CHRISTIANI & NIELSEN (THAI) PCL.

Information Systems (IT) Policy and Procedure

IT Department

เรื่อง กฎระเบียบ และนโยบายระบบสารสนเทศ

Prepared By: _____ Date: 1/8/19

(Somsak Jaturatchaiyaporn)
IT Department Manager

Checked By: _____ Date: 7/8/19

(Surasak Osathanugraha)
Assistant to Managing Director

Approved By: _____ Date: 7-8-19

(Khushroo Wadia)
Managing Director

Distribution : ALL

AMEMDMENT RECORD

Revision No.	Date	Section / Pages	Details
0	01.08.2000	All	Initial for use
1	09.03.2001	Add IT-0	Main Content
2	01.08.2007	All	Revised new procedure
3	01.08.2019	All	Revised new procedure

☑ CONTROLLED DOCUMENT ☐ UNCONTROLLED DOCUMENT

สารบัญหลัก

บททั่วไป

ระบบสารสนเทศของบริษัทฯ หมายถึง เครื่องคอมพิวเตอร์และอุปกรณ์ทุกประเภท ระบบงาน ซอฟแวร์ และข้อมูลต่างๆ ถือเป็นสินทรัพย์ที่จะต้องได้รับการดูแลคุ้มครองและป้องกันไม่ให้ถูกเปิดเผย แก้ไข หรือใช้งานโดยผู้ที่ไม่ได้รับอนุญาต หรือนำไปใช้โดยไม่เหมาะสม รวมถึงจะต้องมีความพร้อมอยู่ตลอดเวลาเพื่อให้สามารถใช้งานได้ทันที

กฎระเบียบและนโยบายระบบสารสนเทศฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดและแนวทางในการปฏิบัติงานของพนักงานทั้งหมดของบริษัท และบริษัทย่อย (บริษัทฯ) รวมถึงพนักงานของผู้ว่าจ้าง ตัวแทนผู้ว่าจ้าง ผู้จำหน่ายหรือรับจ้างพัฒนาซอฟต์แวร์ หรือ ซัพพลายเออร์ ที่ได้รับอนุญาตในการใช้ระบบสารสนเทศของบริษัทฯ ทั้งนี้เพื่อให้การใช้งานในระบบสารสนเทศเป็นไปอย่างถูกต้อง ปลอดภัย และมีประสิทธิภาพ รวมทั้งเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่เหมาะสม จึงได้กำหนด กฎระเบียบและนโยบายระบบสารสนเทศ โดยมีเนื้อหาและสาระสำคัญดังต่อไปนี้

1. ระบบสารสนเทศ
2. ข้อมูล
3. เจ้าหน้าที่ตรวจสอบความปลอดภัยของระบบคอมพิวเตอร์
4. ระบบงาน (Application System)
    - 4.1 การกำหนดเจ้าของระบบงาน
    - 4.2 การพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงาน
    - 4.3 การควบคุมการเข้าถึงระบบงาน
        - 4.3.1 การควบคุมสิทธิการใช้ระบบงาน
        - 4.3.2 User ID ชื่อผู้เข้าใช้งานในระบบงาน
        - 4.3.3 Password (รหัสผ่าน) ที่ใช้แสดงตนในการเข้าใช้ระบบงาน
        - 4.3.4 การใช้งาน User ID พิเศษ (Privilege User ID) ที่มีสิทธิระดับสูงในระบบงาน
        - 4.3.5 การบันทึกการทำงานเพื่อการตรวจสอบการเข้าใช้งานในระบบงาน (Security Audit Logging)

5. ห้องคอมพิวเตอร์
   - 5.1 สภาพแวดล้อมของสถานที่ตั้งห้องคอมพิวเตอร์
   - 5.2 การควบคุมการเข้าห้องคอมพิวเตอร์
   - 5.3 ระบบป้องกันไฟฟ้าขัดข้อง
   - 5.4 ระบบป้องกันไฟไหม้
6. การป้องกันการหยุดชะงักของธุรกิจเนื่องจากระบบงานขัดข้อง
   - 6.1 การบำรุงรักษาระบบคอมพิวเตอร์
   - 6.2 การประกันภัย
   - 6.3 การสำรองข้อมูลในระบบงาน
   - 6.4 แผนรองรับเหตุสุดวิสัย (Disaster Recovery Plan)
7. การใช้งานเครื่องคอมพิวเตอร์ตั้งโต๊ะ (Desk Top) และคอมพิวเตอร์พกพา (Notebook)
8. การกำหนดมาตรฐานเครื่องและอุปกรณ์ระบบคอมพิวเตอร์ (Specification)
9. บทลงโทษ

เอกสารควบคุม (Controlled Document)

เอกสารที่เป็นเอกสารควบคุม (Controlled Document) ของแผนก ได้แก่

1. กฎระเบียบและนโยบายทางด้านระบบสารสนเทศ
2. คู่มือการใช้งานโปรแกรม (Software Users Manual)

