในบริษัทให้มีความมั่นคงปลอดภัยในการดำเนินกิจการของบริษัท

2. คำจำกัดความ (Definition of Terms)

- **"บริษัท"** หมายถึง บริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย
- **"ผู้ใช้งาน"** หมายถึง พนักงานที่ได้รับการว่าจ้างจากบริษัทตามเงื่อนไขและสถานะต่าง ๆ รวมไปถึงบุคคลอื่น ๆ ที่ได้รับอนุญาตให้ใช้ระบบสารสนเทศเชื่อมต่อกับบริษัท ทั้งภายในและภายนอกบริษัท
- **"ผู้ดูแลระบบ"** หมายถึง ผู้ที่ทำหน้าที่บริหาร จัดการระบบคอมพิวเตอร์และระบบเครือข่ายในบริษัท โดยดูแลการติดตั้งและบำรุงรักษาระบบปฏิบัติการ การติดตั้งฮาร์ดแวร์ การติดตั้งและการปรับปรุงซอฟต์แวร์ สร้าง ออกแบบและบำรุงรักษาบัญชีผู้ใช้งาน
- **"บุคคลภายนอก"** หมายถึง บุคคล/นิติบุคคล ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิ์ตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต
- **"ทรัพย์สินสารสนเทศ"** หมายถึง ข้อมูลไฟล์ ข้อมูลซอฟต์แวร์ ฐานข้อมูล เครื่องมือในการพัฒนาอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย เครือข่ายไร้สาย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด
- **"เครือข่าย** (Network)" หมายถึง ระบบเครือข่ายที่ใช้เชื่อมต่อระหว่างแม่ข่ายและลูกข่ายเพื่อให้ระบบคอมพิวเตอร์ที่มีอยู่ในบริษัทสามารถติดต่อกันทั้งภายในและภายนอกบริษัท
- **"เครือข่ายไร้สาย** (Wireless Network)" หมายถึง เทคโนโลยีในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ หรือกลุ่มของเครื่องคอมพิวเตอร์ รวมถึงการติดต่อสื่อสารระหว่างเครื่อง

คอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์ ซึ่งการสื่อสารจะไม่ใช้สายสัญญาณในการเชื่อมต่อ (LAN) แต่จะใช้คลื่นวิทยุ หรือ คลื่น อินฟาเรด ในการรับส่งข้อมูลแทน

- **"ข้อมูล** (Information)" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูลหรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือผ่านวิธีการใด ๆ และไม่ว่าจะจัดทำไว้รูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนที่ ภาพวาด ภาพถ่าย การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
- **"เจ้าของข้อมูล"** หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเสียหาย
- **"อินเทอร์เน็ต** (Internet)" หมายถึง ระบบข้อมูลข่าวสารบริการต่าง ๆ ที่หน่วยงานหรือบุคคลภายนอกเป็นผู้ดำเนินการและเปิดให้บุคคลอื่นเข้าไปใช้บริการหรือค้นหาข้อมูลได้

3. การบริหารความมั่นคงปลอดภัยสำหรับสารสนเทศ และแนวทางในการรักษาความปลอดภัย

การบริหารความมั่นคงปลอดภัยสำหรับสารสนเทศ หมายถึง การสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศ เพื่อเป็นมาตรฐาน และมีประสิทธิภาพคุ้มค่ากับการลงทุน ประกอบด้วยหลักการดังนี้

3.1 Confidentiality มีกระบวนการรักษาความลับที่เหมาะสม ผู้มีสิทธิ์เท่านั้นจึงจะเข้าถึงข้อมูลได้

3.2 Integrity มีความถูกต้องและสมบูรณ์ของเนื้อหาสาระ

3.3 Availability มีความพร้อมใช้งานอยู่เสมอ ผู้ใช้งานสามารถเข้าถึงข้อมูลเมื่อต้องการได้ทุกเวลา

บริษัทกำหนดมาตรการเพื่อรักษาความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศโดยบริษัทใช้แนวทาง ดังนี้

- **นโยบายความมั่นคงปลอดภัย** (Security Policy) ประกอบด้วยแนวทางปฏิบัติ ที่ผู้ใช้งานต้องปฏิบัติตามโดยเคร่งครัด
- **แนวทางปฏิบัติ** (Procedure) จะมีการอ้างอิงถึงขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง

4. ขอบเขตของการสร้างความมั่นคงปลอดภัย

นโยบายฉบับนี้ครอบคลุมการสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศของบริษัท ประกอบด้วย

- พนักงานและลูกจ้างของบริษัททั้งหมด
- ข้อมูลสารสนเทศของบริษัท
- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต่าง ๆ
- เครื่องคอมพิวเตอร์ส่วนบุคคล
- เครื่องคอมพิวเตอร์แบบพกพา
- อุปกรณ์เครือข่าย
- เครือข่ายไร้สาย
- ระบบไฟฟ้าสำรอง
- สายสัญญาณเครือข่าย
- ซอฟท์แวร์ระบบ ซอฟท์แวร์จ้างพัฒนา ซอฟท์แวร์พัฒนาเอง ซอฟท์แวร์สำเร็จรูป
- สื่อบันทึกข้อมูล

5. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย

1. นโยบายรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy)
2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
4. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
5. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)
6. การควบคุมการพัฒนา (System Development) หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Computer System Conversion)
7. การสำรองข้อมูลระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Data Backup and IT Continuity Plan)
8. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation Control)

9. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing Services Control)
10. การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Control)
11. การป้องกันความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูล (Risk Prevention on Data Inaccessible)
12. มาตรฐานระบบคอมพิวเตอร์ (Computer System Standards)
13. ระเบียบการใช้งานอินเทอร์เน็ต (Use of the Internet)
14. ระเบียบการใช้งานจดหมายอิเล็กทรอนิกส์ (Use of the Email)
15. การใช้ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual Property)

6. แนวทางปฏิบัติ

นโยบายแต่ละด้านจะประกอบไปด้วยแนวทางปฏิบัติที่พนักงานหรือผู้ที่เกี่ยวข้องต้องปฏิบัติตามโดยเคร่งครัด ดังต่อไปนี้

6.1 นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ

ผู้บริหารระดับสูง

ผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1. จัดทำนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศและมีการปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือตามความจำเป็นต่อการใช้งาน และนโยบายดังกล่าวต้องได้รับการอนุมัติจากคณะกรรมการบริษัทหรือผู้มีอำนาจที่ได้รับมอบหมาย
2. จัดทำนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้ง่าย
3. จัดให้มีการอบรมหัวข้อที่เกี่ยวข้องกับภัยคุกคามทางอินเทอร์เน็ตใหม่ ๆ อย่างน้อยปีละ 1 ครั้ง เพื่อให้ผู้ใช้งาน มีความตระหนักรับรู้เข้าใจและสามารถป้องกันตนเองได้ในระดับหนึ่ง

4. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยปีละ 1 ครั้งและจัดทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ
5. จัดให้มีการวางแผนกลยุทธ์ด้านสารสนเทศเพื่อให้สอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัท ทั้งแผนระยะสั้นและแผนระยะยาว

6.2 การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

วัตถุประสงค์

เพื่อให้มีการทวนสอบการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์ ซึ่งเป็นการลดความเสี่ยงด้าน Infrastructure Risk

ผู้รับผิดชอบ

ผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1. ต้องจัดให้มีใบกำหนดหน้าที่งานของแต่ละตำแหน่งงานไว้อย่างชัดเจน และพนักงานได้รับทราบถึงขอบเขตและหน้าที่การปฏิบัติงานของตนตามที่ได้กำหนดไว้
2. จัดให้มีการอบรมเพิ่มพูนความรู้ความสามารถของพนักงานฝ่ายเทคโนโลยีสารสนเทศอย่างเหมาะสม รวมทั้งจัดให้มีการเก็บข้อมูลการฝึกอบรม

6.3 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

เพื่อควบคุมมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (Access Risk) แก้ไขเปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (Availability Risk) และเพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ

ผู้รับผิดชอบ

เจ้าหน้าที่ดูแลศูนย์คอมพิวเตอร์

แนวทางปฏิบัติ

1. ควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์
    1.1 ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้ามซึ่งปิดล็อคตลอดเวลา และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง

1.2 ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ในบางครั้ง กำหนดให้ต้องมีเจ้าหน้าที่ของฝ่ายสารสนเทศที่ปฏิบัติงานประจำในศูนย์คอมพิวเตอร์ควบคุมดูแลตลอดเวลาระหว่างที่บุคคลดังกล่าวอยู่ในศูนย์คอมพิวเตอร์

1.3 มีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึก ดังกล่าวอย่างสม่ำเสมอ

