นโยบายความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศ

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ จัดทำขึ้นเพื่อให้พนักงาน
ตระหนักถึงความเข้าใจและมีส่วนร่วมในการใช้งานบนระบบเทคโนโลยีสารสนเทศของ
บริษัท ศรีไทยซุปเปอร์แวร์ จำกัด (มหาชน)

สารบัญ

หน้า

1. วัตถุประสงค์

การกำหนดนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และทราบเกี่ยวกับหน้าที่ความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบายและการปฏิบัติตามนโยบาย

บริษัทฯตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้จัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติให้ผู้ใช้งานมีความตระหนักถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศของบริษัทฯ และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา รวมทั้งเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัทฯด้านอื่นๆ ที่มุ่งเน้นการปฏิบัติงานภายในบริษัทฯให้มีความมั่นคงปลอดภัยในการดำเนินกิจการของบริษัทฯ

2. คำจำกัดความ (Definition of Terms)

- **"บริษัทฯ"** หมายถึง บริษัท ศรีไทยซุปเปอร์แวร์ จำกัด (มหาชน) และบริษัทย่อย
- **"ผู้ใช้งาน"** หมายถึง พนักงานที่ได้รับการว่าจ้างจากบริษัทฯตามเงื่อนไขและสถานะต่างๆ รวมไปถึงบุคคลอื่นๆ ที่ได้รับอนุญาตให้ใช้ระบบสารสนเทศเชื่อมต่อกับบริษัทฯ ทั้งภายในและภายนอกบริษัทฯ
- **"ผู้ดูแลระบบ"** หมายถึง ผู้ที่ทำหน้าที่บริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายภายในบริษัทฯ โดยดูแลการติดตั้งและบำรุงรักษาระบบปฏิบัติการ การติดตั้งฮาร์ดแวร์ การติดตั้งและการปรับปรุงซอฟต์แวร์ รวมถึงการสร้าง ออกแบบและบำรุงรักษาบัญชีผู้ใช้งาน
- **"บุคคลภายนอก"** หมายถึง บุคคล/นิติบุคคล ซึ่งบริษัทฯหรือหน่วยงานในบริษัทฯอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิ์ตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทฯโดยไม่ได้รับอนุญาต
- **"ทรัพย์สินสารสนเทศ"** หมายถึง ข้อมูลไฟล์ ข้อมูลซอฟต์แวร์ ฐานข้อมูล เครื่องมือในการพัฒนาอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย เครือข่ายไร้สาย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด
- **"เครือข่าย (Network)"** หมายถึง ระบบเครือข่ายที่ใช้เชื่อมต่อระหว่างแม่ข่ายและลูกข่าย เพื่อให้ระบบคอมพิวเตอร์ที่มีอยู่ในบริษัทฯสามารถติดต่อกันทั้งภายในและภายนอกบริษัทฯ
- **"เครือข่ายไร้สาย (Wireless Network)"** หมายถึง เทคโนโลยีในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์หรือกลุ่มของเครื่องคอมพิวเตอร์ รวมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่าย

คอมพิวเตอร์ ซึ่งการสื่อสารจะไม่ใช้สายสัญญาณในการเชื่อมต่อ (LAN) แต่จะใช้คลื่นวิทยุ หรือ คลื่นอินฟราเรด ในการรับส่งข้อมูลแทน

- **"ข้อมูล (Information)"** หมายถึง สิ่งที่สื่อสารความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูลหรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือผ่านวิธีการใดๆ และไม่ว่าจะจัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนที่ ภาพวาด ภาพถ่าย การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
- **"เจ้าของข้อมูล"** หมายถึง ผู้มีหน้าที่ที่บริษัทฯมอบหมายให้รับผิดชอบข้อมูลจากการปฏิบัติงานบนระบบงานต่างๆ โดยเจ้าของข้อมูลเป็นผู้จัดทำข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเสียหาย
- **"อินเทอร์เน็ต (Internet)"** หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายทั่วโลกไว้ด้วยกัน เกิดจากการรวมกันของหลายเครือข่ายย่อยทั้งบุคคลและองค์กรเพื่อให้เกิดการสื่อสารและแลกเปลี่ยนข้อมูลร่วมกัน

3. การบริหารความมั่นคงปลอดภัยสำหรับสารสนเทศ และแนวทางในการรักษาความปลอดภัย

การบริหารความมั่นคงปลอดภัยสำหรับสารสนเทศ หมายถึง การสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศ เพื่อให้เป็นมาตรฐานและมีประสิทธิภาพคุ้มค่ากับการลงทุน จึงประกอบด้วยหลักการดังต่อไปนี้

1. **Confidentiality** มีกระบวนการรักษาความลับที่เหมาะสม ผู้มีสิทธิ์เท่านั้นที่จะเข้าถึงข้อมูลได้
2. **Integrity** มีความถูกต้องและสมบูรณ์ของเนื้อหาสาระ
3. **Availability** มีความพร้อมใช้งานอยู่เสมอ ผู้ใช้งานสามารถเข้าถึงข้อมูลเมื่อต้องการได้ทุกเวลา

บริษัทฯกำหนดมาตรการเพื่อรักษาความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศโดยใช้

- **นโยบายความมั่นคงปลอดภัย (Security Policy)** ประกอบด้วยแนวทางปฏิบัติที่ผู้ใช้งานต้องปฏิบัติตามโดยเคร่งครัด
- **แนวทางปฏิบัติ (Procedures)** จะมีการอ้างอิงถึงขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง

4. ขอบเขตของการสร้างความมั่นคงปลอดภัย

นโยบายฉบับนี้ครอบคลุมการสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศของบริษัทฯ ประกอบด้วย

- พนักงานและลูกจ้างของบริษัทฯทั้งหมด
- ข้อมูลสารสนเทศของบริษัทฯ
- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต่างๆ
- เครื่องคอมพิวเตอร์ส่วนบุคคล
- เครื่องคอมพิวเตอร์แบบพกพา
- อุปกรณ์เครือข่าย

- เครือข่ายไร้สาย
- ระบบไฟฟ้าสำรอง
- สายสัญญาณเครือข่าย
- ซอฟต์แวร์ระบบ ซอฟต์แวร์จ้างพัฒนา ซอฟต์แวร์พัฒนาเอง ซอฟต์แวร์สำเร็จรูป
- สื่อบันทึกข้อมูล

5. ระบบบริหารความมั่งคงปลอดภัยสารสนเทศ

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย

1. นโยบายรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy)
2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และป้องกันความเสียหาย (Physical Security)
4. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
5. การควบคุมเข้าถึงระบบเครือข่ายไร้สาย (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 Inaccessibility of Data)
12. มาตรฐานระบบคอมพิวเตอร์ (Computer System Standards)
13. การใช้ซอฟท์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual Property)

6. แนวทางปฏิบัติ

นโยบายแต่ละด้าน ประกอบไปด้วยแนวทางปฏิบัติเพื่อให้พนักงานหรือผู้ที่เกี่ยวข้องปฏิบัติตามโดยเคร่งครัด ดังต่อไปนี้

6.1 *นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)*

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ

ผู้บริหารระดับสูง

ผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1. จัดทำนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศและมีการปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือตามความจำเป็นต่อการใช้งาน และนโยบายดังกล่าวต้องได้รับการอนุมัติจากคณะกรรมการบริษัทหรือผู้มีอำนาจที่ได้รับมอบหมาย
2. จัดทำนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้ง่าย
3. จัดให้มีการอบรมหัวข้อที่เกี่ยวกับภัยคุกคามทางอินเทอร์เน็ตใหม่ๆ อย่างน้อยปีละ 1 ครั้ง เพื่อให้ผู้ใช้งานมีความตระหนักรับรู้เข้าใจและสามารถป้องกันตนเองได้ในระดับหนึ่ง
4. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยปีละ 1 ครั้ง และจัดทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ
5. จัดให้มีการวางแผนกลยุทธ์ด้านสารสนเทศเพื่อให้สอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัทฯ ทั้งแผนระยะสั้นและแผนระยะยาว

6.2 *การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)*

วัตถุประสงค์

เพื่อให้มีการควบคุมและทบทวนการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายเทคโนโลยีสารสนเทศซึ่งเป็นการลดความเสี่ยงด้านการกำกับดูแลงานบริหารและบุคลากรด้านเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ

ผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1. ต้องจัดให้มีใบกำหนดหน้าที่งานของแต่ละตำแหน่งงานไว้อย่างชัดเจน และพนักงานได้รับทราบถึงขอบเขตและหน้าที่การปฏิบัติงานของตนตามที่ได้กำหนดไว้

