นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัท ควิก อีอาร์พี จำกัด

ประวัติการปรับปรุงแก้ไขเอกสาร

ครั้งที่	วันที่	รายละเอียด	ผู้อนุมัติ
00	01/12/2565	จัดทำครั้งแรก	คณะกรรมการบริษัท (07/2565)
01	24/07/2567	ปรับปรุงครั้งที่ 1	คณะกรรมการบริษัท (05/2567)
02	13/08/2567	ปรับปรุงครั้งที่ 2	คณะกรรมการบริษัท (06/2567)
03	12/11/2567	ปรับปรุงครั้งที่ 3	คณะกรรมการบริษัท (07/2567)

สารบัญ

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย และคอมพิวเตอร์ของบริษัท ควิก อีอาร์พี จำกัด (“บริษัทฯ”) ที่ใช้ระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย และสามารถสนับสนุนการดำเนินงานของบริษัทฯ ได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัทฯ

นโยบายฉบับนี้มีผลบังคับใช้กับกรรมการ ผู้บริหาร และพนักงานทุกท่านในบริษัทฯ รวมถึงบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลเทคโนโลยีสารสนเทศของบริษัทฯ ทั้งนี้ บริษัทฯ กำหนดให้มีการสื่อสารนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ แก่เจ้าหน้าที่ ผู้ปฏิบัติงาน และผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบ เพื่อให้เกิดความเข้าใจในความเสี่ยง และปฏิบัติตามนโยบายฉบับนี้

คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้งานในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

1. “บริษัทฯ” หมายความว่า บริษัท ควิก อีอาร์พี จำกัด ที่ใช้ระบบสารสนเทศ และระบบเครือข่ายและคอมพิวเตอร์
2. “ฝ่ายทรัพยากรบุคคล” หมายความว่า ฝ่ายทรัพยากรบุคคล ของ บริษัท ควิก อีอาร์พี จำกัด ซึ่งดูแล การบริหารจัดการด้านทรัพยากรบุคคล ของบริษัทฯ
3. “ฝ่ายเทคโนโลยีสารสนเทศ” หมายความว่า ฝ่ายเทคโนโลยีสารสนเทศของบริษัทฯ
4. “ผู้ใช้งาน” หมายความว่า พนักงาน ผู้ใช้งาน ที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเครือข่ายของบริษัทฯ
5. “ผู้บริหาร” หมายความว่า ประธานเจ้าหน้าที่บริหาร (CEO) หรือผู้ดำรงตำแหน่งระดับบริหารสี่รายแรกนับต่อจากประธานเจ้าหน้าที่บริหาร (CEO) ลงมา และผู้ซึ่งดำรงตำแหน่งเทียบเท่ากับผู้ดำรงตำแหน่งระดับบริหารรายที่สี่ทุกราย และให้หมายความรวมถึงผู้ดำรงตำแหน่งระดับบริหารในสายงานบัญชีหรือการเงินที่เป็นระดับผู้จัดการฝ่ายขึ้นไปหรือเทียบเท่า และให้หมายความรวมถึงกรรมการผู้จัดการตามมาตรา 89/1 ด้วย
6. “ผู้ใช้งานภายนอก” หมายความว่า บุคคล หรือนิติบุคคลที่เป็นคู่สัญญาของบริษัทฯ ที่เข้ามาดำเนินกิจกรรมภายในบริษัทฯ หรือเป็นผู้ใช้งานภายนอกที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเครือข่ายของบริษัทฯ

7. “ผู้ดูแลระบบ” หมายความว่า ประธานเจ้าหน้าที่สายงานเทคโนโลยีสารสนเทศหรือผู้ใช้งานอื่น ที่ได้รับมอบหมายจากผู้บังคับบัญชาระดับประธานเจ้าหน้าที่สายงานเทคโนโลยีสารสนเทศ (Chief Technology Officer) ขึ้นไป ให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และดูแล รักษาระบบสารสนเทศ และระบบเครือข่าย ที่ใช้งานอยู่ในบริษัท หรือหน่วยงานที่มีหน้าที่ และรับผิดชอบในการดูแลระบบสารสนเทศ และระบบเครือข่าย โดยตรง
8. “สารสนเทศ” หมายความว่า ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความหรือกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้
9. “ข้อมูล” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
10. “ระบบสารสนเทศ” หมายความว่า ระบบงานของบริษัทฯ ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟท์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการทำงานของบริษัทฯ
11. “ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัทฯ ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบ Internet และระบบการสื่อสารอื่น ๆ
12. “ทรัพย์สิน” หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับบริษัทฯ ได้แก่ ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟท์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟท์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อบริษัทฯ
13. “ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายของบริษัทฯ โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้าม ปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
14. “สิทธิ์ของผู้ใช้งาน” หมายความว่า ระดับชั้นของการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งาน และผู้ใช้งานภายนอก ได้แก่ สิทธิ์ทั่วไป สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ และระบบเครือข่ายของบริษัทฯ

15. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ
16. “บัญชีผู้ใช้งาน” หมายความว่า บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับผู้ใช้งาน และผู้ใช้งานภายนอก
17. “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
18. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ซึ่งอาจทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
19. “การเข้ารหัส (Encryption)” หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้ จะต้องมี โปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
20. “การยืนยันตัวตน (Authentication)” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบสารสนเทศ และระบบเครือข่าย ซึ่งเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้ว เป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
21. “SSL (Secure Socket Layer)” หมายความว่า เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน
22. “VPN (Virtual Private Network)” หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยใช้การรับส่งข้อมูลจริง ซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะ โดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ ระดับองค์กรที่ดี

(Governance of Enterprise IT)

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ มีจุดมุ่งหมายเพื่อทำให้แน่ใจว่า บริษัทฯ สามารถบรรลุเป้าหมายที่กำหนดไว้ โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุน และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้งานได้อย่างมีประสิทธิภาพ การบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากรและข้อมูลที่มีประสิทธิภาพ เพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายขององค์กรและการบริหารความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่า เทคโนโลยีที่บริษัทฯ นำมาใช้งาน สามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจและสร้างศักยภาพในการแข่งขัน รวมทั้งเพิ่มมูลค่าให้กับบริษัทฯ โดยบริษัทฯ ต้องพิจารณาดำเนินการอย่างน้อยดังต่อไปนี้

1. **การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ** (IT Security Policy)

1.1 บริษัทฯ ต้องจัดให้มีนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และบริษัทฯ ต้องทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในบริษัทฯ เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้

1.2 บริษัทฯ ต้องจัดให้มีการทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

2. **การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ** (IT Risk Management) **ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร** (Corporate Risk Management) **และครอบคลุมในเรื่องดังต่อไปนี้**

2.1 การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

2.2 การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk) ควรครอบคลุมความเสี่ยงสำคัญ เช่น

2.2.1 ระบบสารสนเทศเกิดความเสียหายและไม่สามารถใช้งานได้จนกระทบต่อการดำเนินธุรกิจของบริษัทฯ ได้แก่

- ระบบเครือข่าย ระบบอินเทอร์เน็ตล่มหรือมีปริมาณการใช้งานในระบบเครือข่ายพร้อมกันจำนวนมากจนเครือข่ายหยุดชะงัก
- ผู้ให้บริการระบบ Cloud จากผู้ให้บริการภายนอกไม่สามารถใช้งานได้
- เกิดภัยพิบัติทางธรรมชาติรุนแรง ไม่สามารถควบคุมได้ เช่น อุทกภัยวาตภัย อัคคีภัย แผ่นดินไหว อาคารพังถล่ม เป็นต้น
- กระแสไฟฟ้าขัดข้อง

2.2.2 การนำระบบสารสนเทศไปใช้ผิดวัตถุประสงค์ และ อาจทำให้เกิดความเสียหาย ได้แก่

- ระบบปฏิบัติการไม่สามารถใช้งานได้
- ติด Ransomware มีไวรัสคอมพิวเตอร์ สปายแวร์ โทรจัน เข้าสู่ระบบ
- มีSoftware รบกวนการทำงานของระบบ
- ข้อมูลหรือระบบฐานข้อมูลหรือแฟ้มข้อมูลเสียหายหรือสูญหาย
- ละเมิดลิขสิทธิ์ Software หรือใช้คอมพิวเตอร์ของบริษัทฯ นำเข้าข้อมูลที่ไม่เหมาะสมบนเครือข่าย Social
- ห้อง Server มีบุคคลที่ไม่ได้รับอนุญาติเข้าไปในพื้นที่
- การรั่วไหลของข้อมูลสำคัญของลูกค้า เช่น ข้อมูลส่วนบุคคล หรือข้อมูลความลับทางการค้าของลูกค้า ซึ่งหากเกิดการรั่วไหลของข้อมูล อาจทำให้บริษัทฯ ถูกฟ้องร้องเรียกค่าเสียหาย จนกระทบต่อผลการดำเนินงานของบริษัทฯ ได้

