# ระเบียบและแนวปฏิบัติในการรักษาความปลอดภัยสารสนเทศ

**สารบัญ**

**บทนำ**

บริษัท เจ้าสัว ฟู้ดส์ อินดัสทรี จำกัด(มหาชน) (“บริษัท”) ได้กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ แล้วนั้น เพื่อให้เกิดผลอย่างเป็นรูปธรรม ตามนโยบายดังกล่าวอาศัยอำนาจพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือกฎหมายอื่นที่เกี่ยวข้อง จึงได้ประกาศและแนวปฏิบัติการรักษาความปลอดภัยสารสนเทศ (ฉบับย่อ) ซึ่งผู้ใช้งานระบบสารสนเทศของบริษัทฯ มีหน้าที่และความรับผิดชอบที่จะต้องปฏิบัติตามอย่างเคร่งครัด

**วัตถุประสงค์**

1. เพื่อเป็นหลักฐานสำหรับผู้ใช้งานระบบสารสนเทศของบริษัท ว่ายินยอมรับเงื่อนไขตามนโยบาย ว่าด้วยความปลอดภัยระบบสารสนเทศบริษัททุกประการ
2. เพื่อให้ผู้ใช้งานระบบสารสนเทศของบริษัทได้รับทราบถึงข้อห้าม และข้อปฏิบัติ ที่จะส่งผลให้เกิดความปลอดภัยต่อระบบสารสนเทศ และเกิดการใช้งานให้ตรงตามวัตถุประสงค์การใช้งานระบบสารสนเทศของบริษัท รวมทั้งไม่ละเมิดระเบียบกฎหมาย หรือทำให้เกิดความเสียหายในการปฏิบัติงาน

**ขอบเขต**

ระเบียบและแนวปฏิบัติ มีผลบังคับใช้กับผู้ใช้งานระบบสารสนเทศ ทุกระดับชั้น ทุกตำแหน่ง โดยไม่มีการยกเว้นผู้ใช้งาน รวมถึงผู้บริหาร พนักงาน ลูกจ้างสัญญาจ้าง บุคคลภายนอก ที่ต้องใช้ระบบสารสนเทศของบริษัท

**นิยาม**

“บริษัท” หมายความว่า บริษัท เจ้าสัว ฟู้ดส์ อินดัสทรี จำกัด(มหาชน)และบริษัทในเครือ ที่ใช้ระบบสารสนเทศ และระบบเครือข่ายและคอมพิวเตอร์ร่วมกัน

“เครื่องคอมพิวเตอร์” หมายความว่าอุปกรณ์ประมวลผลข้อมูลที่ทำงานด้วยระบบอิเล็กทรอนิกส์ที่มีความเร็วสูง โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการได้แก่คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์แบบพกพา (Notebook Computer)

“อุปกรณ์คอมพิวเตอร์” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ ปฏิบัติงานได้ตามต้องการ รวมถึงเครื่องคอมพิวเตอร์

“เครือข่ายคอมพิวเตอร์” หมายความว่า เครือข่ายคอมพิวเตอร์ของบริษัท

“ผู้บังคับบัญชา” หมายความว่าผู้มีอำนาจสั่งการตามโครงสร้างของบริษัท

“บุคลากร” หมายความว่า พนักงานบริษัท รวมถึงลูกจ้างทดลองงาน ลูกจ้างชั่วคราวของบริษัท หรือบุคคลอื่นที่ได้รับมอบหมายให้ ปฏิบัติงานตามสัญญาของบริษัท

“ผู้ใช้งาน” (User) หมายความว่า พนักงานบริษัทหรือบุคคลภายนอกที่ได้รับสิทธิ์ ให้ใช้งานระบบคอมพิวเตอร์ของบริษัท “บัญชีผู้ใช้งาน” (User account) หมายความว่า บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบคอมพิวเตอร์ ซึ่งเป็นไปตามข้อตกลง ระหว่างผู้ใช้งานกับผู้ให้บริการระบบคอมพิวเตอร์