กฎระเบียบ และนโยบายระบบสารสนเทศ

1. ระบบสารสนเทศ

หมายความถึง เครื่องคอมพิวเตอร์และอุปกรณ์ทุกประเภท ซอฟต์แวร์ ระบบงานและข้อมูลต่างๆ ซึ่งบริษัทฯ ได้จัดหามาโดยการซื้อหรือเช่า หรือวิธีอื่นใด สำหรับให้พนักงานใช้ประโยชน์ในการปฏิบัติงานตามหน้าที่และความรับผิดชอบ การบริหารงานองค์กร และ/หรือการตัดสินใจใดๆ ของบริษัทฯ ซึ่งประกอบด้วย

- อุปกรณ์คอมพิวเตอร์ของบริษัทฯ หมายถึง เครื่องคอมพิวเตอร์ เช่น คอมพิวเตอร์ตั้งโต๊ะ, คอมพิวเตอร์แบบพกพา (Notebook), Tablet, Smart Phone, เครื่องเวิร์คสเตชั่น, เซิร์ฟเวอร์ รวมถึงอุปกรณ์ที่อยู่ในเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชนิดที่มีการเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์ของบริษัทฯ เช่น อุปกรณ์ต่อพ่วงทั้งแบบมีสายและไร้สาย, อุปกรณ์สำหรับเชื่อมต่อระบบเครือข่ายทั้งภายในบริษัทฯ และเชื่อมต่อเข้าระบบอินเตอร์เน็ต, อุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลต่างๆ เช่น Hard disk, Thumb drive, CD/DVD
- ซอฟต์แวร์ หมายถึงโปรแกรมที่ติดตั้งอยู่บนอุปกรณ์คอมพิวเตอร์ทั้งหมดของบริษัทฯ เพื่อใช้ในการปฏิบัติงาน ที่บริษัทฯ จัดซื้อหรือเช่าเพื่อให้ได้รับสิทธิในการใช้งาน โปรแกรมที่ใช้ในการปฏิบัติงานที่พัฒนาหรือจัดทำขึ้นโดยพนักงานของบริษัทฯ หรือจ้างบริษัทภายนอกจัดทำ เช่น โปรแกมที่ใช้ในงานออกแบบ โปรแกรมด้านบัญชีและการเงิน โปรแกรมบริหารงานทรัพยากรบุคคล ระบบ E-mail ระบบปฏิบัติการคอมพิวเตอร์ รวมถึงเฟิร์มแวร์และซอฟต์แวร์อื่นๆ
- ข้อมูลของบริษัทฯ หมายถึง ข้อมูลทั้งหมดที่ติดตั้งหรือบันทึกอยู่ในอุปกรณ์คอมพิวเตอร์ของบริษัทฯ รวมถึงข้อมูลทั้งหมดที่ได้จากการปฏิบัติงานของพนักงานในระหว่างการเป็นพนักงานของบริษัทฯ

2. ข้อมูลของบริษัทฯ

ข้อมูลของบริษัทฯ ที่ติดตั้งหรือบันทึกอยู่ในอุปกรณ์คอมพิวเตอร์ถือเป็นทรัพย์สินของบริษัทฯ ทั้งนี้ บริษัทฯ มีสิทธิเข้าถึงข้อมูลในอุปกรณ์คอมพิวเตอร์ของบริษัทฯ ได้ตลอดเวลา โดยไม่ต้องแจ้งให้ทราบล่วงหน้า ข้อมูลส่วนตัวและ/หรือข้อมูลที่เป็นความลับของพนักงานที่ติดตั้งหรือบันทึกอยู่ในอุปกรณ์คอมพิวเตอร์จะไม่ถือเป็นข้อมูลที่เป็นความลับ และอาจจะไม่ได้รับความคุ้มครองจากบริษัทฯ ทั้งนี้ พนักงานควรติดตั้งหรือบันทึกข้อมูลส่วนตัวและ/หรือข้อมูลที่เป็นความลับไว้ในอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานเท่านั้น อย่างไรก็ตาม ข้อมูลที่ได้ให้ไว้กับบริษัทฯ อันเป็นการเฉพาะเพื่อใช้ในการสมัครงานตามสัญญาจ้างแรงงาน ระเบียบข้อบังคับเกี่ยวกับการทำงาน นโยบาย หรือข้อมูลอื่นใด ที่บริษัทฯ ร้องขอในระหว่างการเป็นพนักงานของบริษัทฯ จะถือเป็นความลับและได้รับความคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3. เจ้าหน้าที่ตรวจสอบความปลอดภัยของระบบคอมพิวเตอร์

