นโยบายการกำกับดูแลความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ

(Information and Technology Governance Policy)

บริษัท เดอะ แพลทินัม กรุ๊ป จำกัด (มหาชน)

สารบัญ

1. **หลักการและเหตุผล**

บริษัท เดอะ แพลทินัม กรุ๊ป จำกัด (มหาชน) ("บริษัทฯ") ตระหนักถึงความสำคัญของการนำเทคโนโลยีสารสนเทศ และการสื่อสารซึ่งเป็นปัจจัยสำคัญ ที่ช่วยส่งเสริมการดำเนินธุรกิจ และเพิ่มประสิทธิภาพการทำงานให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ

บริษัทฯ จึงกำหนดนโยบายฉบับนี้ขึ้น เพื่อให้กลุ่มบริษัทมีกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี โดยอ้างอิงจากหลักเกณฑ์และแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ตลอดจนกฎหมายอื่นที่เกี่ยวข้อง มาปรับใช้ให้เหมาะสมกับบริบท การดำเนินธุรกิจของกลุ่ม บริษัท โดยนโยบายการดำเนินการด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัทมี ดังนี้

- **นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**
- **นโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ**

2. **วัตถุประสงค์**

เพื่อให้กลุ่มบริษัท มีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ที่สอดคล้องและเหมาะสมกับการดำเนินธุรกิจ รวมทั้งดูแลให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการสนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความเสี่ยง เพื่อให้กลุ่มบริษัท สามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของบริษัทฯ ได้โดยมีการใช้ทรัพยากรและการบริหารสอดคล้องกับการกำกับดูแลกิจการที่ดี จัดการความเสี่ยงอย่างเหมาะสม

3. **ขอบเขตการบังคับใช้**

นโยบายฉบับนี้มีผลบังคับใช้กับกลุ่มบริษัท โดยนโยบายหลักเกณฑ์ ระเบียบปฏิบัติและคำสั่งที่ใช้อยู่ก่อนนโยบายฉบับนี้ ให้ยังมีผลใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับนโยบายฉบับนี้

4. **คำนิยาม**

บริษัทฯ หมายถึง บริษัท เดอะ แพลทินัม กรุ๊ป จำกัด (มหาชน)

กลุ่มบริษัท หมายถึง บริษัทฯ บริษัทร่วม บริษัทย่อยและกิจการร่วมค้าที่บริษัทฯ มีอำนาจควบคุมในการบริหารจัดการ

ผู้บริหาร หมายถึง ผู้บริหาร ระดับผู้จัดการหน่วยงานขึ้นไป

บุคลากร หมายถึง กรรมการ ผู้บริหาร และพนักงานทุกระดับของบริษัทฯ รวมถึงลูกจ้างโครงการ ลูกจ้างชั่วคราว และลูกจ้างรายวันตามสัญญาจ้าง

นโยบาย หมายถึง นโยบายเทคโนโลยีสารสนเทศ

สายงานเทคโนโลยีสารสนเทศ หมายถึง หน่วยงานตามโครงสร้างของบริษัทฯ ที่มีหน้าที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ และวิศวกรรมระบบเทคโนโลยีสารสนเทศ

ผู้ใช้งาน หรือ ผู้ปฏิบัติงาน หมายถึง พนักงานประจำ พนักงานตามสัญญาจ้าง ผู้รับจ้าง ผู้ให้บริการภายนอก คู่ค้าหรือลูกค้า

ผู้ให้บริการภายนอก หมายถึง บุคคลจากภายนอกบริษัทฯ ซึ่งบริษัทฯ ว่าจ้างเพื่อให้บริการที่เกี่ยวข้องกับระบบสารสนเทศ

ระบบเทคโนโลยีสารสนเทศ หรือ ระบบ IT หรือ ระบบสารสนเทศ หรือ เทคโนโลยีสารสนเทศ หมายถึง ระบบสารสนเทศ ระบบฐานข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบการรักษาความปลอดภัยทางสารสนเทศ (Information Security) ระบบงาน (ซอฟต์แวร์สำเร็จรูป ซอฟต์แวร์ประยุกต์) และระบบสื่อสารของบริษัทฯ ทั้งนี้ไม่ว่าระบบดังกล่าวจะเกี่ยวข้องกับข้อมูลส่วนบุคคลหรือไม่ก็ตาม และหมายรวมถึง “ระบบเครือข่ายและคอมพิวเตอร์” ตามที่กำหนดใน “นโยบายการใช้งานระบบเครือข่ายและคอมพิวเตอร์” (Network and Computer Usage Policy)

สารสนเทศ หรือ ข้อมูลสารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความหรือกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้ รวมถึงข้อมูลส่วนบุคคล

ข้อมูล หมายถึง ข้อมูล ข้อความ สารสนเทศ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย

ข้อมูลส่วนบุคคล มีความหมายตามที่กำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลและตามที่ระบุใน “นโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ”