2.3 การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทฯ ยอมรับได้ จัดทำตารางลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

2.4 กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดฝ่ายเทคโนโลยีให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้บริหาร เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

หมวดที่ 2 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security)

1. **แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ** (Information Security Policy)

<u>วัตถุประสงค์</u>

เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และสามารถนำไปปฏิบัติให้เป็นไปตามกฎและระเบียบของบริษัทฯ

<u>แนวทางปฏิบัติ</u>

1.1 ห้าม ผู้ใช้งาน ผู้ใช้งานภายนอก ฝ่ายเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ ใช้ทรัพย์สินและเครือข่ายที่เป็นของบริษัทฯ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น

1.2 ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้

1.3 ห้ามเข้าใช้ระบบสารสนเทศและข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก

1.4 ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของบริษัทฯ โดยไม่ได้รับอนุญาตจากผู้ดูแลข้อมูลนั้น ๆ *(อ้างอิงจากเอกสาร IT101 แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ)*

1.5 ห้ามก่อกวน ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทฯ เกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น

1.6 ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัทฯ และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์

1.7 ผู้ดูแลระบบต้องมีการตั้งค่า ให้ก่อนการใช้งานหรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง

1.8 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในบริษัทฯ

แนวทางปฏิบัติ

2.1 ผู้บริหาร ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ

2.2 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ใช้งานในฝ่ายเทคโนโลยี รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทฯ ใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทฯ

2.3 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ

2.4 ผู้ใช้งานฝ่ายเทคโนโลยีสารสนเทศ ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบสารสนเทศที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบด้วย และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา ทั้งนี้ การขอสร้าง เปลี่ยนแปลง แก้ไข หรือยกเลิกสิทธิที่เป็นผู้ดูแลระบบระดับ Administrator ต้องได้รับอนุมัติจากผู้จัดการฝ่ายเทคโนโลยี และประธานเจ้าหน้าที่สายงานเทคโนโลยีสารสนเทศ (Chief Technology Officer) เท่านั้น

2.5 ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัทฯ ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของบริษัทฯ

แนวทางปฏิบัติ

3.1 ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคคลหรือหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศของบริษัทฯ

3.2 บริษัทฯ กำหนดเกณฑ์ในการตรวจสอบและคัดเลือกพนักงานใหม่อย่างชัดเจน โดยพิจารณาถึงประวัติส่วนตัว ประวัติการศึกษา ประวัติการทำงาน เป็นต้น เพื่อให้มั่นใจว่าบริษัทฯ ได้รับพนักงานที่มีคุณภาพ และลดความเสี่ยงด้านการละเมิดความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

3.3 เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายทรัพยากรบุคคลหรือหน่วยงานที่เกี่ยวข้อง ต้องแจ้งให้ผู้จัดการฝ่ายเทคโนโลยีทราบทันที เมื่อมีเหตุดังนี้

- 3.3.1 การว่าจ้างงาน
- 3.3.2 การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- 3.3.3 การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหารและผู้ใช้งานของบริษัทฯ
- 3.3.4 การโยกย้ายหน่วยงาน

3.4 ผู้ใช้งานใหม่ของบริษัทฯ ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ

3.5 หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ ต้องยกเลิกการเข้าถึงข้อมูลในระบบสารสนเทศทันที โดยผู้ดูแลระบบเป็นผู้ดำเนินการ

4. **การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์** (Computer and Peripheral Access Control)

<u>วัตถุประสงค์</u>

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัทฯ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทฯ ให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

<u>แนวทางปฏิบัติ</u>

4.1 ผู้ใช้งานที่ได้รับมอบทรัพย์สินจากทางบริษัทฯ เช่น เครื่องคอมพิวเตอร์และอุปกรณ์อื่นๆของบริษัทฯ ต้องเป็นผู้รับผิดชอบทรัพย์สิน

