



นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยี

สารสนเทศ

บริษัท ยูโรเอเชีย โทเทิล โลจิสติกส์ จำกัด (มหาชน)

ฉบับที่ 4

ประกาศใช้เมื่อวันที่ 20 กุมภาพันธ์ 2568



ประวัติการจัดทำและอนุมัติ

หมายเลขเอกสาร	ผู้จัดทำ/ผู้ควบคุม	ผู้สอบทาน	ผู้อนุมัติ
CP-BOD-024-01	กรรมการผู้จัดการ	ประธานเจ้าหน้าที่บริหาร	คณะกรรมการบริษัท
	3 มกราคม 2568	30 มกราคม 2568	20 กุมภาพันธ์ 2568

ประวัติการแก้ไขและยกเลิก

ฉบับที่	วันที่จัดทำหรือแก้ไข	วันที่ประกาศใช้	รายละเอียดการเปลี่ยนแปลง
1	10 ตุลาคม 2564	9 พฤศจิกายน 2564	ฉบับแรก
2	5 มกราคม 2565	19 กุมภาพันธ์ 2565	ขั้นตอนการปฏิบัติงานการจัดลำดับชั้นข้อมูล
3	10 มิถุนายน 2565	6 สิงหาคม 2565	แก้ไขชื่อบริษัท ภายหลังการแปรสภาพเป็นบริษัทมหาชน จำกัด
4	3 มกราคม 2568	20 กุมภาพันธ์ 2568	พิจารณาบทบทวนประจำปี 2568

หมายเหตุ: การเพิ่มเติมหรือยกเลิกเอกสารใด ให้ดำเนินการตามที่กำหนดไว้ในระเบียบอำนาจอนุมัติและดำเนินการ



นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย และคอมพิวเตอร์ของบริษัท ยูโรเอเชีย โทเทิล โลจิสติกส์ จำกัด (มหาชน) (“บริษัท”) และบริษัทย่อยที่ใช้ระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ร่วมกันเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้อง สอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัท บริษัทจึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้ในงานนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

1. “บริษัท” หมายความว่า บริษัท ยูโรเอเชีย โทเทิล โลจิสติกส์ จำกัด (มหาชน) และบริษัทย่อย ที่ใช้ระบบสารสนเทศ และระบบเครือข่ายและคอมพิวเตอร์ร่วมกัน
2. “ฝ่ายทรัพยากรบุคคล” หมายความว่า ฝ่ายทรัพยากรบุคคลของบริษัทซึ่งดูแลการบริหารจัดการด้านทรัพยากรบุคคล
3. “ฝ่ายเทคโนโลยี” หมายความว่า ฝ่ายเทคโนโลยีของบริษัท
4. “ผู้ใช้งาน” หมายความว่า กรรมการบริษัท ผู้บริหาร ผู้ปฏิบัติงาน และผู้ใช้งานภายนอก ที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเครือข่ายของบริษัท
5. “ผู้ปฏิบัติงาน” หมายความว่า พนักงาน หรือลูกจ้างของบริษัท
6. “ผู้ใช้งานภายนอก” หมายความว่า บุคคล หรือนิติบุคคลที่เป็นคู่สัญญาของบริษัทที่เข้ามาดำเนินกิจกรรมภายในบริษัท
7. “ผู้ดูแลระบบ” หมายความว่า ผู้จัดการฝ่ายเทคโนโลยี หรือผู้ปฏิบัติงานอื่น ซึ่งมีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และดูแลรักษาระบบสารสนเทศ และระบบเครือข่ายที่ ใช้งานอยู่ในบริษัท หรือหน่วยงานที่มีหน้าที่และรับผิดชอบในการดูแลระบบสารสนเทศและระบบเครือข่าย โดยตรง
8. “สารสนเทศ” หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ เอกสาร แผนผัง แผนที่ ภาพถ่าย ฟิล์ม การบันทึกภาพ การบันทึกเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
9. “ระบบสารสนเทศ” หมายความว่า ระบบงานของบริษัท ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผนการบริหาร และการสนับสนุนกลไกการทำงานของบริษัท