“ผู้ดูแลระบบ” หมายความว่า ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ที่ได้รับมอบหมายจากบริษัท

“ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใดๆไม่ว่าการสื่อความหมายนั้นจะทำ ได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะทำในรูปแบบเอกสารแฟ้ม รายงาน แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพ หรือเสียงการบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“การพิสูจน์ตัวตน” หมายความว่าขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

**หมวด 1 การบริหารจัดการข้อมูลองค์กร** (Corporate Management)

1. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของบริษัทหรือเป็นข้อมูลของบุคคลภายนอก
2. ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัท ถือเป็นทรัพย์สินของบริษัท ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
3. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัท หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย
4. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล
5. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัทจะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่บริษัทต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับบริษัท ซึ่งบริษัทนอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้น ได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ
6. ผู้ใช้งานมีสิทธิ์ขอเพิ่ม/เปลี่ยนแปลง/ยกเลิกสิทธิ์ต่างๆ ในระบบข้อมูล โดยให้พนักงานเขียนแบบฟอร์มขอเพิ่ม/เปลี่ยนแปลง/ยกเลิก พร้อมชี้แจงเหตุผล

**หมวด 2 การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)**

1. ผู้ใช้งานห้ามนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพ็จบนเครือข่ายคอมพิวเตอร์
2. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (BitTorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา
3. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศกฎหมาย หรือกระทบต่อของบริษัท
4. ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัท เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของบริษัท
5. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทเพื่อประโยชน์ทางการค้าส่วนตัว
6. ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัทโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม
7. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัท ต้องหยุดชะงัก
8. ห้ามใช้ระบบสารสนเทศของบริษัท เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ
9. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม
10. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

**หมวด 3 การพิสูจน์ตัวตน** (Accountability, Identification and Authentication)

1. ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดย ห้ามทำการเผยแพร่แจกจ่าย หรือทำให้ผู้ไม่เกี่ยวข้องล่วงรู้รหัสผ่าน (Password)
2. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม
3. ผู้ใช้งานควรตั้งรหัสผ่านให้ตรงตามนโยบายการจัดการรหัสผ่าน (Password management) ดังนี้
   3.1 ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric) โดยยกเว้นระบบที่มีข้อจำกัดการใช้ตัวอักษรตั้งค่ารหัสผ่าน เช่น Senior soft ให้ตั้งเป็นรูปแบบตัวเลข8หลัก
   3.2 ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น “abcdef” “aaaaaa” “123456” “password” “P@ssw0rd” เป็นต้น
   3.3 ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
   3.4 ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
   3.5 ไม่ควรใช้รหัสผ่านซ้ำกับรหัสผ่านเดิม (ในระบบSAP)
   3.6 มีการกำหนดจำนวนครั้งที่อนุญาตให้ใส่รหัสผ่านผิด (ในระบบSAP)
   3.7 ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย
4. ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
5. ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที
6. กรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ Shared Users Licenses เช่นระบบ SAP เป็นต้น ทางผู้ดูแลจะมีการส่งอีเมลแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้น เมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด
7. ผู้ใช้ต้องเปลี่ยนรหัสผ่านทุก90วัน หากระบบไม่สามารถตั้งค่าเปลี่ยนรหัสผ่านอัตโนมัติได้ ให้ใช้เอกสารตรวจสอบนอกระบบแทน
8. ผู้ใช้งานต้องยินยอมให้ทางเจ้าหน้าที่หรือตัวแทนบริษัทเข้าตรวจสอบการพิสูจน์ตัวตนโดยไม่ต้องบอกล่วงหน้า
9. ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