2. จัดให้มีการอบรมเพิ่มพูนความรู้ความสามารถของพนักงานฝ่ายเทคโนโลยีสารสนเทศอย่างเหมาะสม รวมทั้งจัดให้มีการเก็บข้อมูลการฝึกอบรม

6.3 ***การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)***

วัตถุประสงค์

เพื่อควบคุมมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (Access Risk) แก้ไข เปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (Availability Risk) และเพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ

ผู้รับผิดชอบ

เจ้าหน้าที่ดูแลศูนย์คอมพิวเตอร์

แนวทางปฏิบัติ

1. ควบคุมการเข้า - ออกศูนย์คอมพิวเตอร์
   1.1 ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่ายไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้ามซึ่งปิดล็อคตลอดเวลา และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น
   1.2 ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง มีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ในบางครั้ง กำหนดให้ต้องมีเจ้าหน้าที่ของฝ่ายสารสนเทศที่ปฏิบัติงานประจำศูนย์คอมพิวเตอร์ควบคุมดูแลตลอดเวลาระหว่างที่บุคคลดังกล่าวอยู่ในศูนย์คอมพิวเตอร์
   1.3 มีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบการบันทึกดังกล่าวอย่างสม่ำเสมอ
2. การป้องกันความเสียหาย
   2.1 ระบบป้องกันไฟไหม้
   - มีอุปกรณ์เตือนไฟไหม้ ซึ่งมีเครื่องตรวจจับควัน หรือเครื่องตรวจจับความร้อน เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา
   - มีการติดตั้งถังดับเพลิงและอุปกรณ์ดับเพลิงไว้ในศูนย์คอมพิวเตอร์ โดยสารที่ใช้ดับเพลิงจะต้องเป็นสารที่ใช้สำหรับคอมพิวเตอร์โดยเฉพาะ ซึ่งจะไม่ทำให้คอมพิวเตอร์เสียหายและไม่นำไฟฟ้า

   2.2 ระบบป้องกันไฟฟ้าขัดข้อง
   - จัดให้มีระบบไฟฟ้าสำรอง (UPS) สำหรับเครื่องแม่ข่ายและอุปกรณ์เครือข่าย เพื่อป้องกันความเสียหายอันเกิดจากความไม่คงที่ของกระแสไฟฟ้าเพื่อให้การทำงานมีความต่อเนื่อง ซึ่งระบบไฟฟ้าสำรอง (UPS) จะต้องสามารถสำรองไฟฟ้าได้ไม่น้อยกว่า 30 นาที

- เครื่องจ่ายไฟสำรองฉุกเฉิน (UPS) จะต้องมีมาตรฐานตามที่บริษัทฯ หรือผู้ผลิตกำหนด
- ควรทำการตรวจสอบเครื่องจ่ายไฟสำรองฉุกเฉิน (UPS) ทุกๆ 3 เดือน

2.3 ระบบควบคุมอุณหภูมิและความชื้น

- มีการควบคุมให้สภาพแวดล้อมมีอุณหภูมิและความชื้นที่เหมาะสมโดยตั้งอุณหภูมิเครื่องปรับอากาศและความชื้นให้เหมาะสมกับคุณลักษณะของระบบคอมพิวเตอร์

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

วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง และเพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยของข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่ายและระบบเครือข่าย

แนวทางปฏิบัติ

6.4.1 การบริหารจัดการข้อมูล (Data Management)

ผู้รับผิดชอบ

- ข้อมูลด้าน IT (ข้อมูลด้านการจัดการ IT จัดการโครงการ งบประมาณพัฒนา / บำรุงรักษาระบบ)
  - ข้อมูลทั่วไป ดูแลโดยส่วนงานหรือผู้ที่ได้รับมอบหมายให้ดูแลข้อมูลนั้นๆโดยเฉพาะ
  - ข้อมูลลับ ดูแลโดยส่วนงานที่มีหน้าที่รับผิดชอบงานหรือตามโครงสร้างของฝ่ายที่กำหนดหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติงานในเรื่องนั้นๆ
- ข้อมูลของบริษัทฯ/ฝ่าย ที่อยู่ในระบบ IT (ข้อมูลที่ใช้ในกิจการบริษัทฯ ทั้งด้านการให้บริการธุรกรรมต่างๆ และข้อมูลเพื่อการบริหารจัดการที่อยู่ในระบบ IT ที่ฝ่ายเทคโนโลยีสารสนเทศให้การสนับสนุนการใช้งาน ถือเป็นข้อมูลที่มีความสำคัญ)
  - ข้อมูลที่ใช้งานในกิจการบริษัทฯ ดูแลโดยผู้มีสิทธิใช้งานตามที่บริษัทฯกำหนด
  - ข้อมูลที่อยู่ระหว่างประมวลผล ดูแลโดยฝ่ายเทคโนโลยีสารสนเทศ
  - ข้อมูลที่จัดเก็บสำรองตามข้อปฏิบัติด้านระบบ ดูแลโดยฝ่ายเทคโนโลยีสารสนเทศ
- เจ้าของระบบงาน กำหนดให้ผู้มีอำนาจสูงสุดของแต่ละสายงาน เป็นเจ้าของระบบงานของฝ่ายที่ตนเองดูแล หรือตามที่บริษัทฯกำหนด เช่น เจ้าของระบบงานของระบบบัญชีคือผู้มีอำนาจสูงสุดของฝ่ายบัญชี เจ้าของระบบงานของระบบบริหารงานบุคคลคือผู้มีอำนาจสูงสุดของฝ่ายทรัพยากรบุคคล เจ้าของระบบงานของระบบงาน IT คือ ผู้มีอำนาจสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ เป็นต้น ซึ่งเจ้าของระบบงานจะเป็นผู้กำหนดสิทธิ์ในการเข้าถึงข้อมูลให้กับ

ผู้ปฏิบัติงาน หรือผู้ที่ต้องการใช้ข้อมูล ส่วนระบบงานที่มีความเกี่ยวข้องกับหลายฝ่าย ให้ยึดตามฝ่ายที่มีส่วนสำคัญมากที่สุดในระบบงานนั้นๆ โดยให้ผู้มีอำนาจสูงสุดของฝ่ายนั้นเป็นเจ้าของระบบงาน หรือแล้วแต่บริษัทฯจะกำหนด

แนวทางปฏิบัติ

1. กำหนดให้พนักงานทุกระดับมีสิทธิ์เข้าถึงข้อมูลตามแต่ละสายงานและตามตำแหน่งหน้าที่ที่ได้รับมอบหมายเท่านั้น หากมีความจำเป็นต้องเข้าถึงข้อมูลที่ไม่ได้เป็นไปตามตำแหน่งหน้าที่ ต้องได้รับอนุญาต ดังนี้

   1.1 ข้อมูลที่อยู่ในสายงานเดียวกัน ให้ขออนุมัติจากผู้มีอำนาจสูงสุดในสายงาน

   1.2 ข้อมูลข้ามสายงาน จะต้องได้รับการอนุมัติจากกรรมการผู้จัดการเท่านั้น

2. การขอใช้ข้อมูลทุกประเภท ต้องระบุผู้ขอ วัตถุประสงค์ และระยะเวลาในการใช้งานที่ชัดเจน การคืน (ถ้ามี) ให้นำมาคืนเมื่อเสร็จหรือเมื่อถึงกำหนด สำหรับการยกเลิก (ปิด) สิทธิ์การใช้ข้อมูลให้ยกเลิกเมื่อเสร็จหรือเมื่อถึงกำหนด ห้ามทำสำเนาข้อมูลที่ระบุว่า "ห้ามทำสำเนา" โดยมิได้รับอนุญาตจากเจ้าของข้อมูล และผู้ขอข้อมูลต้องปฏิบัติตามขั้นตอนการขอใช้ข้อมูล ตามประเภทของข้อมูลและกลุ่มผู้ขอด้วย

3. กำหนดชั้นความลับของข้อมูลเป็นข้อมูลทั่วไปและข้อมูลลับและกำหนดวิธีการขอใช้ข้อมูล ดังนี้

   3.1 ข้อมูลทั่วไป

   - หากผู้ขอใช้ข้อมูลเป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ให้ผู้ขอแจ้งรายละเอียดกับผู้ดูแลข้อมูล
   - หากผู้ขอใช้ข้อมูลเป็นพนักงานนอกฝ่ายที่เป็นเจ้าของข้อมูล ให้ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้มีอำนาจสูงสุดในสายงานของตนและกรรมการผู้จัดการ เมื่อได้รับอนุมัติแล้วจึงแจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำและส่งข้อมูลให้