Euroasia Total Logistics Public Company Limited

19, 21 Motorway Road, Klongsontoonnoon,

Lat Krabang, Bangkok, 10520 Thailand

Tel: (662) 123 1727

Website: www.etl.co.th

บริษัท ยูโรเอเชีย โทเทิล โลจิสติกส์ จำกัด (มหาชน)

19, 21 ถนนมอเตอร์เวย์ แขวงคลองสองต้นนุ่น

เขตลาดกระบัง กรุงเทพมหานคร 10520

โทรศัพท์: (662) 123 1727

เว็บไซต์: www.etl.co.th



10. **"ระบบเครือข่าย"** หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัท ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบ Internet และระบบการสื่อสารอื่น ๆ
11. **"สินทรัพย์"** หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับบริษัท ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อบริษัท
12. **"ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ"** หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายของบริษัท โดยอ้างไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (non-Repudiation) และความน่าเชื่อถือ (Reliability)
13. **"สิทธิของผู้ใช้งาน"** หมายความว่า ระดับขั้นของการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งาน และผู้ใช้งานภายนอก ได้แก่ สิทธิทั่วไป สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ และระบบเครือข่ายของบริษัท
14. **"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ"** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ
15. **"บัญชีผู้ใช้งาน"** หมายความว่า บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับผู้ใช้งาน และผู้ใช้งานภายนอก
16. **"เหตุการณ์ด้านความมั่นคงปลอดภัย"** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
17. **"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด"** หมายความว่า สถานการณ์ซึ่งอาจทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
18. **"การเข้ารหัส (Encryption)"** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสได้ จะต้องใช้ โปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
19. **"การยืนยันตัวตน (Authentication)"** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้ว เป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
20. **"SSL (Secure Socket Layer)"** หมายความว่า เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน



21. "VPN (Virtual Private Network)" หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยใช้การรับส่งข้อมูลจริง ซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะ โดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง



หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ ระดับองค์กรที่ดี (Governance of Enterprise IT)

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ มีจุดมุ่งหมายเพื่อให้แน่ใจว่าบริษัทสามารถบรรลุเป้าหมายที่กำหนดไว้ โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุน และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้งานได้อย่างมีประสิทธิภาพ การบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากรและข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายขององค์กรและการบริหารความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่าเทคโนโลยีที่บริษัทนำมาใช้งานสามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจและสร้างศักยภาพในการแข่งขัน รวมทั้งเพิ่มมูลค่าให้กับบริษัท โดยบริษัทต้องพิจารณาดำเนินการอย่างน้อยดังต่อไปนี้

1. นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

1.1 บริษัทต้องจัดให้มีหน้าที่ดูแลให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และบริษัทต้องทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในบริษัท เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้

1.2 บริษัทต้องจัดให้มีการทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

2. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และครอบคลุมในเรื่องดังต่อไปนี้

2.1 การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เจ้าหน้าที่ฝ่ายเทคโนโลยีมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

2.2 การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk) ควรครอบคลุมความเสี่ยงสำคัญ เช่น

2.2.1 ความเสี่ยงจากบุคลากร

2.2.2 ความเสี่ยงจาก Software และข้อมูล

2.2.3 ความเสี่ยงจากระบบเครือข่ายและอินเทอร์เน็ต

Euroasia Total Logistics Public Company Limited

19, 21 Motorway Road, Klongsontongnoon,

Lat Krabang, Bangkok, 10520 Thailand

Tel: (662) 123 1727

Website: www.etl.co.th

บริษัท ยูโรเอเชีย โลจิสติกส์ จำกัด (มหาชน)