สินทรัพย์ หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของสายงานเทคโนโลยีสารสนเทศ รวมถึงทรัพย์สินสารสนเทศของบริษัทฯ

ทรัพย์สินสารสนเทศ หมายถึง

1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ
2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด
3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์ และหมายรวมถึงข้อมูลส่วนบุคคลที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์ด้วย
4) ทรัพย์สินสารสนเทศประเภทลิขสิทธิ์ คือ ทรัพย์สินที่เกิดจากการพัฒนา หรือสิทธิ์ในการใช้จากเจ้าของผลิตภัณฑ์

สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล หมายถึง อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยให้การประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอน หรือสถานที่ประมวลผลข้อมูล

5. **บทบาทหน้าที่และความรับผิดชอบ**

สายงานเทคโนโลยีสารสนเทศ

5.1. กำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติที่เกี่ยวข้องกับนโยบาย

5.2. กำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติเฉพาะเรื่องที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์

5.3. ติดตามดูแลให้ผู้ใช้งานปฏิบัติตามนโยบาย หลักเกณฑ์ระเบียบปฏิบัติของบริษัทฯ ที่เกี่ยวข้อง อย่างถูกต้องเหมาะสม และหากมีการปฏิบัติที่ไม่ถูกต้องให้รายงานต่อคณะกรรมการบริหารทราบ

5.4. สื่อสารนโยบายให้แก่ผู้ใช้งาน ผู้ประกอบธุรกิจที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง

6. **นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ** (IT Risk Management)

กลุ่มบริษัทฯ กำหนดให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และครอบคลุมในเรื่องดังต่อไปนี้

6.1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ผู้อำนวยการ/ผู้จัดการสายงานเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ และนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

6.2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)

1) ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้อง มีการควบคุมการเข้า-ออกและการใช้งานการตรวจสอบระบบต่าง ๆ

2) ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของกลุ่มบริษัท เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัย เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจมีชุดคำสั่งไม่พึงประสงค์ ซึ่งรวมถึงมัลแวร์ เช่น ไวรัสคอมพิวเตอร์ เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น

3) ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัท ต้องมีการตรวจสอบและเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต ตรวจสอบและเฝ้าระวังช่องโหว่เชื่อมต่อเครือข่ายภายนอกโดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออก ใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกัน ชุดคำสั่งไม่พึงประสงค์ การกรองข้อมูลรับส่งอีเมล เป็นต้น

4) ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานและการเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่าง ๆ ข้อมูล และข้อมูลส่วนบุคคล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าถึง ใช้ แก้ไข เปลี่ยนแปลง ข้อมูลและข้อมูลส่วนบุคคลโดยมิชอบหรือโดยปราศจากอำนาจ

6.3. การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้

1) ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี
2) ความเสี่ยงจากผู้ปฏิบัติงานหรือความเสี่ยงด้านบุคคล ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลโดยมิชอบหรือปราศจากหรือนอกเหนืออำนาจหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้
3) ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น
4) ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่มีอยู่หรือการนำนโยบายไปปฏิบัติหรือการปฏิบัติงานซึ่งอาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

6.4. การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่กลุ่มบริษัทยอมรับได้ จัดทำตารางลักษณะรายละเอียดความเสี่ยง (Description of Risk) โดยมี หัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

6.5. กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

7. นโยบายการกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของกลุ่มบริษัท ที่ใช้ระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ร่วมกันเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของกลุ่มบริษัท ได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่กลุ่มบริษัท บริษัทฯ จึงประกาศนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

- กลุ่มบริษัท ต้องจัดให้มีหน้าที่ดูแลให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในกลุ่มบริษัท เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้
- กลุ่มบริษัท ต้องจัดให้มีการทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท

การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security)

7.1. แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

วัตถุประสงค์

เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1) ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น
2) ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้งานหรือรหัสผ่านหรือข้อมูลยืนยันตัวตนของผู้อื่นทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
3) ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีมาตรการป้องกันการเข้าถึงของผู้อื่นหรือมาตรการป้องกันการเข้าถึงที่กลุ่มบริษัท กำหนดไว้ เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอกหรือกระทำการอื่นใด โดยปราศจากอำนาจหรือเกินขอบอำนาจ
4) ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน หรือข้อมูลส่วนบุคคลใด ๆ โดยไม่ได้รับอนุญาตจากกลุ่มบริษัท
5) ห้ามรบกวน ขัดขวาง หรือกระทำด้วยประการใด ๆ ให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัทเกิดความเสียหายหรือถูกทำลายหรือไม่สามารถใช้การได้ตามปกติ เช่น การส่งชุดคำสั่งไม่พึงประสงค์ใด ๆ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น
6) ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
7) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาชุดคำสั่งไม่พึงประสงค์ เช่น ไวรัส โปรแกรมป้องกันไวรัสก่อนทุกครั้ง
8) ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตนซึ่งบริษัทฯ กำหนดอนุญาตให้ใช้สิทธิเป็นการเฉพาะตัว