2. การป้องกันความเสียหาย

2.1 ระบบป้องกันไฟไหม้

- มีอุปกรณ์เตือนไฟไหม้ ซึ่งมีเครื่องตรวจจับควัน หรือเครื่องตรวจจับความร้อน เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา
- มีการติดตั้งถังดับเพลิง และอุปกรณ์ดับเพลิงอัตโนมัติไว้ในศูนย์คอมพิวเตอร์ โดยสารที่ใช้ดับเพลิงจะต้องเป็นสารที่ใช้สำหรับคอมพิวเตอร์โดยเฉพาะ ซึ่งจะไม่ทำให้คอมพิวเตอร์เสียหาย และไม่นำไฟฟ้า

2.2 ระบบป้องกันไฟฟ้าขัดข้อง

- จัดให้มีระบบไฟฟ้าสำรอง (UPS) สำหรับเครื่องแม่ข่าย และอุปกรณ์เครือข่าย เพื่อป้องกันความเสียหาย อันเกิดจากความไม่คงที่ของกระแสไฟฟ้าและให้การทำงานมีความต่อเนื่อง ซึ่งระบบไฟฟ้าสำรอง (UPS) จะต้องสามารถสำรองไฟฟ้าได้ไม่น้อยกว่า 30 นาที
- เครื่องจ่ายไฟสำรองฉุกเฉิน (UPS) จะต้องมีมาตรฐานตามที่บริษัท หรือผู้ผลิตกำหนดไว้
- ควรทำการตรวจสอบเครื่องจ่ายไฟสำรองฉุกเฉิน (UPS) ทุก ๆ 3 เดือน

2.3 ระบบควบคุมอุณหภูมิและความชื้น

- ควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยตั้งอุณหภูมิ เครื่องปรับอากาศและความชื้นให้เหมาะสมกับคุณลักษณะของระบบคอมพิวเตอร์

6.4 *การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)*

วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง และเพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious Code ต่าง ๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

แนวทางปฏิบัติ

6.4.1 การบริหารจัดการข้อมูล (Data Management)

ผู้รับผิดชอบ

- การข้อมูลด้าน IT (ข้อมูลด้านการจัดการ IT จัดการโครงการ งบประมาณพัฒนา/บำรุงรักษาระบบ)
  - ข้อมูลทั่วไป ดูแลโดยส่วนงาน / ผู้ที่ได้รับมอบหมายให้ดูแลข้อมูลนั้น ๆ
  - ข้อมูลลับ ดูแลโดยส่วนงาน ที่มีหน้าที่รับผิดชอบงานและหน้าที่กำหนดในโครงสร้างของฝ่าย หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติงานในเรื่องนั้น ๆ
- ข้อมูลของบริษัท / ฝ่าย ที่อยู่ในระบบ IT (ข้อมูลที่ใช้ในกิจการบริษัท ทั้งด้านการให้บริการธุรกรรมต่าง ๆ และข้อมูลเพื่อการบริหารจัดการที่อยู่ในระบบ IT ที่ฝ่ายเทคโนโลยีสารสนเทศให้การสนับสนุนการใช้งานจัดเป็นข้อมูลที่มีความสำคัญ)
  - ข้อมูลที่ใช้งานในกิจการบริษัท ดูแลโดยผู้มีสิทธิใช้งานที่บริษัทกำหนด
  - ข้อมูลที่อยู่ระหว่างประมวลผล ดูแลโดยฝ่ายเทคโนโลยีสารสนเทศ
  - ข้อมูลที่จัดเก็บสำรองตามข้อปฏิบัติด้านระบบ ดูแลโดยฝ่ายเทคโนโลยีสารสนเทศ
- เจ้าของระบบงาน กำหนดให้ผู้มีอำนาจสูงสุดของแต่ละสายงาน เป็นเจ้าของระบบงานของฝ่ายที่ตนเองดูแล หรือตามที่บริษัทกำหนด เช่น ระบบบัญชี เจ้าของระบบงาน คือผู้มีอำนาจสูงสุดของฝ่ายบัญชี ระบบบริหารงานบุคคล เจ้าของระบบงาน คือผู้มีอำนาจสูงสุดของฝ่ายทรัพยากรบุคคล ระบบงาน IT เจ้าของระบบงาน คือผู้มีอำนาจสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเจ้าของระบบงานจะเป็นผู้กำหนดสิทธิ์ในการเข้าถึงข้อมูลให้กับผู้ปฏิบัติงาน หรือผู้ที่ต้องการใช้ข้อมูล ส่วนระบบงานที่มีความเกี่ยวข้องกับหลายฝ่าย ให้ยึดตามฝ่าย

ที่มีส่วนสำคัญมากที่สุดในระบบงานนั้น ๆ โดยให้ผู้มีอำนาจสูงสุดของฝ่ายเป็นเจ้าของระบบงาน หรือแล้วแต่บริษัทจะกำหนด

แนวทางปฏิบัติ

1 กำหนดให้พนักงานทุกระดับมีสิทธิ์เข้าถึงข้อมูลตามแต่ละสายงานและตามตำแหน่งหน้าที่ที่ได้รับมอบหมายเท่านั้น หากมีความจำเป็นต้องเข้าถึงข้อมูลที่ไม่ได้เป็นไปตามตำแหน่งหน้าที่ ต้องได้รับอนุญาต ดังนี้

1.1 ข้อมูลที่อยู่ในสายงานเดียวกัน ให้ขออนุมัติจากผู้มีอำนาจสูงสุดในสายงาน

1.2 ข้อมูลข้ามสายงาน จะต้องได้รับการอนุมัติจากประธานเจ้าหน้าที่บริหารเท่านั้น

2 การขอใช้ข้อมูลทุกประเภท ต้องระบุผู้ขอ วัตถุประสงค์ และระยะเวลา ในการใช้งาน ที่ชัดเจน การคืน (ถ้ามี) ให้นำมาคืนเมื่อเสร็จหรือเมื่อกำหนด การยกเลิก (ปิด) สิทธิ์การใช้ข้อมูลให้ยกเลิกเมื่อเสร็จ หรือเมื่อครบกำหนด ห้ามทำสำเนาข้อมูลที่ระบุไว้ว่า "ห้ามทำสำเนา" โดยมิได้รับอนุญาตจากเจ้าของข้อมูล ผู้ขอข้อมูลต้องปฏิบัติตามขั้นตอนการขอใช้ข้อมูล ที่กำหนดแตกต่างกันตามประเภทข้อมูล และกลุ่มผู้ขอ

3 กำหนดชั้นความลับของข้อมูลเป็นข้อมูลทั่วไป และข้อมูลลับและกำหนดวิธีการขอใช้ข้อมูลไว้ดังนี้

3.1 ข้อมูลทั่วไป

- ถ้าผู้ขอใช้ข้อมูลเป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ให้ผู้ขอแจ้งรายละเอียดกับผู้ดูแลข้อมูล
- ถ้าผู้ขอใช้ข้อมูลเป็นพนักงานนอกฝ่ายที่เป็นเจ้าของข้อมูล ให้ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้มีอำนาจสูงสุดในสายงานของตน และประธานเจ้าหน้าที่บริหาร เมื่อได้รับอนุมัติแล้วจึงแจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่ง ข้อมูลให้

3.2 ข้อมูลลับ

- ถ้าผู้ขอใช้ข้อมูลเป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ให้ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้มีอำนาจสูงสุดในสายงาน เมื่อได้รับอนุมัติแล้วจึงแจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่งข้อมูลให้
- ถ้าผู้ขอใช้ข้อมูลเป็นพนักงานนอกฝ่ายที่เป็นเจ้าของข้อมูล ให้ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้มีอำนาจสูงสุดในสายงานของตน และประธานเจ้าหน้าที่บริหาร เมื่อได้รับอนุมัติแล้วจึงแจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่ง ข้อมูลให้

- ถ้าผู้ขอใช้เป็นบุคคลภายนอก ให้ทำหนังสือขอจากหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้น ๆ โดยผู้พิจารณาอนุมัติต้องเป็นผู้บริหารระดับ ประธานเจ้าหน้าที่ขึ้นไป
- การจัดทำ/ส่งข้อมูลลับ ต้องได้รับการเข้ารหัส (Encryption) ทุกครั้ง และการส่งมอบรหัส กับข้อมูล ไม่ควรจัดส่งไปพร้อมกัน และใช้วิธีเดียวกันในการส่ง และให้ผู้ขอทำการลบข้อมูล และรหัส ทันทีหลังจากเสร็จกสิ้นการใช้งาน

