SHRINKflex

นโยบายความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศ

สำหรับ
บริษัท ชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน)

อนุมัติโดย :_____

(ดร. กฤษณะ วจีไกรลาศ)

ประธานกรรมการบริษัท

บริษัท ชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน) ตั้งอยู่เลขที่ 88/8 หมู่ 12 ตำบลบางปะกง อำเภอบางปะกง จังหวัดฉะเชิงเทรา 24130 ประเทศไทย ประกอบกิจการผลิต จำหน่าย ฉลากฟิล์มพลาสติกหดรัดรูปและบรรจุภัณฑ์อ่อนตัว เพื่อแสดงถึงความมุ่งมั่น นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Information Technology Security Policy) บริษัทฯจึงได้กำหนดนโยบายดังต่อไปนี้

ส่วนที่ 1

แนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศ

(Acceptable Use Policy)

ด้วยบริษัทได้กำหนดให้มี นโยบายว่าด้วยความปลอดภัยระบบสารสนเทศ บริษัท ชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน) แล้วนั้น

เพื่อให้เกิดผลเป็นรูปธรรม ตามนโยบายดังกล่าวอาศัยอำนาจพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงได้จัดทำหนังสือยินยอมรับเงื่อนไขนโยบายว่าด้วยความปลอดภัยระบบสารสนเทศขึ้น ประกอบด้วย 10 หมวด โดยมีรายละเอียดดังต่อไปนี้

วัตถุประสงค์

1. เพื่อเป็นหลักฐานเชิงประจักษ์ (ลายลักษณ์อักษร) สำหรับผู้ใช้งานระบบสารสนเทศของบริษัท ว่ายินยอมรับเงื่อนไขตามนโยบาย ว่าด้วยความปลอดภัยระบบสารสนเทศบริษัททุกประการ

2. เพื่อให้ผู้ใช้งานระบบสารสนเทศของบริษัทได้รับทราบถึงข้อห้าม และข้อปฏิบัติ ที่จะส่งผลให้เกิดความปลอดภัยต่อระบบสารสนเทศ และเกิดการใช้งานตรงตามวัตถุประสงค์การใช้งานระบบสารสนเทศของบริษัท รวมทั้งไม่ละเมิดระเบียบกฎหมาย หรือทำให้เกิดความเสียหายในการปฏิบัติงาน

3. เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมยทำลายแทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อ

การดำเนินธุรกิจของบริษัท

ขอบเขต

หนังสือนี้มีผลบังคับใช้กับผู้ใช้งานระบบสารสนเทศ ทุกระดับชั้น ตำแหน่ง โดยไม่มีการยกเว้นผู้ใช้งานรวมถึงผู้บริหาร พนักงาน ลูกจ้างสัญญาจ้าง บุคคลภายนอก ที่ต้องใช้ระบบสารสนเทศของบริษัท

นิยามศัพท์

“บริษัท” หมายความถึง บริษัท ชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน) และสาขาย่อยที่ใช้ระบบเครือข่ายคอมพิวเตอร์และระบบข้อมูลร่วมกัน

“เครื่องคอมพิวเตอร์” หมายความว่า อุปกรณ์ประมวลผลข้อมูลที่ทำงานด้วยระบบอิเล็กทรอนิคส์ที่มีความเร็วสูง โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ ได้แก่ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์แบบพกพา (Notebook Computer)

“อุปกรณ์คอมพิวเตอร์” หมายความว่า อุปกรณ์อิเล็กทรอนิคส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ รวมถึงเครื่องคอมพิวเตอร์

“เครือข่ายคอมพิวเตอร์” หมายความว่า เครือข่ายคอมพิวเตอร์ของบริษัท

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างของบริษัท

“บุคลากร” หมายความว่า พนักงานบริษัท รวมถึงลูกจ้างทดลองงาน ลูกจ้างชั่วคราวของบริษัท หรือบุคคลอื่นที่ได้รับมอบหมายให้ปฏิบัติงานตามสัญญาของบริษัท