กำหนดให้มีเจ้าหน้าที่ตรวจสอบความปลอดภัยของระบบคอมพิวเตอร์โดยมีหน้าที่ดังต่อไปนี้

- พัฒนาและปรับปรุงนโยบายความปลอดภัยของการใช้ระบบคอมพิวเตอร์ รวมไปถึงการตรวจสอบควบคุม และดูแลการใช้งานด้านคอมพิวเตอร์ในบริษัทฯ ให้เป็นไปตามกฎระเบียบและนโยบายระบบสารสนเทศ ฉบับนี้
- ให้คำแนะนำและเสนอแนะต่อผู้บริหารในการกำหนดนโยบายและมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล
- ตรวจสอบ ซอฟท์แวร์และข้อมูลที่ติดตั้งในอุปกรณ์คอมพิวเตอร์ทั้งหมดของบริษัทฯ
- จัดทำรายงานเกี่ยวกับการปฏิบัติตามกฎระเบียบและนโยบายสารสนเทศ เสนอผู้บริหารเป็นระยะตามความเหมาะสม

4. ระบบงาน (Application System)

ระบบงาน หมายถึง ระบบงานบัญชี ระบบ Fixed Assets ระบบงานจัดซื้อจัดจ้าง ระบบบริหารงานทรัพยากรบุคคล ระบบ JDE เป็นต้น

4.1 การกำหนดเจ้าของระบบงาน

- ระบบงานทุกระบบต้องมีการกำหนดหน่วยงานหรือบุคคลที่เป็นเจ้าของระบบงานไว้อย่างชัดเจน
- เจ้าของระบบงาน มีหน้าที่และความรับผิดชอบในการให้ความยินยอมในการขอใช้ระบบงานและหรือการพัฒนาเปลี่ยนแปลงแก้ไขระบบงาน/ข้อมูล ตามที่ได้รับการอนุมัติจากผู้มีอำนาจอย่างถูกต้องตามขั้นตอน

4.2 การพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงาน

- ระบบคอมพิวเตอร์ระดับ Server ซึ่งใช้จัดเก็บระบบงานที่อาจมีการแก้ไขโปรแกรมของระบบงานนั้น จะแยกออกเป็น 2 ส่วนดังนี้
  - ส่วนที่เป็น Production สำหรับใช้ในการประมวลผลข้อมูลจริง
  - ส่วนที่เป็น Development สำหรับใช้ในการพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงาน
- การขอพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงาน ผู้ร้องขอต้องจัดทำบันทึกคำร้องโดยระบุรายละเอียดที่ต้องการเป็นลายลักษณ์อักษรตามแบบฟอร์มที่กำหนดโดยแผนกเทคโนโลยีสารสนเทศ และต้องได้รับอนุมัติจากผู้มีอำนาจและเจ้าของระบบงานทุกครั้ง
- ระบบงานที่พัฒนาหรือเปลี่ยนแปลงแก้ไขแล้ว ต้องผ่านการทดสอบจากผู้ร้องขอว่ามีความถูกต้องครบถ้วนตามที่ต้องการเป็นลายลักษณ์อักษร และได้รับความยินยอมจากเจ้าของระบบงานก่อนการเริ่มใช้งาน

- ในการโอนย้ายระบบงานที่พัฒนาหรือเปลี่ยนแปลงแก้ไขจากส่วน Development ไปยังส่วน Production ต้องมีการตรวจสอบความถูกต้องและบันทึกการโอนย้ายเป็นลายลักษณ์อักษรทุกครั้ง
- ในการพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงานใดๆ จะต้องปรับปรุงแก้ไขเอกสารต่างๆ ที่เกี่ยวข้องให้มีความทันสมัยอยู่เสมอ เช่น เอกสารแสดงข้อมูลรายละเอียดในการพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงาน คู่มือระบบงาน คู่มือผู้ใช้งาน ข้อมูลที่เกี่ยวกับระบบความปลอดภัย (Security) เป็นต้น
- ต้องจัดเก็บและบันทึกการจัดเก็บโปรแกรม Version ก่อนการพัฒนาหรือเปลี่ยนแปลงแก้ไขเพื่อให้สามารถนำกลับมาใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาด
- ผู้ร้องขอต้องมีการสอบทานระบบงานที่ได้แก้ไขหรือพัฒนา หลังจากมีการใช้งานไปแล้วระยะหนึ่งเพื่อประเมินผลการใช้งานจริง และแจ้งผลต่อเจ้าของระบบงาน

4.3 การควบคุมการเข้าถึงระบบงาน

4.3.1 การควบคุมสิทธิการใช้ระบบงาน

- ในการขออนุญาตเพื่อใช้ระบบงาน ต้องได้รับการอนุมัติจากผู้บังคับบัญชาโดยตรงของผู้ขอใช้งานและต้องได้รับความยินยอมจากเจ้าของระบบงานเป็นลายลักษณ์อักษร
- กำหนดให้มีการสอบถาม User ID และ Password ทุกครั้งในการใช้ระบบงาน
- กำหนดให้สิทธิในการใช้ระบบงานและระบบคอมพิวเตอร์ ตามความเหมาะสมกับหน้าที่ความรับผิดชอบ และความจำเป็นในการปฏิบัติหน้าที่ของผู้ใช้เท่านั้น
- หน้าที่และความรับผิดชอบของบุคคลที่เกี่ยวข้องกับระบบงานมีดังต่อไปนี้
  - เจ้าของระบบงาน (Application Owner) สามารถใช้ข้อมูลในระบบงานที่ตนเป็นเจ้าของ และเป็นผู้อนุมัติหรือให้ความยินยอมแก่ผู้ใช้อื่นในการเข้ามาใช้ระบบงาน
  - End User สามารถใช้งานได้เฉพาะส่วน Production ที่เจ้าของระบบงานได้กำหนดไว้เท่านั้น
  - ผู้วิเคราะห์ระบบงาน (System Analyst) และ ผู้พัฒนาโปรแกรมไม่สามารถใช้งานใน Production
  - ผู้ที่ปฏิบัติหน้าที่ Operator สามารถใช้งานได้เฉพาะคำสั่งของระบบคอมพิวเตอร์เพื่อใช้ในการจัดการข้อมูลของระบบงาน เช่น การสำรองข้อมูล เป็นต้น
  - Security Administrator ใช้งานได้เฉพาะคำสั่งที่ใช้ในการจัดการกับ User ID และ Password ของระบบงานและเครื่องคอมพิวเตอร์ที่ใช้ในระบบงาน

- System Administrator เป็น User ที่มีความสามารถสูงสุดในการใช้งานหรือแก้ไขปัญหาระบบงานงานและเครื่องคอมพิวเตอร์ที่ใช้ในระบบงาน

- โปรแกรมหรือคำสั่งที่มีลักษณะการใช้งานเฉพาะด้านในระบบงาน สามารถใช้โดยผู้ที่ได้รับการอนุมัติจากเจ้าของระบบงานแล้วเท่านั้น

4.3.2 User ID ชื่อผู้เข้าใช้งานในระบบงาน

- User ID แบ่งเป็น User ID ทั่วไป และ User ID พิเศษ (Privilege User ID)
- ผู้ใช้งานแต่ละรายต้องมี User ID เป็นของตนเอง และไม่ให้มีการใช้ User ID ร่วมกัน
- ในการขอสร้าง เปลี่ยนแปลง หรือยกเลิก User ID ของแต่ละระบบงาน ให้เป็นไปตามขั้นตอนดังต่อไปนี้
  - ผู้ร้องขอต้องได้รับอนุมัติจากผู้บังคับบัญชาโดยตรง และต้องได้รับความยินยอมจากเจ้าของระบบงานนั้นๆ อย่างเป็นลายลักษณ์อักษร ตามแบบฟอร์มคำขอที่กำหนดโดยแผนกเทคโนโลยีสารสนเทศ
  - Security Administrator จะตรวจสอบความถูกต้องของรายละเอียดและการอนุมัติก่อนดำเนินการ
  - Security Administrator จะส่งมอบ User ID และ Password ให้แก่ผู้ใช้งานอย่างเป็นลายลักษณ์อักษร
  - เมื่อผู้ใช้งาน Sign on เข้าระบบในครั้งแรก ระบบคอมพิวเตอร์จะกำหนดให้ผู้ใช้งานเปลี่ยน Password โดยทันที
  - ในกรณีที่มีการเปลี่ยนแปลงสถานภาพของเจ้าของ User ID ผู้บังคับบัญชาของผู้ใช้ User ID ดังกล่าวหรือเจ้าของระบบงาน จะต้องแจ้งให้ผู้ดูแล User ID ทราบเป็นลายลักษณ์อักษร เพื่อที่จะดำเนินการเปลี่ยนแปลงแก้ไขโดยทันที
  - หลังการสร้าง เปลี่ยนแปลงหรือยกเลิกจะต้องมีการสอบทานให้ถูกต้องโดยผู้ร้องขอ
- Security Administrator ต้องจัดทำสรุปรายชื่อผู้ใช้งาน User ID ของระบบงานต่างๆ จัดส่งให้เจ้าของระบบงานเพื่อตรวจสอบอย่างสม่ำเสมอ และหากตรวจพบ User ID ที่ไม่มีสิทธิในการใช้ระบบงานหรือลาออกแล้ว เจ้าของระบบงานต้องแจ้งระงับการใช้ User ID ดังกล่าวโดยทันที

4.3.3 Password (รหัสผ่าน) ที่ใช้แสดงตนในการเข้าใช้ระบบงาน

- Security Administrator ต้องตั้งค่าเงื่อนไขการกำหนด Password ในการเข้าใช้ระบบงาน อย่างน้อยให้เป็นไปตามที่ระบุไว้ดังนี้

- Password ต้องมีความยาวอย่างน้อย 8 ตัวอักษร โดยต้องมีการผสมกันของอักษรตัวเล็ก ตัวใหญ่ ตัวเลขและอักขระพิเศษ (ถ้าทำได้) อย่างน้อยชนิดละ 1 ตัวอักษร เพื่อให้ยากแก่การคาดเดาของผู้อื่น
- ผู้ใช้ต้องเปลี่ยน Password อย่างสม่ำเสมอทุก 60 วัน หรือน้อยกว่า
- ไม่อนุญาตให้กำหนด Password ซ้ำกับ Password ครั้งก่อนหน้านี้
- อนุญาตให้ใส่ Password ผิดได้ไม่เกิน 5 ครั้ง หากเกินกำหนดระบบจะระงับการใช้งานทันที

- เจ้าของ User ID ต้องเก็บรักษา Password ของตนไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น รวมถึงไม่เขียน Password ไว้ในที่ต่างๆ เพื่อป้องกันไม่ให้ผู้อื่นแอบนำ User ID และ Password ของตนไปใช้งาน
- Password ที่เก็บอยู่ในแฟ้มข้อมูลจะต้องผ่านการแปลงรหัสประเภท One Way Encryption ซึ่งไม่สามารถแปลงรหัสกลับได้

4.3.4 การใช้งาน User ID พิเศษ (Privilege User ID) ที่มีสิทธิระดับสูงในระบบงาน (System Administrator)

- User ID พิเศษ (System Administrator) จะต้องเป็นผู้จัดการแผนกเทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายจากผู้จัดการแผนกเทคโนโลยีสารสนเทศเท่านั้น
- ในการเข้าใช้งาน Privilege User ID ของระบบงาน จะต้องได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาเท่านั้น
- การใช้งาน Privilege User ID ต้องเป็นกรณีจำเป็นที่ User ID ทั่วไปไม่สามารถใช้หรือแก้ปัญหาของระบบงานในขณะนั้นได้
- ต้องบันทึกการใช้งาน Privilege User ID ทุกครั้ง
- หลังจากเลิกใช้งานทุกครั้งต้องมีการเปลี่ยน Password ของ Privilege User ID
- ต้องสอบทานการใช้งาน Privilege User ID อย่างสม่ำเสมอ

4.3.5 การบันทึกการทำงานเพื่อการตรวจสอบการใช้งานในระบบงาน (Security Audit Logging)

- มีการบันทึกกิจกรรมที่ทำโดย User ID และที่ดำเนินการโดยระบบ
- มีการตรวจสอบบันทึกอย่างสม่ำเสมอโดยเจ้าหน้าที่ตรวจสอบความปลอดภัยของระบบงาน

- ในกรณีที่ตรวจพบการฝ่าฝืนกฎเกณฑ์ในการใช้ระบบงาน จะมีการบันทึก ตักเตือน หรือลงโทษทางวินัยตามระเบียบข้อบังคับเกี่ยวกับการทำงานของบริษัทฯ ที่ประกาศและมีผลบังคับใช้ในขณะนั้น

5. ห้องคอมพิวเตอร์

5.1 สภาพแวดล้อมของสถานที่ตั้งห้องคอมพิวเตอร์

- ห้องคอมพิวเตอร์ไม่ควรตั้งอยู่ในบริเวณที่อยู่ใกล้ท่อแก๊ส เครื่องทำความร้อน/เย็นขนาดใหญ่ และสถานที่ที่เก็บกระดาษหรือวัตถุที่เป็นเชื้อเพลิงจำนวนมาก
- ห้องคอมพิวเตอร์ไม่ควรอยู่ในบริเวณที่มีฟ้าร้องหรือฟ้าผ่าในปริมาณสูง
- ผนังห้อง พื้นและเพดานของห้องคอมพิวเตอร์ ควรเป็นวัสดุที่สามารถทนความร้อนได้เป็นพิเศษ
- เครื่องคอมพิวเตอร์จะต้องไม่ติดตั้งอยู่ในสถานที่ซึ่งมีสภาพแวดล้อมดังนี้
  - มีความร้อนสูงหรือแสงแดดส่องถึงเป็นเวลานาน
  - มีฝุ่นมาก
  - มีระดับไฟฟ้าสถิตสูง
  - มีความชื้นสูง
  - มีควันหรืออากาศเสียในปริมาณสูง
  - บริเวณที่มีความสั่นสะเทือนสูง
  - มีคลื่นวิทยุและคลื่นไฟฟ้ารบกวน

5.2 การควบคุมการเข้าห้องคอมพิวเตอร์

- เครื่องคอมพิวเตอร์ให้จัดไว้ในห้องแยกต่างหาก โดยมีระบบรักษาความปลอดภัยอย่างเพียงพอ
- ประตูห้องคอมพิวเตอร์จะต้องปิดและล็อคอยู่ตลอดเวลา
- มีการควบคุมการเข้าออกห้องคอมพิวเตอร์และให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาต
- ให้มีการใช้บัตรหรือรหัสเปิด/ปิดประตูในการเข้าหรือออกห้องคอมพิวเตอร์
- มีรายงานบันทึกชื่อบุคคลที่เข้าหรือออกห้องคอมพิวเตอร์เพื่อการตรวจสอบ

5.3 ระบบป้องกันไฟฟ้าขัดข้อง

- ติดตั้งระบบสำรองไฟฟ้า UPS เพื่อเป็นระบบไฟฟ้าสำรองและสามารถควบคุมความคงที่ของกระแสไฟได้
- ระบบไฟฟ้าสำรองควรจ่ายไฟฟ้าได้อย่างน้อยเท่ากับระยะเวลาของการประมวลผลโปรแกรมที่ใช้เวลานานที่สุดของระบบงาน