3.3 ข้อมูลของบริษัท / ฝ่าย ที่อยู่ในระบบ IT

- ถ้าผู้ขอใช้เป็นพนักงานบริษัท ให้แจ้งรายละเอียดเพื่อขออนุมัติ จากผู้บังคับบัญชาของตน (ระดับผู้อำนวยการฝ่ายขึ้นไป)
- ถ้าผู้ขอใช้เป็นบุคคลภายนอก ให้ทำหนังสือขอจากหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้น ๆ โดยผู้พิจารณาอนุมัติต้องเป็นผู้บริหารระดับ ประธานเจ้าหน้าที่ ขึ้นไป
- เมื่อต้นสังกัด หรือฝ่ายที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกอนุมัติแล้ว ให้ส่งเรื่องขออนุมัติใช้ข้อมูลไปยังสายงานที่ดูแล IT ผู้ดูแลข้อมูล (ระดับผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ)
- เมื่อสายงานที่ดูแล IT ผู้ดูแลข้อมูล พิจารณาอนุมัติให้ใช้ข้อมูลได้ ผู้ดูแลข้อมูลจะสั่งการตามสายงานเพื่อให้เจ้าหน้าที่ผู้ดูแลจัดทำ / ส่ง / เปิดระบบให้ใช้ข้อมูล (ตามแต่วัตถุประสงค์ของผู้ขอ)
- กรณีผู้ขอใช้ เป็นบุคคลภายนอก เจ้าหน้าที่ผู้ดูแลจะส่งข้อมูลให้ฝ่ายที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้น ๆ เพื่อดำเนินการติดต่อกับผู้ขอใช้ (บุคคลภายนอก) ต่อไป
- เมื่อครบระยะเวลาใช้งาน หรือผู้ใช้แจ้งใช้งานเสร็จสิ้น (ก่อนครบกำหนด) ผู้ดูแลข้อมูลปิดระบบการเข้าใช้งาน

4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ทุกครั้ง และการส่งมอบรหัส กับข้อมูล ไม่ควรจัดส่งไปพร้อมกัน และใช้วิธีเดียวกันในการส่ง และให้ผู้ขอทำการลบข้อมูล และรหัส ทันทีหลังจากเสร็จสิ้นการใช้งาน

6.4.2 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Information Access Control)

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1 กระบวนการหลักในการควบคุมการเข้าถึงระบบ

1.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

1.2 ผู้ดูแลระบบจะต้องตรวจสอบข้อมูลของผู้ที่ต้องการเข้าใช้งานระบบด้วยการพิจารณาอย่าถ้วนถี่ในกรณีที่มีความจำเป็นต้องให้สิทธิ์แก่บุคคลอื่นใช้งานระบบคอมพิวเตอร์ เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่าง ๆ ต้องมีการขออนุมัติจากผู้บริหารฝ่ายที่เป็นเจ้าของระบบงาน หรือเจ้าของข้อมูล ก่อนทุกครั้ง

1.3 ผู้ดูแลระบบจะทบทวนสิทธิ์ผู้ร้องขอที่ผ่านการพิจารณาและอนุมัติจากผู้บริหารฝ่าย/หัวหน้าฝ่าย โดยตรวจสอบจากเอกสารการขอเปิดสิทธิ์และจัดเก็บเอกสารนั้นไว้เป็นหลักฐาน

1.4 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไข เปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลได้

1.5 ผู้ดูแลระบบจะต้องกำหนดขั้นตอนการปฏิบัติในการขอสิทธิ์เปิดสิทธิ์การใช้งาน รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน ในกรณีพนักงานลาออก ผู้ดูแลระบบต้องดำเนินการปิดสิทธิ์การเข้าถึงระบบภายใน 24 ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงาน ต้องดำเนินการเปลี่ยนแปลงสิทธิ์ภายใน 7 วัน

1.6 บริษัทต้องมีการสอบทานสิทธิ์การเข้าใช้งานโดยผู้มีอำนาจอนุมัติสิทธิ์การใช้งานว่าสิทธิ์ดังกล่าวยังมีความเหมาะสมอยู่หรือไม่ โดยควรมีการสอบทานสิทธิ์อย่างน้อยปีละ 1 ครั้ง

2 การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

2.1 กำหนดมาตรฐานการเข้าใช้งาน

- บริษัทได้กำหนดสิทธิ์การเข้าใช้งานของผู้ใช้งานเพื่อยืนยันตัวตนของผู้ใช้งานก่อนเข้าสู่ระบบ คอมพิวเตอร์แยกเป็นรายบุคคลดังต่อไปนี้
  - การกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร
  - การขอ Username และ Email สำหรับพนักงานเข้าใหม่ ต้องดำเนินการร้องขอโดยฝ่ายทรัพยากรบุคคล (HR) ซึ่งเป็นผู้ดำเนินการขอเปิดสิทธิ์ให้ครั้งแรกเพื่อตรวจสอบประวัติ และข้อมูลส่วนตัวพนักงานใหม่ให้ถูกต้อง โดยจะต้องกรอกแบบฟอร์มการขอซึ่งอนุมัติโดยผู้จัดการฝ่ายทรัพยากรบุคคลขึ้นไป
  - การขอยกเลิก Username และ Email ต้องดำเนินการร้องขอโดยหัวหน้าฝ่ายในสายงานนั้น ๆ โดยจะต้องกรอกแบบฟอร์มการขอยกเลิกซึ่งอนุมัติโดยผู้มีอำนาจสูงสุดในสายงาน
  - การขอเพิ่ม ปรับปรุง หรือเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบใด ๆ ให้กับพนักงาน จะต้องได้รับการอนุมัติจากผู้บริหารฝ่ายที่เป็นเจ้าของระบบงาน หรือเจ้าของข้อมูล ก่อนทุกครั้ง
- ผู้ใช้งานต้องเก็บและรักษา Password สำหรับทุกระบบงานที่ได้รับมอบมาให้เป็นความลับ และควรเปลี่ยน Password หลังจากเข้าใช้งานในครั้งแรกโดยทันที
- การขอรหัสผ่านใหม่ของผู้ใช้งาน เนื่องจากลืมรหัสผ่าน หรือถูกล็อครหัสผ่าน จะต้องมีการยืนยันตัวตนของผู้ขอก่อนการให้รหัสผ่านใหม่ทุกครั้ง
- การขอรหัสผ่านใหม่ที่ไม่ใช่ของตน ไม่สามารถกระทำได้ เว้นแต่กรณีฉุกเฉินและไม่สามารถติดต่อเจ้าของสิทธิ์ได้ หรือกรณีที่เจ้าของสิทธิ์ไม่ยอมมอบรหัสผ่านให้ โดยการขอรหัสผ่านใหม่นั้นต้องได้รับการอนุมัติจากหัวหน้าฝ่ายในสายงานนั้น ๆ หรือบุคคลที่มีอำนาจสูงกว่าตามสายงาน เป็นลายลักษณ์อักษร

- ผู้ใช้งานต้องใช้ Username และ Password ส่วนบุคคลสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์ ที่ตนเองครอบครองอยู่เท่านั้น กรณีที่จำเป็นต้องใช้งานเครื่องคอมพิวเตอร์อื่น ๆ จะต้องได้รับอนุญาตจากผู้ที่ครอบครองหรือผู้ที่มีอำนาจเสียก่อน
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านใหม่โดยทันที
- ผู้ใช้งานต้องไม่ใช้โปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำ Password ส่วนบุคคลของตนโดยอัตโนมัติ (Save Password) เพื่อป้องกันไม่ให้ผู้อื่นเข้าใช้งานได้โดยไม่ต้องใส่ Password
- ผู้ใช้งานต้องไม่จดหรือบันทึก Password ส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- กรณีที่มีความจำเป็นที่จะต้องบอก Password แก่ผู้อื่น เนื่องจากความจำเป็นของงาน หลังจากใช้งานแล้วให้ทำการเปลี่ยน Password ใหม่ทันที

2.2 หลักเกณฑ์การกำหนด Username และ Password มีดังนี้

- การตั้งชื่อ Username จะต้องมีความยาวอย่างน้อย 6 ตัวอักษร โดยกำหนดให้ใช้ชื่อภาษาอังกฤษ ของพนักงานเป็น Username ส่วนกรณีชื่อซ้ำกันให้ใช้ '.' คั่นแล้วตามด้วยตัวอักษรตัวแรกของนามสกุล
- Password ต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร ให้มีความซับซ้อน เช่น มีการผสมกันระหว่างตัวอักษรพิมพ์เล็ก, พิมพ์ใหญ่ และตัวเลขหรือตัวอักษรพิเศษ
- ให้กำหนดวันหมดอายุการใช้งานของ Password เช่น 30, 60, 90 วัน สำหรับความปลอดภัยสูง และ 120, 150, 180 วันสำหรับความปลอดภัยต่ำ และเมื่อครบกำหนด ต้องมีการบังคับให้เปลี่ยน (Force Change)
- มีการป้องกันการใช้ Password ซ้ำ ๆ กันของแต่ละบุคคล โดยกำหนดให้ Password ที่เคยถูกใช้งานไปแล้ว ไม่สามารถนำกลับมาใช้งานได้อีก ในจำนวน 3 ครั้งล่าสุดที่มีการเปลี่ยน Password
- ไม่กำหนด Password ส่วนบุคคลจากส่วนหนึ่งส่วนใดของ ชื่อ นามสกุล ชื่อเล่น วันเดือนปีเกิด รหัสพนักงาน หรือรหัสใด ๆ ที่เกี่ยวข้องกับตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ คำศัพท์ที่ใช้ในพจนานุกรม หรือจากคำที่มักใช้ติดต่อสื่อสารกันโดยทั่วไป