“ผู้ใช้งาน” (User) หมายความว่า พนักงานบริษัทหรือบุคคลภายนอกที่ได้รับสิทธิ์ให้ใช้งานระบบคอมพิวเตอร์ของบริษัท

“บัญชีผู้ใช้งาน” (User Account) หมายความว่า บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบคอมพิวเตอร์ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบคอมพิวเตอร์

“ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใดๆไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะทำในรูปแบบเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“การพิสูจน์ตัวตน” หมายความว่า ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

“ผู้ดูแลระบบ” หมายความว่า ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ที่ได้รับมอบหมายจากบริษัท

ข้อบังคับ

ผู้ใช้งานระบบสารสนเทศของบริษัท มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุวัตถุตามวัตถุประสงค์

- ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
- ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงอมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้
- ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ
- การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนขันตัวตนที่สมบูรณ์แล้วเท่านั้น
- การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความ

หมวด 1

ว่าด้วยการพิสูจน์ตัวตน

(Accountability, Identification and Authentication)

ข้อ 1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)

ข้อ 2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 3 ผู้ใช้งานควรตั้งรหัสผ่านให้ตรงตาม นโยบายการจัดการรหัสผ่าน ดังนี้

นโยบายการจัดการรหัสผ่าน

(Password Management)

รหัสผ่านครอบคลุมบัญชีชื่อผู้ใช้งานดังนี้ คือ

ข้อ 1 Computer User ทั้งที่เป็น Domain User และ Local User, E-mail, Internet, SAP หรือ บัญชีผู้ใช้งานระดับบริหารจัดการระบบสารสนเทศต่างๆ

ข้อ 2 รหัสผ่านต้องมีอย่างน้อย 8 ตัวอักษร

ข้อ 3 ประกอบด้วยอักขระภาษาอังกฤษ (Alphabet) ตัวเลข (Numeric Character) และอักขระพิเศษ (Special character) เช่น !@#$ โดยจัดเรียงแบบไหนก็ได้

ข้อ 4 รหัสผ่านต้องไม่เป็นลักษณะตัวเลขหรืออักขระที่เรียงกันหรือซ้ำเกิน 3 ตัวอักษร หรือตัวอักขระ ที่เหมือนกับบัญชีชื่อผู้ใช้งานเกิน 3 ตัวอักษร

ข้อ 5 ต้องไม่ใช้รหัสผ่านซ้ำกับรหัสผ่านที่เคยใช้มาแล้ว

ข้อ 6 ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษ (Super User) ต้องมีการควบคุมการใช้งานอย่างรัดกุม

6.1 ต้องได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

6.2 มีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6.3 หลังการใช้งาน ผู้ถือครอง Supper User ต้องทำการเปลี่ยนรหัสผ่านทันที หากไม่มีการขอใช้งานเป็นเวลานาน ผู้ถือครอง Supper User ควรทำการเปลี่ยนรหัสผ่านทุกๆ 60 วัน

ข้อ 7 Password age อายุหรือความถี่ในการเปลี่ยนรหัสผ่าน

7.1 ผู้ใช้งานทั่วไป ต้องเปลี่ยนรหัสผ่าน ทุกๆ หรือไม่เกิน 90 วัน

7.2 ผู้ใช้งานระดับ Super User หรือ ผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริการระบบ (System Administrator) ต้องเปลี่ยนทุกๆ 60 วัน

7.3 ผู้ใช้งานที่เกี่ยวเนื่องกับ Out Source ต้องมีการเปลี่ยนทุกครั้งหลังใช้งาน

ข้อ 8 มีระบบจัดเก็บรหัสผ่านที่มีการเข้ารหัส และเข้าถึงได้ด้วยการ Authentication 2 ครั้ง