7.2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในกลุ่มบริษัท

แนวทางปฏิบัติ

1) ผู้บริหารระดับสูง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ

2) ผู้อำนวยการ/ผู้จัดการสายงานเทคโนโลยีสารสนเทศ ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในงานระบบเทคโนโลยีสารสนเทศ รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทฯ ใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกลุ่มบริษัท
3) ผู้อำนวยการ/ผู้จัดการสายงานเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตามและทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของกลุ่มบริษัท
4) เจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบด้วย และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา
5) ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของกลุ่มบริษัทในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกลุ่มบริษัท ซึ่งรวมถึงนโยบายการใช้งานระบบเครือข่ายและคอมพิวเตอร์ (Network and Computer Usage Policy) นอกจากนี้จะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และการคุ้มครองข้อมูลส่วนบุคคล

7.3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของกลุ่มบริษัท

แนวทางปฏิบัติ

1) ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ อย่างเป็นลายลักษณ์อักษรสำหรับบุคคลหรือหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศของกลุ่มบริษัท
2) ต้องมีการลงนามในสัญญาระหว่างผู้ปฏิบัติงานและหน่วยงาน ว่าจะไม่เปิดเผยความลับของบริษัทฯ ซึ่งรวมถึงการไม่เปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของบริษัทฯ (Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างผู้ปฏิบัติงานนั้น ๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
3) ในกรณีที่ผู้ปฏิบัติงานซึ่งเป็นบุคคลหรือหน่วยงานภายนอกดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลในระบบสารสนเทศของบริษัทฯ โดยมีลักษณะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องมีการลงนามในสัญญาประมวลผลข้อมูลส่วนบุคคล (Personal data processing agreement) กับผู้ปฏิบัติงานซึ่งข้อสัญญาต้องกำหนดให้ผู้ปฏิบัติงานทำการเฉพาะตามคำสั่งของบริษัทฯ และมีหน้าที่จัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

4) เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด เจ้าหน้าที่บริหารทรัพยากรบุคคลหรือหน่วยงานที่เกี่ยวข้อง ต้องแจ้งให้ผู้จัดการงานระบบเทคโนโลยีสารสนเทศทราบทันที เมื่อมีเหตุดังนี้
    - การว่าจ้างงาน
    - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
    - การลาออกจากงาน หรือการสิ้นสุดการเป็นกรรมการและผู้ปฏิบัติงานของบริษัทฯ
    - การโยกย้ายหน่วยงาน
5) ต้องให้ผู้ใช้งานและหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และนโยบายอื่นที่เกี่ยวข้อง เช่น นโยบายคุ้มครองข้อมูลส่วนบุคคล
6) ผู้ปฏิบัติงานใหม่ของบริษัทฯ ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ
7) หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน การจ้างทำของ การใช้บริการ หรือสิ้นสุดโครงการ ต้องยกเลิกบัญชีผู้ใช้งาน รหัสผ่าน และสิทธิของผู้ใช้งานหรือผู้ปฏิบัติงานในการเข้าถึงข้อมูลรวมทั้งข้อมูลส่วนบุคคลในระบบสารสนเทศทันที

7.4. การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัทฯ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทฯ ให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

1) ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัทฯ ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
2) ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ เพื่อประกอบธุรกิจการค้า หรือบริการใด ๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
3) ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของบริษัทฯ เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจาก ผู้มีอำนาจสูงสุดของหน่วยงาน
4) ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ 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 ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
10) ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
11) การเคลื่อนย้ายเครื่องหรืออุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทฯ ออกนอกบริษัทฯ รวมทั้งต้องปฏิบัติตามข้อกำหนดหรือระเบียบหรือแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มบริษัท (หากมี)
12) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องหรืออุปกรณ์คอมพิวเตอร์ทิ้งไว้ในที่สาธารณะหรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

7.5. การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจการใช้โปรแกรมที่ถูกต้องตามพระราชบัญญัติลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

แนวทางปฏิบัติ

ข้อกำหนดสำหรับผู้ดูแลระบบ

1) มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทฯ ตามสิทธิ์การใช้งานที่กำหนด
2) มีหน้าที่รับผิดชอบในการติดตั้ง และอัปเกรดโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย
3) ทำการถอดและยกเลิกสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัทฯ และ/หรือหน่วยงานแจ้งยกเลิกและ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์

ข้อกำหนดสำหรับผู้ใช้งาน

1) ต้องใช้โปรแกรมคอมพิวเตอร์อย่างเช่นวิญญูชนพึงจะใช้ทรัพย์สินของตนเอง โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับกลุ่มบริษัท
2) โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทฯ เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน
3) ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาตโดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย

4) ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทฯ อย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทฯ มีอยู่มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว นอกจากนี้ หากโปรแกรมที่ไม่ชอบด้วยกฎหมายดังกล่าวส่งผลกระทบให้เกิดการสูญหาย แก้ไขเปลี่ยนแปลง ข้อมูลส่วนบุคคล ผู้ใช้งานอาจต้องมีความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอีกด้วย
5) การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

7.6. การควบคุมทรัพย์สินสารสนเทศและการเข้าใช้งานระบบคอมพิวเตอร์ (Computer Assets and Systems)

วัตถุประสงค์

เพื่อให้สินทรัพย์ของบริษัทฯ และการเข้าใช้งานระบบคอมพิวเตอร์ได้รับการป้องกันและปกป้องอย่างเหมาะสม

แนวทางปฏิบัติ

ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ ข้อมูลสารสนเทศ รวมถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ อยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิหรือผู้ใช้งานที่ทำการเกินขอบอำนาจหน้าที่ และควบคุมไม่ให้มีการเข้าถึงในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

1) ออกจากระบบสารสนเทศ (Log out) โดยทันทีเมื่อเสร็จสิ้นงาน
2) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน
3) ต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย การจัดเก็บข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ในรูปแบบดังนี้
    - ในฐานข้อมูลของระบบ Application นั้น ๆ ที่จัดเก็บภายใน Data Center ของบริษัทฯ การ Export ข้อมูลออกมาจากระบบ Application สามารถทำได้ ตามสิทธิ์ที่ได้รับ
    - สามารถจัดเก็บใน Shared File (Drive กลาง) ใน Folder ตามสิทธิ์ที่ได้รับ
4) ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
5) การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อก (Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 10 นาที
6) ให้มีการขออนุมัติจากผู้มีอำนาจสูงสุดของสายงานขึ้นไป ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึกข้อมูล ข้อมูล อุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกบริษัทฯ ทุกครั้ง โดยปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทฯ ออกนอกบริษัทฯ

7) ระมัดระวังและดูแลทรัพย์สินสารสนเทศและทรัพย์สินอื่นใดของบริษัทฯ ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

7.7. การควบคุมการเข้าถึงข้อมูลระบบเครือข่ายอินเทอร์เน็ต (Internet)

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของกลุ่มบริษัทฯ เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย อีกทั้งเพื่อให้ผู้ใช้งานมีความตระหนักในการใช้งานเว็บไซต์ต่าง ๆ ผ่านระบบเครือข่ายของบริษัทฯ

แนวทางปฏิบัติ

ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูลสารสนเทศ รวมถึงข้อมูลส่วนบุคคล อยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิหรือผู้ใช้งานที่ทำการเกินขอบอำนาจหน้าที่ และควบคุมไม่ให้มีการเข้าถึงในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

1) งานระบบเทคโนโลยีสารสนเทศ ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น
2) เครื่องคอมพิวเตอร์ของบริษัทฯ ก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันโปรแกรมไม่พึงประสงค์ เช่น ไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการก่อน
3) หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
4) ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของกลุ่มบริษัท
5) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับและความลับทางการค้าของกลุ่มบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของกลุ่มบริษัท
6) ห้ามผู้ใช้งานเปิดเผยหรือโอนหรือส่งต่อข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของบริษัทฯ เว้นแต่เป็นการดำเนินการตามขอบเขตของสิทธิและหน้าที่ภายใต้เงื่อนไขของนโยบายนี้และนโยบายคุ้มครองข้อมูลส่วนบุคคลของกลุ่มบริษัท
7) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
8) ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน
9) ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัทฯ เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น

10) ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดสิทธิของบุคคลอื่น ๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อกลุ่มบริษัท รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทฯ ในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติหรือข้อกำหนดหรือระเบียบที่บริษัทฯ กำหนดไว้อย่างเคร่งครัด

7.8. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

วัตถุประสงค์

เพื่อควบคุม มิให้บุคคลใด เข้าถึง ใช้ เปิดเผย หรือแก้ไขเปลี่ยนแปลง ข้อมูลหรือการทำงานของระบบสารสนเทศโดยไม่มีสิทธิหรือไม่มีอำนาจหรือเกินขอบอำนาจหน้าที่

แนวทางปฏิบัติ

การบริหารจัดการข้อมูล

1) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL (Secure Socket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น
2) ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลและข้อมูลสำคัญที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output)
3) ควรมีมาตรการรักษาความปลอดภัยข้อมูลและข้อมูลสำคัญ ซึ่งรวมถึงข้อมูลส่วนบุคคล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัทฯ เช่น ส่งซ่อม โดยมาตรการรักษาความปลอดภัยดังกล่าวรวมถึงการทำลายหรือทำให้ข้อมูลส่วนบุคคลที่เก็บอยู่ในสื่อบันทึกอยู่ในรูปแบบที่ไม่สามารถระบุตัวตนบุคคลได้

การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

1) ต้องควบคุมการเข้าถึงข้อมูล ข้อมูลสำคัญ ข้อมูลส่วนบุคคล และอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิพนักงานหรือบุคคลใดให้เป็นผู้ใช้งานที่มีหน้าที่รับผิดชอบและมีสิทธิเข้าถึงข้อมูลสำคัญและข้อมูลส่วนบุคคล รวมทั้งดำเนินการเพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
2) ต้องกำหนดสิทธิ์การใช้ข้อมูล ข้อมูลสำคัญ ข้อมูลส่วนบุคคล และระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็น ลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

3) ในกรณีมีความจำเป็นต้องใช้ ผู้ใช้งาน หรือ User ที่มีสิทธิ์พิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น บริษัทฯ จะใช้ปัจจัยประกอบการพิจารณาในภาพรวมดังต่อไปนี้

- ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
- ควรควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิ์พิเศษอย่างเข้มงวด เช่น จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็น ในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น
- ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องหรืออุปกรณ์คอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น
- ผู้ใช้งานหรือผู้ปฏิบัติงานที่ได้รับสิทธิเข้าถึงระบบสารสนเทศและระบบเครือข่ายของบริษัทฯ ไม่สามารถอนุญาตหรือให้สิทธิบุคคลอื่น เว้นแต่มีเหตุจำเป็นและเป็นระยะเวลาชั่วคราว โดยต้องมีการขออนุมัติจากผู้บังคับบัญชาหรือผู้มีอำนาจของบริษัทฯ ก่อน ภายใต้เงื่อนไขขั้นตอนหรือวิธีปฏิบัติที่บริษัทฯ กำหนด รวมทั้ง ต้องบันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว
- ในกรณีผู้ใช้งานหรือผู้ปฏิบัติงานได้รับอนุญาตในการให้สิทธิผู้ใช้งานหรือผู้ปฏิบัติงานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลในความรับผิดชอบของตนในกรณีจำเป็นดังกล่าวข้างต้น เช่น การ Share Files ผู้ใช้งานจะต้องให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ์ดังกล่าวทันทีเมื่อสิ้นสุดเหตุความจำเป็น ตามที่ได้รับอนุญาต รวมทั้งต้องบันทึกหลักฐานการให้สิทธิ์ดังกล่าวเพื่อการตรวจสอบด้วย

การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

1) ต้องมีระบบตรวจสอบตัวตนและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศและข้อมูลสารสนเทศ รวมถึงข้อมูลสำคัญและข้อมูลส่วนบุคคล ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัทฯ จะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
2) ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric)
3) ควรใช้อักขระพิเศษประกอบ เช่น : ; < > $ @ # เป็นต้น

4) สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 3 เดือน ส่วนผู้ใช้งานที่มีสิทธิ์พิเศษ เช่น ผู้จัดการระบบ (System Administrator) ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 6 เดือน และผู้ใช้งานที่ติดมากับระบบ (Default User) ควรเปลี่ยนรหัสผ่านทันที
5) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม 3 ครั้งหลังสุด สำหรับระบบที่สามารถกำหนดได้
6) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น “abcdef” “aaaaaa” “123456” “password” “P@ssw0rd” เป็นต้น
7) ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
8) ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
9) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ก่อนการล็อกหรือปิดกั้นบัญชีผู้ใช้งานชั่วคราว ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 3 ครั้ง
10) ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น แยกส่งรหัส โดยตรงกับผู้ใช้งาน
11) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที หรือกำหนดให้ระบบบังคับเปลี่ยนรหัสผ่านใหม่
12) ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรเปิดเผยหรือทำให้ปรากฏแก่การรับรู้ของบุคคลอื่น เช่น ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที
13) ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญและระบบงานที่เกี่ยวข้องกับข้อมูลสำคัญและข้อมูลส่วนบุคคลอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ปฏิบัติงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยนรหัสผ่าน เป็นต้น

7.9. การรักษาความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

การควบคุมการเข้าออกห้องศูนย์กลางข้อมูล (Data Center Room) มีวัตถุประสงค์เพื่อป้องกัน มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ เปิดเผย แก้ไขเปลี่ยนแปลง ทำให้เสียหายหรือทำลาย ข้อมูล ข้อมูลส่วนบุคคล และระบบคอมพิวเตอร์ ส่วนการป้องกันความเสียหาย มีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูล ข้อมูลส่วนบุคคล และระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออก Data Center Room และระบบป้องกันความเสียหายต่าง ๆ ที่บริษัทฯ ควรจัดให้มีภายใน Data Center Room

แนวทางปฏิบัติ

การควบคุมห้องศูนย์กลางข้อมูล (Data Center Room)

1) ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ใน Data Center Room หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิ์การเข้าออก Data Center Room ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้ดูแลระบบ เป็นต้น
2) ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออก Data Center Room ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีผู้ดูแลระบบ และ/หรือผู้ปฏิบัติงานที่เกี่ยวข้องควบคุมดูแลการทำงานตลอดเวลา เป็นต้น
3) ต้องมีระบบเก็บบันทึกการเข้าออก Data Center Room โดยบันทึกดังกล่าว ต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

การป้องกันความเสียหาย

1) ระบบป้องกันไฟไหม้
   - ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา
   - Data Center Room หลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับศูนย์คอมพิวเตอร์สำรอง หรืออย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น
2) ระบบป้องกันไฟฟ้าขัดข้อง
   - ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า
   - ต้องมีระบบสำรองไฟฟ้าสำหรับระบบงานคอมพิวเตอร์ที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์เพื่อให้การดำเนินงานมีความต่อเนื่อง
3) ระบบควบคุมอุณหภูมิและความชื้น
   - ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม
4) ระบบเตือนภัยน้ำรั่ว
   - ในกรณีที่มีการยกระดับพื้นของ Data Center Room เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและ/หรือ สายเครือข่ายด้านล่าง ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา หาก Data Center Room ตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่ว ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่ อย่างสม่ำเสมอ

7.10. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของกลุ่มบริษัท เป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการสูญหาย เข้าถึง ล่วงรู้ เปิดเผย แก้ไขเปลี่ยนแปลง ทำให้เสียหายหรือทำลาย ข้อมูล ข้อมูลส่วนบุคคล และระบบคอมพิวเตอร์ รวมทั้งการป้องกันโปรแกรมไม่พึงประสงค์

แนวทางปฏิบัติ

1) จัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบสารสนเทศที่สำคัญของบริษัทฯ เพื่อป้องกันความผิดพลาดในการปฏิบัติงานด้านสารสนเทศ
2) กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ เป็นต้น
3) ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ
4) ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบสารสนเทศ เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต
5) ระบบที่มีความสำคัญสูง ควรแยกระบบการพัฒนาออกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
6) ต้องสำรวจข้อมูล จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล
7) ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกบริษัทฯ
8) ต้องทดสอบสภาพพร้อมใช้งานระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
9) ต้องมีมาตรการทางเทคนิคและมาตรการทางด้านองค์กรเพื่อป้องกันโปรแกรมไม่พึงประสงค์ เช่น
    - เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพาส่วนบุคคล ก่อนเชื่อมต่อระบบเครือข่ายของบริษัทฯ ต้องติดตั้งโปรแกรมป้องกันโปรแกรมไม่พึงประสงค์ เช่น ไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์
    - ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการและโปรแกรมที่ใช้งานที่ได้มีการออก Patch และ/หรือ Hotfix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่
    - ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอีเมล จะต้องตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
    - ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ที่ทางบริษัทฯ ได้จัดเตรียมไว้ให้ หากต้องการติดตั้งซอฟต์แวร์อื่นนอกเหนือจากที่บริษัทฯ เตรียมไว้ให้ ต้องแจ้งงานระบบเทคโนโลยีสารสนเทศเพื่อตรวจสอบความปลอดภัยก่อนการติดตั้ง

7.11. การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Email)

วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สามารถสนับสนุนการปฏิบัติงานและเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมาย ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของบริษัทฯ ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์ หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

แนวทางปฏิบัติ

ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูลสารสนเทศอยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิหรือผู้ใช้งานที่ทำการเกิน ขอบเขตอำนาจหน้าที่ และควบคุมไม่ให้มีการเข้าถึงในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

1) ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศหรือนโยบายอื่นใดที่บริษัทฯ กำหนด
2) หน่วยงานหรือผู้ปฏิบัติงานผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัทฯ จะต้องใช้จดหมายอิเล็กทรอนิกส์เพื่อผลประโยชน์ของบริษัทฯ ภายใต้ขอบเขตสิทธิการใช้งานที่บริษัทฯ กำหนดเท่านั้น
3) ผู้ปฏิบัติงานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ปฏิบัติงานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรมนุษย์
4) ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่ง ข้อมูล เว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
5) การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
6) การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัทฯ หรือติดต่อกับหน่วยงานหรือบุคคลอื่นใดที่เกี่ยวข้องกับการปฏิบัติงานของบริษัทฯ ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาเป็นหนังสือหรือทางอิเล็กทรอนิกส์แล้วเท่านั้น
7) การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของบริษัทฯ หรือก่อให้เกิดความเสียหายต่อกลุ่มบริษัท

8) ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือกระทบต่อการดำเนินงานของกลุ่มบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของกลุ่มบริษัท
9) ห้ามผู้ใช้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีการกระทำดังกล่าว ให้ถือว่าเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์ หรือเจ้าของบัญชีใช้งานสื่อสังคมออนไลน์ เป็นผู้รับผิดชอบการกระทำดังกล่าวแต่ผู้เดียว
10) ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chain Mail) การส่งจดหมายจำนวนมาก (Spam Mail) การส่งจดหมายต่อเนื่อง (Letter Bomb) การส่งจดหมายเพื่อการแพร่กระจายโปรแกรมไม่พึงประสงค์ เช่น ไวรัสคอมพิวเตอร์ เป็นต้น
11) ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทฯ ให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของกลุ่มบริษัท
12) การส่งข้อมูลข่าวสารที่เป็นความลับหรือความลับทางการค้าของบริษัทฯ รวมถึงข้อมูลส่วนบุคคลของบุคคลใดที่อยู่ในความควบคุมของบริษัทฯ โดยควรมีการเข้ารหัสข้อมูลข่าวสารนั้น และไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
13) ในการใช้ระบบจดหมายอิเล็กทรอนิกส์ส่งข้อมูลใดที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ผู้ใช้จะต้องตรวจสอบการดำเนินการให้สอดคล้องกับนโยบายคุ้มครองข้อมูลส่วนบุคคลของกลุ่มบริษัทด้วย
14) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง
15) ในกรณีบริษัทฯ ได้รับการร้องเรียนหรือร้องขอหรือบริษัทฯ ตรวจสอบพบการกระทำหรือเหตุการณ์ใดที่เกี่ยวข้องกับการใช้ระบบจดหมายอิเล็กทรอนิกส์อันมีความเสี่ยงต่อความไม่ปลอดภัยต่อระบบเครือข่ายและคอมพิวเตอร์ของกลุ่มบริษัท หรือความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล หรือความเสี่ยงต่อการกระทำใด ๆ อันฝ่าฝืนกฎหมาย บริษัทฯ มีสิทธิยกเลิกหรือระงับการบริการชั่วคราวแก่ผู้ใช้งานหรือปฏิบัติงานที่เกี่ยวข้อง เพื่อสอบสวนและตรวจสอบสาเหตุ
16) หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด หรือความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลใด ๆ เกิดขึ้นในบริษัทฯ ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัทฯ
17) การกระทำใด ๆ ที่เกี่ยวข้องกับการเผยแพร่หรือส่งต่อหรือนำเข้าสู่ระบบ ซึ่งข้อมูลทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และโฮมเพจของผู้ใช้บริการให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการเท่านั้น ผู้ดูแลระบบและบริษัทฯ ไม่มีส่วนเกี่ยวข้องใด ๆ

7.12. การรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (Email Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ไม่ละเมิดสิทธิ์กระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวทางปฏิบัติ

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1) ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์สารสนเทศ บริษัทฯ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที
2) ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้
3) ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน
4) ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
5) การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของบริษัทฯ ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
6) การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง
7) การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของบริษัทฯ หรือก่อให้เกิดความเสียหายต่อบริษัทฯ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อเผยแพร่ ข้อมูลข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของบริษัทฯ การส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
8) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

7.13. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

วัตถุประสงค์

เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจากบุคคล รวมทั้งโปรแกรมไม่พึงประสงค์ (Malicious Code) ต่าง ๆ เช่น ไวรัส มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูล ข้อมูลส่วนบุคคล หรือการทำงานของระบบสารสนเทศ

แนวทางปฏิบัติ

การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security Management)

1) กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย
2) ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับบริษัทฯ

การถ่ายโอนข้อมูล (Information Transfer)

1) ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุม การปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
2) ต้องมีการลงนามในสัญญาระหว่างบริษัทฯ และหน่วยงานภายนอกว่าจะไม่เปิดเผยข้อมูลความลับทางการค้าและความลับของบริษัทฯ (Non-Disclosure Agreement: NDA)
3) ในกรณีที่มีการถ่ายโอนข้อมูลสารสนเทศที่เป็นข้อมูลส่วนบุคคลจากบริษัทฯ ไปยังหน่วยงานหรือบุคคลภายนอก จะต้องมีการลงนามในสัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ระหว่างบริษัทฯ และหน่วยงานหรือบุคคลภายนอก ซึ่งกำหนดให้หน่วยงานหรือบุคคลภายนอกต้องทำการเฉพาะตามคำสั่งของบริษัทฯ และ มีหน้าที่รักษาความปลอดภัยของข้อมูลส่วนบุคคลด้วย

7.14. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Network)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

แนวทางปฏิบัติ

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของบริษัทฯ มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1) การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด
2) ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access Point, Wireless Router, Wireless USB Client หรือ Wireless Card
3) ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ Network

กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

1) ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริง ๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)
2) ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง
3) ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย
4) ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration
5) ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point)
6) ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน
7) ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการศูนย์สารสนเทศทราบทันที

7.15. นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

วัตถุประสงค์

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในบริษัทฯ ให้มีความมั่นคงปลอดภัย