19, 21 ถนนมอเตอร์เวย์ แขวงคลองสองต้นนุ่น

เขตลาดกระบัง กรุงเทพมหานคร 10520

โทรศัพท์: (662) 123 1727

เว็บไซต์: www.etl.co.th



2.2.4 ความเสี่ยงจาก Hardware และอุปกรณ์คอมพิวเตอร์

2.2.5 ความเสี่ยงจากการเงิน

2.2.6 ความเสี่ยงจากอุทกภัย วาตภัย

2.2.7 ความเสี่ยงจากแผ่นดินไหว อาการพังถล่ม

2.2.8 ความเสี่ยงจากอัคคีภัย

2.2.9 ความเสี่ยงจากการโจรกรรม

2.2.10 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง

2.3 การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้ จัดทำตารางลักษณะรายละเอียด ความความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

2.4 กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

หมวดที่ 2 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security)

1. แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ (Information Security Policy)

วัตถุประสงค์

เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1.1 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น

1.2 ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้

1.3 ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก

Euroasia Total Logistics Public Company Limited

19, 21 Motorway Road, Klongsontongnoon,

Lat Krabang, Bangkok, 10520 Thailand

Tel: (662) 123 1727

Website: www.etl.co.th

บริษัท ยูโรเอเชีย โลจิสติกส์ จำกัด (มหาชน)

19, 21 ถนนมอเตอร์เวย์ แขวงคลองสองต้นนุ่น

เขตลาดกระบัง กรุงเทพมหานคร 10520

โทรศัพท์: (662) 123 1727

เว็บไซต์: www.etl.co.th



- 1.4 ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้น ๆ
- 1.5 ห้ามก่อวินาศกรรม หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น
- 1.6 ห้ามลักลอบดักจับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
- 1.7 ก่อนการใช้งานสื่อบันทึกทุกประเภทต่าง ๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง
- 1.8 ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในบริษัท

แนวทางปฏิบัติ

- 2.1 ผู้บริหารระดับสูง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท
- 2.2 หัวหน้าฝ่ายเทคโนโลยี ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในฝ่ายเทคโนโลยี รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท
- 2.3 หัวหน้าฝ่ายเทคโนโลยี เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท
- 2.4 ผู้ปฏิบัติงานฝ่ายเทคโนโลยีที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบด้วย และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา
- 2.5 ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัท ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตลอดจนกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล



3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของบริษัท

แนวทางปฏิบัติ

- 3.1 ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคคลหรือหน่วยงานภายนอกที่จ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท
- 3.2 ต้องมีการลงนามในสัญญาระหว่างผู้ใช้งานและหน่วยงานว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างผู้ใช้งานนั้น ๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
- 3.3 เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายทรัพยากรบุคคลหรือหน่วยงานที่เกี่ยวข้อง ต้องแจ้งให้หัวหน้าฝ่ายเทคโนโลยีทราบทันที เมื่อมีเหตุดังนี้
 - 3.3.1 การว่าจ้างงาน
 - 3.3.2 การเปลี่ยนแปลงสภาพการว่าจ้างงาน
 - 3.3.3 การลาออกจากงาน หรือการสิ้นสุดการเป็นกรรมการและผู้ใช้งานของบริษัท
 - 3.3.4 การโยกย้ายหน่วยงาน
- 3.4 ต้องให้ผู้ใช้งานและหน่วยงานภายนอกที่จ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- 3.5 ผู้ปฏิบัติงานใหม่ของบริษัทต้องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ
- 3.6 หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ ต้องยกเลิกการเข้าถึงข้อมูลในระบบสารสนเทศทันที



4. การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

- 4.1 ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
- 4.2 ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใด ๆ ที่เป็นของส่วนตัว และไม่เหมาะสม
- 4.3 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
- 4.4 ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
- 4.5 ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อนชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
- 4.6 ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- 4.7 ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน
- 4.8 ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่
- 4.9 หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- 4.10 ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
- 4.11 การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
- 4.12 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย



5. การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจการใช้โปรแกรมที่ถูกต้องลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง

แนวทางปฏิบัติ

5.1 ข้อกำหนดสำหรับผู้ดูแลระบบ

- 5.1.1 มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทตามสิทธิการใช้งานที่กำหนด
- 5.1.2 มีหน้าที่รับผิดชอบในการติดตั้ง และอัปเดตโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย
- 5.1.3 ทำการถอดและยกเลิกสิทธิการใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัทและ/หรือหน่วยงานแจ้งยกเลิก และ/หรือย้ายสิทธิการใช้งานโปรแกรมคอมพิวเตอร์

5.2 ข้อกำหนดสำหรับผู้ใช้งาน

- 5.2.1 ต้องใช้โปรแกรมคอมพิวเตอร์อย่างเช่นวิญญูชนพึงจะใช้ทรัพย์สินของตนเอง โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัท
- 5.2.2 โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งาน
- 5.2.3 ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย
- 5.2.4 ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทมีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- 5.2.5 การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี



6. การควบคุมสินทรัพย์ด้านสารสนเทศและการใช้งานระบบคอมพิวเตอร์

วัตถุประสงค์

เพื่อควบคุมไม่ให้สินทรัพย์ด้านสารสนเทศอยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ ขณะที่ไม่มีผู้ใช้งานอุปกรณ์

แนวทางปฏิบัติ

6.1 ต้องควบคุมไม่ให้สินทรัพย์ด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูลสารสนเทศ อยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ ขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

6.1.1 ออกจากระบบสารสนเทศ (Log Out) โดยทันทีเมื่อเสร็จสิ้นงาน

6.1.2 มีการป้องกันเครื่องคอมพิวเตอร์ โดยการใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนการใช้งาน

6.1.3 ต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย การจัดเก็บข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ในรูปแบบดังนี้

(ก) ในฐานข้อมูลของระบบ Application นั้น ๆ ที่จัดเก็บภายใน Data Center ของบริษัท การ Export ข้อมูลออกจากระบบ Application ไม่สามารถทำได้

(ข) สามารถจัดเก็บใน Shared File (Drive กลาง) ใน Folder ตามสิทธิที่ได้รับ

6.1.4 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง

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

6.1.6 ให้มีการขออนุมัติจากผู้มีอำนาจสูงสุดของฝ่ายขึ้นไป ในกรณีที่ต้องการนำทรัพย์สินด้านสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกบริษัททุกครั้ง โดยปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท

6.1.7 ระวังระวังและดูแลทรัพย์สินของบริษัทที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเล็กน้อย ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

6.1.8 ติด tag ไว้ที่อุปกรณ์คอมพิวเตอร์ และคอมพิวเตอร์อันเป็นสินทรัพย์ของบริษัท



7. การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารจดหมายอิเล็กทรอนิกส์ สามารถสนับสนุนการปฏิบัติงานและเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมาย ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัย ข้อมูลข่าวสารของบริษัท ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่าย อินเทอร์เน็ต โดยผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ หรือกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

แนวทางปฏิบัติ

- 7.1 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทกำหนด
- 7.2 หน่วยงาน หรือผู้ใช้งาน ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์เพื่อผลประโยชน์ของบริษัท
- 7.3 ผู้ใช้งานจะได้รับสิทธิในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ให้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ใช้งานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรบุคคล
- 7.4 ไม่ให้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ
- 7.5 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
- 7.6 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
- 7.7 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่นยุยง เสียชื่อเสียง ในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท
- 7.8 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อการดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัท



7.9 ห้ามผู้ให้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีกระทำความดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ หรือเจ้าของผู้ให้บริการ เป็นผู้รับผิดชอบการกระทำความดังกล่าว

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

7.11 ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัท

7.12 การส่งข้อมูลข่าวสารที่เป็นความลับบริษัท ควรมีการเข้ารหัสข้อมูลข่าวสารนั้น

7.13 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง

7.14 กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่ผู้ใช้นั้น ๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ

7.15 หากผู้ให้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด เกิดขึ้นในบริษัท ให้แจ้งเบาะแสไปที่กรรมการผู้จัดการ อีเมล krishavan@etlgps.com

8. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control) การใช้งานระบบเครือข่ายของบริษัท

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของบริษัท เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย และเพื่อให้ผู้ใช้งานมีความตระหนักในการใช้งานเว็บไซต์ต่าง ๆ ผ่านระบบเครือข่ายของบริษัท

แนวทางปฏิบัติ

8.1 ฝ่ายเทคโนโลยี ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น

8.2 เครื่องคอมพิวเตอร์ของบริษัท ก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการก่อน

8.3 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

8.4 ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัท

Euroasia Total Logistics Public Company Limited

19, 21 Motorway Road, Klongsontongnoon,

Lat Krabang, Bangkok, 10520 Thailand

Tel: (662) 123 1727

Website: www.etl.co.th

บริษัท ยูโรเอเชีย โทเทิล โลจิสติกส์ จำกัด (มหาชน)

19, 21 ถนนมอเตอร์เวย์ แขวงคลองสองต้นนุ่น

เขตลาดกระบัง กรุงเทพมหานคร 10520

โทรศัพท์: (662) 123 1727

เว็บไซต์: www.etl.co.th



8.5 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัท

8.6 ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

8.7 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน

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

8.9 ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่น ๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัท รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด

9. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล้วงรู้ หรือแก้ไขเปลี่ยนแปลง ข้อมูลหรือการทำงานของระบบสารสนเทศในส่วนที่มีได้มีอำนาจหน้าที่เกี่ยวข้อง

แนวทางปฏิบัติ

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 ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเกี่ยวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

9.1.4 ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม เป็นต้น หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

9.1.5 ขั้นตอนการปฏิบัติงานเกี่ยวกับการจัดลำดับชั้นข้อมูล

ลำดับชั้นข้อมูล	คุณลักษณะ	ตัวอย่าง	ระดับการปกป้องข้อมูล
ข้อมูลที่เป็นความลับมาก	- มีความสำคัญต่อองค์กรในระดับสูงมาก - หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลกระทบต่อองค์กรในระดับสูงมาก - เกี่ยวข้องกับแผนกลยุทธ์ และทิศทางหลักในการดำเนินธุรกิจ - จำเป็นต้องมีมาตรการควบคุมการเผยแพร่ข้อมูลที่เข้มงวด โดยพิจารณาจำกัดรายชื่อผู้ได้รับอนุญาตให้เข้าถึงอย่างรอบคอบ	- แผนการควบคุมรวมกิจการ กลยุทธ์ การลงทุน กลยุทธ์ทางการตลาด - แผนธุรกิจ และทิศทางดำเนินธุรกิจ	ต้องปกป้องข้อมูล ให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น (Highest Security level)
ข้อมูลที่เป็นความลับ	- มีความสำคัญต่อองค์กรในระดับสูง - หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลกระทบต่อองค์กร - เกี่ยวข้องกับทิศทางการปฏิบัติงานขององค์กร (มีผลในช่วงเวลาหนึ่ง) - จำเป็นต้องมีมาตรการควบคุมการเผยแพร่ข้อมูลที่เข้มงวด โดยจำกัดการเข้าถึงให้กับกลุ่มคนบางกลุ่มเท่านั้น และต้องได้รับการปกป้องอย่างเหมาะสม	- ข้อมูลเกี่ยวกับรายได้ ต้นทุน กำไร หรือข้อมูลทางการเงินอื่นๆ - แผนการปฏิบัติงาน - ข้อมูลเกี่ยวกับลูกค้า และพันธมิตรทางธุรกิจ - ข้อมูลส่วนตัวพนักงาน - รหัสผ่านของบัญชีผู้ใช้งานระบบสำคัญ - Network Diagram	ต้องปกป้องข้อมูลจากการเข้าถึงโดยบุคคลภายนอก และบุคคลที่ไม่ได้รับอนุญาต (High Security Level)



ข้อมูลที่ใช้ภายใน	- ข้อมูลทางธุรกิจ ข้อมูลที่ใช้งานภายในองค์กร และไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกองค์กร - หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลกระทบต่อองค์กรในระดับต่ำ	- กฎและข้อบังคับ - Operational Manual - Standard Operating Procedures	ต้องปกป้องข้อมูลจากการเข้าถึงโดยบุคคลภายนอก (Normal Security Level)
ข้อมูลที่เปิดเผยต่อสาธารณชนได้	- ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความมั่นคงปลอดภัยเป็นพิเศษ - ข้อมูลสำหรับการเผยแพร่ต่อสาธารณชน ผ่านช่องทางที่เหมาะสมซึ่งองค์กรพิจารณาอนุมัติแล้ว	- ข้อมูลที่มีการเผยแพร่ผ่านเว็บไซต์แล้ว - ข้อมูลจากการแถลงข่าว หรือรายงานประจำที่มีการเผยแพร่สาธารณะชนแล้ว	ปกป้องเฉพาะความถูกต้องครบถ้วนของข้อมูล

9.2 การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

9.2.1 ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนด โดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

9.2.2 ต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิการใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

9.2.3 ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิ์พิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น บริษัทจะใช้ปัจจัยประกอบการพิจารณาในภาพรวมดังต่อไปนี้

- (ก) ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
- (ข) ควรควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิ์พิเศษอย่างเข้มงวด เช่น จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- (ค) ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว



(ง) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการทำงาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ควรเปลี่ยนรหัสผ่านทุก 2 เดือน เป็นต้น

9.2.4 ในกรณีที่ไม่มีกรปฏิบัติการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มีได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่ไม่ได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

9.2.5 ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิ์ผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้ สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ์ดังกล่าวในกรณีที่ผู้ใช้งานไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิ์ดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

9.2.6 ในกรณีที่ความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิ์ใช้งานระบบสารสนเทศและระบบเครือข่ายในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

9.3 การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

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

(ก) ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric)

(ข) ควรใช้อักขระพิเศษประกอบ เช่น: <>\$@# เป็นต้น

(ค) ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 2 เดือน

(ง) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม 3 ครั้งหลังสุด

(จ) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น "abcdef" "aaaaaa" "123456" "password" "P@ssword" เป็นต้น

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

(ช) ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม



(ซ) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด (Logon Attempt -Retires) ซึ่งในทางปฏิบัติโดยทั่วไปให้อยู่ที่ 5 ครั้ง หากการใส่รหัสผ่านผิดเป็นจำนวนครั้งที่กำหนดไว้ระบบงานหรือโปรแกรมจะไม้อนุญาตหรือระงับการใช้งาน

(ณ) ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น

(ญ) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

(ฎ) ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการลวงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

(ฏ) สำหรับกรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ Shared Users Licenses ทางผู้ดูแลจะมีการส่งอีเมลแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้น เมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด

9.3.2 ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการลวงรู้หรือแก้ไขเปลี่ยนแปลง

9.3.3 ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มีได้สิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ใช้งานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยนรหัสผ่าน เป็นต้น

10. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

การควบคุมการเข้าออกห้องศูนย์กลางข้อมูล (Data Center Room) มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ลวงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ สำหรับการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออก Data Center Room และระบบป้องกันความเสียหายต่างๆ ที่บริษัทควรจัดให้มีภายใน Data Center Room



แนวทางปฏิบัติ

10.1 การควบคุมห้องศูนย์กลางข้อมูล (Data Center Room)

10.1.1 ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ใน Data Center Room หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิ์การเข้าออก Data Center Room ให้เฉพาะ บุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้ดูแลระบบ เป็นต้น

10.1.2 ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออก Data Center Room ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีผู้ดูแลระบบ และ/หรือ ผู้ใช้งานที่เกี่ยวข้อง ควบคุมดูแลการทำงาน ตลอดเวลา เป็นต้น

10.1.3 ต้องมีระบบเก็บบันทึกการเข้าออก Data Center Room โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

10.1.4 ควรจัด Data Center Room ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ส่วนเครื่องสำรองไฟฟ้า (UPS Zone) ส่วนแบตเตอรี่เครื่องสำรองไฟฟ้า (Battery UPS Zone) เป็นต้น เพื่อความสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญ ต่างๆ มีประสิทธิภาพมากขึ้น

10.2 การป้องกันความเสียหาย

10.2.1 ระบบป้องกันไฟไหม้

(ก) ต้องมีอุปกรณ์เตือนไฟไหม้เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

