นโยบายทางด้านเทคโนโลยีสารสนเทศ

นโยบายทางด้านเทคโนโลยีสารสนเทศ
บริษัท อมรินทร์ คอร์เปอเรชั่นส์ จำกัด (มหาชน)

วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของ บริษัท อมรินทร์ คอร์เปอเรชั่นส์ จำกัด (มหาชน) มีความมั่นคง ปลอดภัย และมิให้ผู้กระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อเผยแพร่ข้อมูลอันเป็นเท็จซึ่งอาจก่อให้เกิดความเสียหายแก่บริษัทฯและเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับปัจจุบัน

นิยามศัพท์

“บริษัทฯ” หมายถึง บริษัท อมรินทร์ คอร์เปอเรชั่นส์ จำกัด (มหาชน)

“กรรมการผู้จัดการ” หมายถึง กรรมการผู้จัดการสายธุรกิจต่างๆในบริษัท ฯ

“ฝ่ายเทคโนโลยีสารสนเทศ” หมายถึง ฝ่ายเทคโนโลยีสารสนเทศสายธุรกิจต่างๆ ในบริษัทฯ

“ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ” หมายถึง ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศสายธุรกิจต่าง ๆ ในบริษัทฯ

“ทรัพย์สิน” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศบริษัทฯ ภายใต้การกำกับดูแลของฝ่ายเทคโนโลยีสารสนเทศ

“ระบบเครือข่าย” หมายถึง เครือข่ายคอมพิวเตอร์ของบริษัทฯ ภายใต้การกำกับดูแลของฝ่ายเทคโนโลยีสารสนเทศ

“ผู้ใช้งาน” หมายถึง พนักงาน ลูกจ้างของบริษัทฯ รวมถึงบุคคลอื่นที่บริษัทฯ มอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

“ผู้ดูแลระบบ” หมายถึง พนักงานที่ได้รับมอบหมายจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่าย ซึ่งสามารถเข้าถึงโปรแกรมเครือข่าย เพื่อจัดการฐานข้อมูลของระบบเครือข่าย

หน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ

- ดูแลทรัพย์สินทางด้านสารสนเทศ ของบริษัทฯ
- กำหนดให้แหล่งข้อมูลกลาง (Datacenter Room) เป็นบริเวณที่ต้องรักษาความปลอดภัยและจัดให้มีการควบคุมการเข้า-ออก เฉพาะผู้ได้รับอนุญาตเท่านั้น
- สำรองข้อมูลอย่างสม่ำเสมอตามขั้นตอนการปฏิบัติงานเรื่องการสำรองข้อมูลและนำกลับมาใช้ใหม่
- จัดทำแผนกู้ระบบสารสนเทศเพื่อสามารถรับมือกับอุบัติภัยที่เกิดขึ้นและกู้คืนระบบให้สามารถกลับมาใช้งานได้ตามเป้าหมายที่กำหนด

- บริหารจัดการบัญชีผู้ใช้งาน และรหัสผ่าน เพื่อให้ผู้ใช้งานสามารถใช้งานระบบเครือข่ายและระบบสารสนเทศได้ตามสิทธิ์ที่ได้รับ รวมถึงการจัดการบัญชีผู้ใช้งานระบบ กลุ่มพิเศษ ตามภาคผนวก ก.
- จัดการ/แก้ไข ปัญหาด้านเทคโนโลยีสารสนเทศตามขั้นตอนการปฏิบัติงาน การจัดการปัญหา ทางด้านเทคโนโลยีสารสนเทศ
- ตรวจสอบระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติมหรือติดตั้งใหม่เพื่อไม่ให้เกิดผลกระทบต่อระบบสารสนเทศก่อนนำระบบนั้นมาติดตั้งใช้งาน ตามขั้นตอนการปฏิบัติงาน เรื่อง การขอแก้ไขโปรแกรมในระบบคอมพิวเตอร์
- ป้องกันตรวจจับโปรแกรมที่ไม่ประสงค์ดีเช่น ไวรัส เวิร์ม โทรจัน สปายแวร์ ฯลฯ
- ควบคุมการใช้งานเชื่อมต่อระบบเครือข่ายจากระยะไกล (remote access)
- ควบคุมการให้บริการของหน่วยงานภายนอก (Outsource) ที่เกี่ยวข้องกับระบบสารสนเทศและให้ปฏิบัติตามนโยบายทางด้านเทคโนโลยีสารสนเทศ
- จัดเก็บข้อมูลจราจรคอมพิวเตอร์ตามพรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฯ

นโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศ

1. **การควบคุมการเข้าถึงระบบ** (Access control Policy)

   ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของบริษัทฯ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นและเหมาะสมกับหน้าที่ความรับผิดชอบ รวมทั้งขั้นตอนปฏิบัติสำหรับ ยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือ การเปลี่ยนตำแหน่งงานภายในหน่วยงาน ในระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น

2. **การพิสูจน์ตัวตน** (Accountability, Identification and Authentication)

   2.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแลรักษาข้อมูลบัญชี ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นความลับ โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

   2.2 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 7 ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

   2.3 ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย 4 รหัสผ่าน

   2.4 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ 90 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

   2.5 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของบริษัทฯ และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านการโดนล็อคก็ดีหรือเกิดจากความผิดพลาดใด ๆ ก็ดีผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

2.6 ผู้ใช้งานไม่ควรให้เครื่องคอมพิวเตอร์จดจำบัญชีผู้ใช้งาน / รหัสผ่าน (remember password) เนื่องจากอาจมีบุคคลอื่นมาใช้งานรหัสผ่านดังกล่าว ได้

2.7 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

3. **การบริหารจัดการทรัพย์สิน** (Assets Management)

3.1 ผู้ใช้งานต้องไม่เข้าไปในแหล่งข้อมูลกลาง (Datacenter Room) ที่เป็นเขตหวงห้ามโดยเด็ดขาดเว้นแต่ได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

3.2 ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

3.3 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบตามมูลค่าทรัพย์สินต่อความเสียหายที่เกิดขึ้นหากผู้ใช้งานทรัพย์สินมาติดตั้ง เปลี่ยนแปลงทำซ้ำหรือต่อเติมกับอุปกรณ์ ของบริษัทฯโดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศหรือไม่มีการติดต่อ ประสานงาน และขอคำปรึกษาจากผู้ดูแลระบบก่อนติดตั้ง

4. **การบริหารจัดการข้อมูลองค์กร** (Corporate Management)

4.1 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของ บริษัทฯ หรือเป็นข้อมูลของบุคคลภายนอก

4.2 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัทฯถือเป็นทรัพย์สินของบริษัทฯ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจาก กรรมการผู้จัดการ

5. **การบริหารจัดการระบบสารสนเทศ** (IT Infrastructure Management)

5.1 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit torrent) เป็นต้น เว้นแต่จะได้รับอนุญาตจาก กรรมการผู้จัดการ

5.2 ห้ามเปิดหรือใช้งาน (Run) โปรแกรม ทุกประเภทเพื่อความบันเทิงเช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาทำการของบริษัทฯ

5.3 ห้ามกระทำการใดๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัทฯ โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

5.4 ห้ามกระทำการใดๆ อันมีลักษณะเพื่อจะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

5.5 ห้ามกระทำการใดๆ อันมีลักษณะซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

5.6 ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

5.7 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

5.8 ห้ามเผยแพร่ หรือจัดเก็บข้อมูลที่มีลักษณะลามกอนาจารและขัดต่อศีลธรรมอันดีและห้ามเผยแพร่ข้อมูลภาพตัดต่อเติมหรือดัดแปลงภาพของบุคคลอื่นด้วยวิธีการใด ๆ ซึ่งจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

5.9 ห้ามกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของผู้อื่น

5.10 ห้ามใช้ทรัพย์สินที่เป็นของบริษัทฯเพื่อประโยชน์ทางการค้า

5.11 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัทฯ เกิดการชะลอตัว หรือหยุดชะงัก

6. **การป้องกันโปรแกรมไม่ประสงค์ดี** (Preventing Malware)

6.1 คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus)ตามที่บริษัทฯ ได้กำหนด

6.2 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

6.3 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

6.4 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้ง แก่ผู้ดูแลระบบ

6.5 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายกับระบบสารสนเทศ ของบริษัทฯ

7. **การใช้งานระบบจดหมายอิเล็กทรอนิกส์** (Electronic mail)

7.1 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานโดยยื่นคำขอกับผู้ดูแลระบบ

7.2 ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งาน ในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

7.3 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

7.4 การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

8. **การใช้งาน อินเตอร์เน็ต** (Internet)

8.1 ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับบริษัทฯ

8.2 ห้ามเปิดเผยข้อมูลสาคัญที่เป็นความลับเกี่ยวกับงานของบริษัทฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์ โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

8.3 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ หรือ สื่อสังคมอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัทฯ การทำลายความสัมพันธ์กับบุคลากรของ หน่วยงานอื่นๆ

8.4 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้วให้ปิดเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

9. **การเปิดเผยข้อมูล การยกเลิกหรือสิ้นสุดการให้บริการระบบสารสนเทศ**

9.1 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ อาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้งาน เพื่อปฏิบัติตามกฎหมาย หรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมาย เพื่อปกป้องสิทธิ์หรือทรัพย์สินของบริษัทฯ หรือของผู้ใช้งานอื่น

9.2 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ อาจยกเลิกสิทธิการเข้าใช้งานระบบ หากผู้ใช้งานมิได้เข้าใช้งานในระบบเครือข่าย ภายในระยะเวลาติดต่อกันเกิน 90 วัน

9.3 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศอาจยกเลิกการให้บริการ หากพบว่าผู้ใช้งานละเมิดนโยบายการใช้งาน หรือ ทำให้การให้บริการระบบเครือข่ายขัดข้องโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

10. **ซอฟต์แวร์และลิขสิทธิ์** (Software Licensing and intellectual property)

10.1 บริษัทฯ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทฯ อนุญาตให้ใช้งาน หรือ ที่บริษัทฯ มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและบริษัทฯ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์ อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทฯ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะ ต้องรับผิดชอบแต่เพียงผู้เดียว

10.2 ซอฟต์แวร์ (Software) ที่บริษัทฯ ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไขหรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

11. **การปฏิบัติตามกฎหมายและข้อบังคับ** (Law and Compliance)

บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งนโยบายทางด้านเทคโนโลยีสารสนเทศของบริษัทฯ ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิด ดังนั้นหากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ประกาศ ณ วันที่ 1 มกราคม 2569