แนวทางการปฏิบัติ

แนวทางการปฏิบัติและบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบการบุกรุกเครือข่าย มี ดังนี้

1) IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของบริษัทฯ และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง
2) ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS
3) โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ
4) มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ
5) มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ
6) IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบเทคโนโลยีสารสนเทศตามปกติ
7) เครื่องแม่ข่ายที่มีการติดตั้งโฮสต์เบสไอดี (Host-Based IDS) จะต้องมีการตรวจสอบข้อมูลประจำวัน
8) พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ
9) พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบภายใน 1 ชั่วโมงที่ตรวจพบ
10) การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน
11) มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน
12) บริษัทฯ มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบโดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า
13) ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของบริษัทฯ พยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของบริษัทฯ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

7.16. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ (Integrity Risk) โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้น ซึ่งได้แก่ การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

แนวทางปฏิบัติ

1) ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน
2) ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็น และขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง
3) ในกรณีมีบุคคลหรือหน่วยงานภายนอกบริษัทฯ เข้ามาออกแบบหรือพัฒนาหรือเปลี่ยนแปลงหรือบำรุงรักษาระบบสารสนเทศ และมีความเกี่ยวข้องกับข้อมูลส่วนบุคคล จะต้องมีการลงนามในสัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ระหว่างบริษัทฯ และหน่วยงานหรือบุคคลภายนอก ซึ่งกำหนดให้หน่วยงานหรือบุคคลภายนอกต้องทำการเฉพาะตามคำสั่งของบริษัทฯ และมีหน้าที่รักษาความปลอดภัยของข้อมูลส่วนบุคคลด้วย
4) ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตามการควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

การร้องขอ

1) การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร โดยอาจเป็นการดำเนินการทางอิเล็กทรอนิกส์ (Electronic Transaction) เช่น อีเมล เป็นต้น และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หรือผู้รับผิดชอบระบบสารสนเทศ เป็นต้น
2) ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
3) ควรสอบทานกฎหมายที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎหมาย

การปฏิบัติงานพัฒนาระบบงาน

1) ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น

รวมทั้งการแบ่งส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ การแบ่งส่วนดังกล่าวอาจกระทำโดยแยกใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

2) ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้อง ควรมีส่วนร่วมในกระบวนการออกแบบหรือพัฒนาหรือแก้ไขเปลี่ยนแปลงหรือบำรุงรักษาเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
3) ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

การทดสอบ

1) ผู้ที่ร้องขอและงานระบบเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบทดลอง ตรวจสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

การโอนย้ายระบบงานเพื่อใช้งานจริง

1) ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ
2) ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
3) ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิ์ใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน
4) ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

การทดสอบหลังการใช้งาน (Post-Implementation Test)

ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

การสื่อสารการเปลี่ยนแปลง

ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

7.17. การใช้บริการระบบสารสนเทศจาก ผู้ให้บริการภายนอก (IT Outsourcing)

วัตถุประสงค์

เพื่อเป็นการป้องกันสินทรัพย์ของกลุ่มบริษัทที่มีการเข้าถึงโดย ผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ (IT Outsourcing) และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

แนวทางปฏิบัติ

1) ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัทฯ เมื่อมีความจำเป็นต้องให้ผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ (IT Outsourcing) เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัทฯ โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของบริษัทฯ
2) กรณีที่ขอบเขตการปฏิบัติงานของผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ (IT Outsourcing) นั้นมีส่วนเกี่ยวข้องกับการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล ที่อยู่ในความครอบครองหรือควบคุมของบริษัทฯ จะต้องมีการลงนามในสัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ระหว่างบริษัทฯ และผู้ให้บริการดังกล่าว ซึ่งกำหนดให้ผู้ให้บริการต้องทำการเฉพาะตามคำสั่งของบริษัทฯ และมีหน้าที่จัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลด้วย
3) ต้องสื่อสาร และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัทฯ เมื่อมีความจำเป็นต้องให้ผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ (IT Outsourcing) เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัทฯ ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
4) ในข้อตกลงการให้บริการระหว่างบริษัทฯ และผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ (IT Outsourcing) นั้นจะต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการอย่างสม่ำเสมอ

นโยบายการกำกับดูแลความมั่นคงความปลอดภัยด้านเทคโนโลยีสารสนเทศ ฉบับปรับปรุงนี้ ได้รับการพิจารณาทบทวนและอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 4/2568 เมื่อวันที่ 11 พฤศจิกายน 2568 โดยกำหนดให้มีผลบังคับใช้ตั้งแต่วันที่ 11 พฤศจิกายน 2568 เป็นต้นไป

---- *พลากร สุวรรณรัฐ* ----

นายพลากร สุวรรณรัฐ

ประธานกรรมการบริษัท

วันที่ 11 พฤศจิกายน 2568