2.3 การ Login เข้าใช้งานระบบคอมพิวเตอร์

- ผู้ใช้งานจะต้อง Login เข้าระบบด้วยตนเองห้ามมิให้ผู้อื่นดำเนินการให้
- ผู้ใช้งาน ไม่ควรอนุญาตให้ผู้อื่นใช้ Username และ Password ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน
- ไม่อนุญาตให้นำ Username ของตนเอง Login เข้าสู่ระบบแล้วให้ผู้อื่นใช้งาน
- ให้ Logout ออกจากระบบเมื่อใช้งานแล้วเสร็จ หรือมิได้อยู่ที่หน้าเครื่องคอมพิวเตอร์เป็นเวลานาน
- ถ้าผู้ใช้งานใส่ Password ผิดติดต่อกันเกิน 6 ครั้ง ระบบจะทำการล็อคบัญชี ชื่อผู้ใช้งานนั้นทันที และจะปลดล็อคโดยอัตโนมัติเมื่อเวลาผ่านไป 30 นาที หรือให้ติดต่อเจ้าหน้าที่ที่ดูแลระบบ

6.4.3 การควบคุมของระบบฐานข้อมูล (Database Access Control)

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1 กำหนดมาตรฐานการติดตั้งระบบฐานข้อมูล

1.1 ผู้ติดตั้งระบบฐานข้อมูล จะต้องเป็นพนักงานในส่วนสนับสนุนสารสนเทศ หรือพนักงานของบริษัท ซึ่งบริษัทได้มอบหมายให้ทำหน้าที่ดังกล่าว แต่ทั้งนี้จะต้องมีพนักงานในส่วนสนับสนุนสารสนเทศร่วมดำเนินการด้วย

1.2 ผู้ติดตั้งระบบฐานข้อมูลจะต้องใช้ซอฟท์แวร์ที่มีลิขสิทธิ์การใช้งานตามกฎหมาย

1.3 ส่วนสนับสนุนสารสนเทศ หรือพนักงานของบริษัท ที่ได้รับมอบหมาย ให้เป็นผู้ติดตั้งโปรแกรมปรับปรุงข้อมูลหรือระบบ ของระบบฐานข้อมูลจะต้องคำนึงถึง

- ผลกระทบของการติดตั้งต่อผู้ใช้งานหรือต่อระบบงานที่เกี่ยวข้อง
- การประเมินความเสี่ยงของการติดตั้ง Patch ดังกล่าว
- การแจ้งให้ส่วนที่เกี่ยวข้องได้รับทราบ
- การเตรียมการเพื่อย้อนกลับมาสู่ระบบเดิมหากการติดตั้งไม่สำเร็จ รวมทั้งรายงานผลการติดตั้งให้กับผู้บังคับบัญชาได้รับทราบด้วย

2 กำหนดมาตรฐานของผู้ใช้งาน (User Identification) และการอนุมัติการใช้งาน (Authorization)

2.1 ต้องมีการกำหนดกลุ่มใช้งาน ดังนี้

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

หากมีความจำเป็นต้องเพิ่มกลุ่มผู้ใช้งานใหม่ ต้องขออนุมัติอย่างเป็นลายลักษณ์อักษรกับผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

2.2 มาตรฐานการอนุมัติการใช้งาน (Authorization)

- เมื่อผู้ใช้งานได้รับความเห็นชอบจากหัวหน้าฝ่ายและผู้บริหารสูงสุดของฝ่ายต้นสังกัดแล้ว จะต้องขออนุมัติจากเจ้าของระบบงานตามลำดับขั้นในการขอใช้งานระบบฐานข้อมูล และผู้ดูแลระบบฐานข้อมูล ต้องจัดทำทะเบียนผู้ใช้งานให้สอดคล้องกับกลุ่มของผู้ใช้งานตามข้อ 2.1

3 กำหนดมาตรฐานในการเข้าใช้งาน (Login) และการเข้าถึงข้อมูล (Access Control) ในระบบฐานข้อมูล

3.1 กำหนดให้ใช้หลักเกณฑ์การกำหนด Username และ Password เหมือนกันกับหัวข้อที่ 6.4.2 ข้อย่อย 2.2

3.2 กำหนดมาตรฐานการเข้าถึงข้อมูล (Access Control)

- กำหนดวิธีการเข้าถึงข้อมูลให้สอดคล้องกับกลุ่มของผู้ใช้งานระบบ โดยกำหนดกลุ่มเบื้องต้นดังนี้
  - Super User = ALL (เข้าถึงระบบฐานข้อมูลได้ทั้งหมด)
  - DBA User = Tables (Create/Drop/Read/Write/Insert/Delete), Grant Privilege (เข้าถึงตารางข้อมูลทั้งหมดและมีสิทธิ์เต็ม)
  - Developer = Read /Write ขึ้นกับความจำเป็นของระบบงาน
  - Operator User = Read (For Backup อ่านข้อมูลได้อย่างเดียว)
  - Audit User = Read (อ่านข้อมูลได้อย่างเดียว)

4 กำหนดมาตรฐานของการตรวจสอบการเข้าใช้งาน (Audit Trail) และความถูกต้องของข้อมูล (Data Integrity) ในระบบฐานข้อมูล

4.1 ตรวจสอบการเข้าใช้ระบบฐานข้อมูลโดยผู้ใช้งานและรายงานสรุปให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

4.2 ตรวจสอบความถูกต้องของข้อมูล (Data Integrity) ร่วมกับฝ่ายตรวจสอบภายในและจัดทำรายงานผลการตรวจสอบให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

5 กำหนดมาตรฐานการสำรองข้อมูลและการนำกลับมาใช้ เพื่อป้องกันข้อมูลเสียหาย

5.1 ส่วนสนับสนุนสารสนเทศ ต้องพิจารณาจัดหา Media ที่มีประสิทธิภาพเพื่อใช้ในการสำรองข้อมูล

5.2 ส่วนสนับสนุนสารสนเทศ และฝ่าย/ส่วนงานที่เกี่ยวข้อง ต้องร่วมกันพิจารณาถึงวิธีการสำรองข้อมูล และ ติดตั้งข้อมูลของแต่ละระบบงาน

5.3 ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบการสำรองข้อมูลว่าทำสำเร็จหรือไม่ และหากไม่สำเร็จต้องรีบดำเนินการแก้ไข ภายใน 1 วัน

5.4 การ Restore Data สามารถกระทำได้เฉพาะผู้ที่ได้รับมอบหมาย ซึ่งจะต้องได้รับอนุญาตจากเจ้าของระบบงานก่อนทุกครั้ง และได้รับการสั่งจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

5.5 ส่วนสนับสนุนสารสนเทศ ต้องจัดเก็บ Media ที่ใช้ในการสำรองข้อมูลไว้ในสภาพแวดล้อมที่เหมาะสมและมีระบบรักษาความปลอดภัยที่ดี

5.6 ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบสภาพ Media และข้อมูลที่อยู่ใน Media อย่างสม่ำเสมอว่ายังอยู่ในสภาพที่ใช้งานได้ดีหรือไม่ หากพบปัญหาให้รีบดำเนินการแก้ไข

6.4.4 การรักษาความปลอดภัยระบบคอมพิวเตอร์เครือข่ายและการควบคุมการเข้าถึงระบบเครือข่าย (Computer Network Security and Network Access Control)

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1 การบริหารจัดการการเข้าถึงระบบเครือข่าย

1.1 ผู้ดูแลระบบต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้ใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

1.2 ผู้ดูแลระบบต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งาน

1.3 ผู้ดูแลระบบต้องป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน เช่น ผู้ใช้งานห้ามนำอุปกรณ์จากภายนอกเชื่อมต่อเข้ามาใช้ในบริษัทโดยไม่ได้รับอนุญาต หรือห้ามเชื่อมต่อระบบ Network อื่นใดเข้ากับระบบ Network ของบริษัทโดยไม่ได้รับอนุญาต

1.4 ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก ต้องเชื่อมต่อผ่านอุปกรณ์ Firewall หรือ ฮาร์ดแวร์อื่น ๆ ที่มีระบบป้องกันการถูกโจมตีผ่านระบบเครือข่ายหรือการลักลอบขโมยข้อมูลผ่านระบบเครือข่าย รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

1.5 ผู้ดูแลระบบต้องตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้ทุกเดือน

- ความพยายามในการบุกรุกผ่านระบบเครือข่าย
- การใช้งานในลักษณะที่ผิดปกติ
- การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

1.6 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายของบริษัทต้องผ่านความเห็นชอบจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศทุกกรณี

1.7 สำหรับ Server ที่จะทำการติดตั้งเข้ากับเครือข่ายของบริษัท บริษัทผู้ดูแลการติดตั้ง Server ดังกล่าวต้องส่งรายละเอียดของระบบปฏิบัติการ (Operating System) และ Service Pack หรืออื่น ๆ ที่จำเป็นสำหรับการ

ติดตั้งให้กับส่วนสนับสนุนสารสนเทศ รับทราบข้อมูลก่อน หลังจากนั้นจึงจะจ่าย IP Address ให้และให้ทำการ Monitor Port ที่จ่ายให้กับ Server ดังกล่าวไม่น้อยกว่า 1 สัปดาห์อย่างใกล้ชิดพร้อมกันรายงานผลต่อผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

1.8 การเชื่อมต่อเครือข่ายทั้งภายในและภายนอกหน่วยงานโดยผ่านทางอินเทอร์เน็ต จำเป็นต้องทำการล็อกอินผ่าน User Account ที่ได้รับอนุญาตเท่านั้น และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง และเข้าใช้งานเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

1.9 ห้ามใช้ Community Name ของอุปกรณ์สื่อสารข้อมูลทุกชนิดหรืออุปกรณ์อื่นที่ใช้ Protocol SNMP ที่ถูกกำหนดชื่อมาโดยผู้ผลิตอุปกรณ์ เมื่อเริ่มใช้งานกับระบบงานของบริษัท ให้ดำเนินการเปลี่ยนชื่อนั้นโดยทันที

1.10 จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก รวมถึงอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

1.11 ให้ส่วนสนับสนุนสารสนเทศ เป็นผู้ถือกุญแจห้องอุปกรณ์สื่อสาร/ห้อง Server ของบริษัท

1.12 เครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัท ควรติดตั้ง Service Pack ตลอดจน Patch ต่าง ๆ ให้ทันสมัยรวมทั้ง Software Antivirus ตามที่บริษัทกำหนด

1.13 จัดหาอุปกรณ์รักษาความปลอดภัยที่ทันต่อความเปลี่ยนแปลงของภัยคุกคามทางด้านเครือข่าย โดยจัดให้มีการทบทวนภาพรวมของการรักษาความปลอดภัยบนเครือข่ายในทุก ๆ 1 ปี เพื่อดำเนินการจัดหาอุปกรณ์ป้องกันต่อไป

1.14 จัดเก็บทะเบียนเลขหมายประจำเครื่องคอมพิวเตอร์ (IP Address) ที่มีการควบคุมการใช้งาน

1.15 จัดทำและปรับปรุง Configuration ของระบบเครือข่ายให้มีความทันสมัยและปลอดภัยอยู่เสมอ

1.16 ทำการ Backup Configuration ของอุปกรณ์สื่อสารข้อมูลเป็นประจำทุก 3 เดือน หรือทุกครั้งที่มีการเปลี่ยนแปลง

1.17 จัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ศ. 2560 (หรือฉบับล่าสุด)

- ต้องมีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ของบริษัท ทั้งนี้จะต้องเป็นไปตามข้อกำหนดของ พรบ. คอมพิวเตอร์ โดยจะต้องเก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้ไม่ต่ำกว่า 90 วัน
- กรณีที่ผู้ใช้งานอินเทอร์เน็ตเป็นบุคคลภายนอก จะต้องกรอกข้อมูลโดยระบุชื่อ นามสกุล บุคคลที่ติดต่อ วันเวลาที่ใช้งาน เพื่อขอรับ Username และ Password ในการใช้งานก่อนทุกครั้ง และกำหนดให้รหัสผ่านแต่ละรหัสนั้นมีอายุไม่เกิน 7 วัน นับจากการเปิดใช้งาน เว้นแต่เข้ามาปฏิบัติงานเป็นระยะเวลานานอนุญาตให้ลงทะเบียนอุปกรณ์เพื่อเข้าใช้ตลอดระยะเวลาที่เข้ามาปฏิบัติงานได้ และจะต้องเก็บข้อมูลประวัติการใช้งานไว้ไม่ต่ำกว่า 90 วัน

2 กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

2.1 ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของบริษัท

2.2 บริษัท ไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการ อินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร หรือเพื่อกิจการใด ๆ ที่ไม่มีส่วนเกี่ยวข้องกับบริษัท

2.3 ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานจะต้องไม่อ่าน, เขียน, ลบ, เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัย รวมไปถึงเข้าสู่เครื่องคอมพิวเตอร์ของบริษัท หรือหน่วยงานอื่น ๆ การเผยแพร่ข้อมูล เนื้อหา หรือข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว บริษัทไม่มีส่วนรับผิดชอบความเสียหายดังกล่าว

2.4 ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของบริษัท

2.5 บริษัทให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน หรือจ่ายแจกสิทธิ์นี้ ให้กับผู้อื่นไม่ได้

2.6 บัญชีผู้ใช้งาน (User Account) ที่บริษัทให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบ ผลต่าง ๆ อันอาจจะเกิดมีขึ้นรวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

2.7 ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศผ่านทางเครือข่ายได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงได้เท่านั้น

2.8 ผู้ใช้งานทั้งที่อยู่ภายในและภายนอกบริษัทต้องทำการยืนยันตัวบุคคลผ่านบัญชีผู้ใช้งาน (User Account) ที่ได้รับ ซึ่งประกอบด้วย Username และ Password ก่อนที่จะได้รับอนุญาตให้สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของบริษัทได้

2.9 ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไข ในการรับทราบกฎระเบียบ หรือนโยบายต่าง ๆ ที่บริษัทกำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบ หรือนโยบายของบริษัทมิได้

2.10 บริษัททรงไว้ซึ่งสิทธิที่จะปฏิเสธการเชื่อมต่อและ/หรือการใช้งาน และทรงไว้ซึ่งสิทธิที่จะยกเลิกหรือระงับการเชื่อมต่อและ/หรือการใช้งานใด ๆ ของผู้ใช้งานที่ล่วงละเมิดหรือพยายามจะล่วงละเมิดกฎระเบียบนี้ของบริษัทโดยไม่มีการแจ้งให้ทราบก่อนล่วงหน้า

6.4.5 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server Security)

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1 ผู้ดูแลระบบ ต้องทำการติดตั้งไฟร์วอลล์ (Firewall) สำหรับตรวจจับการบุกรุกเครือข่ายของบริษัท

2 ค่าเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ (Firewall) เช่น ค่าพารามิเตอร์การกำหนดใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

3 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ต (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

4 การติดตั้งเครื่องคอมพิวเตอร์ Server ต้องมีการจัดแบ่งหมวดหมู่ตามที่ส่วนสนับสนุนสารสนเทศได้กำหนดไว้

5 การติดตั้งเครื่องคอมพิวเตอร์ Server หรืออุปกรณ์สื่อสารข้อมูล หรืออุปกรณ์รักษาความปลอดภัยต่าง ๆ ต้องมีการจัดทำแบบแปลนการติดตั้งอุปกรณ์บนตู้ Rack แสดงตำแหน่งต่าง ๆ ของอุปกรณ์บนตู้ Rack โดยจัดเก็บไว้ในส่วนสนับสนุนสารสนเทศ

6 การติดตั้งอุปกรณ์สื่อสารข้อมูลทุกชนิดกับระบบงานต่าง ๆ ของบริษัท ให้อยู่ในความควบคุมดูแลของส่วนงานสนับสนุนสารสนเทศ

7 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในนั้นจะอนุญาตให้เฉพาะผู้ดูแลระบบตามสิทธิ์ที่ได้รับเท่านั้น กรณีที่ไม่ได้เป็นผู้ดูแลระบบจะต้องขออนุญาตจากผู้บังคับบัญชาของตน (ระดับผู้อำนวยการฝ่ายขึ้นไป) เมื่ออนุมัติแล้ว ให้ส่งเรื่องขออนุมัติไปยังผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

8 ผู้ดูแลระบบต้องคอยเฝ้าระวังประเมินความเสี่ยงช่องโหว่ติดตามและตรวจสอบ Log ของระบบเครือข่ายเพื่อใช้วิเคราะห์หาข้อผิดพลาดหรือจุดอ่อนอย่างสม่ำเสมอเพื่อจะได้ดำเนินการแก้ไขได้ทันท่วงที

9 เครื่องแม่ข่ายคอมพิวเตอร์ (Server) เครื่องคอมพิวเตอร์ทุกเครื่องในบริษัท และอุปกรณ์ต่าง ๆ ที่มีการตั้งค่าเวลา ต้องตั้งเวลาให้ตรงกันโดยอ้างอิงเวลาตามมาตรฐานกลางของโลกเพื่อช่วยในการตรวจสอบเวลาหากระบบคอมพิวเตอร์ของบริษัทถูกบุกรุก