   3.2 ข้อมูลลับ

   - หากผู้ขอใช้ข้อมูลเป็นพนักงานในฝ่ายที่เป็นเจ้าของข้อมูล ให้ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้มีอำนาจสูงสุดในสายงาน เมื่อได้รับอนุมัติแล้วจึงแจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำและส่งข้อมูลให้
   - หากผู้ขอใช้ข้อมูลเป็นพนักงานนอกฝ่ายที่เป็นเจ้าของข้อมูล ให้ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้มีอำนาจสูงสุดในสายงานของตนและกรรมการผู้จัดการ เมื่อได้รับอนุมัติแล้วจึงแจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำและส่งข้อมูลให้

- หากผู้ขอใช้เป็นบุคคลภายนอก ให้ทำหนังสือขอจากหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ โดยผู้พิจารณาอนุมัติต้องเป็นผู้บริหารระดับรองกรรมการผู้จัดการขึ้นไป
- การจัดทำและส่งข้อมูลลับ ต้องใส่ Password หรือได้รับการเข้ารหัส (Encryption) ทุกครั้ง และไม่ควรจัดส่งข้อมูลและ Password ไปพร้อมกันหรือใช้วิธีเดียวกันในการส่ง และควรให้ผู้ขอใช้ข้อมูลทำการลบข้อมูล และ Password ทันทีหลังเสร็จสิ้นการใช้งาน

3.3 ข้อมูลของบริษัทฯ/ฝ่าย ที่อยู่ในระบบ IT

- หากผู้ขอใช้เป็นพนักงานบริษัทฯ ให้แจ้งรายละเอียดเพื่อขออนุมัติจากผู้บังคับบัญชาของตน (ระดับผู้อำนวยการส่วนขึ้นไป)
- หากผู้ขอใช้เป็นบุคคลภายนอก ให้ทำหนังสือขอจากหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้น ๆ โดยผู้พิจารณาอนุมัติต้องเป็นผู้บริหารระดับรองกรรมการผู้จัดการขึ้นไป
- เมื่อต้นสังกัดหรือฝ่ายที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกได้รับผลการอนุมัติแล้ว ให้ส่งเรื่องขออนุมัติใช้ข้อมูลไปยังผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ
- เมื่อสายงาน IT ผู้ดูแลข้อมูลพิจารณาอนุมัติให้ใช้ข้อมูลได้ ผู้ดูแลข้อมูลจะสั่งการตามสายงานเพื่อให้เจ้าหน้าที่ผู้ดูแลจัดทำ/ส่ง/เปิดระบบให้ใช้ข้อมูล (ตามวัตถุประสงค์ของผู้ขอ)
- กรณีผู้ขอใช้เป็นบุคคลภายนอก เจ้าหน้าที่ผู้ดูแลจะส่งข้อมูลให้ฝ่ายที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้น ๆ เพื่อดำเนินการติดต่อกับผู้ขอใช้ (บุคคลภายนอก) ต่อไป
- เมื่อครบระยะเวลาการใช้งานหรือผู้ใช้แจ้งใช้งานเสร็จสิ้น (ก่อนครบกำหนด) ผู้ดูแลข้อมูลจึงปิดระบบการเข้าใช้งาน

4. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ทุกครั้ง และไม่ควรจัดส่งข้อมูลและรหัสไปพร้อมกันหรือใช้วิธีเดียวกันในการจัดส่ง และควรให้ผู้ขอข้อมูลทำการลบข้อมูล และรหัสทันทีหลังเสร็จสิ้นการใช้งาน

6.4.2 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Information Access Control)

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. กระบวนการควบคุมการเข้าถึงระบบ

1.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

1.2 ผู้ดูแลระบบจะต้องตรวจสอบข้อมูลของผู้ที่ต้องการเข้าใช้งานระบบด้วยการพิจารณาอย่างถี่ถ้วน ในกรณีที่มีความจำเป็นต้องให้สิทธิ์แก่บุคคลอื่นใช้งานระบบคอมพิวเตอร์ เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่างๆ ต้องขออนุมัติจากผู้บริหารฝ่ายที่เป็นเจ้าของระบบงาน หรือเจ้าของข้อมูลก่อนทุกครั้ง

1.3 ผู้ดูแลระบบจะทบทวนสิทธิ์ผู้ร้องขอที่ผ่านการพิจารณาและอนุมัติจากผู้บริหารฝ่าย/หัวหน้าฝ่ายโดยตรวจสอบจากเอกสารการขอเปิดสิทธิ์และจัดเก็บเอกสารนั้นไว้เป็นหลักฐาน

1.4 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

1.5 ผู้ดูแลระบบจะต้องกำหนดขั้นตอนการปฏิบัติในการขอสิทธิ์ เปิดสิทธิ์การใช้งาน รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน ในกรณีพนักงานลาออก ผู้ดูแลระบบต้องดำเนินการปิดสิทธิ์การเข้าถึงระบบภายใน 24 ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานต้องดำเนินการเปลี่ยนแปลงสิทธิ์ภายใน 7 วัน

1.6 บริษัทฯต้องมีการสอบทานสิทธิ์การเข้าใช้งาน โดยผู้มีอำนาจอนุมัติสิทธิ์การใช้งานว่าสิทธิ์ดังกล่าวยังมีความเหมาะสมอยู่หรือไม่ โดยควรมีการสอบทานสิทธิ์อย่างน้อยปีละ 1 ครั้ง

2. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

2.1 กำหนดมาตรฐานการเข้าใช้งาน

- บริษัทฯ ได้กำหนดสิทธิ์การเข้าใช้งานของผู้ใช้งานเพื่อยืนยันตัวตนของผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ โดยแยกเป็นรายบุคคลดังต่อไปนี้
    - การกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร
    - การขอ Username และ Email สำหรับพนักงานเข้าใหม่ ต้องดำเนินการร้องขอโดยผู้จัดการฝ่ายของสายงานนั้น ๆ โดยกรอกแบบฟอร์มการขอซึ่งอนุมัติโดยผู้มีอำนาจสูงสุดในสายงาน
    - การขอยกเลิก Username และ Email ต้องดำเนินร้องขอโดยหัวหน้าฝ่ายในสายงานนั้น ๆ โดยจะต้องกรอกแบบฟอร์มการขอยกเลิกซึ่งอนุมัติโดยผู้มีอำนาจสูงสุดในสายงาน
    - การขอเพิ่ม ปรับปรุง หรือเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบใดๆให้กับพนักงาน จะต้องได้รับการอนุมัติจากผู้บริหารฝ่ายที่เป็นเจ้าของระบบงานหรือเจ้าของข้อมูลก่อนทุกครั้ง

- ผู้ใช้งานต้องเก็บและรักษา Password สำหรับทุกระบบงานที่ได้รับมาให้เป็นความลับ และควรเปลี่ยน Password หลังจากเข้าใช้งานในครั้งแรกโดยทันที
- การขอรหัสผ่านใหม่ของผู้ใช้งาน เนื่องจากลืมรหัสผ่าน หรือถูกล็อครหัสผ่าน จะต้องมีการยืนยันตัวตนของผู้ขอก่อนการให้รหัสผ่านใหม่ทุกครั้ง
- การขอรหัสผ่านใหม่ที่ไม่ใช่ของตน ไม่สามารถกระทำได้ เว้นแต่กรณีฉุกเฉินและไม่สามารถติดต่อเจ้าของสิทธิ์ได้ หรือกรณีที่เจ้าของสิทธิ์ไม่ยอมมอบรหัสผ่านให้ โดยการขอรหัสผ่านใหม่นั้นต้องได้รับการอนุมัติจากหัวหน้าฝ่ายในสายงานนั้นๆ หรือบุคคลที่มีอำนาจสูงกว่าตามสายงานเป็นลายลักษณ์อักษร
- ผู้ใช้งานต้องใช้ Username และ Password ส่วนบุคคลสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์ที่ตนเองครอบครองอยู่เท่านั้น กรณีที่จำเป็นต้องใช้งานเครื่องคอมพิวเตอร์อื่น ๆ จะต้องได้รับอนุญาตจากผู้ที่ครอบครองหรือผู้ดูแลระบบ
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านใหม่โดยทันที
- ผู้ใช้งานต้องไม่ใช้โปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำ Password ส่วนบุคคลของตนโดยอัตโนมัติ (Save Password) เพื่อป้องกันไม่ให้ผู้อื่นเข้าใช้งานได้โดยไม่ต้องใส่ Password
- ผู้ใช้งานต้องไม่จดหรือบันทึก Password ส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของผู้อื่น
- กรณีที่มีความจำเป็นที่จะต้องบอก Password แก่ผู้อื่น เนื่องจากความจำเป็นของงาน หลังจากใช้งานแล้วให้ทำการเปลี่ยน Password ใหม่ทันที