**หมวด 4 การบริหารจัดการทรัพย์สิน** (Assets Management)

1. ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
2. ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
3. ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
4. ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
5. ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
6. ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
7. ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน
8. ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่
9. หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
10. ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
11. การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
12. ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย
13. คอมพิวเตอร์จำเป็นต้องได้รับการดูแลรักษาเครื่องทุกปี และมีรอบการเปลี่ยนเครื่องทุก5ปีหรือพิจารณาตามสภาพ เพื่อให้อุปกรณ์พร้อมใช้งานอยู่เสมอ ในกรณีอุปกรณ์สูญหายหรืออายุถึงรอบ มีแนวทางปฏิบัติดังนี้
    1. หลักการประเมินอายุคอมพิวเตอร์และมูลค่าเครื่องตามเกณฑ์ ดังนี้
        1.1 ค่าใช้จ่ายอุปกรณ์คอมพิวเตอร์หาย เครื่องอายุไม่เกิน1ปี คิดที่80%ของราคาที่ทุน
        1.2 ค่าใช้จ่ายอุปกรณ์คอมพิวเตอร์หาย เครื่องอายุ1-2ปี คิดที่60%ของราคาที่ทุน
        1.3 ค่าใช้จ่ายอุปกรณ์คอมพิวเตอร์หาย เครื่องอายุ2-3ปี คิดที่50%ของราคาที่ทุน
        1.4 ค่าใช้จ่ายอุปกรณ์คอมพิวเตอร์หาย เครื่องอายุ3-4ปี คิดที่40%ของราคาที่ทุน
        1.5 ค่าใช้จ่ายอุปกรณ์คอมพิวเตอร์หาย เครื่องอายุ4-5ปี คิดที่20%ของราคาที่ทุน
        1.6 ค่าใช้จ่ายอุปกรณ์คอมพิวเตอร์หาย เครื่องมากกว่า5 ปี มูลค่าตามเกณฑ์ (3,500/4,500/5,500)

**ตัวอย่าง** คอมพิวเตอร์ราคาเครื่องละ 25,000 บาท

| ปีที่ | ไม่เกิน 1ปี | ไม่เกิน 2ปี | ไม่เกิน 3ปี | ไม่เกิน 4ปี | ไม่เกิน 5ปี | 5ปี ขึ้นไป |
|---|---|---|---|---|---|---|
| คิดเป็น%จากราคาทุน | 80% | 60% | 50% | 40% | 20% | - |
| คิดเป็นบาท | 20,000 | 15,000 | 12,500 | 10,000 | 5,000 | 3,500 |

2. หลักการประเมินคอมพิวเตอร์เพื่อตั้งราคาเสนอขาย หากอายุครบตามรอบเปลี่ยน5ปี จะประกาศขายเป็นระยะเวลา1เดือนหรือเวลาตามกำหนด โดยเสนอขายตามแบ่งมูลค่าตามระดับคอมพิวเตอร์

1.1 เครื่องทั่วไป มูลค่าตั้งแต่ 10,000 – 25,000 บาท คิดเป็น 3,500 บาท

1.2 เครื่องระดับกลาง มูลค่าตั้งแต่ 25,001 – 45,000 บาท คิดเป็น 4,500 บาท

1.3 เครื่องระดับสูง มูลค่าตั้งแต่ 45,001 บาท ขึ้นไป คิดเป็น 5,500 บาท

1.4 ราคาอาจเปลี่ยนแปลงขึ้นอยู่กับสภาพเครื่อง

## หมวด 5 การปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของบริษัท ถือเป็นสิ่งสำคัญ ที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้นหากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

## หมวด 6 ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

1. บริษัทได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทอนุญาตให้ใช้งานหรือที่บริษัทมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และบริษัทห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว
2. ซอฟต์แวร์ ที่บริษัทได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

## หมวด 7 การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

1. คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) ตามที่บริษัทได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นันเป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกันโดยต้องได้รับอนุญาตจากผู้บังคับบัญชา
2. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาให้ใช้งานหรือเก็บบันทึกทุกครั้ง
3. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น
4. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

5. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ
6. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินของบริษัท หรือของผู้อื่นโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ
7. ห้ามทำเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ (Malware) หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัท

## หมวด 8 การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

1. ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตาม “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550” หมวด 1 มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

### กฎข้อห้าม

1. ผู้ใช้งานที่ต้องการใช้งาน E-Mail ของหน่วยงานต้องทำการกรอกข้อมูลคำขอเข้าใช้งาน และยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์ ชื่อผู้ใช้งานรายใหม่ และรหัสผ่าน
2. ต้องใช้ E-Mail ของหน่วยงานเพื่อติดต่องานของบริษัทเท่านั้น
3. ไม่ควรใช้ E-Mail Address ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของE-Mail และให้ถือว่าเจ้าของ E-Mail เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ใน E-Mail ของตน
4. ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง
5. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
6. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
7. ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิ์ของบุคคลอื่น
8. ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
9. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น
10. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
11. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัทผ่านทางจดหมายอิเล็กทรอนิกส์

**หมวด 9 ว่าด้วยการควบคุมการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)**

1. ต้องมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) ขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน
2. ต้องให้เจ้าหน้าที่ IT ควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัทฯ (onsite service) และให้เจ้าหน้าที่ IT ตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ remote access และปิด VPN service หรือ Remote Access service ทันทีที่การให้บริการเสร็จสิ้น
3. ดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ
4. ต้องกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข
5. ต้องมีขั้นตอนในการตรวจรับงานของผู้ให้บริการจากผู้ใช้งานที่เกี่ยวข้อง และมีการตรวจรับงานจากผู้มีอำนาจหน้าที่

**หมวด 10 ว่าด้วยการพัฒนาระบบเทคโนโลยีสารสนเทศ (System development)**

1. มีแผนในการพัฒนาระบบเทคโนโลยีสารสนเทศ และมีการทบทวนแผนอย่างน้อยปีละ 1 ครั้ง
2. แผนต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่

## บทลงโทษและการบังคับใช้

**ความผิด**

1. ผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบายเกี่ยวกับความปลอดภัยระบบสารสนเทศของบริษัท แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์ก็ให้ถือว่ามีความผิดโดยสมบูรณ์

**การลงโทษ**

1. วิธีดำเนินการความผิดเกี่ยวกับนโยบายและข้อบังคับของบริษัท ให้ลงโทษผู้กระทำผิดตามระเบียบของบริษัท
2. หากผู้ใช้งานไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศก่อให้เกิดความเสียหายต่อบุคคลอื่น หรือต่อทรัพย์สินของบริษัท จะต้องรับโทษตามบทลงโทษ ต่อไปนี้
   2.1 โทษขั้นต้น ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสารเป็นเวลา 7 วัน
   2.2 โทษขั้นกลาง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสารเป็นเวลา 30 วัน
   2.3 โทษขั้นร้ายแรง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสารเป็นเวลา 3 เดือน และหากการละเมิดฝ่าฝืนให้เกิดความเสียหายต่อผู้อื่น หรือต่อทรัพย์สินของบริษัทอย่างร้ายแรง ให้ลงโทษผู้กระทำความผิดตามระเบียบกฎหมายที่เกี่ยวข้องนั้นๆ

จึงประกาศมาเพื่อดำเนินการและปฏิบัติ

ประกาศ ณ วันที่ 1 ธันวาคม 2566

..... ผู้จัดทำ

ชุติมา อิทธิอมรเลิศ

ผู้จัดการแผนกสารสนเทศ

..... ผู้ตรวจสอบ

อินทุอร โมรินทร์

ผู้อำนวยการฝ่ายบัญชี

..... ผู้อนุมัติ

สิริณัฏฐ์ ชญาน์นันท์

กรรมการผู้จัดการ

.....ผู้อนุมัติ

ณภัทร โมรินทร์

ประธานเจ้าหน้าที่บริหาร