6.4.6 การป้องกันไวรัสคอมพิวเตอร์ / มัลแวร์ (Virus / Malware Protection)

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1 ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ สำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Server Protect and Office Scan) รวมถึงเครื่องที่ให้บริการต่าง ๆ เช่น E-mail Server (Scan Mail), Web Server, File Server, Print Server เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้งต้องจัดให้มีการอัพเดตข้อมูลจากเจ้าของผลิตภัณฑ์นั้น ๆ ทุก 24 ชั่วโมง

2 กำหนดหน้าที่และความรับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์

2.1 กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการตรวจจับ และทำลายไวรัสคอมพิวเตอร์/มัลแวร์ บนเครื่องคอมพิวเตอร์ส่วนบุคคล ไม่ให้แพร่กระจายทำความเสียหายกับข้อมูลของบริษัท

2.2 กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ ต้องมีการแจ้งข่าวเกี่ยวกับไวรัสคอมพิวเตอร์/มัลแวร์ทันที หากมีการระบาดของไวรัสคอมพิวเตอร์/มัลแวร์ตัวใหม่

2.3 กำหนดให้ส่วนเทคนิคปฏิบัติการส่วนเครือข่าย มีหน้าที่รับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์ อย่างสม่ำเสมอบน Server และอุปกรณ์เครือข่าย เพื่อป้องกันความเสียหายกับข้อมูลของบริษัท

3 ผู้ใช้งานที่พบเหตุไม่พึงประสงค์ที่อาจสร้างความเสี่ยงหรืออาจจะมีผลกระทบต่อการดำเนินธุรกิจและระบบสารสนเทศ เช่น พบช่องโหว่, Malware, Virus จะต้องแจ้งมายังฝ่ายเทคโนโลยีสารสนเทศรับทราบโดยเร็ว

6.5 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. ผู้ดูแลระบบเครือข่ายไร้สายมีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1.1 เครือข่ายแบบไร้สายเป็นสมบัติของบริษัท ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้าม ต้องได้รับโทษจากทางบริษัทและรับโทษตามกฎหมาย

1.2 การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

1.3 ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

1.4 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

1.5 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย ในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศทราบทันที

2. ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

2.1 ห้ามผู้ใช้งาน นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access Point, Wireless Router, Wireless USB Client หรือ Wireless Card

2.2 กำหนดให้ใช้หลักเกณฑ์การควบคุมการเข้าถึงและใช้บริการระบบเครือข่ายเหมือนกันกับหัวข้อที่ 6.4.2

6.6 *การควบคุมการพัฒนา (System Development) หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Computer System Conversion)*

วัตถุประสงค์

เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. การกำหนดขั้นตอนการปฏิบัติงาน

1.1 จัดให้มีขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบและขั้นตอนในการโอนย้ายระบบงาน

1.2 จัดให้มีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

1.3 มีการสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

2. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

2.1 การร้องขอ

- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ต้องจัดทำให้เป็นลายลักษณ์อักษร และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
- มีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
- มีการสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ

2.2 การปฏิบัติงานพัฒนาระบบงาน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้การแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

2.3 การทดสอบ

- ผู้ที่ร้องขอและฝ่ายคอมพิวเตอร์ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการ

ประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

- ในระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง

2.4 การโอนย้ายระบบงานเพื่อใช้งานจริง

- ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

2.5 การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา

- ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
- ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน
- ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

2.6 การทดสอบหลังการใช้งาน (Post- Implementation Test)

- ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

2.7 การสื่อสารการเปลี่ยนแปลง

- ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

6.7 *การสำรองข้อมูลระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Data Backup and IT Continuity Plan)*

วัตถุประสงค์

เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability Risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. การสำรองข้อมูลและระบบคอมพิวเตอร์

1.1 การสำรอง

- ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง
- ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้
  - ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
  - ประเภทสื่อบันทึก (Media)
  - จำนวนที่ต้องสำรอง (Copy)
  - ขั้นตอนและวิธีการสำรองโดยละเอียด
  - สถานที่และวิธีการเก็บรักษาสื่อบันทึก
  - ระยะเวลาในการเก็บรักษาข้อมูลสำรอง
- ควรมีการบันทึกการปฏิบัติงาน (Log Book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
- ข้อกำหนดในการสำรองข้อมูลมีดังนี้

- ข้อมูลระบบที่ยังคงใช้งานอยู่ในปัจจุบัน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 1 ครั้ง/เดือน เก็บไว้อย่างน้อย 6 เดือน
- ข้อมูลระบบที่ไม่ได้ใช้งาน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 2 เดือนล่าสุดก่อนที่จะหยุดใช้งาน และให้เก็บข้อมูลไว้จนกว่าจะไม่มีการเรียกใช้งานหรือกู้ข้อมูลบนระบบอีกต่อไป หรืออย่างน้อย 5 ปี
- ข้อมูลสำคัญของฝ่ายต่าง ๆ ที่ยังคงใช้งานอยู่ในปัจจุบัน ให้สำรองข้อมูลแบบ Incremental Backup ทุกวัน และ Full Backup อย่างน้อย 1 ครั้ง/สัปดาห์ เก็บไว้อย่างน้อย 6 เดือน
- ข้อมูลสำคัญของฝ่ายต่าง ๆ ที่ไม่ได้ใช้งาน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 2 เดือนล่าสุดก่อนที่จะหยุดใช้งาน และให้เก็บข้อมูลไว้จนกว่าจะไม่มีการเรียกใช้งานหรือกู้ข้อมูลบนระบบอีกต่อไป หรืออย่างน้อย 5 ปี
- ฐานข้อมูล (Database) ที่ยังคงใช้งานอยู่ในปัจจุบัน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 1 ครั้ง/วัน เก็บไว้อย่างน้อย 24 สัปดาห์
- ฐานข้อมูล (Database) ที่ไม่ได้ใช้งาน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 2 เดือนล่าสุดก่อนที่จะหยุดใช้งาน และให้เก็บข้อมูลไว้จนกว่าจะไม่มีการเรียกใช้งานหรือกู้ข้อมูลบนระบบอีกต่อไป หรืออย่างน้อย 5 ปี
- ข้อมูลอื่น ๆ ที่ยังคงใช้งานอยู่ในปัจจุบัน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 1 ครั้ง/สัปดาห์ เก็บไว้อย่างน้อย 4 เดือน

1.2 การทดสอบ

- ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลรวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้
- ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

1.3 การเก็บรักษา

- ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงาน

ได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย

- ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน
- ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด
- การขอใช้งานสื่อบันทึกข้อมูลสำรองต้องได้รับอนุมัติจากผู้บริหารระดับสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และวันเวลา
- ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่าง ๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน Recycle Bin
- การลบข้อมูลสำรอง ที่เกินกำหนดระยะเวลาเก็บรักษา ให้ผู้ปฏิบัติงานขออนุมัติจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศก่อนดำเนินการทุกครั้ง

2. การเตรียมพร้อมกรณีฉุกเฉิน

2.1 ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้

- ต้องจัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน
- ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
- ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์
- ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด
- ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (Specification) ขั้นต่ำ ค่า Configuration และอุปกรณ์เครือข่าย

- ในกรณีที่บริษัทมีศูนย์คอมพิวเตอร์สำรอง ก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่
- ควรปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

2.2 ควรทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

2.3 ควรสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

2.4 ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

6.8 *การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation Control)*

วัตถุประสงค์

เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่าง ๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk และ Availability Risk

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

1.1 จัดทำขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญ เป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

1.2 กำหนดให้มีระบบการตรวจสอบการ Login เข้ามาใช้งาน โดยต้องบันทึกข้อมูลที่เกี่ยวข้องกับการ Login นั้นไว้ และให้บันทึกทั้งการ Login ที่ทำได้สำเร็จ และไม่สำเร็จเพื่อใช้ในการตรวจสอบภายหลัง

1.3 ควรกำหนดให้มีการบันทึก (Log Book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่าง ๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้

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

2. การติดตามการทำงานของระบบคอมพิวเตอร์ (Monitoring)

2.1 ต้องติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้ อย่างต่อเนื่องและมีประสิทธิภาพ เช่น การรับส่งข้อมูลของระบบซื้อขายหลักทรัพย์ การเชื่อมต่อระหว่างบริษัทกับตลาดหลักทรัพย์ การใช้งานฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ (Capacity) ของระบบ

2.2 บำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ

3. การจัดการปัญหาต่าง ๆ

3.1 ต้องกำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน เช่น กำหนดผู้รับผิดชอบในการแก้ไขปัญหาระบบซื้อขายหลักทรัพย์ รวมถึงเบอร์โทรศัพท์ของผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา

3.2 ควรมีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

4. การควบคุมการจัดทำรายงาน

4.1 การขอให้จัดพิมพ์รายงานต่าง ๆ ควรได้รับความเห็นชอบจากผู้บริหารสูงสุดของฝ่ายที่เกี่ยวข้องนั้น หรือประธานเจ้าหน้าที่ขึ้นไป