2.2 หลักเกณฑ์การกำหนด Username และ Password มีดังนี้

- การตั้งชื่อ Username จะต้องมีความยาวอย่างน้อย 6 ตัวอักษร โดยกำหนดให้ใช้ชื่อภาษาอังกฤษของพนักงาน (First name) ตามด้วยจุด (dot) และต่อด้วยตัวอักษรสามตัวแรกของนามสกุล (Surname) เป็น Username
- Password ต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร และกำหนดความซับซ้อนเพิ่มขึ้น โดยประกอบด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ และตัวเลขหรือตัวอักษรพิเศษ
- กำหนดวันหมดอายุการใช้งานของ Password เช่น 30 60 หรือ 90 วัน สำหรับความปลอดภัยสูง และ 120 150 หรือ 180 วัน สำหรับความปลอดภัยต่ำ และเมื่อครบกำหนดต้องมีการบังคับให้เปลี่ยน (Forced Change)

- ป้องกันการใช้ Password ซ้ำๆ กันของแต่ละบุคคล โดยกำหนดให้ Password ที่เคยถูกใช้งานไปแล้ว ไม่สามารถนำกลับมาใช้งานได้อีกสำหรับจำนวน 3 ครั้งล่าสุดที่มีการเปลี่ยน Password
- ไม่กำหนด Password ส่วนบุคคลจากส่วนหนึ่งส่วนใดของชื่อ นามสกุล ชื่อเล่น วันเดือนปีเกิด รหัสพนักงาน หรือรหัสใด ๆ ที่เกี่ยวข้องกับตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ คำศัพท์ที่ใช้ในพจนานุกรม หรือจากคำที่มักใช้ติดต่อสื่อสารกันโดยทั่วไป

2.3 การ Login เข้าใช้งานระบบคอมพิวเตอร์

- ผู้ใช้งานจะต้อง Login เข้าระบบด้วยตนเอง ห้ามมิให้ผู้อื่นดำเนินการเข้าระบบให้
- ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ Username และ Password ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน
- ไม่อนุญาตให้นำ Username ของตนเอง Login เข้าสู่ระบบ แล้วให้ผู้อื่นใช้งาน
- ให้ Login ออกจากระบบเมื่อใช้งานเสร็จแล้ว หรือมิได้อยู่ที่หน้าเครื่องคอมพิวเตอร์เป็นเวลานาน
- ถ้าผู้ใช้งานใส่ Password ผิดติดต่อกันเกิน 6 ครั้ง ระบบจะทำการล็อคบัญชีชื่อผู้ใช้งานนั้นทันที และจะปลดล็อคอัตโนมัติเมื่อเวลาผ่านไป 30 นาที หรือให้ติดต่อเจ้าหน้าที่ผู้ดูแลระบบ

6.4.3 การควบคุมของระบบฐานข้อมูล (Database Access Control)

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. กำหนดมาตรฐานการติดตั้งระบบฐานข้อมูล

1.1 ผู้ติดตั้งระบบฐานข้อมูลจะต้องเป็นพนักงานในส่วนสนับสนุนสารสนเทศหรือพนักงานของบริษัทฯซึ่งได้รับมอบหมายให้ทำหน้าที่ดังกล่าว แต่ทั้งนี้จะต้องมีพนักงานในส่วนสนับสนุนสารสนเทศร่วมดำเนินการด้วย

1.2 ผู้ติดตั้งระบบฐานข้อมูลจะต้องใช้ซอฟท์แวร์ที่มีลิขสิทธิ์การใช้งานตามกฎหมายเท่านั้น

1.3 ส่วนสนับสนุนสารสนเทศหรือพนักงานของบริษัทฯที่ได้รับมอบหมายให้เป็นผู้ติดตั้งโปรแกรมปรับปรุงข้อมูล (Patch) หรือโปรแกรมของระบบฐานข้อมูลจะต้องคำนึงถึง

- ผลกระทบของการติดตั้งต่อผู้ใช้งานหรือต่อระบบงานที่เกี่ยวข้อง
- การประเมินความเสี่ยงของการติดตั้ง Patch ดังกล่าว
- การแจ้งให้ส่วนที่เกี่ยวข้องทราบ

- 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 หากมีความจำเป็นต้องเพิ่มกลุ่มผู้ใช้งานใหม่ต้องขออนุมัติอย่างเป็นลายลักษณ์อักษรกับผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

2.2 มาตรฐานการอนุมัติการใช้งาน (Authorization)

- เมื่อผู้ใช้งานได้รับความเห็นชอบจากหัวหน้าฝ่ายและผู้บริหารสูงสุดของฝ่ายต้นสังกัดแล้ว จะต้องขออนุมัติจากเจ้าของระบบงานตามลำดับขั้นในการขอใช้งานระบบฐานข้อมูล และผู้ดูแลระบบฐานข้อมูลต้องจัดทำทะเบียนผู้ใช้งานให้สอดคล้องกับกลุ่มของผู้ใช้งานตามข้อ 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)

- กำหนดวิธีการเข้าถึงข้อมูลให้สอดคล้องกับกลุ่มผู้ใช้งานระบบโดยกำหนดกลุ่มเบื้องต้น ดังนี้
    - 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) ร่วมกับฝ่ายตรวจสอบภายในและจัดทำรายงานผลการตรวจสอบให้ผู้บังคับบัญชาให้ทราบอย่างสม่ำเสมอ

5. กำหนดมาตรฐานการสำรองข้อมูลและการนำกลับมาใช้ เพื่อป้องกันข้อมูลเสียหาย

5.1 ส่วนสนับสนุนสารสนเทศ ต้องพิจารณาจัดหา Storage Media ที่มีประสิทธิภาพเพื่อใช้ในการสำรองข้อมูล

5.2 ส่วนสนับสนุนสารสนเทศ และฝ่ายหรือส่วนงานที่เกี่ยวข้อง ต้องร่วมกันพิจารณาถึงวิธีการสำรองข้อมูล และติดตั้งข้อมูลของแต่ละระบบงาน

5.3 ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบการสำรองข้อมูลว่าทำสำเร็จหรือไม่ และหากไม่สำเร็จต้องรีบดำเนินการแก้ไขภายใน 1 วัน

5.4 การ Restore Data สามารถกระทำได้เฉพาะผู้ที่ได้รับมอบหมาย ซึ่งจะต้องได้รับอนุญาตจากเจ้าของระบบงานก่อนทุกครั้ง รวมทั้งคำสั่งจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

5.5 ส่วนสนับสนุนสารสนเทศ ต้องจัดเก็บ Storage Media ที่ใช้ในการสำรองข้อมูลไว้ในสภาพแวดล้อมที่เหมาะสมและมีระบบรักษาความปลอดภัยที่ดี

5.6 ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบสภาพ Storage Media และข้อมูลที่อยู่ใน Storage Media อย่างสม่ำเสมอว่ายังอยู่ในสภาพที่ใช้งานได้ดีหรือไม่ หากพบปัญหาให้รีบดำเนินการแก้ไข

6.4.4 การรักษาความปลอดภัยระบบคอมพิวเตอร์เครือข่ายและการควบคุมการเข้าถึงระบบเครือข่าย (Computer Network Security and Network Access Control)

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. การบริหารจัดการการเข้าถึงระบบเครือข่าย

1.1 ผู้ดูแลระบบต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งาน ให้ใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

1.2 ผู้ดูแลระบบต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งาน

1.3 ผู้ดูแลระบบต้องป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน เช่น ผู้ใช้งานห้ามนำอุปกรณ์จากภายนอกเชื่อมต่อเข้ามาใช้ในบริษัทฯ โดยไม่ได้รับอนุญาต หรือห้ามเชื่อมต่อระบบ Network อื่นใดเข้ากับระบบ Network ของบริษัทฯ โดยไม่ได้รับอนุญาต

1.4 ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก ต้องเชื่อมต่อผ่านอุปกรณ์ Firewall หรือ ฮาร์ดแวร์อื่นๆ ที่มีระบบป้องกันการถูกโจมตีผ่านระบบเครือข่ายหรือการลักลอบขโมยข้อมูลผ่านระบบเครือข่ายรวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

1.5 ผู้ดูแลระบบต้องตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้ทุกเดือนเป็นอย่างน้อย

- ความพยายามในการบุกรุกผ่านระบบเครือข่าย
- การใช้งานในลักษณะที่ผิดปกติ
- การใช้งานและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้อง