ข้อ 9 ห้ามส่งต่อ รหัสผ่านกับผู้ใช้งานโดยการส่ง E-Mail เพื่อป้องการการรั่วไหลและความปลอดภัยในการเข้าใช้งาน

ข้อ 10 ผู้ใช้งานต้องยินยอมให้ทางเจ้าหน้าที่หรือตัวแทนบริษัทเข้าตรวจสอบการพิสูจน์ตัวตนโดยไม่ต้องบอกล่วงหน้า

หมวด 2

ว่าด้วยการบริหารจัดการทรัพย์สิน

(Assets Management)

ข้อ 1 ต้องมีระบบทะเบียนทรัพย์สิน เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์และผู้รับผิดชอบ มีการลงบันทึกรายละเอียดและปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ 2 ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

ข้อ 3 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ 4 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้ง

ข้อ 5 ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ 6 ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม Computer หรือ Notebook ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ 7 ทรัพย์สินและระบบสารสนเทศต่างๆ ที่บริษัท จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์ เพื่อการใช้งานของบริษัทเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัท

ข้อ 8 ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ 7 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ข้อ 9 บริษัทมีตารางเวลา รายละเอียดการบำรุงรักษาและการ Maintenance Checklist ของอุปกรณ์สารสนเทศแต่ละชิ้น

หมวด 3

ว่าด้วยการบริหารจัดการข้อมูลองค์กร

(Corporate Management)

ข้อ 1 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัทหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ 2 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัท ถือเป็นทรัพย์สินของบริษัท ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 3 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัท หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ 4 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ 5 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัทจะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่บริษัท ต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับบริษัท ซึ่งบริษัทอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ 6 ผู้ใช้งานมีสิทธิ์ขอเพิ่ม/เปลี่ยนแปลง/ยกเลิก สิทธิ์ต่างๆในระบบข้อมูลโดยให้พนักงานเขียนแบบฟอร์มขอเพิ่ม/เปลี่ยนแปลง/ยกเลิก พร้อมชี้แจ้งเหตุผล

หมวด 4

ว่าด้วยการบริหารจัดการระบบสารสนเทศ

(IT Infrastructure Management)

ข้อ 1 ผู้ใช้งานห้ามนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพ็จบนเครือข่ายคอมพิวเตอร์

ข้อ 2 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 3 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของบริษัท

ข้อ 4 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัท เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของบริษัท

ข้อ 5 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทเพื่อประโยชน์ทางการค้าส่วนตัว

ข้อ 6 ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัท โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ 7 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัท ต้องหยุดชะงัก

ข้อ 8 ห้ามใช้ระบบสารสนเทศของบริษัท เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 9 ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ 10 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัท โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด 5

ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ

(Law and Compliance)

ข้อ 1 บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของบริษัท ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด 6

ว่าด้วยซอฟต์แวร์และลิขสิทธิ์

(Software Licensing and intellectual property)

ข้อ 1 บริษัท ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัท อนุญาตให้ใช้งานหรือที่บริษัท มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและบริษัทห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์บริษัทถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ 2 ซอฟต์แวร์ ที่บริษัทได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด 7

ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี

(Preventing Malware)

ข้อ 1 คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ตามที่บริษัทได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 2 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาให้ใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 3 ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ 4 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ 5 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ 6 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินของบริษัท หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 7 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัท

หมวด 8

ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์

(Electronic mail)

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

กฎข้อห้าม

ข้อ 1. ผู้ใช้งานที่ต้องการใช้งาน E-Mail ของหน่วยงานต้องทำการกรอกข้อมูลคำขอเข้าใช้งานและยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน

ข้อ 2. ต้องใช้ E-Mail ของหน่วยงานเพื่อติดต่องานของบริษัทเท่านั้น

ข้อ 3. ไม่ควรใช้ E-Mail Address ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ E-Mail และให้ถือว่าเจ้าของ E-Mail เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ใน E-Mailของตน