4.2 ควรมีทะเบียนคุมการพิมพ์และการจัดส่งรายงาน จัดเก็บรายงานต่าง ๆ ที่ได้จัดพิมพ์แล้วอย่างรัดกุม และกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

6.9 *การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing Services Control)*

วัตถุประสงค์

เพื่อให้บริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

ผู้รับผิดชอบ

ผู้บริหารระดับสูง

ผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

พนักงานส่วนพัฒนาระบบสารสนเทศ

แนวทางปฏิบัติ

1. การคัดเลือกผู้ให้บริการจากภายนอก

   การคัดเลือกผู้ให้บริการจากภายนอกให้เป็นไปตามระเบียบวิธีการคัดเลือกตามกระบวนการจัดซื้อจัดจ้าง โดยการพิจารณาคัดเลือกต้องครอบคลุมเรื่องดังต่อไปนี้

   1.1 การเปรียบเทียบข้อเสนอกับความต้องการของบริษัท

   1.2 การประเมินผลงานที่ผ่านมาของผู้ให้บริการภายนอก

   1.3 ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

   1.4 กำหนดมาตรฐานของอุปกรณ์ที่นำมาติดตั้งใช้งานจะต้องเป็นอุปกรณ์ที่มีคุณภาพและได้มาตรฐาน

   - อุปกรณ์ที่นำมาติดตั้งต้องมีมาตรฐานรับรองจากบริษัทหรือจากผู้ผลิตโดยตรง
   - อุปกรณ์ที่นำมาติดตั้งใช้งาน จะต้องมีมาตรฐานที่เป็นสากล (Standard)

2. การควบคุมด้านความมั่นคงปลอดภัย

   2.1 กำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ที่บริษัททำสัญญาว่าจ้างให้มาปฏิบัติงานซึ่งสอดคล้องกับนโยบายความมั่นคงปลอดภัยของบริษัทและให้ผู้ปฏิบัติงานนั้นลงนามในเอกสารดังกล่าว

2.2 เมื่อสิ้นสุดการจ้างงานหรือการเปลี่ยนแปลงลักษณะการจ้างงานของหน่วยงานภายนอกจะต้องถอนสิทธิ์การเข้าถึงระบบสารสนเทศและทรัพย์สินสารสนเทศโดยทันที

3. การควบคุมระหว่างการให้บริการ

3.1 ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่บริษัทควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัท (Onsite Service) และให้เจ้าหน้าที่บริษัทตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และให้ปิดการเชื่อมต่อทันทีที่การให้บริการเสร็จสิ้น

3.2 ต้องควบคุมผู้ให้บริการจากภายนอกว่ามีการปฏิบัติตามข้อกำหนดที่จัดทำขึ้นอย่างสม่ำเสมอ เช่น ดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่าง ๆ

3.3 ต้องมีการกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือการให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การปรับปรุงเทคโนโลยี ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

3.4 ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

3.5 ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข

3.6 ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

6.10 การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Control)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งจะช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้งานควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของบริษัท ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. การใช้งานทั่วไป

    1.1 เครื่องคอมพิวเตอร์ที่บริษัทอนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินของบริษัท ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของบริษัท และควรใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่น ๆ ที่ตนเองรับผิดชอบด้วยความระมัดระวัง กรณีชำรุดหรือเสียหายต้องรีบแจ้งให้เจ้าหน้าที่ IT รับทราบโดยทันที

    1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท ต้องเป็นโปรแกรมที่มีลิขสิทธิ์อย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

    1.3 ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัท

    1.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ IT เท่านั้น

    1.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ IT เท่านั้น

    1.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

    1.7 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

1.8 ไม่ควรเก็บข้อมูลสำคัญของบริษัทไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

1.9 ไม่ควรเก็บข้อมูลส่วนบุคคลใด ๆ ที่ไม่เกี่ยวข้องกับงานของบริษัทไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่เป็นทรัพย์สินของบริษัท หรือเก็บไว้บนพื้นที่จัดเก็บข้อมูลใด ๆ ของบริษัท ถ้าเจ้าหน้าที่ IT ตรวจพบอนุญาตให้ดำเนินการลบทิ้งได้โดยทันที

1.10 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของบริษัท

1.11 ผู้ใช้ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้

- ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่ควรวางสื่อแม่เหล็ก เช่น ลำโพง ไว้ใกล้เครื่องคอมพิวเตอร์, External Hard Disk หรือ Disk Drive
- ปิดเครื่อง (Shutdown) ทุกครั้งหลังจากเสร็จสิ้นการใช้งาน

1.12 กรณีใช้คอมพิวเตอร์แบบพกพา ควรปฏิบัติดังนี้

- ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ
- ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้
- การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์
- การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
- ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

- ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ
- ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น
- ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
- การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
- ผู้ใช้ ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ
- ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

2. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

2.1 ผู้ใช้ ควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

2.2 ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (Email) หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

2.3 ไม่ควรเปิดจดหมายอิเล็กทรอนิกส์ (Email) หรือไฟล์ที่แนบมากับ Email ที่ไม่รู้จักผู้ส่ง

2.4 ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์

2.5 ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ถ้าไม่แน่ใจให้แจ้งเจ้าหน้าที่ IT

2.6 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์ที่ใช้งานติดไวรัส หรือ Malware ให้ทำการตัดการเชื่อมต่อกับระบบเครือข่ายโดยทันที และห้ามมิให้ผู้ใช้ ใช้งานใด ๆ รวมถึงเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายใด ๆ เพื่อป้องกันการแพร่กระจายของไวรัส หรือ Malware ไปยังเครื่องอื่น ๆ และให้แจ้งเจ้าหน้าที่ IT โดยทันที

6.11 การป้องกันความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูล (Risk Prevention on Data Inaccessible)

วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติให้สามารถดูแลการทำงานของระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ โปรแกรมระบบงาน และฐานข้อมูลต่าง ๆ กรณีที่ไม่สามารถเข้าถึงข้อมูลและไม่สามารถทำงานต่อเนื่องได้ เพื่อให้เกิดผลกระทบต่อการบริการของบริษัทแก่ลูกค้าให้น้อยที่สุด และเพื่อให้บริษัท สามารถดำเนินธุรกิจต่อได้โดยไม่ติดขัด

ผู้รับผิดชอบ

ผู้บริหารระดับสูง

ผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. เพื่อให้สามารถดูแลการทำงานของระบบคอมพิวเตอร์และฐานข้อมูลต่าง ๆ ได้อย่างต่อเนื่องทางฝ่ายเทคโนโลยีสารสนเทศและผู้ถือ Username และ Password มีหน้าที่ดังนี้

    1.1 จัดรวบรวม Username และ Password สำคัญ เพื่อการเข้าถึงระบบงานคอมพิวเตอร์ต่าง ๆ และทำสรุปเก็บเป็นความลับ 1 ชุด ให้ประธานเจ้าหน้าที่บริหารเป็นผู้เก็บรักษาไว้

    1.2 ต้องมีการจัดทำ ผังโครงสร้างระบบโครงข่ายพร้อมตำแหน่งที่วางอุปกรณ์คอมพิวเตอร์ สำคัญทั้งหมด นำส่งให้กับประธานเจ้าหน้าที่บริหารทุก 6 เดือน

6.12 มาตรฐานระบบคอมพิวเตอร์ (Computer System Standards)

วัตถุประสงค์

เพื่อให้การใช้งานระบบคอมพิวเตอร์ของบริษัทเป็นไปอย่างมีประสิทธิภาพ รวดเร็ว ปลอดภัย และรองรับการใช้งานของผู้ใช้ในปัจจุบัน เพื่อเสริมสร้างศักยภาพในการแข่งขันทางธุรกิจให้กับบริษัท