1.6 การเชื่อมต่อกับหน่วยงานภายนอกเข้ากับระบบเครือข่ายของบริษัทฯ ต้องได้รับความเห็นชอบจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศทุกกรณี

1.7 สำหรับ Server ที่จะทำการติดตั้งเข้ากับเครือข่ายของบริษัทฯ บริษัทผู้ดูแลการติดตั้ง Server ดังกล่าว ต้องส่งรายละเอียดของระบบปฏิบัติการ (Operating System) และ Service Pack หรืออื่น ๆ ที่จำเป็นสำหรับการติดตั้งให้กับส่วนสนับสนุนสารสนเทศรับทราบข้อมูลก่อน หลังจากนั้นจึงจะจ่าย IP Address ให้ และให้ทำการ Monitor Port ที่จ่ายให้กับ Server ดังกล่าวไม่น้อยกว่า 1 สัปดาห์อย่างใกล้ชิดพร้อมกันรายงานผลต่อผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

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

1.9 ห้ามใช้ Community Name ของอุปกรณ์สื่อสารข้อมูลทุกชนิดหรืออุปกรณ์อื่นที่ใช้ SNMP Protocol ที่ถูกกำหนดชื่อมาโดยผู้ผลิตอุปกรณ์ เมื่อเริ่มใช้งานกับระบบงานของบริษัทฯ ให้ดำเนินการเปลี่ยนชื่อนั้นโดยทันที

1.10 จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก รวมถึงอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

1.11 ให้ส่วนงานสนับสนุนสารสนเทศ เป็นผู้ถือกุญแจห้องอุปกรณ์สื่อสาร/ห้อง Sever ของบริษัทฯ

1.12 เครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัทฯ ควรติดตั้ง Service Pack ตลอดจน Patch ต่างๆ ให้ทันสมัย รวมทั้ง Antivirus Software ตามที่บริษัทฯกำหนด

1.13 จัดหาอุปกรณ์รักษาความปลอดภัยที่ทันต่อความเปลี่ยนแปลงของภัยคุกคามทางด้านเครือข่าย โดยจัดให้มีการทบทวนภาพรวมของการรักษาความปลอดภัยบนเครือข่ายในทุกๆ 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.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 และ พ.ศ. 2560 (หรือฉบับล่าสุด)

- ต้องมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของบริษัทฯ ซึ่งจะต้องเป็นไปตามข้อกำหนดของพรบ.คอมพิวเตอร์ โดยจะต้องเก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้ไม่ต่ำกว่า 90 วัน
- กรณีที่ผู้ใช้งานอินเทอร์เน็ตเป็นบุคคลภายนอก จะต้องกรอกข้อมูลโดยระบุชื่อ นามสกุล บุคคลที่ติดต่อ วันเวลาที่ใช้งาน เพื่อขอรับ Username และ Password ในการใช้งานก่อนทุกครั้ง และกำหนดให้รหัสผ่านแต่ละรหัสนั้นมีอายุไม่เกิน 7 วันนับจากการเปิดใช้งาน เว้นแต่เข้ามาปฏิบัติงานเป็นระยะเวลานาน บริษัทฯอนุญาตให้ลงทะเบียนอุปกรณ์เพื่อเข้าใช้ตลอดระยะเวลาที่เข้ามาปฏิบัติงานได้ และจะต้องเก็บข้อมูลประวัติการใช้งานไว้ไม่ต่ำกว่า 90 วัน

2. กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

2.1 ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของบริษัทฯ

2.2 ไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร หรือเพื่อกิจการใดๆ ที่ไม่มีส่วนเกี่ยวข้องกับบริษัทฯ

2.3 ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่อาจทำลายกลไกรักษาความปลอดภัย รวมไปถึงเข้าสู่เครื่องคอมพิวเตอร์ของบริษัทฯ หรือหน่วยงานอื่นๆ การเผยแพร่ข้อมูล เนื้อหา หรือข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาที่ไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว โดยบริษัทฯไม่มีส่วนรับผิดชอบความเสียหายที่อาจเกิดขึ้นดังกล่าว

2.4 ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของบริษัทฯ

2.5 บริษัทฯให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน หรือมอบสิทธิ์นี้ให้กับผู้อื่นไม่ได้

2.6 บัญชีผู้ใช้งาน (User Account) ที่บริษัทฯให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดขึ้นรวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

2.7 ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศผ่านทางเครือข่ายได้ภายใต้การบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

2.8 ผู้ใช้งานที่อยู่ภายในและภายนอกบริษัทฯ ต้องทำการยืนยันตัวบุคคลผ่านบัญชีผู้ใช้งาน (User Account) ที่ได้รับ ซึ่งประกอบด้วย Username และ Password ก่อนที่จะได้รับอนุญาตให้สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของบริษัทฯได้

2.9 ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไข ในการรับทราบกฎระเบียบหรือนโยบายต่างๆที่บริษัทฯกำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบายของบริษัทฯมิได้

2.10 บริษัทฯทรงไว้ซึ่งสิทธิที่จะปฏิเสธการเชื่อมต่อและ/หรือการใช้งาน และทรงไว้ซึ่งสิทธิที่จะยกเลิกหรือระงับการเชื่อมต่อและ/หรือการใช้งานใดๆ ของผู้ใช้งานที่ล่วงละเมิดหรือพยายามจะล่วงละเมิดกฎระเบียบของบริษัทฯ โดยไม่มีการแจ้งให้ทราบก่อนล่วงหน้า

6.4.5 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Sever Security)

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. ผู้ดูแลระบบต้องทำการติดตั้งไฟร์วอลล์ (Firewall) สำหรับตรวจจับการบุกรุกเครือข่ายของบริษัทฯ
2. ค่าเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ (Firewall) เช่น ค่าพารามิเตอร์การกำหนดใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
3. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายนั้น จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ต (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง
4. การติดตั้งเครื่องคอมพิวเตอร์ Server ต้องมีการจัดแบ่งหมวดหมู่ตามที่ฝ่ายสนับสนุนสารสนเทศได้กำหนดไว้
5. การติดตั้งเครื่องคอมพิวเตอร์ Server หรืออุปกรณ์สื่อสารข้อมูล หรืออุปกรณ์รักษาความปลอดภัยต่างๆ ต้องมีการจัดทำแบบแปลนการติดตั้งอุปกรณ์บนตู้ Rack แสดงตำแหน่งต่างๆ ของอุปกรณ์บนตู้ Rack โดยจัดเก็บไว้ในฝ่ายสนับสนุนสารสนเทศ
6. การติดตั้งอุปกรณ์สื่อสารข้อมูลทุกชนิดกับระบบงานต่างๆ ของบริษัทฯ ให้อยู่ในการควบคุมดูแลของส่วนงานสนับสนุนสารสนเทศ
7. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในนั้นจะอนุญาตให้เฉพาะผู้ดูแลระบบตามสิทธิ์ที่ได้รับเท่านั้น กรณีที่ไม่ได้เป็นผู้ดูแลระบบจะต้องขออนุญาตจากผู้บังคับบัญชาของตน (ระดับผู้อำนวยการฝ่ายขึ้นไป) เมื่อได้รับการอนุมัติแล้ว ให้ส่งเรื่องขออนุมัติไปยังผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ
8. ผู้ดูแลระบบต้องคอยเฝ้าระวัง ประเมินความเสี่ยงช่องโหว่ ติดตามและตรวจสอบ Log ของระบบเครือข่ายเพื่อใช้วิเคราะห์หาข้อผิดพลาดหรือจุดอ่อนอย่างสม่ำเสมอเพื่อจะได้ดำเนินการแก้ไขได้ทันท่วงที
9. เครื่องแม่ข่ายคอมพิวเตอร์ (Server) เครื่องคอมพิวเตอร์ทุกเครื่องในบริษัทฯ และอุปกรณ์ต่างๆ ที่มีการตั้งค่าเวลา ต้องตั้งเวลาให้ตรงกันโดยอ้างอิงเวลาตามมาตรฐานกลางของโลกเพื่อช่วยในการตรวจสอบเวลา หากระบบคอมพิวเตอร์ของบริษัทฯถูกบุกรุกหรือโจมตี

6.4.6 **การป้องกันไวรัสคอมพิวเตอร์ / มัลแวร์ (Virus/Malware Protection)**

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ สำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Server Protect and Office Scan) รวมถึงเครื่องที่ให้บริการต่างๆ เช่น E-mail Server (Scan Mail), Web Server, File Server, Print Server เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้งต้องจัดให้มีการอัพเดทข้อมูลจากเจ้าของผลิตภัณฑ์นั้นๆ ทุก 24 ชั่วโมง
2. กำหนดหน้าที่และความรับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์