4.2 ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ เพื่อประกอบธุรกิจการค้า หรือบริการใด ๆ ที่เป็นของส่วนตัวและไม่เหมาะสม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น

4.3 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัทฯด้วยตนเอง เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน

4.4 ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม

4.5 ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน

4.6 ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน

4.7 หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

4.8 ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อผู้ดูแลระบบในสภาพที่พร้อมใช้งาน

5. การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจการใช้โปรแกรมที่มีลิขสิทธิ์ถูกต้องและปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

แนวทางปฏิบัติ

5.1 ข้อกำหนดสำหรับผู้ดูแลระบบ

5.1.1 ผู้ดูแลระบบมีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทฯ ตามสิทธิ์การใช้ตามหน้าที่การใช้งาน

5.1.2 มีหน้าที่รับผิดชอบในการติดตั้ง และอัพเกรดโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย

5.1.3 ผู้ดูแลระบบทำการถอดและยกเลิกสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัทฯ และ/หรือหน่วยงานแจ้งยกเลิกและ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์

5.2 ข้อกำหนดสำหรับผู้ใช้งาน

5.2.1 ต้องใช้โปรแกรมคอมพิวเตอร์อย่างเช่นวิญญูชนพึงจะใช้ทรัพย์สินของตนเอง โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัทฯ

5.2.2 โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทฯ เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ที่ไม่ใช่ทรัพย์สินของบริษัทฯ หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน

5.2.3 ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย

5.2.4 ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทฯ อย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทฯ มีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้น ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

5.2.5 การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

5.2.6

6. การควบคุมทรัพย์สินด้านสารสนเทศและการเข้าใช้งานระบบคอมพิวเตอร์

วัตถุประสงค์

เพื่อควบคุมไม่ให้ทรัพย์สินอยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์ และที่ไม่มีผู้ใช้งานอุปกรณ์

แนวทางปฏิบัติ

6.1 ต้องควบคุมไม่ให้ทรัพย์สินด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูลสารสนเทศอยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์ ขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

6.1.1 ออกจากระบบสารสนเทศ (Log out) โดยทันทีเมื่อเสร็จสิ้นงาน

6.1.2 มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

6.1.3 ฝ่ายเทคโนโลยีต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญของบริษัทฯ ไว้ในที่ที่ปลอดภัย

6.1.4 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง

6.1.5 การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 10 นาที

6.1.6 ในกรณีที่ต้องการนำทรัพย์สินด้านสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึกข้อมูล ออกนอกบริษัทฯ ต้องมีการแจ้งให้ผู้ดูแลระบบทราบทุกครั้ง

6.1.7 ระมัดระวังและดูแลทรัพย์สินของบริษัทฯ ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

7. การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สามารถสนับสนุนการปฏิบัติงานและเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของบริษัทฯ ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์ หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

แนวทางปฏิบัติ

7.1 ผู้ใช้งานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียน

7.2 หน่วยงานหรือผู้ใช้งานผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัทฯ จะต้องใช้จดหมายอิเล็กทรอนิกส์ เพื่อผลประโยชน์ของบริษัทฯ

7.3 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทฯกำหนด

7.4 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ใช้งานที่ได้รับแจ้งมาจากฝ่ายเทคโนโลยี ต้องไม่ใช้จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่อเปิดอ่าน หรือรับส่งข้อความ

7.5 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น

7.6 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัทฯ ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ขัดข้อง และต้องได้รับอนุญาตจากหัวหน้าแผนกแล้วเท่านั้น

7.7 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัทฯ หรือก่อให้เกิดความเสียหายต่อบริษัทฯ

7.8 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ที่บริษัทฯ มอบหมายให้แก่ผู้ใช้งาน เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อการดำเนินงานของบริษัทฯ ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัทฯ

7.9 ห้ามผู้ใช้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีการกระทำดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์หรือเจ้าของผู้ใช้บริการ เป็นผู้รับผิดชอบการกระทำดังกล่าว

7.10 ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chain mail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์ เป็นต้น

7.11 ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทฯ ให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัทฯ

7.12 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง

7.13 กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่ผู้ใช้งานนั้น ๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ

7.14 หากผู้ใช้งานพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด เกิดขึ้นในบริษัทฯ ให้แจ้งไปที่ผู้บริหารหรือหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ

8. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

การใช้งานระบบเครือข่ายของบริษัทฯ

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของบริษัทฯ เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย และเพื่อให้ผู้ใช้งานมีความตระหนักในการใช้งานเว็บไซต์ต่าง ๆ ผ่านระบบเครือข่ายของบริษัทฯ

<u>แนวทางปฏิบัติ</u>

8.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ตโดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น

8.2 ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดตารางควบคุมสิทธิ (Access Authorization Matrix) เพื่อจำกัดให้ผู้ใช้งานได้เข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศสอบทานและทบทวนตารางควบคุมสิทธิ (Access Authorization Matrix) เป็นประจำอย่างน้อยปีละ 1 ครั้ง

8.3 เครื่องคอมพิวเตอร์ของบริษัทฯ ก่อนทำการเชื่อมต่อระบบเครือข่าย ฝ่ายเทคโนโลยีต้องมีการติดตั้งและตรวจสอบโปรแกรมป้องกันไวรัส

8.4 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

8.5 ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ของผู้ใช้งานที่ได้รับ ตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัทฯ

8.6 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัทฯ ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัทฯ

8.7 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

8.8 ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัทฯ เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น

8.9 ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่น ๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัทฯ รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทฯ ในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทฯ กำหนดไว้อย่างเคร่งครัด

8.10 ผู้ดูแลระบบต้องจัดเก็บข้อมูลและบันทึกหลักฐานการใช้งานอินเตอร์เน็ตโดยผ่านระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ โดยย้อนหลังได้ไม่น้อยกว่า 90 วัน และจัดเก็บข้อมูลให้ครบถ้วนเพียงพอ รวมถึงสามารถนำมายืนยันและระบุตัวตนของ ผู้ใช้งาน และผู้ใช้งานภายนอก ได้ อย่างครบถ้วนชัดเจน

9. **การควบคุมการเข้ารหัสข้อมูล** (Cryptographic Control)

<u>วัตถุประสงค์</u>

เพื่อควบคุมและป้องกันบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ หรือแก้ไขเปลี่ยนแปลง ข้อมูลหรือการทำงานของระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง

<u>แนวทางปฏิบัติ</u>

9.1 การบริหารจัดการข้อมูล

9.1.1 ต้องมีการจัดลำดับชั้นความลับ ต้องมีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการยกเลิกหรือการนำกลับมาใช้ใหม่

9.1.2 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL (Secure Socket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น

9.1.3 ต้องมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัทฯ เช่น ส่งซ่อม เป็นต้น หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

9.2 การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

9.2.1 ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

9.2.2 ต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

9.2.3 ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

9.2.4 ในกรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่น ให้มีสิทธิ์ใช้งานระบบสารสนเทศและระบบเครือข่ายในลักษณะฉุกเฉินหรือชั่วคราว ต้องได้รับการอนุมัติจากผู้บริหารหรือผู้ดูแลระบบทุกครั้งโดยบันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และผู้ดูแลระบบต้องระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

9.2.5 บริษัทฯ ต้องจัดให้ผู้ดูแลระบบทำการตรวจสอบสิทธิ์การเข้าถึงและตรวจสอบบันทึกเหตุการณ์ที่เกี่ยวกับการเข้าใช้งานของผู้ใช้งานบนระบบข้อมูลและระบบงานสารสนเทศอย่างสม่ำเสมอ อย่างน้อยไตรมาสละ 1 ครั้ง

9.3 การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

9.3.1 ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัทฯ จะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

(ก) ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric) และต้องใช้อักขระพิเศษประกอบ เช่น : ; < > $ @ # เป็นต้น

(ข) ฝ่ายเทคโนโลยีสารสนเทศกำหนดให้ผู้ใช้งาน ต้องทำการยืนยันตัวต้นเพิ่มเติมหลังจากทำการยืนยันตัวตนโดยการใช้รหัสผ่าน Multi-factor authentication (MFA) เช่น ยืนยันตัวต้นผ่าน SMS บนมือถือ หรือ ผ่าน App Authenticator

(ค) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น “abcdef” “aaaaaa” “123456” “password” “P@ssw0rd” เป็นต้น