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ที่ใช้งานมานาน ควรเปลี่ยนใหม่ทดแทน เพื่อป้องกันความเสี่ยง กรณีเครื่องเสียหาย โดยกำหนดมาตรฐานอายุการใช้งานของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ดังนี้
    1.1 เครื่องคอมพิวเตอร์แม่ข่าย (Server) 5 ปี ต้องมี MA ตลอดการใช้งาน
    1.2 เครื่องคอมพิวเตอร์ทั่วไป (PC) 5 ปี
    1.3 เครื่องคอมพิวเตอร์พกพา (Notebook) 5 ปี
    1.4 อุปกรณ์จัดเก็บข้อมูล Hard Disk 4 ปี , SSD 6 ปี
    1.5 อุปกรณ์ระบบเครือข่าย (Switch, Access Point) 6 ปี
    1.6 อุปกรณ์ไฟร์วอลล์ (Firewall) 5 ปี ต้องมี MA ตลอดการใช้งาน
    1.7 อุปกรณ์สำรองไฟ (UPS) 5 ปี ควรเปลี่ยนแบตเตอรี่ทุกๆ 2 ปี
2. เครื่องคอมพิวเตอร์ที่ใช้งานจะต้องสามารถรองรับการใช้งานในปัจจุบันของผู้ใช้ได้อย่างเพียงพอ
3. เครื่องคอมพิวเตอร์ที่ใช้งานจะต้องติดตั้งโปรแกรมพื้นฐานที่จำเป็นต่อการใช้งาน และจะต้องติดตั้งโปรแกรม Anti-Virus ตามที่บริษัทกำหนด
4. เครื่องคอมพิวเตอร์ที่ใช้งานควรจะมีมาตรฐานดังต่อไปนี้
    4.1 มาตรฐานของเครื่องคอมพิวเตอร์สำหรับระดับพนักงานออฟฟิศทั่วไปดังนี้
        - หน่วยประมวลผล (CPU) ขั้นต่ำ Intel Core i3 หรือ Core i5
        - หน่วยความจำ (RAM) 4 GB. – 8 GB.
        - พื้นที่จัดเก็บข้อมูล (Hard disk) 500 GB. – 1 TB.
        - ความเร็วในการเชื่อมต่อเครือข่ายระดับ Gigabit
        - จอ (LCD Monitor) 19" – 24" กรณี PC, 14" – 15.6" กรณี Notebook

- Wireless LAN กรณี Notebook จะต้องรองรับตามมาตรฐาน 802.11b/g/n
- เครื่องสำรองไฟ (UPS) 500VA – 1,000VA ควรเปลี่ยนแบตเตอรี่ทุกๆ 2 ปี สำรองไฟได้ไม่ต่ำกว่า 10 นาที

4.2 มาตรฐานของเครื่องคอมพิวเตอร์สำหรับระดับพนักงานฝ่ายบริหารหรือฝ่ายโครงการที่ต้องใช้งานประสิทธิภาพสูงดังนี้

- หน่วยประมวลผล (CPU) ขั้นต่ำ Intel Core i5 หรือ Core i7
- หน่วยความจำ (RAM) 8 GB. – 16 GB.
- พื้นที่จัดเก็บข้อมูล (Hard disk) SSD 128GB – 256GB. และ Hard disk 500 TB. – 1 TB.
- ความเร็วในการเชื่อมต่อเครือข่ายระดับ Gigabit
- การ์ดจอ (Graphic Card) 2GB – 4GB GDDR5
- จอ (LCD Monitor) 24" – 27" กรณี PC, 13" – 15.6" กรณี Notebook
- Wireless LAN กรณี Notebook จะต้องรองรับตามมาตรฐาน 802.11b/g/n/ac

6.13 ระเบียบการใช้งานอินเทอร์เน็ต (Use of the Internet)

วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น ทำให้ระบบคอมพิวเตอร์ของบริษัทถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

ผู้ใช้งานอินเทอร์เน็ตทั้งหมด

แนวทางปฏิบัติ

1. ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่บริษัทจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่าน

ช่องทางอื่น เช่น Dial-Up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษรแล้ว

2. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์(Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่
3. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง เว้นแต่มีการเปิดโหมดการป้องกันไวรัสแบบตลอดเวลา (Real time)
4. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม
5. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท
6. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับบริษัท
7. ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัท ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต
8. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
9. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
10. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
11. ผู้ใช้งานจะต้องตรวจสอบเรื่องลิขสิทธิ์ในการนำข้อมูล เนื้อหา ภาพ สัญลักษณ์หรือข้อความใด ๆ ของบุคคลอื่นที่อาจจะมีลิขสิทธิ์คุ้มครองก่อนนำไปใช้งาน
12. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

13. การใช้งานเว็บบอร์ด (Web Board) ของบริษัท หรือของที่อื่น ๆ ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของบริษัท
14. ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัท ทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
15. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

6.14 ระเบียบการใช้งานจดหมายอิเล็กทรอนิกส์ (Use of the Email)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัทให้ความสำคัญและเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด อันจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัทเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัท ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก
2. ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท
3. สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
4. กำหนดให้ใช้หลักเกณฑ์การกำหนด Username และ Password เหมือนกันกับหัวข้อที่ 6.4.2 ข้อย่อย 2.2

5. รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น "x" ในการพิมพ์แต่ละตัวอักษร
6. ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 5 ครั้ง
7. ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ Logout ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
8. ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
9. ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน
10. ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัทหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท
11. ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
12. ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อการทำงานของบริษัทเท่านั้น
13. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
14. ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com, .bat, .vbs
15. ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
16. ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัท เกิดความแตกแยกระหว่างบริษัทผ่านทางจดหมายอิเล็กทรอนิกส์
17. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
18. ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

19. ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์
20. ผู้ใช้ไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้

6.15 การใช้ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual Property)

วัตถุประสงค์

ลิขสิทธิ์ เป็นทรัพย์สินทางปัญญา ที่กฎหมายให้ความคุ้มครองโดยให้เจ้าของลิขสิทธิ์ถือสิทธิแต่เพียงผู้เดียวที่จะกระทำการใดๆ เกี่ยวกับงานสร้างสรรค์ที่ตนได้กระทำขึ้น กฎหมายลิขสิทธิ์จึงมีวัตถุประสงค์ให้ความคุ้มครอง ป้องกันผลประโยชน์ทั้งทางเศรษฐกิจและทางศีลธรรม ซึ่งบุคคล พึงได้รับจากผลงานสร้างสรรค์อันเกิดจากความนึกคิด และสติปัญญาของตน บริษัทให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา จึงกำหนดให้ใช้งานซอฟต์แวร์ที่บริษัทมีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัท ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว
2. ซอฟต์แวร์ (Software) ที่บริษัท ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น
3. บริษัท ไม่อนุญาตให้พนักงานแจกจ่ายซอฟต์แวร์ (Software) ของบริษัท ให้แก่บุคคลภายนอกหรือให้บุคคลภายนอกใช้ซอฟต์แวร์ (Software) ของบริษัทหรือที่บริษัทถือลิขสิทธิ์ไว้ เว้นแต่ได้รับการอนุญาตจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ
4. ฝ่ายเทคโนโลยีสารสนเทศ สงวนสิทธิ์ที่จะเข้าตรวจสอบข้อมูลการใช้ซอฟต์แวร์ (Software) บนเครื่องคอมพิวเตอร์ที่พนักงานใช้ ได้ตลอดเวลา โดยไม่ต้องแจ้งล่วงหน้า

7. การพิจารณาโทษทางวินัยและการเรียกค่าเสียหาย

1. ผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบาย เงื่อนไข ข้อตกลงตามเอกสารฉบับนี้ แม้ว่าการฝ่าฝืนจะกระทำไม่สำเร็จโดยสมบูรณ์ก็ให้ถือว่ามีความผิดโดยสมบูรณ์
2. พนักงานและลูกจ้างที่ฝ่าฝืนข้อกำหนดนโยบายด้านความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศ โดยจงใจหรือประมาทเลินเล่อ และก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัท หรือบุคคลหนึ่งบุคคลใด บริษัทจะพิจารณาดำเนินการทางวินัย ความผิดทางแพ่งและอาญาแก่พนักงานและลูกจ้างนั้น ตามกฎหมาย ข้อบังคับ ระเบียบ หรือประกาศที่เกี่ยวข้อง
3. ผู้บังคับบัญชาผู้ใด งดเว้น หรือละเว้นการปฏิบัติตามหน้าที่ และเป็นเหตุให้พนักงานหรือลูกจ้างที่อยู่ภายใต้การบังคับบัญชาของตน ฝ่าฝืนข้อกำหนดของนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ ให้นำบทบัญญัติในวรรคก่อนมาใช้บังคับโดยไม่อนุโลม
4. การฝ่าฝืนข้อกำหนดใด ๆ ตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ แม้จะไม่ก่อให้เกิดความเสียหายแก่บริษัท หรือบุคคลหนึ่งบุคคลใดก็ตาม ถ้าผู้บังคับบัญชาเห็นว่ามีเหตุอันสมควร อาจจะบันทึกในประวัติการปฏิบัติงานและจะใช้เป็นข้อมูลประกอบการพิจารณาต่ออายุสัญญาจ้าง การขึ้นเงินเดือน หรือ เลื่อนตำแหน่งด้วยก็ได้
5. ผู้กระทำความผิดเกี่ยวกับ กฎ ระเบียบ เงื่อนไข หรือนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทจะต้องถูกลงโทษตามระเบียบบริษัท โดยฝ่ายทรัพยากรบุคคลจะเป็นผู้ดำเนินการสอบสวนและลงโทษทางวินัย

คุณเชิดศักดิ์ กู้เกียรตินันท์

ประธานเจ้าหน้าที่บริหาร

บริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย