



(0107537000513)

**บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)**

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

**CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED**

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

## นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

### บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)

#### 1. บทนำ

บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน) ความมุ่งมั่นในการจัดตั้งและพัฒนาระบบเทคโนโลยี สารสนเทศในองค์กร ให้มีความมั่นคงปลอดภัย คงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ

บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน) จึงได้จัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ ฉบับนี้ เพื่อใช้กำกับ กำหนดทิศทาง และสนับสนุนการบริหาร จัดการความมั่นคงปลอดภัยสารสนเทศ รวมทั้งสร้างความเชื่อมั่นในกิจกรรมการดำเนินการทางสารสนเทศให้มีความปลอดภัยและสอดคล้องกับ ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ มาตรฐานความมั่นคงปลอดภัยสารสนเทศสากล รวมถึงกฎหมาย และข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

#### 2. ขอบเขต

นโยบายฉบับนี้มีผลบังคับใช้กับ บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน) รวมถึงกรรมการ ผู้บริหาร พนักงาน และผู้ให้บริการบุคคลภายนอก ที่ได้รับอนุญาต ให้เข้าถึงข้อมูลสารสนเทศ ในแต่ละระดับ ชั้นความลับ

#### 3. คำจำกัดความ

- 3.1. บริษัท หมายถึง "บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)" และให้หมายความรวมถึง ผู้ซึ่งได้รับมอบหมาย ให้ทำงานแทนบริษัท ผู้มีอำนาจกระทำการแทนบริษัท และผู้ที่ได้รับ มอบหมายจากผู้มีอำนาจกระทำการแทนบริษัท ให้ทำการแทนด้วย
- 3.2. กรรมการ หมายถึง ผู้ที่ได้รับการแต่งตั้งให้ทำหน้าที่กำหนดทิศทาง กลยุทธ์ และการดำเนินงาน บริษัท
- 3.3. ผู้บริหาร หมายถึง ผู้กระทำการแทน หรือผู้ที่ได้รับมอบหมายให้กระทำการแทนผู้บริหาร ซึ่งในที่นี้ หมายความรวมถึง ผู้บังคับบัญชา ที่ได้รับการแต่งตั้งให้ทำงานในตำแหน่ง ที่มีหน้าที่ในการสั่งการ มอบหมายงาน กำกับ หรือควบคุมการปฏิบัติงานของพนักงานอื่น
- 3.4. พนักงาน หมายถึง บุคคลที่ตกลงทำงานให้แก่บริษัท เพื่อรับค่าตอบแทนภายหลัง ซึ่งในที่นี้ หมายความ รวมถึง พนักงานที่ได้ผ่านพ้นกำหนดระยะเวลาทดลองงาน พนักงานทดลองงาน ลูกจ้างชั่วคราว พนักงานที่มีสัญญาจ้างพิเศษ พนักงานรายเดือน และพนักงานรายวัน
- 3.5. บุคคลภายนอกที่ได้รับอนุญาต หมายถึง บุคคลที่ไม่ใช่กรรมการ ผู้บริหาร หรือพนักงาน ไม่ได้รับค่าตอบแทน จากบริษัท โดยตรง ที่ได้รับอนุญาตให้เข้าถึงข้อมูลสารสนเทศ
- 3.6. ข้อมูลสารสนเทศ ซึ่งต่อไปนี้เรียกว่า "ข้อมูล" หมายถึง ข่าวสาร ข้อเท็จจริง ข้อมูลในรูปแบบใด ๆ หรือข้อมูลที่มีการประมวลผลใด ๆ ทั้งในเหตุการณ์หรือกิจกรรมต่าง ๆ

#### 4. การสื่อสารและแนวทางการปฏิบัติ

- 4.1. ผู้บริหารระดับสูง และผู้บริหารทุกระดับมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศ ให้การ สนับสนุน การดำเนินงานด้านความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงกำหนดบทบาท หน้าที่ความรับผิดชอบ และมอบหมายงานให้ชัดเจน ตลอดจนจัดให้มีการบริหารความเสี่ยง ทั้งในระดับองค์กร และระดับปฏิบัติการรวมทั้งมีส่วนร่วมรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใด ๆ ที่อาจเกิดขึ้นกับระบบสารสนเทศ



(0107537000513)

**บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)**

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

**CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED**

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

- 4.2. นโยบายจะต้องได้รับการเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับทราบ เพื่อให้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศ ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
  - 4.3. จัดให้มีการติดตามประสิทธิผลและประสิทธิผลระบบการบริหารรักษาความปลอดภัยสารสนเทศด้วยวิธีการตรวจสอบภายในอย่างน้อยปีละ 1 ครั้ง
  - 4.4. กำหนดให้ทบทวนนโยบายเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ
  - 4.5. พนักงานและ/หรือ หน่วยงานภายนอกที่ละเมิดนโยบายฉบับนี้ จะถูกดำเนินการทางวินัยตามกฎหมายข้อบังคับของบริษัท รวมถึงการเลิกจ้าง การยกเลิกสัญญา แล้วแต่กรณี และหากเป็นการกระทำที่เป็นการฝ่าฝืนต่อกฎหมาย อาจถูกฟ้องร้องดำเนินคดีทั้ง ทางแพ่ง และทางอาญา
5. **หลักเกณฑ์ที่ใช้อ้างอิง**
- 5.1. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 4) พ.ศ. 2562
  - 5.2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2 พ.ศ. 2560)
  - 5.3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
  - 5.4. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2553
  - 5.5. แนวปฏิบัติในการเปิดเผยและรักษาข้อมูลที่มีผลกระทบต่อราคาหลักทรัพย์
6. **องค์ประกอบของนโยบาย**

นโยบายแบ่งออกเป็น 8 หมวด ได้แก่

- 6.1. การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศ
- 6.2. การบริหารจัดการผู้ให้บริการภายนอก
- 6.3. การควบคุมการเข้าถึง
- 6.4. การแลกเปลี่ยนข้อมูลสารสนเทศ
- 6.5. ความมั่นคงปลอดภัยในการดำเนินการ
- 6.6. ความมั่นคงปลอดภัยในระบบเครือข่าย
- 6.7. การเข้ารหัส
- 6.8. ความมั่นคงปลอดภัยพื้นที่



(0107537000513)

บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

## หมวดที่ 1

### การจัดการ การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศ

วัตถุประสงค์: เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นส่วนหนึ่งตลอดอายุของระบบเทคโนโลยีสารสนเทศ

#### 1. การจัดการและการพัฒนา

- 1.1. การจัดการและพัฒนาระบบงานมีการเก็บข้อมูลความต้องการทางธุรกิจ และออกแบบระบบให้สอดคล้องกับความต้องการการปฏิบัติงาน (Operation) ความมั่นคงปลอดภัยสารสนเทศ (Information Security) และการทำงาน (Functionality)
- 1.2. ก่อนเริ่มดำเนินการจัดการพัฒนาจะต้องมีการอนุมัติอย่างเป็นทางการเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล และเจ้าของ ระบบงาน และมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญใน ด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) การทำงาน (Functionality) ข้อกำหนดด้านกฎหมาย หรือระเบียบของบริษัท (Compliance) และความเสี่ยง (Risk)
- 1.3. การพัฒนาเป็นไปตามหลักวิศวกรรมด้านความมั่นคงปลอดภัย (Secure System Engineering Principles) ซึ่งรวมถึงวงจรการพัฒนาาระบบสารสนเทศ (SDLC) และการเขียนซอร์สโค้ด(source code)แบบปลอดภัย (Secure Coding)
- 1.4. กำหนดให้จัดทำเอกสารที่จำเป็นในการออกแบบระบบงาน ได้แก่
  - 1.4.1. User Specification
  - 1.4.2. Functional Specification
  - 1.4.3. System Document เช่น Data Flow Diagram, Data Dictionary, File Layout, ER Diagram, Structure Chart, Screen Layout, Report Layout เป็นต้น
  - 1.4.4. เอกสารอื่น ๆ ตามความเหมาะสม
- 1.5. เจ้าของข้อมูล และเจ้าของระบบงานตรวจสอบ และติดตามผลการดำเนินงานภายใต้แผนการ ดำเนินงานโครงการที่กำหนดไว้
- 1.6. มีการควบคุมการเข้าถึงและใช้งานซอร์สโค้ด(source code) และข้อมูลที่จำเป็น ในการพัฒนา ระบบงาน ซึ่งการเข้าถึงดังกล่าวจะต้องครอบคลุมไปถึงหน่วยงานภายนอก ที่จ้างในการพัฒนา ระบบ
- 1.7. จัดให้มีการควบคุมเวอร์ชันของระบบงานที่พัฒนาเพื่อป้องกันการแก้ไขไม่ถูกต้อง
- 1.8. การจ้างหน่วยงานภายนอกพัฒนาระบบงาน จะต้องกำหนดให้หน่วยงานภายนอกเข้าถึงเฉพาะ ส่วนที่มีไว้สำหรับการพัฒนาระบบ (Development Environment) เท่านั้น และไม่สามารถเข้าถึงระบบการใช้งานจริง (Production Environment)
- 1.9. การนำระบบที่พัฒนาไปใช้งานจริงจะต้องได้รับอนุมัติจากผู้มีอำนาจ และมีการทดสอบก่อน โอนย้ายไปใช้งานจริง
- 1.10. จำกัดการแก้ไขโปรแกรมสำเร็จรูป หากมีความจำเป็นต้องแก้ไข จะต้องได้รับการอนุมัติจาก ผู้มีอำนาจก่อนเสมอ

#### 2. การแบ่งแยกสภาพแวดล้อม

- 2.1. จะต้อง แบ่งแยกสภาพแวดล้อมระบบที่ใช้สำหรับการพัฒนา (Development Environment) การทดสอบ (Testing Environment) และการใช้งานจริง (Production Environment) ออกจากกัน และควบคุมการเข้าถึงได้เฉพาะผู้มี ส่วนเกี่ยวข้องเท่านั้น
- 2.2. สภาพแวดล้อมระบบที่ใช้สำหรับการพัฒนา (Development Environment) การทดสอบ (Testing Environment) และการใช้งานจริง (Production Environment) จะต้องเหมือน หรือใกล้เคียงกัน เพื่อป้องกันความผิดพลาดจากการใช้สภาพแวดล้อมต่างกัน
- 2.3. ระบบสารสนเทศที่มีความสำคัญสูง ให้แยกออกจากระบบเครือข่ายที่ใช้งานทั่วไป



บริษัท เชียงใหม่ฟรอสเฟนฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

(0107537000513)

3. ความมั่นคงปลอดภัยของข้อมูลที่ใช้ทดสอบ

- 3.1. หลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลเพื่อทดสอบ หากจำเป็นให้กำหนดวิธีการทำให้ไม่สามารถย้อนกลับไปยังข้อมูลจริงได้ ได้แก่ การสลับตำแหน่ง (Scrambling) การลบข้อมูลระบุตัวตน เช่น หมายเลขบัตรประจำตัวประชาชน เป็นต้น
- 3.2. การส่งออก (Extract) ข้อมูลจากระบบใช้งานจริง กระทำโดยบุคคลที่ได้รับอนุญาตเท่านั้น
- 3.3. ไม่นำข้อมูลที่ใช้ทดสอบระบบไปใช้ผิดวัตถุประสงค์ และลบข้อมูลทันทีภายหลัง การทดสอบ เสร็จสิ้น

4. การทดสอบระหว่างการพัฒนาและบำรุงรักษา

- 4.1. ผู้ที่ร้องขอ และแผนกเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องมีส่วนร่วมในการ ทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง มีการ ทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการ
- 4.2. ระบบงานสำคัญควรมีหน่วยงาน หรือทีมงานอิสระ เข้าตรวจสอบว่ามีปฏิบัติตามขั้นตอนการ พัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง
- 4.3. ระบบงานที่เชื่อมต่อกับระบบเครือข่ายสาธารณะจะต้องมีการทดสอบเจาะระบบ (Penetration Test) เพื่อสร้างความเชื่อมั่นด้านความมั่นคงปลอดภัยสารสนเทศ

5. การบำรุงรักษา

- 5.1. การบำรุงรักษาดำเนินการโดยบุคคลที่มีความรู้ และได้รับการอบรมเพียงพอ
- 5.2. หากมีความจำเป็นต้องแก้ไขเปลี่ยนแปลง ให้ขออนุญาตอย่างเป็นทางการเป็นลายลักษณ์อักษร และนำเข้ากระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure)
- 5.3. ตรวจสอบการทำงาน และความถูกต้อง ของระบบงานทุกครั้งที่มีการเปลี่ยนแปลง ซึ่งรวมถึงการเปลี่ยนแปลงในระบบปฏิบัติการ
- 5.4. จัดทำและปรับปรุงคู่มือบำรุงรักษาระบบงานให้เป็นปัจจุบันอยู่เสมอ ซึ่งรวมถึงเอกสารระบบงาน (System Document) และเอกสารจำเป็นอื่น ๆ เช่น Data Dictionary เป็นต้น
- 5.5. จัดให้มีการควบคุมเวอร์ชันของระบบงานที่พัฒนาสำเร็จ (Compiled Code) แยกออกจาก เวอร์ชันของระบบที่ใช้ในการพัฒนา และกำหนดสิทธิเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต



(0107537000513)

บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

## หมวดที่ 2

### การบริหารจัดการผู้ให้บริการภายนอก

วัตถุประสงค์: เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับผู้ให้บริการภายนอก

#### 1. การคัดเลือกผู้ให้บริการ

- 1.1. หลักเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการคัดเลือกผู้ให้บริการภายนอก มีดังนี้
  - 1.1.1. ผู้ให้บริการภายนอกที่เชื่อถือได้นำเสนอผลงานคุณภาพ และไม่มีประวัติการทิ้งงาน
  - 1.1.2. พนักงานของผู้ให้บริการภายนอกมีความรู้ความสามารถ ซึ่งอาจรวมถึง ประกาศนียบัตร รับรองความรู้ความสามารถ
  - 1.1.3. มีประวัติการให้บริการ ประวัติการรับรองผลงาน หรือรายชื่อลูกค้า หรือผู้รับบริการ อ้างอิง
  - 1.1.4. มีความสามารถในการรองรับแผนการบริหารความต่อเนื่อง หรือแผนฉุกเฉินในสถานการณ์ต่าง ๆ
  - 1.1.5. ยอมรับหลักเกณฑ์ในการเข้าตรวจสอบวิธีการปฏิบัติงาน รวมถึงการปฏิบัติตาม ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศอื่น ๆ ตามที่ได้ร้องขอ

#### 2. การบริหารความเสี่ยง

บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน) ดำเนินการประเมินความเสี่ยง และแนวทาง จัดการความ เสี่ยงที่เกิดจากบริการของผู้ให้บริการภายนอก หยุดชะงัก

#### 3. การจัดทำสัญญาและข้อตกลงในการรักษาความลับ

- 3.1. สัญญา รวมถึงข้อตกลงที่ทำร่วมกันต้องส่งให้หน่วยงานด้านกฎหมายตรวจสอบพิจารณา เพื่อลดช่องโหว่จากการระบุข้อความไม่ถูกต้องครบถ้วน
- 3.2. สัญญาต้องระบุขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) รวมทั้ง สิ่งส่งมอบ และเงื่อนไขการตรวจรับงาน
- 3.3. กรณีระบบงานที่มีความสำคัญสูงควรมีจัดตั้งคณะกรรมการเพื่อพิจารณาการตรวจรับ
- 3.4. สัญญา รวมถึงข้อตกลงที่ทำร่วมกัน จะต้องระบุข้อตกลงรักษาความลับไว้ในสัญญาเสมอ รวมทั้งพิจารณาเซ็นสัญญารักษาความลับ (Non-disclosure Agreement) เพิ่มเติมตามความเหมาะสมของลักษณะของงานที่ใช้บริการ
- 3.5. การรักษาความมั่นคงปลอดภัยสารสนเทศของวิธีการที่ใช้สำหรับ รับ-ส่ง ระหว่างบริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด(มหาชน) และผู้ให้บริการภายนอก เป็นหน้าที่ที่ปฏิบัติร่วมกัน และใช้ความระมัดระวัง หรือมาตรการป้องกันการรับ-ส่งข้อมูลที่มีความสำคัญสูง
- 3.6. เมื่อสิ้นสุดสัญญา ต้องยกเลิกสิทธิการเข้าถึงของผู้ให้บริการภายนอกทั้งหมด ทั้งส่วนที่เป็นการ เข้าถึงกายภาพ (Physical Access) และการเข้าถึงระบบงาน (Logical Access)
- 3.7. ข้อตกลงด้านความมั่นคงปลอดภัยอื่น ๆ ที่ควรระบุในสัญญา ตัวอย่างเช่น
  - 3.7.1. การปฏิบัติตามกฎหมาย และกฎระเบียบที่เกี่ยวข้อง
  - 3.7.2. การให้สิทธิการตรวจสอบคุณสมบัติ ประวัติของผู้ปฏิบัติงาน
  - 3.7.3. การรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล
  - 3.7.4. การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล
  - 3.7.5. การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล



(0107537000513)

**บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)**

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

**CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED**

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

- 3.7.6. การป้องกันการจ้างช่วง
- 3.7.7. การให้สิทธิในการเข้าตรวจสอบ (Audit)
- 3.7.8. การรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ
- 3.7.9. ผลของการละเมิดเงื่อนไข
- 3.8. การเปลี่ยนแปลงใดๆ ในสัญญา ให้จัดทำข้อตกลงที่เป็นลายลักษณ์อักษร รวมทั้งประเมินผล กระทบ และความเสียหายจากการเปลี่ยนแปลงข้อตกลง
4. การติดตามประเมินผลและตรวจสอบการให้บริการ
  - 4.1. จัดให้มีการติดตามประเมินผลและตรวจสอบการให้บริการตามที่ได้ระบุไว้ในสัญญา
  - 4.2. การติดตามประเมินผล จะต้องรวมถึงการปฏิบัติตามข้อกำหนดด้านความปลอดภัยสารสนเทศ
  - 4.3. จัดให้มีการตรวจสอบ (Audit) การให้บริการที่มีความสำคัญสูงตามข้อกำหนดที่ระบุไว้ในสัญญา



(0107537000513)

บริษัท เชียงใหม่ฟรอสเฟนฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

### หมวดที่ 3

#### การควบคุมการเข้าถึง

วัตถุประสงค์: เพื่อป้องกันความเสียหายจากการเข้าถึงโดยไม่ได้รับอนุญาต

#### 1. ข้อกำหนดทั่วไป

- 1.1. สิทธิการเข้าถึงอยู่บนหลักการอนุญาตให้เข้าถึงให้น้อยที่สุด (Least Privilege)
- 1.2. การเข้าถึงข้อมูลสารสนเทศ และข้อมูลในแอปพลิเคชันเป็นไปตามหลักการ Need-to-know และระดับชั้นความลับที่กำหนด
- 1.3. ออกแบบโปรแกรมให้แสดงหน้าจอ หรือเมนูตามสิทธิที่ได้รับ
- 1.4. การขอสิทธิการเข้าถึงจะต้องขออนุญาตและบันทึกไว้เป็นลายลักษณ์อักษรทุกครั้ง โดยกำหนดไม่ให้สิทธิการเข้าถึงก่อนที่มีการอนุมัติ และผู้อนุมัติจะต้องไม่เป็นบุคคลเดียวกับผู้ร้องขอ
- 1.5. การขอสิทธิพิเศษ (Privileges Access) เช่น Administrator, Super User เป็นต้น จะต้องได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ซึ่งดูแลสิทธิพิเศษนั้น ๆ
- 1.6. การขอสิทธิในลักษณะฉุกเฉินหรือชั่วคราว จะต้องบันทึกเหตุผลและความจำเป็น รวมถึงระยะเวลาสิ้นสุด และยกเลิกสิทธิทันทีเมื่อพ้นระยะเวลาดังกล่าว
- 1.7. สิทธิการเข้าถึงของหน่วยงานภายนอก และผู้ให้บริการต่าง ๆ จะต้องระบุระยะเวลาสิ้นสุด และให้สิทธิสูงสุดไม่เกิน 1 ปี โดยจะต้องขออนุญาตใหม่ทุกครั้ง
- 1.8. ผู้มีสิทธิอนุมัติการเข้าถึง ได้แก่ เจ้าของข้อมูล และ/หรือระบบงาน โดยมีแผนกเทคโนโลยี เป็นผู้ให้คำแนะนำในการจัดสรรสิทธิได้อย่างถูกต้อง
- 1.9. การเข้าถึงจะต้องใช้วิธีการพิสูจน์ตัวตนที่มีความปลอดภัย และสามารถตรวจสอบข้อมูล ย้อนหลังได้ เช่น การใช้ User Name และ Password เป็นต้น
- 1.10. จัดให้มีการทบทวนสิทธิ์การเข้าถึงอยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง
- 1.11. เมื่อสิ้นสุดความจำเป็นที่ต้องใช้งาน การเปลี่ยนแปลงโยกย้ายการสิ้นสุดสัญญาให้ยกเลิก สิทธิการเข้าถึงทันที

#### 2. การเข้าถึงระบบเครือข่ายและบริการเครือข่าย

- 2.1. จัดให้มีการแบ่งแยกระบบเครือข่าย โดยแยกระบบสารสนเทศที่มีความสำคัญสูง ออกจาก ระบบเครือข่ายที่ใช้งานทั่วไป
- 2.2. ก่อนเข้าถึงระบบเครือข่ายและบริการเครือข่ายจะต้องพิสูจน์ตัวตนก่อนทุกครั้ง
- 2.3. การอนุญาตให้เข้าถึงบริการเครือข่ายด้วยวิธีการรีโมท จะต้องดำเนินการผ่าน Protocol ที่มีความปลอดภัย เช่น SSH เป็นต้น
- 2.4. การอนุญาตให้เข้าถึงระบบเครือข่ายด้วยวิธีการรีโมทจะต้องอยู่ในโซน หรืออุปกรณ์ที่ได้รับ อนุญาตเท่านั้น เช่น กำหนด Management Zone หรือการลงทะเบียน MAC Address เป็นต้น
- 2.5. จำกัดเวลารีโมท โดยให้ตัดการเชื่อมต่อทุก 5 นาที เมื่อไม่มีการใช้งาน (Interactive Session)

#### 3. การเชื่อมต่อจากระยะไกล

- 3.1. การเชื่อมต่อจากระยะไกลให้ใช้งานผ่าน VPN เพื่อให้ข้อมูลที่รับ-ส่งมีความปลอดภัย
- 3.2. กำหนดระยะเวลาเชื่อมต่อสูงสุดในระบบ VPN โดยให้ตัดการเชื่อมต่อ และพิสูจน์ตัวตนใหม่ทุกๆ 12 ชั่วโมง
- 3.3. เครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อจากระยะไกลมีการป้องกันไวรัส และปรับปรุงแพตช์ให้เป็น ปัจจุบันเสมอ

#### 4. การพิสูจน์ตัวตนและการจัดการรหัสผ่าน

- 4.1. ห้ามไม่ให้บัญชีผู้ใช้และรหัสผ่านที่เป็น Default หรือข้อมูลตั้งต้นที่มาจากผู้ผลิต
- 4.2. บัญชีผู้ใช้งานไม่ควรสื่อถึงตำแหน่งและความรับผิดชอบ เช่น Administrator เป็นต้น



(0107537000513)

**บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)**

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

**CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED**

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

- 4.3. บัญชีผู้ใช้งานของแต่ละคนไม่ซ้ำกัน (Unique User Account) หากมีความจำเป็นต้องใช้บัญชี ผู้ใช้งานร่วมกัน (Shared User Account) ให้ระบุรายชื่อผู้ใช้งาน และทบทวนให้เป็นปัจจุบัน อยู่เสมอ
- 4.4. การใช้งานบัญชีผู้ใช้งาน (Shared Account) ให้เปลี่ยนรหัสผ่านทันทีที่สมาชิกในกลุ่มสิ้นสุดหน้าที่ความรับผิดชอบในการปฏิบัติงาน
- 4.5. การแจ้งรหัสผ่านให้กับผู้ใช้งานให้ใช้วิธีการที่ปลอดภัย
- 4.6. ข้อกำหนดการตั้งรหัสผ่าน มีดังนี้
  - 4.6.1. รหัสผ่านจะต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร
  - 4.6.2. รหัสผ่านจะต้องประกอบด้วยตัวอักษรพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และ/หรือ ตัวอักษรพิเศษ
  - 4.6.3. ระบบบังคับให้มีการเปลี่ยนรหัสผ่านทันทีที่ใช้งานครั้งแรก
- 4.7. ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านเองได้
- 4.8. การส่งรหัสผ่านไม่ใช่รูปแบบ Plain Text
- 4.9. ไม่อนุญาตให้ติดตั้งโปรแกรม เอเจนท์ โปรแกรมอรรถประโยชน์ ยูทิลิตี้ หรือคำสั่งใด ๆ ที่ลดขั้นตอนการพิสูจน์ตัวตนก่อนเข้าถึงระบบสารสนเทศ



(0107537000513)

บริษัท เชียงใหม่ฟรอสเฟนฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

## หมวดที่ 4

### การแลกเปลี่ยนข้อมูลสารสนเทศ

วัตถุประสงค์: เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลที่แลกเปลี่ยนภายในและภายนอกองค์กร

#### 1. ข้อกำหนดทั่วไป

- 1.1. เลือกใช้ช่องทางแลกเปลี่ยนข้อมูลที่มีความปลอดภัย และรักษาความถูกต้องสมบูรณ์ของ ข้อมูลจนถึงปลายทาง
- 1.2. เลือกใช้ช่องทางที่มีความปลอดภัย และสามารถแจ้งเตือน หรือป้องกันไวรัส รวมถึงมัลแวร์ ประเภทต่าง ๆ
- 1.3. การเลือกใช้วิธีการแลกเปลี่ยนข้อมูลเป็นไปตามระดับชั้นความลับของข้อมูลที่ต้องการแลกเปลี่ยน
- 1.4. เลือกใช้ช่องทางแลกเปลี่ยนข้อมูลสามารถตรวจสอบข้อมูลย้อนหลังได้ ได้แก่ ข้อมูลผู้ส่ง ปลายทางที่รับข้อมูล รวมถึงสาระและเนื้อหาสำคัญ
- 1.5. การแลกเปลี่ยนข้อมูลที่เป็นข้อมูลส่วนบุคคลให้ปฏิบัติตาม นโยบายข้อมูลส่วนบุคคล (Data Privacy Policy)

#### 2. การแลกเปลี่ยนข้อมูลโดยใช้ระบบอีเมล

- 2.1. ผู้ใช้งานตรวจสอบชื่อผู้รับให้ถูกต้องก่อนส่งอีเมล
- 2.2. ห้ามไม่ให้ใช้ระบบอีเมลสาธารณะ เช่น Gmail เป็นต้น ในการรับ-ส่งข้อมูลที่มีความสำคัญสูง
- 2.3. ไม่ควรเปิดอ่านอีเมลไม่ทราบแหล่งที่มา หรือมีเหตุต้องสงสัย และแจ้งให้แผนกเทคโนโลยีสารสนเทศเข้าตรวจสอบ
- 2.4. งดใช้ฟังก์ชันช่วยจำเพื่อตัดขั้นตอนพิสูจน์ตัวตนในระบบอีเมล
- 2.5. ตรวจสอบและสำรองข้อมูลในระบบอีเมลอยู่เสมอ

#### 3. การแลกเปลี่ยนข้อมูลโดยใช้สื่อบันทึกแบบพกพา

- 3.1. เลือกใช้สื่อบันทึกแบบพกพา ที่มีความสามารถในการเข้ารหัส หรือสามารถยืนยันตัวตนผู้ใช้งาน
- 3.2. ตรวจสอบไวรัส และมัลแวร์ประเภทต่าง ๆ ในสื่อบันทึกแบบพกพาอยู่เสมอ
- 3.3. ตรวจสอบข้อมูลที่บันทึกไว้ในสื่อบันทึกแบบพกพาอยู่เสมอ และเก็บข้อมูลในสื่อบันทึกแบบ พกพา ให้น้อยที่สุดเนื่องจากเป็นสื่อบันทึกที่สูญหายได้ง่าย

#### 4. การแลกเปลี่ยนข้อมูลโดยใช้ File Sharing

- 4.1. ให้ประเมินความเสี่ยงและผลกระทบทุกครั้งก่อนนำข้อมูลสำคัญไปเก็บไว้ที่ File Sharing โดยจะต้องขออนุญาตจากเจ้าของข้อมูลเสมอ ซึ่งการแลกเปลี่ยนข้อมูลโดยใช้ File Sharing รวมถึงแหล่งเก็บข้อมูลประเภท Own-cloud, Alfresco, Google Drive, Drop-box, MS One drive เป็นต้น
- 4.2. ห้ามไม่ให้แลกเปลี่ยนข้อมูลโดยใช้โปรโตคอลที่ไม่ปลอดภัย เช่น FTP เป็นต้น
- 4.3. ตรวจสอบรายชื่อผู้มีสิทธิในระดับโนโพลเดอรัอยู่เสมอ

#### 5. การแลกเปลี่ยนข้อมูลโดยใช้โปรแกรมประเภท Messaging

- 5.1. ห้ามไม่ให้ส่งข้อมูลสำคัญโดยใช้โปรแกรมประเภท Message instant เช่น Line, Whats App, Facebook messenger, We chat เป็นต้น



(0107537000513)

บริษัท เชียงใหม่ฟรอสเฟนฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแองโกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

## หมวดที่ 5

### ความมั่นคงปลอดภัยในการดำเนินการ

วัตถุประสงค์: เพื่อให้มีกระบวนการดำเนินการมีความมั่นคงปลอดภัย

#### 1. ข้อกำหนดทั่วไป

- 1.1. แผนกเทคโนโลยีสารสนเทศ จัดทำเอกสารขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำ ในด้านต่าง ๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่ผู้ใช้งานระบบคอมพิวเตอร์ (User Operator) เช่น ขั้นตอนในการ เปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการ ตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ
- 1.2. การปฏิบัติงานผ่านทางเมนู โปรแกรม และใช้ Command Line เท่าที่จำเป็น
- 1.3. ห้ามไม่ให้ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการดำเนินงานในระบบสารสนเทศ และห้ามไม่ให้ใช้งานโปรแกรมผิดกฎหมายโดยเด็ดขาด
- 1.4. เปิดให้บริการ (Service) ในระบบสารสนเทศเท่าที่จำเป็น
- 1.5. กำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน รวมถึงข้อมูลการติดต่อผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา

#### 2. การแบ่งแยกอำนาจหน้าที่

- 2.1. ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารควบคุมระบบ (Operation support) ซึ่งควบคุมการปฏิบัติงานในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment)
- 2.2. ต้องจัดให้มี Job Description ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคน ภายในแผนกเทคโนโลยีสารสนเทศอย่างชัดเจนเป็น ลายลักษณ์อักษร
- 2.3. จัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น เช่น ผู้บริหารระบบ (System Administrator) เจ้าหน้าที่เทคโนโลยีสารสนเทศ (Information Technology Support) เป็นต้น

#### 3. การบริหารการเปลี่ยนแปลง

- 3.1. จัดทำเอกสารกระบวนการเพื่อใช้บริหารจัดการการเปลี่ยนแปลง
- 3.2. ก่อนการดำเนินการเปลี่ยนแปลงใด ๆ จะต้องได้รับการอนุมัติจาก เจ้าของข้อมูล และ/หรือ เจ้าของระบบงานเสมอ
- 3.3. จัดทำเกณฑ์เพื่อใช้ประเมินผลกระทบ และความเสี่ยงที่เกิดจากการเปลี่ยนแปลง
- 3.4. กำหนดแผนสำรองหรือแผนกู้คืน (Fallback Plan) เพื่อใช้ดำเนินการหากการเปลี่ยนแปลง ไม่สำเร็จ
- 3.5. ก่อนการเปลี่ยนแปลงใด ๆ ควรมีจัดให้มีการทดสอบอยู่เสมอ ยกเว้นมีข้อจำกัดทางเทคนิค
- 3.6. ภายหลังการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการ ควรแจ้งให้เจ้าของระบบ หรือผู้ใช้งาน ตรวจสอบความถูกต้องในการประมวลผลระบบสารสนเทศอยู่เสมอ

#### 4. การบริหารทรัพยากรในระบบ

- 4.1. จัดให้มีการตรวจสอบการใช้งานทรัพยากรในระบบ เช่น CPU, Memory, Disk เป็นต้น อยู่เสมอ
- 4.2. การจัดหาและการเปลี่ยนแปลงในระบบสารสนเทศ จะต้องพิจารณาความเพียงพอ ของทรัพยากรในระบบเสมอ
- 4.3. การจัดหาทรัพยากรในระบบเพิ่มเติม จะต้องคำนึงถึงอัตราการเติบโตของข้อมูล เพื่อให้สามารถรองรับกับความต้องการทางธุรกิจ



(0107537000513)

บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

การสำรองข้อมูล

5.
  - 5.1. การออกแบบ และเลือกใช้วิธีการสำรองข้อมูลเป็นไปตามความสำคัญของข้อมูลทางธุรกิจ
  - 5.2. มีการทดสอบข้อมูลที่ทำสำรองไว้อยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง
  - 5.3. สื่อบันทึกที่ใช้สำรองข้อมูลสามารถรองรับความต้องการทางด้านอายุการจัดเก็บ รวมถึงมีเทคโนโลยีที่รองรับการเรียกดูข้อมูลในอนาคต
  - 5.4. ข้อมูลที่สำรอง รวมถึงสื่อบันทึกข้อมูลจะต้องไม่จัดเก็บไว้ในตำแหน่ง หรือสถานที่เดียวกับ การเก็บข้อมูลตามปกติ
6. การจัดเก็บข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs)
  - 6.1. จัดให้มีการเก็บข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) เช่น System Access Logs, Application Logs เป็นต้น ตามความต้องการทางธุรกิจ และข้อกำหนดทางกฎหมาย
  - 6.2. จัดให้มีการเก็บข้อมูลบันทึกกิจกรรมที่เกิดจากการดูแลระบบ (Administrator and Operator Logs)
  - 6.3. ข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) จะต้องได้รับการป้องกันการแก้ไข ลบ หรือทำลาย
  - 6.4. ข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) อ้างอิงสัญญาณนาฬิกาจากแหล่งเดียวกัน
  - 6.5. ข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) มีอายุอย่างน้อย 90 วัน
7. การบริหารจัดการแพทช์
  - 7.1. จัดทำเอกสารกระบวนการเพื่อใช้บริหารจัดการแพทช์
  - 7.2. ตรวจสอบและติดตามให้มีการติดตั้งแพทช์อย่างสม่ำเสมอ การยกเว้นหรือไม่ติดตั้งแพทช์ จะต้องได้รับการอนุมัติจากผู้มีอำนาจ
  - 7.3. จัดให้มีผู้รับผิดชอบติดตามข่าวสารแพทช์โดยตรง โดยเฉพาะแพทช์ที่เกี่ยวข้องด้านความมั่นคง ปลอดภัย (Security Patch) ที่ต้องรีบดำเนินการตามคำแนะนำของผู้ผลิต
8. การจัดการช่องโหว่ (System Hardening)
  - 8.1. จัดทำเอกสาร Security Baseline ในระบบที่มีความสำคัญ เพื่อใช้กำหนดค่าพารามิเตอร์ ได้อย่างถูกต้อง
  - 8.2. จัดให้มีการตรวจสอบทางเทคนิค เพื่อหาจุดอ่อนในระบบสารสนเทศสำคัญอยู่เสมอ



(0107537000513)

บริษัท เชียงใหม่ฟรอสเฟนฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

## หมวดที่ 6

### ความมั่นคงปลอดภัยในระบบเครือข่าย

วัตถุประสงค์: เพื่อบริหารจัดการระบบเครือข่ายให้มีความปลอดภัย

#### 1. การออกแบบและจัดการระบบเครือข่าย

- 1.1. ผู้ดูแลระบบออกแบบและจัดการให้ระบบเครือข่ายมีความปลอดภัย และมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย เช่น Firewall, IPS, IDS, Data Leak เป็นต้น
- 1.2. ออกแบบและเลือกใช้โปรโตคอลที่มีความปลอดภัยในระบบเครือข่าย
- 1.3. ตรวจสอบและควบคุมเส้นทางเครือข่ายให้เป็นไปตามกระบวนการทางธุรกิจ และสอดคล้องตามข้อกำหนดด้านความมั่นคงปลอดภัย
- 1.4. ปิดพอร์ตที่ไม่มีความจำเป็นต้องใช้งาน หรืออาจทำให้เกิดผลเสียต่อระบบ ทั้งพอร์ตทางกายภาพ และพอร์ตสำหรับ Diagnostic and Configuration Port
- 1.5. จัดทำเอกสารระบบ ได้แก่ Network Diagram และคู่มือปฏิบัติงานต่าง ๆ ให้เป็นปัจจุบันเสมอ
- 1.6. ระบบเครือข่ายมีความสามารถในการตรวจจับ และป้องกันเหตุการณ์ ดังต่อไปนี้
- 1.7. ความพยายามในการบุกรุกผ่านระบบเครือข่าย
  - 1.7.1. การใช้งานในลักษณะที่ผิดปกติ
  - 1.7.2. การใช้งาน และการแก้ไขระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
- 1.8. ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามหลักความมั่นคงปลอดภัย โดยอย่างน้อยแบ่งออก เป็น 3 ส่วน ได้แก่
  - 1.8.1. ส่วนเซิร์ฟเวอร์(Server Zone)
  - 1.8.2. ส่วนเครื่องปฏิบัติงาน(Operation Zone)
  - 1.8.3. ส่วนผู้เข้าเยี่ยมชม(Visitor Zone)
- 1.9. ตรวจสอบสิทธิในการเข้าถึง และความปลอดภัยของอุปกรณ์คอมพิวเตอร์ ก่อนเชื่อมต่อกับระบบ เครือข่าย เช่น ตรวจสอบระบบตัวตนเครื่องที่เข้าถึงเครือข่าย ตรวจสอบไวรัสและภัยคุกคามที่ อาจมีในเครื่อง ตรวจสอบการ กำหนดค่า Parameter ต่าง ๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องปิดการเชื่อมต่อเครื่อง คอมพิวเตอร์ (Filter MAC Address) และจุดเชื่อมต่อ (Disable Fort) ที่ไม่รับอนุญาตให้ใช้งานหรือไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง.
- 1.10. การแก้ไข หรือเปลี่ยนแปลงค่าพารามิเตอร์ต่าง ๆ ในระบบเครือข่าย และอุปกรณ์เครือข่าย ให้สำรองข้อมูลพารามิเตอร์ก่อนการเปลี่ยนแปลงทุกครั้ง
- 1.11. จัดทำเอกสาร Security Baseline ในอุปกรณ์เครือข่ายที่มีความสำคัญ เพื่อใช้กำหนดค่า พารามิเตอร์ได้อย่างถูกต้อง
- 1.12. การตรวจสอบโดยใช้เครื่องมือทางเทคนิคในระบบเครือข่ายจะต้องจัดทำแผน ขอบเขต วันที่ดำเนินการ เครื่องมือที่ใช้ และผู้ดำเนินการเพื่อขออนุมัติก่อนดำเนินงาน
- 1.13. ข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) สามารถตรวจสอบหมายเลขเครือข่ายของอุปกรณ์ ทั้งจากต้นทางและปลายทางได้
- 1.14. การจัดเก็บข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) รวมถึงการเก็บข้อมูลการจราจร (Traffic Logs) ให้เป็นไปตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง



(0107537000513)

บริษัท เชียงใหม่ฟรozenฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแอง โกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

## หมวดที่ 7

### การเข้ารหัส

วัตถุประสงค์: เพื่อให้มีความคุ้มครองการใช้งานเทคโนโลยีการเข้ารหัสที่มีคุณภาพ และสอดคล้องกับความต้องการองค์กร

#### 1. นโยบายการเข้ารหัส

- 1.1. ไม่อนุญาตให้ใช้เทคโนโลยีการเข้ารหัสที่ผิดกฎหมาย หรือไม่ได้รับการยอมรับจากหน่วยงาน กำกับดูแล
- 1.2. การรับ-ส่งข้อมูลที่มีการเข้ารหัสระหว่างประเทศ จะต้องเป็นไปตามกฎหมายของประเทศที่เกี่ยวข้อง และไม่ขัดต่อหลักสากล
- 1.3. ออกแบบ และใช้งานเทคโนโลยีการเข้ารหัสที่ปลอดภัยและเชื่อถือได้ โดยอย่างน้อยต้องมี ความยาวรหัสที่ 256 บิต หรือเทียบเท่า
- 1.4. กำหนดให้ใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) เพื่อรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูล
- 1.5. ระบบสารสนเทศที่เชื่อมต่อกับระบบเครือข่ายสาธารณะจะต้องใช้โปรโตคอลเข้ารหัสที่มีความปลอดภัย ได้แก่ SSH, S-HTTP หรือโปรโตคอลที่เทียบเท่าหรือมีความปลอดภัยมากกว่า