2.1 กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการตรวจจับ และทำลายไวรัสคอมพิวเตอร์/มัลแวร์ บนเครื่องคอมพิวเตอร์ส่วนบุคคล ไม่ให้แพร่กระจายทำความเสียหายกับข้อมูลของบริษัทฯ

2.2 กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ ต้องแจ้งข่าวเกี่ยวกับไวรัสคอมพิวเตอร์/มัลแวร์ทันที หากมีการระบาดของไวรัสคอมพิวเตอร์/มัลแวร์ตัวใหม่

2.3 กำหนดให้ส่วนเทคนิคปฏิบัติการส่วนเครือข่าย มีหน้าที่รับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์ อย่างสม่ำเสมอบน Server และอุปกรณ์เครือข่าย เพื่อป้องกันความเสียหายกับข้อมูลของบริษัทฯ

3. หากผู้ใช้งานพบเหตุไม่พึงประสงค์ที่อาจเกิดความเสี่ยงหรือมีผลกระทบต่อระบบสารสนเทศและการดำเนินธุรกิจ เช่น พบช่องโหว่ Malware หรือ Virus จะต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศให้ทราบโดยเร็ว

6.5 *การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)*

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยผู้ใช้ระบบต้องทำการพิสูจน์ตัวตนจริงจากระบบว่า ได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. ผู้ดูแลระบบเครือข่ายไร้สายมีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1.1 เครือข่ายแบบไร้สายเป็นสมบัติของบริษัทฯ ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบ ต้องได้รับโทษทางวินัยจากบริษัทฯและรับโทษตามกฎหมาย

1.2 การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ไม่ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

1.3 ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็น ต้องวางในระบบเครือข่ายภายในที่เป็น Internal Network และเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication & Encryption)

1.4 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สาย เข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆของหน่วยงาน

1.5 ผู้ดูแลระบบควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย 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

เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. การกำหนดขั้นตอนการปฏิบัติงาน
   1.1 จัดให้มีขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลงขั้นตอนในการทดสอบ รวมถึงขั้นตอนในการโอนย้ายระบบงาน
   1.2 จัดให้มีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง
   1.3 มีการสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตามขั้นตอน
2. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน
   2.1 การร้องขอ
   - การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษรและได้รับอนุมัติจากผู้มีอำนาจ เช่น ผู้บริหารส่วนงานที่ร้องขอ เจ้าหน้าที่ผู้ดำเนินการ และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เป็นต้น
   - มีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
   - มีการสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ

   2.2 การปฏิบัติงานพัฒนาระบบงาน
   - ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Development Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้การแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
   - ผู้ที่ร้องขอและผู้ใช้งานที่เกี่ยวข้อง ควรมีส่วนร่วมในการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้สามารถพัฒนาระบบงานได้ตรงกับความต้องการ

- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และความพร้อมใช้ของระบบงานต่างๆ เพื่อการเข้าใช้งาน (Availability) ตั้งแต่ในช่วงเริ่มต้นของการพัฒนาหรือการแก้ไขเปลี่ยนแปลง

2.3 การทดสอบ

- ผู้ที่ร้องขอ ฝ่ายคอมพิวเตอร์รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้อง ต้องมีส่วนร่วมในการทดสอบเพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง
- 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 การสื่อสารเปลี่ยนแปลง

- ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

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

วัตถุประสงค์

เพื่อให้ข้อมูลและระบบคอมพิวเตอร์มีความพร้อมสำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability Risk) สอดคล้องกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งมีการทดสอบและการรักษา รวมถึงแนวทางในการจัดทำและการทดสอบแผนฉุกเฉิน

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. การสำรองข้อมูลและระบบคอมพิวเตอร์

1.1 การสำรอง

- ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง
- ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้
  - ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
  - ประเภทสื่อบันทึก (Storage Media)
  - จำนวนที่ต้องสำรอง (Number of Copy)
  - ขั้นตอนและวิธีการสำรองโดยละเอียด
  - สถานที่และวิธีการเก็บรักษาสื่อบันทึก
  - ระยะเวลาในการเก็บรักษาข้อมูลสำรอง
- ควรมีการบันทึกการปฏิบัติงาน (Log Book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
- ข้อกำหนดในการสำรองข้อมูลมีดังนี้
  - ข้อมูลระบบที่ยังคงใช้งานอยู่ในปัจจุบัน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 1 ครั้งต่อเดือน และเก็บไว้อย่างน้อย 6 เดือน
  - ข้อมูลระบบที่ไม่ได้ใช้งาน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 2 เดือนล่าสุดก่อนที่จะหยุดใช้งาน และให้เก็บข้อมูลไว้จนกว่าจะไม่มีการเรียกใช้งานหรือกู้ข้อมูลบนระบบอีกต่อไป หรืออย่างน้อย 5 ปี

- ข้อมูลสำคัญของฝ่ายต่างๆ ที่ยังคงใช้งานอยู่ในปัจจุบัน ให้สำรองข้อมูลแบบ Incremental Backup ทุกวัน และ Full Backup อย่างน้อย 1 ครั้งต่อสัปดาห์และเก็บไว้อย่างน้อย 6 เดือน
- ข้อมูลสำคัญของฝ่ายต่าง ๆ ที่ไม่ได้ใช้งาน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 2 เดือนล่าสุดก่อนที่จะหยุดใช้งาน และให้เก็บข้อมูลไว้จนกว่าจะไม่มีการเรียกใช้งานหรือกู้ข้อมูลบนระบบอีกต่อไปหรืออย่างน้อย 5 ปี
- ฐานข้อมูล (Database) ที่ยังคงใช้งานอยู่ในปัจจุบัน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 1 ครั้งต่อวันและเก็บไว้อย่างน้อย 6 เดือน
- ฐานข้อมูล (Database) ที่ไม่ได้ใช้งาน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 2 เดือนล่าสุดก่อนที่จะหยุดใช้งาน และให้เก็บข้อมูลไว้จนกว่าจะไม่มีการเรียกใช้งานหรือกู้ข้อมูลบนระบบอีกต่อไปหรืออย่างน้อย 5 ปี
- ข้อมูลอื่น ๆ ที่ยังคงใช้งานอยู่ในปัจจุบัน ให้สำรองข้อมูลแบบ Full Backup อย่างน้อย 1 ครั้งต่อสัปดาห์และเก็บไว้อย่างน้อย 4 เดือน

1.2 การทดสอบ

- ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลรวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้
- ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

1.3 การเก็บรักษา

- ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย
- ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน
- ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็วและเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด
- การขอใช้งานสื่อบันทึกข้อมูลสำรอง ต้องได้รับอนุมัติจากผู้บริหารระดับสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และวันเวลา

- ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้วซึ่งรวมถึงข้อมูลสำคัญต่าง ๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน Recycle Bin
- การลบข้อมูลสำรองที่เกินกำหนดระยะเวลาเก็บรักษา ให้ผู้ปฏิบัติงานขออนุมัติจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศก่อนดำเนินการทุกครั้ง

2. การเตรียมพร้อมกรณีฉุกเฉิน

2.2 ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้

- ต้องจัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงานและระยะเวลาในการกู้แต่ละระบบงาน
- ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
- ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์
- ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด
- ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (Specification) ขั้นต่ำ ค่า Configuration และอุปกรณ์เครือข่าย
- ในกรณีที่บริษัทฯมีศูนย์คอมพิวเตอร์สำรองก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่
- ควรปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

2.3 ควรทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริงเพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

2.4 ควรสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

2.5 ในกรณีเกิดเหตุการณ์ฉุกเฉินควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหาและวิธีการแก้ไขปัญหาไว้ด้วย

6.8 *การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation Control)*

วัตถุประสงค์

เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้องต่อเนื่องและมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่าง ๆ ซึ่งได้แก่ การติดตามการ

ทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน เพื่อลดความเสี่ยงด้าน Integrity Risk และ Availability Risk