ข้อ 4. ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

ข้อ 5. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ 6. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ 7. ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิ์ของบุคคลอื่น

ข้อ 8. ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ 9. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้ โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

ข้อ 10. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ 11. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัทผ่านทางจดหมายอิเล็กทรอนิกส์

หมวด 9

ว่าด้วยการควบคุมการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น

(IT Outsourcing)

ข้อ 1 ต้องมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

ข้อ 2 ต้องให้เจ้าหน้าที่ IT ควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัทฯ(Onsite Service) และให้เจ้าหน้าที่ IT ตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และปิด VPN service หรือ Remote Access Service ทันทีที่การให้บริการเสร็จสิ้น

ข้อ 3 ดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ 4 ต้องกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

ข้อ 5 ต้องมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ จากผู้มีใช้งานที่เกี่ยวข้อง และมีการรองรับการตรวจรับงานจากผู้มีอำนาจหน้าที่

หมวด 10

ว่าด้วยการพัฒนาระบบเทคโนโลยีสารสนเทศ

(System development)

ข้อ 1 มีแผนในการพัฒนาระบบเทคโนโลยีสารสนเทศ และมีการทบทวนแผนอย่างน้อยปีละ 1 ครั้ง

ข้อ 2 แผนต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่

ส่วนที่ 2

นโยบายความปลอดภัยของการควบคุมการเข้าถึง

(Access Control Policy)

หมวด 1

ว่าด้วยการควบคุมการเข้าถึงระบบสารสนเทศ

(Data Access Control And Management)

ข้อ 1 กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บัญชาการ

ข้อ 2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูล ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ

ข้อ 3 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ 4 ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ มีหลักฐานการขอเข้าถึงระบบสารสนเทศอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ5 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

ข้อ 6 เพื่อให้การใช้งานในระบบสารสนเทศเกิดความปลอดภัยสูงสุด ต้องจัดให้มีการอบรม อย่างน้อยปีละ 2 ครั้ง เพื่อสร้างความรู้ความเข้าใจกับผู้ใช้งาน และสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) อันจะเกิดจากความรู้เท่าไม่ถึงการณ์หรือความไม่ระมัดระวัง

หมวด 2

การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อมห้องแม่ข่าย

(Server Physical and Environment Security)

ข้อ 1 อาคาร สถานที่และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ 2 ให้เจ้าหน้าที่ หรือผู้ดูแลระบบ และผู้ได้รับอนุญาตเท่านั้น เป็นผู้มีสิทธิ์เข้า-ออก และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

ข้อ 3 มีระบบกล้องวงจรปิด ภายในห้องคอมพิวเตอร์แม่ข่าย และทางเข้าออก และมีการตรวจสอบสภาพให้พร้อมใช้งานเสมอ

ข้อ 4 มีระบบการพิสูจน์ตัวตนและจัดเก็บบันทึกการเข้าออก เช่น ระบบ Access Control เป็นต้น

ข้อ 5 ระบบสำรองไฟและระบบปรับอากาศ จะต้องมีความปลอดภัยและเหมาะสม โดยจัดให้มีระบบสำรองไฟและระบบปรับอากาศสำรอง เพื่อใช้งานเมื่อไฟฟ้าขัดข้องและรักษาอุณหภูมิในห้อง

ข้อ 6 ต้องมีมาตรการป้องกันอัคคีภัย ภายในห้องติดตั้งเครื่อง Server ต้องมีการติดตั้งอุปกรณ์ดับเพลิงสำหรับใช้กรณีฉุกเฉินเมื่อเกิดอัคคีภัย

ข้อ7การเก็บรักษาสื่อหรืออุปกรณ์เก็บข้อมูลและสำรองข้อมูลจะต้องถูกจัดเก็บไว้อย่างปลอดภัยมีระบบสำรองข้อมูลที่มีประสิทธิภาพ

ข้อ 8 ต้องมีแผนและนโยบายเตรียมรับสถานการณ์ฉุกเฉิน เช่นแผนแก้ไขปัญหาจากความไม่แน่นอนและภัยพิบัติ (Contingency Plan)

หมวด 3

นโยบายความปลอดภัยของการสำรองข้อมูล

(Backup Policy)

ข้อ 1 ต้องมีการสำรองข้อมูลเก็บไว้ ครอบคลุมถึงข้อมูลทั้งบริษัท ทั้งที่เป็นข้อมูลดิบ (Raw Data) และฐานข้อมูล (Data Base) โดยแบ่งการสำรองออกเป็นแต่ละหน่วยงานอย่างชัดเจน

ข้อ 2 มีขั้นตอนการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง โดยแยกตามในแต่ละระบบสารสนเทศ และมีการติดตามความสมบูรณ์ของการสำรองข้อมูลอย่างต่อเนื่อง

ข้อ 3 ต้องมีแผนเตรียมความพร้อมกรณีฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ในเวลาที่เหมาะสม

หมวดที่ 4

ความปลอดภัยของเครือข่ายและคอมพิวเตอร์แม่ข่าย

(Network and Server Policy)

ข้อ 1 กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมคอมพิวเตอร์แม่ข่าย (Server)

ข้อ 2 ห้ามผู้ใช้งาน นำเครื่องคอมพิวเตอร์หรืออุปกรณ์มาเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายของบริษัท เว้นแต่ได้รับอนุญาตจากทางผู้บังคับบัญชา

ข้อ 3 ห้ามผู้ใช้งาน ติดตั้งเพิ่มเติม เคลื่อนย้ายหรือทำการใดๆกับอุปกรณ์ส่วนกลางระบบเครือข่ายของบริษัท เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 4 ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงระบบเครือข่าย จำกัดสิทธิ์ให้ใช้งานในระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น เพื่อบริหารจัดการระบบเครือข่ายอย่างมีประสิทธิภาพ

ข้อ 5 การเข้าสู่ระบบเครือข่ายภายในบริษัท โดยผ่าน Internet จำเป็นต้องมีการลงชื่อเข้าใช้ และมีการพิสูจน์ยืนยันตัวตน (Login and Authentication)

ข้อ 6 ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดครอบคลุม เครือข่ายภายใน เครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ข้อ 7 ต้องมีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ของระบบเครือข่าย (Log) อย่างน้อย 90 วัน

ข้อ 8 ควรตรวจสอบบันทึกของผู้ใช้งานระบบสม่ำเสมอ

ข้อ 9 บุคคลจากภายนอกต้องการใช้งานเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บังคับบัญชา

ข้อ 10 มีการควบคุมช่องทาง (Port) ใช้ในการเข้าสู่ระบบอย่างรัดกุม

ข้อ 11 การเข้าสู่ระบบจากระยะไกล ต้องได้รับอนุญาตจากประธานเจ้าหน้าที่บริหารเท่านั้น และต้องมีการควบคุม Port ในการใช้งานอย่างรัดกุม ยกเว้นผู้ดูแลระบบ (เฉพาะบุคคลภายในบริษัทเท่านั้น)

ข้อ 12 ระบบเครือข่ายของบริษัท ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ นอกบริษัท ต้องเชื่อมต่อผ่านอุปกรณ์ ที่ป้องการจากบุกรุกต่างๆ เช่น Firewall , Proxy เท่านั้น

บทลงโทษและการบังคับใช้

ความผิด

ข้อ 1 ผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบาย เกี่ยวกับความปลอดภัยระบบสารสนเทศของบริษัท แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์ก็ให้ถือว่ามีความผิดโดยสมบูรณ์

การลงโทษ

ข้อ 1 วิธีดำเนินการความผิดเกี่ยวกับ นโยบายและข้อบังคับของบริษัท ให้ลงโทษผู้กระทำผิดตามระเบียบของบริษัท