#### 2. การจัดการกุญแจเข้ารหัส

- 2.1. การสร้างกุญแจเข้ารหัสจะต้องใช้วิธีการที่ปลอดภัย และดำเนินการโดยผู้ที่มีหน้าที่รับผิดชอบ
- 2.2. เก็บรักษากุญแจเข้ารหัสไว้ในที่ปลอดภัยเพื่อป้องกันการสูญหาย ฆโมย และการลักลอบใช้งาน ตลอดจนอายุการใช้งาน
- 2.3. กุญแจเข้ารหัสจะต้องเก็บไว้เป็นความลับ และไม่แจกจ่ายไปยังผู้ที่ไม่เกี่ยวข้อง
- 2.4. มีการเก็บรักษาและสำเนากุญแจเข้ารหัสให้สอดคล้องกับอายุของข้อมูลเพื่อให้สามารถอ่าน ข้อมูลได้



(0107537000513)

บริษัท เชียงใหม่ฟรอสเฟนฟู๊ดส์ จำกัด (มหาชน)

149/34 ซอยแองโกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

## หมวดที่ 8

### ความมั่นคงปลอดภัยพื้นที่

วัตถุประสงค์: เพื่อป้องกันความเสียหายที่เกิดจากการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงภัยธรรมชาติ และอุบัติเหตุ ต่าง ๆ

#### 1. ข้อกำหนดทั่วไป

- 1.1. ออกแบบพื้นที่สำคัญสูง ให้แยกส่วนออกจากพื้นที่สำนักงานทั่วไป
- 1.2. ติดตั้งระบบยืนยันตัวตนบุคคลควบคุมการเข้าออกในจุดสำคัญ
- 1.3. ติดตั้งอุปกรณ์ป้องกันภัย และรักษาสภาพแวดล้อมให้เหมาะสม อาทิเช่น ระบบป้องกันไฟไหม้ ระบบป้องกันกระแสไฟฟ้าขัดข้อง ระบบป้องกันน้ำรั่วซึม ระบบควบคุมอุณหภูมิและความชื้น ระบบกล้องวงจรปิด และระบบยืนยันตัวตน และควบคุมการเข้าออก เป็นต้น
- 1.4. ติดป้ายแสดงตำแหน่งที่อยู่ (Floor Plan) และแสดงป้ายทางหนีไฟชัดเจน
- 1.5. ดำเนินการซ้อมอพยพเหตุการณ์ฉุกเฉิน และตรวจสอบความพร้อมใช้งานของอุปกรณ์ เช่น ไฟส่องสว่างตามทางเดิน รวมทั้งการใช้อุปกรณ์ และปุ่มฉีดสารดับเพลิงต่างๆ เป็นต้น
- 1.6. ไม่ติดป้ายแสดงข้อความหรือระบุพื้นที่สำคัญ
- 1.7. สายไฟ และสายเคเบิลจะต้องแยกจากกันหรือมีวิธีการป้องกันสัญญาณรบกวนที่เหมาะสม

#### 2. ความมั่นคงปลอดภัยในศูนย์คอมพิวเตอร์ (Data Center Security)

- 2.1. จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ใน ศูนย์คอมพิวเตอร์ หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเข้าถึงได้เท่านั้น
- 2.2. จัดทำข้อควรปฏิบัติ ติดไว้ที่ศูนย์คอมพิวเตอร์ เพื่อให้ผู้ปฏิบัติงานได้รับทราบ
- 2.3. อุปกรณ์คอมพิวเตอร์ที่สำคัญจะต้องจัดวางในตู้เซิร์ฟเวอร์ และล็อกตู้อยู่เสมอ
- 2.4. ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ จะต้องได้รับการอนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ และกำหนดให้มีเจ้าหน้าที่ เทคโนโลยีสารสนเทศควบคุมดูแลการทำงานตลอดเวลา
- 2.5. มีระบบเก็บบันทึกการเข้า-ออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียด เกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก วัตถุประสงค์ และขั้นตอนการปฏิบัติงานในศูนย์ คอมพิวเตอร์ และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
- 2.6. การจัดพื้นที่ในศูนย์คอมพิวเตอร์แยกเป็นสัดส่วน เพื่อจำกัดการเข้าถึงพื้นที่ให้เป็นไปตามหน้าที่ และความรับผิดชอบของเจ้าหน้าที่ ได้แก่
  - 2.6.1. ส่วนของระบบเครือข่าย (Network Zone)
  - 2.6.2. ส่วนเครื่องแม่ข่าย (Server Zone)
  - 2.6.3. ส่วนอุปกรณ์สนับสนุน (Facility Zone)
- 2.7. การนำอุปกรณ์สารสนเทศ และเครือข่าย ออกนอกบริษัทฯ จะต้องได้รับการอนุมัติจาก ระดับผู้ช่วยผู้จัดการฝ่าย ขึ้นไป



(0107537000513)

**บริษัท เชียงใหม่ฟรozenฟูคส์ จำกัด (มหาชน)**

149/34 ซอยแองโกลพลาซ่า ถนนสุรวงศ์ กรุงเทพฯ 10500

**CHIANGMAI FROZEN FOODS PUBLIC COMPANY LIMITED**

149/34 Soi Anglo Plaza Surawongse Rd., Bangkok 10500 Thailand

Tel : (662) 634-0061-4, 238-4091 Fax : (622) 238-4090

นโยบายและมาตรการรักษาความปลอดภัยของระบบสารสนเทศนี้

ให้ใช้บังคับตั้งแต่วันที่ 25 พฤษภาคม พ.ศ. 2563 เป็นต้นไป

อังกูร พลพิพัฒน์พงศ์

กรรมการผู้จัดการบริษัท

บริษัท เชียงใหม่ฟรozenฟูคส์ จำกัด (มหาชน)

21 พ.ค. 2563