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์
   1.1 จัดทำขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้กับเจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบ ตารางเวลาในการปฏิบัติงาน โดยปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ
   1.2 กำหนดให้มีระบบการตรวจสอบการ Login เข้ามาใช้งาน โดยต้องบันทึกข้อมูลที่เกี่ยวข้องกับการ Login นั้นไว้ และให้บันทึกทั้งการ Login ที่ทำได้สำเร็จและไม่สำเร็จ เพื่อใช้ในการตรวจสอบภายหลัง
   1.3 ควรกำหนดให้มีการบันทึก (Log Book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้
      - ผู้ปฏิบัติงาน
      - เวลาปฏิบัติงาน
      - รายละเอียดการปฏิบัติงาน
      - ปัญหาที่เกิดขึ้นและการแก้ไข
      - สถานะของระบบ
      - ผู้ตรวจทานการปฏิบัติงาน
2. การติดตามการทำงานของระบบคอมพิวเตอร์ (Monitoring)
   2.1 ต้องติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เช่น การใช้งานระบบ Oracle ERP เพื่อรองรับการทำงานของบริษัทฯ มีการใช้งานฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ (Capacity) ของระบบ
   2.2 บำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ
3. การจัดการปัญหาต่างๆ

3.1 ต้องกำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน เช่น กำหนดผู้รับผิดชอบในการแก้ไขปัญหาระบบ Oracle ERP รวมถึงเบอร์โทรศัพท์ของผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา

3.2 ควรมีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอเพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

4. การควบคุมการจัดทำรายงาน

4.1 การขอให้จัดพิมพ์รายงานต่าง ๆ ควรได้รับความเห็นชอบจากผู้บริหารสูงสุดของฝ่ายที่เกี่ยวข้องนั้น หรือรองกรรมการผู้จัดการขึ้นไป

4.2 ควรมีทะเบียนคุมการพิมพ์และการจัดส่งรายงาน จัดเก็บรายงานต่างๆที่ได้จัดพิมพ์แล้วอย่างรัดกุม และกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

6.9 *การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing Control)*

วัตถุประสงค์

เพื่อให้บริษัทฯใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพและสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

ผู้รับผิดชอบ

ผู้บริหารระดับสูง

ผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1. การคัดเลือกผู้ให้บริการจากภายนอก

การคัดเลือกผู้ให้บริการจากภานนอกให้เป็นไปตามระเบียบวิธีการคัดเลือกตามกระบวนการจัดซื้อจัดจ้าง

โดยการพิจารณาคัดเลือกต้องครอบคลุมเรื่องดังต่อไปนี้

1.1 การเปรียบเทียบข้อเสนอกับความต้องการของบริษัทฯ

1.2 การประเมินผลงานที่ผ่านมาของผู้ให้บริการภายนอก

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

1.4 กำหนดมาตรฐานของอุปกรณ์ที่นำมาติดตั้งใช้งาน ต้องเป็นอุปกรณ์ที่มีคุณภาพและได้มาตรฐาน

- อุปกรณ์ที่นำมาติดตั้งต้องมีมาตรฐานรับรองจากบริษัทหรือจากผู้ผลิตโดยตรง
- อุปกรณ์ที่นำมาติดตั้งใช้งาน จะต้องมีมาตรฐานที่เป็นสากล (International Standard)

2. การควบคุมด้านความมั่นคงปลอดภัย

2.1 กำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ที่บริษัทฯทำสัญญาว่าจ้างให้มาปฏิบัติงาน ซึ่งสอดคล้องกับนโยบายความมั่นคงปลอดภัยของบริษัทฯและให้ผู้ปฏิบัติงานนั้นลงนามในเอกสารดังกล่าว

2.2 เมื่อสิ้นสุดการจ้างงานหรือการเปลี่ยนแปลงลักษณะการจ้างงานของหน่วยงานภายนอก จะต้องถอนสิทธิ์การเข้าถึงระบบสารสนเทศและทรัพย์สินสารสนเทศโดยทันที

3. การควบคุมระหว่างการให้บริการ

3.1 ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Development Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่บริษัทฯควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัทฯ (Onsite Service) และให้เจ้าหน้าที่บริษัทฯตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และให้ปิดการเชื่อมต่อทันทีที่การให้บริการเสร็จสิ้น

3.2 ต้องควบคุมผู้ให้บริการจากภายนอกว่ามีการปฏิบัติตามข้อกำหนดที่จัดทำขึ้นอย่างสม่ำเสมอ เช่น สังเกตจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ

3.3 ต้องปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือการให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การปรับปรุงเทคโนโลยี ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

3.4 ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

3.5 ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

3.6 ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

6.10 *การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Control)*

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งจะช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้งานควรทำความเข้าใจและ

ปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของบริษัทฯ ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. การใช้งานทั่วไป
   1.1 เครื่องคอมพิวเตอร์ที่บริษัทฯอนุญาตให้ใช้งานเป็นทรัพย์สินของบริษัทฯ ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของบริษัทฯและควรใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่น ๆ ที่ตนเองรับผิดชอบด้วยความระมัดระวัง กรณีชำรุดหรือเสียหายต้องรีบแจ้งให้เจ้าหน้าที่ IT ทราบโดยทันที
   1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัทฯต้องเป็นโปรแกรมที่มีลิขสิทธิ์อย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
   1.3 ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัทฯ
   1.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ IT เท่านั้น
   1.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลเพื่อตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ IT เท่านั้น
   1.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม
   1.7 ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
   1.8 ไม่ควรเก็บข้อมูลสำคัญของบริษัทฯไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่
   1.9 ไม่ควรเก็บข้อมูลส่วนบุคคลใดๆ ที่ไม่เกี่ยวข้องกับงานของบริษัทฯไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่เป็นทรัพย์สินของบริษัทฯ หรือเก็บไว้บนพื้นที่จัดเก็บข้อมูลใดๆ ของบริษัทฯ หากเจ้าหน้าที่ IT ตรวจพบ จะดำเนินการลบทิ้งได้โดยทันที
   1.10 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของบริษัทฯ
   1.11 ผู้ใช้มีหน้าที่และความรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้
      - ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

- ไม่ควรวางสื่อแม่เหล็ก เช่น ลำโพงไว้ใกล้เครื่องคอมพิวเตอร์, External Hard Disk หรือ Disk Drive
- ปิดเครื่อง (Shutdown) ทุกครั้งหลังจากเสร็จสิ้นการใช้งาน

1.12 กรณีใช้เครื่องคอมพิวเตอร์แบบพกพา ควรปฏิบัติ ดังนี้

- ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายอาจเกิดขึ้นจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ
- ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจ จากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้
- การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์
- การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ยกจากฐานภายใต้แป้นพิมพ์และห้ามยกเครื่องโดยการดึงหน้าจอภาพขึ้น
- ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน
- ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ
- ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้กับอุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
- ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
- การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
- ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

2. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

2.1 ผู้ใช้ ควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

2.2 ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (Email) หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนการใช้งาน

2.3 ไม่ควรเปิดจดหมายอิเล็กทรอนิกส์ (Email) หรือไฟล์ที่แนบมากับ Email ที่ไม่รู้จักผู้ส่ง

2.4 ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์

2.5 ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูล ระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หากไม่แน่ใจให้แจ้งเจ้าหน้าที่ IT

2.6 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์ที่ใช้งานติดไวรัส หรือ Malware ให้ทำการตัดการเชื่อมต่อกับระบบเครือข่ายโดยทันที และห้ามมิให้ผู้ใช้ ใช้งานใดๆ รวมถึงเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายใด ๆ เพื่อป้องกันการแพร่กระจายของไวรัส หรือ Malware ไปยังเครื่องอื่นๆ และให้แจ้งเจ้าหน้าที่ IT โดยทันที

6.11 *การป้องกันความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูล (Risk Prevention on Inaccessibility of Data)*

วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติให้สามารถดูแลการทำงานของระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ โปรแกรมระบบงานและฐานข้อมูลต่างๆ กรณีที่ไม่สามารถเข้าถึงข้อมูลและไม่สามารถทำงานต่อเนื่องได้ เพื่อให้เกิดผลกระทบต่อการบริการของบริษัทฯแก่ลูกค้าให้น้อยที่สุด และเพื่อให้บริษัทฯสามารถดำเนินธุรกิจต่อไปได้โดยไม่ติดขัด

ผู้รับผิดชอบ

ผู้บริหารระดับสูง

ผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. เพื่อให้สามารถดูแลการทำงานของระบบคอมพิวเตอร์และฐานข้อมูลต่างๆ ได้อย่างต่อเนื่อง ฝ่ายเทคโนโลยีสารสนเทศและผู้ถือ Username และ Password มีหน้าที่ดังนี้

1.1 จัดรวบรวม Username และ Password ที่สำคัญ เพื่อการเข้าถึงระบบงานคอมพิวเตอร์ต่าง ๆ และทำสรุปเก็บเป็นความลับ 1 ชุด ให้กรรมการผู้จัดการหรือผู้ได้รับมอบอำนาจจากกรรมการผู้จัดการเป็นผู้เก็บรักษาไว้