ข้อ 2 หากผู้ใช้งานไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ ก่อให้เกิดความเสียหายต่อบุคคลอื่น หรือต่อทรัพย์สินของบริษัท จะต้องรับโทษตามบทลงโทษ ต่อไปนี้

(1) โทษขั้นต้น ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นเวลา 7 วัน

(2) โทษขั้นกลาง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นเวลา 30 วัน

(3) โทษขั้นสูง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นเวลา 3 เดือน

(4) โทษขั้นร้ายแรง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นเวลา 1 ปีและ หากการละเมิดฝ่าฝืนให้เกิดความเสียหายต่อผู้อื่น หรือต่อทรัพย์สินของบริษัทอย่างร้ายแรง ให้ลงโทษ ผู้กระทำความผิดตามระเบียบกฎหมายที่เกี่ยวข้องนั้น ๆ

การบังคับใช้

ข้อ 1 ประธานเจ้าหน้าที่บริหาร ผู้จัดการฝ่าย ผู้จัดการแผนก หัวหน้าฝ่าย หัวหน้าแผนก มีหน้าที่ควบคุมผู้ใต้บังคับบัญชา ให้ปฏิบัติตามนโยบาย และข้อบังคับ อย่างเคร่งครัด หากพบว่าผู้ใต้บังคับบัญชากระทำความผิด ให้ผู้บังคับบัญชารายงานตามลำดับชั้นเพื่อเอาโทษต่อผู้กระทำความผิดอย่างเคร่งครัด การละเว้นการปฏิบัติหน้าที่ถือเป็นความผิดเช่นเดียวกับผู้กระทำผิด

ผนวก

ระเบียบปฏิบัติในการเข้าถึงข้อมูลที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

ปัจจุบันระบบสารสนเทศเป็นสิ่งสำคัญที่เข้ามาอำนวยความสะดวก และสนับสนุนการปฏิบัติงานของบริษัท ส่งผลให้การเข้าถึงข้อมูลข่าวสารมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพสูงขึ้น อย่างไรก็ตามแม้ว่าระบบ เครือข่ายดังกล่าวจะมีประโยชน์ และอำนวยความสะดวกในการปฏิบัติงาน แต่ในขณะเดียวกันก็มีความเสี่ยงสูง และก่อให้เกิดภัยอันตราย หรือสร้างความเสียหายต่อการปฏิบัติงานของบริษัทได้เช่นกัน เพราะการใช้งานระบบสารสนเทศเปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอก ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้ รวมถึงการขโมยข้อมูลหรือความลับทางบริษัท

ดังนั้นผู้ใช้งาน และผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทจำเป็นต้องตระหนักรู้ และให้ความสำคัญในการรักษาความมั่นคงปลอดภัยด้านข้อมูล เพื่อให้ระบบสารสนเทศของบริษัท สามารถดำเนินการหรือให้บริการต่าง ๆ ได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัยและเชื่อถือได้ ทางบริษัทได้จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฉบับนี้ขึ้น เพื่อให้ผู้ใช้งาน และผู้ดูแลระบบสารสนเทศในบริษัทรับทราบ และยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดอย่างเคร่งครัด เพื่อให้การดำเนินงานด้วยวิธีการระบบสารสนเทศของบริษัทมีความมั่นคงปลอดภัยและเชื่อถือได้และเป็นไปตามระเบียบปฏิบัติที่เกี่ยวข้องต่อไป

การทบทวน

บริษัทฯตั้งเป้าหมายในการทบทวนนโยบายระบบสารสนเทศเพื่อให้ทันสมัย และมีความสอดคล้องกับบริษัทฯ โดยกำหนดให้มีการทบทวนทุก ๆ 1 ปี หรือหากมีกรณีเร่งด่วนจะนำมาทบทวน ปรับปรุงก่อนครบกำหนดระยะเวลาดังกล่าว