5.4 ระบบป้องกันไฟไหม้

- มีเครื่องมือดับเพลิงชนิดที่ใช้สารเคมีที่ไม่ก่อให้เกิดการสึกหรอของระบบเครื่องคอมพิวเตอร์ และเก็บไว้ในสถานที่ที่สะดวกต่อการนำมาใช้
- มีการบำรุงรักษาเครื่องมือเหล่านี้อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
- มีการอบรมวิธีการใช้และบำรุงรักษาเครื่องมือดับเพลิงแก่พนักงานเพื่อให้สามารถใช้งานได้
- มีการทดสอบระบบป้องกันไฟไหม้และเตือนภัยอย่างสม่ำเสมอ

6. การป้องกันการหยุดชะงักของธุรกิจเนื่องจากระบบงานขัดข้อง

6.1 การบำรุงรักษาระบบคอมพิวเตอร์

- เจ้าของหรือผู้ที่มีหน้าที่ดูแลระบบเครื่องคอมพิวเตอร์ ต้องจัดให้มีการตรวจสอบเพื่อบำรุงรักษาระบบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง และมีการบันทึกรายละเอียดการตรวจสอบไว้เป็นลายลักษณ์อักษร
- ในกรณีที่ระบบคอมพิวเตอร์มีปัญหาขัดข้อง ผู้ที่มีหน้าที่ดูแลต้องดำเนินการแก้ไขในทันที และบันทึกปัญหาและวิธีการแก้ไขไว้เป็นลายลักษณ์อักษร

6.2 การประกันภัย

ให้มีการทำประกันความเสียหายของระบบคอมพิวเตอร์และอุปกรณ์ เพื่อให้มั่นใจว่าหากเกิดกรณีฉุกเฉิน การหยุดชะงักของระบบงานจากไฟไหม้ น้ำท่วม การโจรกรรม กิจการยังสามารถเรียกร้องค่าสินไหมทดแทนจากการประกันภัยในอัตราที่เหมาะสมกับวงเงินประกันภัย

6.3 การสำรองข้อมูลในระบบงาน

- Operator จะสำรองข้อมูลเก็บไว้อย่างน้อยเดือนละ 1 ครั้ง
- จัดทำตารางเวลาในการสำรองข้อมูลของระบบงานและข้อมูลจากการปฏิบัติงานอย่างสม่ำเสมอ โดยมีรายละเอียดดังต่อไปนี้
  - วันที่และเวลาในการสำรองข้อมูล
  - ชื่อและประเภทของแฟ้มข้อมูล
  - ชื่อ Volume และ Label ของอุปกรณ์ที่ใช้ในการเก็บสำรองข้อมูล เช่น Tape หรือ Diskette
  - จำนวนชุดที่ทำการสำรองข้อมูลแต่ละครั้ง
- จัดทำ Directory ของอุปกรณ์ที่ใช้ในการเก็บสำรองข้อมูลทั้งหมด
- มีการสำรองแฟ้มข้อมูล และโปรแกรมที่ใช้งานเก็บไว้ทั้งในและนอกที่ทำการของบริษัทฯ

- ในการจัดเก็บอุปกรณ์ที่ใช้ในสำรองข้อมูล เช่น Tape หรือ Diskette ต้องบันทึกข้อมูลการจัดเก็บ เช่นที่เก็บ, ชื่อ Label ของอุปกรณ์ และสถานที่เก็บ เพื่อไว้ตรวจสอบหรือค้นหาได้อย่างง่ายดาย
- มีการระบุระยะเวลาและเงื่อนไขในการนำอุปกรณ์ที่ใช้ในการสำรองข้อมูลกลับมาใช้ใหม่
- มีการทดสอบอุปกรณ์ที่ใช้ในการสำรองข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

6.4 แผนรองรับเหตุสุดวิสัย (Disaster Recovery Plan)