(ง) ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น

(จ) ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

(ฉ) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด (Logon Attempt -Retires) ซึ่งในทางปฏิบัติโดยทั่วไปให้อยู่ที่ 5 ครั้ง หากการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนดไว้ระบบงานหรือโปรแกรมจะไม่อนุญาตหรือระงับการใช้งาน

(ช) ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย

(ซ) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

(ฌ) ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

(ญ) ผู้ใช้งานไม่สามารถกำหนดรหัสผ่านซ้ำเดิมที่เคยใช้ในระยะเวลา 1 ปีได้

(ฎ) บริษัทฯ กำหนดให้รหัสผ่านมีอายุการใช้งาน 6 เดือน โดยผู้ใช้งานจะได้รับอีเมล์แจ้งเตือนหรัสผ่านหมดอายุ และการเปลี่ยนรหัสผ่านล่วงหน้า 7 วัน

(ฏ) สำหรับกรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ Shared Users Licenses เช่นระบบ BC เป็นต้น ทางผู้ดูแลจะมีการส่งอีเมลแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้น เมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด

9.3.2 ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ใช้งานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยน รหัสผ่าน เป็นต้น

10. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

การควบคุมการเข้าออกห้องศูนย์กลางข้อมูล (Data Center Room) มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออก Data Center Room และระบบป้องกันความเสียหายต่าง ๆ ที่บริษัทฯ ควรจัดให้มีภายใน Data Center Room

แนวทางปฏิบัติ

10.1 การควบคุมห้องศูนย์กลางข้อมูล (Data Center Room)

(ก) ผู้ดูแลระบบต้องกำหนดให้พื้นที่สำหรับ จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น หรือ Data center room เป็นพื้นที่หวงห้าม และต้องกำหนดสิทธิ์การเข้าออก Data Center Room ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้ดูแลระบบ ฝ่ายเทคโนโลยีสารสนเทศ เป็นต้น

(ข) ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออก Data Center Room ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีผู้ดูแลระบบ และ/หรือ ผู้ใช้งานที่เกี่ยวข้องควบคุมดูแลการทำงานตลอดเวลา เป็นต้น

(ค) ต้องมีระบบเก็บบันทึกการเข้าออก Data Center Room โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

10.2 การป้องกันความเสียหาย

10.2.1 ระบบป้องกันไฟไหม้

(ก) ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

(ข) Data Center Room หลัก ต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

10.2.2 ระบบป้องกันไฟฟ้าขัดข้อง

(ก) ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า

(ข) ต้องมีระบบสำรองไฟฟ้าสำหรับระบบงานคอมพิวเตอร์ที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์เพื่อให้การดำเนินงานมีความต่อเนื่อง

10.2.3 ระบบควบคุมอุณหภูมิและความชื้น

(ก) ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

11. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของบริษัทฯ เป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการสูญหายของข้อมูล และได้รับการปกป้องจากโปรแกรมไม่ประสงค์ดี

แนวทางปฏิบัติ

11.1 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบสารสนเทศที่สำคัญของบริษัทฯ เพื่อป้องกันความผิดพลาดในการปฏิบัติงานด้านสารสนเทศ และต้องทบทวนคู่มือหรือขั้นตอนปฏิบัติงานดังกล่าวเป็นประจำอย่างน้อยปีละ 1 ครั้ง

11.2 ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบสารสนเทศ เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่ในส่วนของเซิฟเวอร์ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต

11.3 ระบบเทคโนโลยีสารสนเทศที่อยู่ในการพัฒนา ต้องแยกออกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

11.4 ฝ่ายเทคโนโลยีสารสนเทศต้องสำรวจข้อมูล จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล ทั้งนี้ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่การสำรองมาก

11.5 ต้องทดสอบและประเมินสภาพพร้อมใช้งานระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

11.6 ต้องมีมาตรการป้องกันโปรแกรมไม่ประสงค์ดี เช่น

เครื่องคอมพิวเตอร์แบบพกพาส่วนบุคคลของบริษัทฯ ก่อนเชื่อมต่อระบบเครือข่ายของบริษัทฯ ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์

(ก) ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการและโปรแกรมที่ใช้งาน ที่ได้มีการออก Patch และ/หรือ HotFix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่

(ข) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอีเมล จะต้องตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