(ข) Data Center Room หลักต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

(ค) ระบบป้องกันไฟฟ้าขัดข้อง

(ง) ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า

(จ) ต้องมีระบบสำรองไฟฟ้าสำหรับระบบงานคอมพิวเตอร์ที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์ เพื่อให้การดำเนินงานมีความต่อเนื่อง

(ฉ) ระบบควบคุมอุณหภูมิและความชื้น

(ช) ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศ และตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม



11. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของบริษัทเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการสูญหายของข้อมูลและได้รับการปกป้องจากโปรแกรมไม่ประสงค์ดี

แนวทางปฏิบัติ

- 11.1 จัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบสารสนเทศที่สำคัญของบริษัท เพื่อป้องกันความผิดพลาดในการปฏิบัติงานด้านสารสนเทศ
- 11.2 กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ เป็นต้น
- 11.3 ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ
- 11.4 ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบสารสนเทศ เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต
- 11.5 ระบบที่มีความสำคัญสูง ควรแยกระบบการพัฒนารอกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
- 11.6 ต้องสำรองข้อมูล จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล
- 11.7 ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีการสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกบริษัท
- 11.8 ต้องทดสอบสภาพพร้อมใช้งานระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
- 11.9 ต้องมีมาตรการป้องกันโปรแกรมไม่ประสงค์ดี เช่น
 - (ก) เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพาส่วนบุคคล ก่อนเชื่อมต่อระบบเครือข่ายของบริษัท ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์
 - (ข) ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการและโปรแกรมที่ใช้กันอย่างสม่ำเสมอ โดยสามารถดาวน์โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่
 - (ค) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอีเมล จะต้องตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
 - (ง) ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ที่ทางบริษัทได้จัดเตรียมไว้ให้ หากต้องการติดตั้งซอฟต์แวร์อื่นนอกเหนือจากที่บริษัทเตรียมไว้ให้ ต้องแจ้งฝ่ายเทคโนโลยีเพื่อตรวจสอบความปลอดภัยก่อนการติดตั้ง



12. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

วัตถุประสงค์

เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจากบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศ

แนวทางปฏิบัติ

12.1 การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security Management)

- (ก) กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย
- (ข) ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้งานนอกที่ติดต่อกับบริษัท

12.2 การถ่ายโอนข้อมูล (Information Transfer)

- (ก) ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
- (ข) ต้องมีการลงนามในสัญญาระหว่างบริษัทและหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของ บริษัท (Non-Disclosure Agreement: NDA)
- (ค) ต้องมีมาตรการในการติดตามและตรวจสอบการปฏิบัติงานและคุณภาพการให้บริการของผู้ให้บริการภายนอกว่าเป็นไปตามสัญญาและข้อตกลง

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

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไข เปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอจนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไข เปลี่ยนแปลงไปใช้งานจริง



แนวทางปฏิบัติ

13.1 ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

13.2 ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

13.3 ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

13.4 การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

13.4.1 การร้องขอ

(ก) การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร โดยอาจเป็น Electronic Transaction เช่น อีเมล เป็นต้น และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หรือผู้รับผิดชอบระบบสารสนเทศ เป็นต้น

(ข) ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง

(ค) ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณี อาจส่งผลกระทบต่อการใช้ปฏิบัติตามกฎเกณฑ์ของทางการ

13.4.2 การปฏิบัติงานพัฒนาระบบงาน

(ก) ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

(ข) ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานภายนอก ควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

(ค) ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

Euroasia Total Logistics Public Company Limited

19, 21 Motorway Road, Klongsontongnoon,

Lat Krabang, Bangkok, 10520 Thailand

Tel: (662) 123 1727

Website: www.etl.co.th

บริษัท ยูโรเอเชีย โลจิสติกส์ จำกัด (มหาชน)