- มีการจัดทำแผนป้องกันการหยุดชะงักของระบบงานเพื่อรองรับเหตุสุดวิสัยต่างๆ
- มีการกำหนดผู้รับผิดชอบในการวางแผนงานรองรับการหยุดชะงักของระบบงาน
- ในแผนรองรับเหตุสุดวิสัยควรมีการระบุรายละเอียดดังต่อไปนี้
  - ผลกระทบของเหตุสุดวิสัยที่มีต่อธุรกิจของแต่ละระบบงาน
  - ความเสี่ยงหรือโอกาสที่ระบบงานแต่ละระบบหรือโดยรวมจะเกิดเหตุสุดวิสัย
  - ระยะเวลาสูงสุดที่ใช้ในการนำระบบงานแต่ละระบบกลับมาใช้ใหม่โดยไม่ส่งผลกระทบที่รุนแรงต่อธุรกิจ
  - รายละเอียดเกี่ยวกับระบบงานทั้งหมดตลอดจนความสัมพันธ์กันของแต่ละระบบงาน
  - รายละเอียดของระบบคอมพิวเตอร์ และระบบสื่อสารที่ใช้รวมถึงอุปกรณ์ต่อเชื่อมต่างๆ
  - ข้อมูลเกี่ยวกับ Suppliers ของเครื่องคอมพิวเตอร์และอุปกรณ์ทั้งหมด
  - รายละเอียดของการแก้ไขปัญหาและผู้รับผิดชอบในแต่ละขั้นตอน
  - สถานที่และรายชื่อของศูนย์คอมพิวเตอร์สำรอง ถ้ามี
  - รายชื่อและสถานที่ติดต่อของผู้รับผิดชอบและผู้ที่เกี่ยวข้องทั้งหมด
- แผนรองรับเหตุสุดวิสัยจะต้องได้รับการอนุมัติโดยผู้บริหาร
- ต้องเผยแพร่ให้บุคลากรที่เกี่ยวข้องได้รับรู้และเข้าใจแผนรองรับเหตุสุดวิสัยในส่วนที่เกี่ยวข้องอย่างชัดเจน
- ต้องมีการกำหนดตารางเวลาเพื่อจัดให้มีการทดสอบแผนรองรับเหตุสุดวิสัยดังกล่าวอย่างสม่ำเสมอเพื่อให้บุคลากรที่เกี่ยวข้องมีความคุ้นเคย และปรับปรุงแผนให้ทันสมัยอยู่ตลอดเวลา
- ในกรณีเกิดเหตุการณ์ฉุกเฉิน ต้องมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุและวิธีการแก้ไขปัญหา
- สถานที่ประมวลผลและระบบคอมพิวเตอร์สำรอง
  - ควรมีระบบคอมพิวเตอร์สำรองซึ่งตั้งแยกจากสถานที่ประมวลผลปกติ เพื่อใช้สำหรับการประมวลผลระบบงานที่สำคัญในกรณีที่ระบบคอมพิวเตอร์ปัจจุบันไม่สามารถประมวลผลได้
  - ระบบคอมพิวเตอร์สำรอง ต้องมีความสามารถเพียงพอในการประมวลผลระบบงานที่สำคัญ

- ในกรณีที่ใช้บริการระบบคอมพิวเตอร์สำรองของผู้ให้บริการภายนอก ต้องมีสัญญาการใช้บริการที่เป็นลายลักษณ์อักษร
- ต้องจัดเก็บข้อมูลและโปรแกรมสำรองไว้ไม่ไกลจากสถานที่ประมวลผลสำรอง
- ต้องมีการทดสอบการประมวลผลในสถานที่สำรองอย่างสม่ำเสมอ
- หลังจากการทดสอบเสร็จสิ้นแล้วต้องลบข้อมูลที่ใช้ในการทดสอบออกจากระบบสำรองทุกครั้ง และต้องแน่ใจว่าไม่สามารถนำข้อมูลที่ลบทิ้งแล้วกลับมาใช้ใหม่ได้

7. การใช้งานเครื่องคอมพิวเตอร์ตั้งโต๊ะ (Desk Top) และคอมพิวเตอร์พกพา (Notebook)

- กำหนดให้ใช้ Password สำหรับแสดงตัวทุกครั้งในการเปิดเครื่องเพื่อใช้งาน
- กำหนดให้ผู้ใช้งานมีสถานะเป็น User เท่านั้น และไม่สามารถติดตั้งโปรแกรมใดๆ ได้ด้วยตนเอง
- หลีกเลี่ยงการใช้ข้อมูลส่วนตัวในการตั้ง Password เช่น ชื่อสกุล ชื่อสถานที่ปฏิบัติงาน นามแฝง วันเกิด เบอร์โทรศัพท์ หรือข้อมูลอื่นๆ ที่ง่ายต่อการคาดเดา
- กำหนดให้ล็อคหน้าจอทุกครั้งเมื่อต้องออกห่างหน้าจอเป็นระยะเวลาชั่วคราว และให้สอบถาม Password เพื่อแสดงตัวทุกครั้งก่อนใช้
- ห้ามไม่ให้พนักงานนำข้อมูลส่วนตัวและ/หรือข้อมูลที่เป็นความลับของพนักงานเข้าสู่ระบบสารสนเทศและคอมพิวเตอร์ของบริษัทฯ ตามที่ระบุไว้ใน “ข้อ 2. ข้อมูล ใน กฎระเบียบและนโยบายระบบสารสนเทศ” ฉบับนี้
- หากจำเป็นที่ต้องนำอุปกรณ์เชื่อมต่อ หรืออุปกรณ์บันทึกข้อมูลใดๆ จากภายนอกมาใช้กับเครื่องคอมพิวเตอร์จะต้องมีการตรวจสอบไวรัสก่อนทุกครั้ง
- ติดตั้งโปรแกรมเพื่อป้องกันไวรัสคอมพิวเตอร์พร้อมทั้งมีการปรับปรุงข้อมูลจัดการไวรัสที่ทันสมัยเสมอ
- ห้ามพนักงาน download หรือติดตั้งโปรแกรมใดๆ ในอุปกรณ์คอมพิวเตอร์ของบริษัทฯ หากมีความจำเป็นต้องติดตั้งโปรแกรมใดเพื่อการปฏิบัติงานตามหน้าที่และความรับผิดชอบ โปรแกรมดังกล่าวจะต้องได้รับการอนุมัติจากผู้บังคับบัญชาโดยตรง และเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศจะเป็นผู้ดำเนินการในลำดับต่อไป
- บริษัทฯ สามารถตรวจสอบโปรแกรมและข้อมูลที่ติดตั้งในอุปกรณ์คอมพิวเตอร์ของบริษัทฯ ได้ โดยไม่ต้องแจ้งล่วงหน้า รวมถึงการกำหนดหรือติดตั้งระบบในการตรวจสอบดังกล่าว และจะไม่ถือเป็นการละเมิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ห้ามพนักงานนำโปรแกรมทุกชนิดที่ไม่มีลิขสิทธิ์ถูกต้องมาใช้กับงานของบริษัทฯ
- ผู้ใช้ต้องทำการสำรองข้อมูล (Back up) ที่ใช้ในการปฏิบัติงานของตนเองอย่างสม่ำเสมอ