(ค) ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ที่ทางบริษัทฯ ได้จัดเตรียมไว้ให้ หากต้องการติดตั้งซอฟต์แวร์อื่นนอกเหนือจากที่บริษัทฯ เตรียมไว้ให้ ต้องแจ้งฝ่ายเทคโนโลยีเพื่อตรวจสอบความปลอดภัยก่อนการติดตั้ง

12. **การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่าย** (Communications Security)

<u>วัตถุประสงค์</u>

เพื่อป้องกันข้อมูล สารสนเทศ ระบบสารสนเทศ ในเครือข่ายจากบุคคล ไวรัส รวมทั้ง Malicious Code ต่าง ๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศ

<u>แนวทางปฏิบัติ</u>

12.1 การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security Management)

(ก) กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย

(ข) ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับบริษัทฯ

12.2 การถ่ายโอนข้อมูล (Information Transfer)

(ก) ต้องมีมาตรการในการติดตามและตรวจสอบการปฏิบัติงานและคุณภาพการให้บริการของผู้ให้บริการภายนอก ว่าเป็นไปตามสัญญาและข้อตกลง เช่น ผู้ให้บริการ Cloud บริษัทฯ ตรวจสอบใบรับรองมาตรฐานคุณภาพ ISO 27001 จากเว็บไซต์ผู้ให้บริการ อย่างน้อยปีละ 1 ครั้ง

(ข) ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง อย่างน้อยปีละ 1 ครั้ง

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

วัตถุประสงค์

การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบสารสนเทศที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอจนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

แนวทางปฏิบัติ

13.1 ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

13.2 ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจอนุมัติทุกครั้ง

14. **การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการด้านสารสนเทศ** (IT Outsourcing)

วัตถุประสงค์

เพื่อเป็นการป้องกันทรัพย์สินของบริษัทฯ ที่มีการเข้าถึงโดยผู้รับดำเนินการด้านสารสนเทศ (IT Outsourcing) และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

แนวทางปฏิบัติ

14.1 ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัทฯ เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือทรัพย์สินของบริษัทฯ โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของบริษัทฯ

14.2 ฝ่ายเทคโนโลยีต้องสื่อสาร และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัทฯ เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือทรัพย์สินของบริษัทฯ ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

14.3 ในข้อตกลงการให้บริการ ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ

14.4 หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

15. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ

แนวทางปฏิบัติ

15.1 ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ

15.2 ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน

15.3 หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อฝ่ายเทคโนโลยี

15.4 กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใชงานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

15.5 ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน

15.6 ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

15.7 ต้องจัดเก็บบันทึกหลักฐาน(Log) ได้แก่ บันทึกการเข้าถึงระบบสารสนเทศและระบบงานสารสนเทศ(Access log) และบันทึกหลักฐานการดำเนินงานในระบบสารสนเทศและระบบสารสนเทศ(Activity Log) ของทุกระบบที่บริษัทฯใช้งาน ทั้งนี้รวมถึง บันทึกหลักฐานการเข้าถึงและใช้งานระบบอินเตอร์เน็ตผ่านเครือข่ายคอมพิวเตอร์ของบริษัทฯ โดยจัดเก็บบันทึกหลักฐาน ต้องสามารถตรวจสอบย้อนหลังได้ไม่ได้น้อยกว่า 90 วัน

16. **การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ** (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของบริษัทฯ อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของบริษัทฯ

แนวทางปฏิบัติ

16.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan – BCP) ที่อาจจะเกิดขึ้นกับระบบสารสนเทศของบริษัทฯ

16.2 ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้น อย่างน้อย ปีละ 1 ครั้ง

16.3 ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

การทบทวนนโยบาย

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามที่ระบุในนโยบายฉบับนี้ควรได้รับการทบทวนและปรับปรุงให้สอดคล้องกับสภาพการดำเนินธุรกิจและความเสี่ยงขององค์กร โดยดำเนินการอย่างน้อยปีละ 1 ครั้ง หากมีการแก้ไขที่เป็นสาระสำคัญ

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 12 พฤศจิกายน 2567 เป็นต้นไป

ประกาศ ณ วันที่ 12 พฤศจิกายน 2567

_____

(ผศ.ดร.อัครวิทย์ กาญจนโอภาษ)

ประธานกรรมการบริษัท

บริษัท ควิก อีอาร์พี จำกัด