1.2 ต้องมีการจัดทำ ผังโครงสร้างระบบโครงข่ายพร้อมตำแหน่งที่วางอุปกรณ์คอมพิวเตอร์ที่สำคัญทั้งหมด นำส่งให้กับกรรมการผู้จัดการทุก 6 เดือน

6.12 ***มาตรฐานระบบคอมพิวเตอร์ (Computer System Standards)***

วัตถุประสงค์

เพื่อให้การใช้งานระบบคอมพิวเตอร์ของบริษัทฯเป็นไปอย่างมีประสิทธิภาพ รวดเร็ว ปลอดภัย และรองรับการใช้งานของผู้ใช้งานในปัจจุบัน และเสริมสร้างศักยภาพในการแข่งขันทางธุรกิจให้กับบริษัทฯ

ผู้รับผิดชอบ

พนักงานส่วนสนับสนุนระบบสารสนเทศ

แนวทางปฏิบัติ

1. เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่ใช้งานมานาน ควรเปลี่ยนใหม่ทดแทนเพื่อป้องกันความเสี่ยงในกรณีเครื่องเสียหาย โดยกำหนดมาตรฐานอายุการใช้งานของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ดังนี้
   1.1 เครื่องคอมพิวเตอร์แม่ข่าย (Server) 5 ปี โดยมีสัญญาบำรุงรักษาตลอดการใช้งาน
   1.2 เครื่องคอมพิวเตอร์ทั่วไป (PC) 5 - 7 ปี
   1.3 เครื่องคอมพิวเตอร์พกพา (Notebook/Laptop) 5 ปี
   1.4 อุปกรณ์จัดเก็บข้อมูล Hard Disk 4 ปี และ SSD 6 ปี
   1.5 อุปกรณ์ระบบเครือข่าย (Switch, Access Point) 6 ปี
   1.6 อุปกรณ์ไฟร์วอลล์ (Firewall) 5 ปี โดยมีสัญญาบำรุงรักษาตลอดการใช้งาน
   1.7 อุปกรณ์สำรองไฟ (UPS) 5 ปี ควรเปลี่ยนแบตเตอรี่ทุกๆ 2 ปี
2. เครื่องคอมพิวเตอร์ที่ใช้งานจะต้องสามารถรองรับการใช้งานในปัจจุบันของผู้ใช้ได้อย่างเพียงพอ
3. เครื่องคอมพิวเตอร์ที่ใช้งานจะต้องติดตั้งโปรแกรมพื้นฐานที่จำเป็นต่อการใช้งาน และต้องติดตั้งโปรแกรม Anti-Virus ตามที่บริษัทฯกำหนด
4. เครื่องคอมพิวเตอร์ที่ใช้งานควรกำหนดมาตรฐานสำหรับการใช้งาน
   4.1 มาตรฐานของเครื่องคอมพิวเตอร์สำหรับระดับพนักงานออฟฟิศทั่วไป ดังนี้
   - หน่วยประมวลผล (CPU) ขั้นต่ำ Intel Core i3 หรือ Core i5
   - หน่วยความจำ (RAM) 4 GB. - 8GB.
   - พื้นที่จัดเก็บข้อมูล (Hard disk) 500 GB. - 1 TB.
   - ความเร็วในการเชื่อมต่อเครือข่ายระดับ Gigabit
   - จอ (LCD Monitor) 17" - 22" กรณี PC และ 14" – 15.6" กรณี Notebook
   - Wireless LAN กรณี Notebook จะต้องรองรับตามมาตรฐาน 802.11b/g/n

- เครื่องสำรองไฟ (UPS) 500VA – 1,000VA ควรเปลี่ยนแบตเตอรี่ทุก ๆ 2 ปี สำรองไฟได้ไม่ต่ำกว่า 10 นาที

4.2 มาตรฐานของเครื่องคอมพิวเตอร์สำหรับพนักงานฝ่ายบริหารหรือฝ่ายโครงการที่ต้องใช้งานประสิทธิภาพสูง ดังนี้

- หน่วยประมวลผล (CPU) ขั้นต่ำ Intel Core i5 หรือ Core i7
- หน่วยความจำ (RAM) 8 GB – 16 GB
- พื้นที่จัดเก็บข้อมูล (Hard disk) SSD 128 GB หรือ Hard disk 500 GB ขึ้นไป
- ความเร็วในการเชื่อมต่อเครือข่ายระดับ Gigabit
- การ์ดจอ (Graphic Card) 2 GB – 4 GB GDDR5
- จอ (LED Monitor) 19" – 27" กรณี PC และ 13" – 15.6" กรณี Notebook
- Wireless LAN กรณี Notebook จะต้องรองรับตามมาตรฐาน 802.11b/g/n/ac

6.13 ***การใช้ซอฟท์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual Property)***

วัตถุประสงค์

ลิขสิทธิ์ ถือเป็นทรัพย์สินทางปัญญาที่กฎหมายให้ความคุ้มครอง โดยให้เจ้าของลิขสิทธิ์ถือสิทธิแต่เพียงผู้เดียวที่จะกระทำการใดๆ เกี่ยวกับงานสร้างสรรค์ที่ตนได้กระทำขึ้น กฎหมายลิขสิทธิ์จึงมีวัตถุประสงค์ให้ความคุ้มครอง ป้องกันผลประโยชน์ทั้งทางเศรษฐกิจและทางศีลธรรม ซึ่งบุคคลพึงได้รับจากผลงานสร้างสรรค์อันเกิดจากความนึกคิดและสติปัญญาของตน บริษัทฯให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา จึงกำหนดให้ใช้งานซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

ผู้รับผิดชอบ

พนักงานทุกคน

แนวทางปฏิบัติ

1. ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น ห้ามไม่ให้ผู้ใช้งานทำการติดตั้ง หรือใช้งานซอฟท์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทฯถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว
2. ซอฟท์แวร์ (Software) ที่บริษัทฯได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น
3. บริษัทฯไม่อนุญาตให้พนักงานแจกจ่ายซอฟท์แวร์ (Software) ของบริษัทฯให้แก่บุคคลภายนอก หรือให้บุคคลภายนอกใช้ซอฟท์แวร์ (Software) ที่บริษัทฯได้รับอนุญาตให้ใช้ เว้นแต่ได้รับการอนุญาตจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

4. ฝ่ายเทคโนโลยีสารสนเทศ สงวนสิทธิ์ที่จะเข้าตรวจสอบข้อมูลการใช้ซอฟท์แวร์ (Software) บนเครื่องคอมพิวเตอร์ที่พนักงานใช้ได้ตลอดเวลา โดยไม่ต้องแจ้งล่วงหน้า

7 **การพิจารณาโทษทางวินัยและการเรียกค่าเสียหาย**

1. ผู้ใช้งานที่เจตนาฝ่าฝืนนโยบาย เงื่อนไข ข้อตกลงตามเอกสารฉบับนี้ แม้ว่าการฝ่าฝืนจะกระทำไม่สำเร็จโดยสมบูรณ์ก็ตาม ให้ถือว่ามีความผิดโดยสมบูรณ์
2. พนักงานและลูกจ้างที่ฝ่าฝืนข้อกำหนดนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยจงใจหรือประมาทเลินเล่อ และก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัทฯหรือบุคคลหนึ่งบุคคลใด บริษัทฯจะพิจารณาดำเนินการทางวินัยความผิดทางแพ่งและอาญาแก่พนักงานและลูกจ้างนั้นตามกฎหมาย ข้อบังคับ ระเบียบ หรือประกาศที่เกี่ยวข้อง
3. ผู้บังคับบัญชาผู้ใด งดเว้นหรือละเว้นการปฏิบัติหน้าที่และเป็นเหตุให้พนักงานหรือลูกจ้างที่อยู่ภายใต้การบังคับบัญชาของตน ฝ่าฝืนข้อกำหนดของนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ ให้นำบทบัญญัติในวรรคก่อนมาใช้บังคับ
4. การฝ่าฝืนข้อกำหนดใดๆ ตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ แม้จะไม่ก่อให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใดก็ตาม หากผู้บังคับบัญชาเห็นว่ามีเหตุอันสมควร อาจจะบันทึกในประวัติการปฏิบัติงานและจะใช้เป็นข้อมูลประกอบการพิจารณาต่ออายุสัญญาจ้าง การขึ้นเงินเดือน หรือ เลื่อนตำแหน่ง ด้วยก็ได้

ประกาศ ณ วันที่ 29 เมษายน 2565

.....

(นายสนั่น อังอุบลกุล)

กรรมการผู้จัดการ