- ห้ามทำการถ่ายสำเนาหรือโอนย้ายข้อมูลและโปรแกรมการใช้งานต่างๆ ของบริษัทฯ เพื่อนำไปใช้งานหรือกิจการที่ไม่เกี่ยวข้องกับงานของบริษัทฯ โดยไม่ได้รับอนุมัติหรืออนุญาตจากผู้บังคับบัญชาโดยตรงตามสายงาน
- ข้อมูลที่ได้จากการปฏิบัติงานของพนักงานในระหว่างการเป็นพนักงานของบริษัทฯ จะต้องส่งมอบคืนให้กับบริษัทฯ ในวันที่พนักงานพ้นสภาพจากการเป็นพนักงาน
- กรณีที่มีการใช้งานเชื่อมต่อกับระบบเครือข่ายต้องปฏิบัติดังนี้
  - การแบ่งปัน (Sharing) การใช้ข้อมูลหรือเครื่องพิมพ์ เจ้าของข้อมูลหรือเครื่องพิมพ์นั้น ต้องกำหนดให้ sharing เป็นแบบอ่านอย่างเดียว (read only) เท่านั้น
  - การใช้ E-mail ต้องเป็นไปเพื่อการใช้งานของบริษัทฯ เท่านั้น และต้องใช้งานให้ถูกต้องตามธรรมเนียมปฏิบัติที่ดีในการใช้เครือข่าย เช่น ไม่ส่ง E-mail แบบกระจายถึงทุกคนที่เป็นสมาชิกในเครือข่ายโดยไม่จำเป็น และห้ามส่ง E-mail โดยใช้ข้อความที่ไม่สุภาพหรือเป็นเท็จ การแนบเอกสารหรือสื่อที่ผิดกฎหมาย หรือลามกอนาจารไปยังบุคคลอื่น เป็นต้น
  - การใช้ Internet ต้องเป็นการใช้เพื่องานของบริษัทฯ หรือเพื่อแสวงหาข้อมูลและความรู้ที่เป็นประโยชน์ต่อการปฏิบัติงาน พนักงานพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพโดยห้ามเป็นเครื่องมือในการค้นหาหรือ download ไฟล์ใดๆ ที่ไม่เกี่ยวข้องกับการทำงาน รวมถึงจะต้องไม่เข้าเว็บไซต์ที่ผิดกฎหมายหรือละเมิดศีลธรรมอันดีงาม
- ในการใช้ Internet และ E-mail รวมไปถึงการบันทึกข้อมูลต่างๆ ที่ไม่เหมาะสม เช่นภาพลามกอนาจาร โดยใช้อุปกรณ์คอมพิวเตอร์ของบริษัทฯ และหรือผ่านช่องทางการสื่อสารของบริษัทฯ จะถือว่าพนักงานฝ่าฝืนข้อบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และอาจได้รับการลงโทษทางวินัยจากบริษัทฯ หรือตามกฎหมายต่างๆ ที่เกี่ยวข้อง

8. การกำหนดมาตรฐานเครื่องและอุปกรณ์ระบบคอมพิวเตอร์ (Specification)

กำหนดมาตรฐานในการจัดหาระบบเครื่องคอมพิวเตอร์ ทั้งในส่วนของ Hardware และ Software ให้เป็นไปตามที่ระบุไว้ในเอกสาร “มาตรฐานระบบคอมพิวเตอร์” ใน ภาคผนวกที่ 2.1

9. บทลงโทษ

กรณีที่พนักงานฝ่าฝืน กฎระเบียบและนโยบายสารสนเทศ ฉบับนี้ จะถูกพิจารณาลงโทษทางวินัยตามระเบียบข้อบังคับเกี่ยวกับการทำงานของบริษัทฯ ที่ประกาศและมีผลบังคับใช้ ณ ขณะนั้น หรือตามบทบัญญัติโทษตามกฎหมายที่เกี่ยวข้อง