19, 21 ถนนมอเตอร์เวย์ แขวงคลองสองต้นนุ่น

เขตลาดกระบัง กรุงเทพมหานคร 10520

โทรศัพท์: (662) 123 1727

เว็บไซต์: www.etl.co.th



13.4.3 การทดสอบ

(ก) ผู้ที่ร้องขอและฝ่ายเทคโนโลยี รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบเพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

13.4.4 การโอนย้ายระบบงานเพื่อใช้งานจริง

(ก) ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

(ข) การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา

(ค) ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

(ง) ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

(จ) ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

13.4.5 การทดสอบหลังการใช้งาน (Post-Implementation Test)

(ก) ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน

13.4.6 การสื่อสารการเปลี่ยนแปลง

(ก) ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานภายนอกได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้ถูกต้อง



14. การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการด้านสารสนเทศ (IT Outsourcing)

วัตถุประสงค์

เพื่อเป็นการป้องกันสินทรัพย์ของบริษัทที่มีการเข้าถึงโดยผู้รับดำเนินการด้านสารสนเทศ (IT Outsourcing) และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการ ให้บริการ

แนวทางปฏิบัติ

14.1 ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท เมื่อมีความจำเป็นต้องให้ผู้รับดำเนินการด้านสารสนเทศ (IT Outsourcing) เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของบริษัท และต้องเข้าทำสัญญาการประมวลผลข้อมูลส่วนบุคคลกับผู้รับดำเนินการด้านสารสนเทศ (IT Outsourcing) กรณีที่บริษัทมอบหมายให้ผู้รับดำเนินการด้านสารสนเทศ (IT Outsourcing) ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัท

14.2 ต้องสื่อสาร และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท เมื่อมีความจำเป็นต้องให้ผู้รับดำเนินการด้านสารสนเทศ (IT Outsourcing) เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

14.3 ในข้อตกลงการให้บริการ ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ

14.4 หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

15. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ

แนวทางปฏิบัติ

15.1 ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท

15.2 ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน

15.3 หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อฝ่ายเทคโนโลยี

Euroasia Total Logistics Public Company Limited

19, 21 Motorway Road, Klongsontoonnoon,

Lat Krabang, Bangkok, 10520 Thailand

Tel: (662) 123 1727

Website: www.etl.co.th

บริษัท ยูโรเอเชีย โลจิสติกส์ จำกัด (มหาชน)

19, 21 ถนนมอเตอร์เวย์ แขวงคลองสองต้นนุ่น

เขตลาดกระบัง กรุงเทพมหานคร 10520

โทรศัพท์: (662) 123 1727

เว็บไซต์: www.etl.co.th



15.4 กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

15.5 ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน

15.6 ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหมายหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

15.7 ในกรณีที่เหตุอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศก่อให้เกิดการละเมิดข้อมูลส่วนบุคคล ฝ่ายเทคโนโลยีจะต้องประสานงานกับผู้รับผิดชอบและคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลของบริษัท เพื่อดำเนินการแจ้งเหตุละเมิดดังกล่าวแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ที่ได้ทราบเหตุเท่าที่สามารถจะกระทำได้ และในกรณีที่การละเมิดนั้นมีความเสี่ยงสูงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล บริษัทจะต้องแจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมแนวทางเยียวยาโดยไม่ชักช้าด้วย

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

วัตถุประสงค์

เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของบริษัท อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของบริษัท

แนวทางปฏิบัติ

16.1 ฝ่ายเทคโนโลยี ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤต (Crisis Management Plan) ของบริษัท

16.2 ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้น อย่างน้อย ปีละ 1 ครั้ง

16.3 ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

16.4 ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง อย่างน้อยปีละ 1 ครั้ง



นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ คณะกรรมการบริษัทได้พิจารณาและอนุมัติ ในการประชุมคณะกรรมการบริษัท ครั้งที่ 2/2568 เมื่อวันที่ 20 กุมภาพันธ์ 2568 ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 20 กุมภาพันธ์ 2568 เป็นต้นไป

นายกมล รุ่งเรืองยศ

ประธานคณะกรรมการบริษัท

บริษัท ยูโรเอเชีย โทเทิล โลจิสติกส์ จำกัด (มหาชน)