บริษัท ล็อกซเล่ย์ จำกัด (มหาชน)

ชื่อเอกสาร : นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	รหัสเอกสาร : LOXLEY-ISMS-POLICY
ประเภทเอกสาร : เอกสารเผยแพร่	ลำดับการแก้ไข : 00
วันที่ประกาศใช้ : วันที่ 15 พฤษภาคม 2566	หน้าที่ : 1 ของ 5

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท ล็อกซเล่ย์ จำกัด (มหาชน)

บริษัท ล็อกซเล่ย์ จำกัด (มหาชน) และบริษัทในเครือ (ตามเอกสารแนบ) ต่อไปนี้เรียกว่า "บริษัท" ได้จัดให้มีการใช้งานระบบสารสนเทศเพื่ออำนวยความสะดวก เพิ่มประสิทธิภาพ และให้ประสิทธิผลต่อการทำงาน อีกทั้งด้วยแนวคิด "GRC" (Governance, Risk and Compliance) ทำให้หลายองค์กรเกิดความตื่นตัวในเรื่อง "Regulatory Compliance" หรือ "การปฏิบัติตามกฎหมายและกฎระเบียบต่าง ๆ" เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายอื่นที่เกี่ยวข้อง

ทั้งนี้เพื่อให้การใช้บริการและการให้บริการของบริษัทสามารถดำเนินการได้อย่างต่อเนื่องเหมาะสม สอดคล้องกับนโยบายทางธุรกิจของบริษัท และป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องทั้งจากผู้ใช้งานและภัยคุกคามทั้งภายในและภายนอก ซึ่งอาจส่งผลกระทบต่อธุรกิจของบริษัทให้ได้รับความเสียหายได้ และเพื่อให้ระบบสารสนเทศของบริษัทมีกรอบการบริหารจัดการที่ดี มีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยอ้างอิงจากหลักเกณฑ์และแนวปฏิบัติตามมาตรฐานด้านการรักษาความปลอดภัยของระบบสารสนเทศ ตลอดจนกฎหมายอื่นที่เกี่ยวข้อง บริษัทจึงได้กำหนดนโยบายการรักษาความปลอดภัยระบบสารสนเทศไว้ดังนี้

1. **การจัดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและความรับผิดชอบ** (Organization of Information Security)

   บริษัทต้องกำหนดบทบาทและหน้าที่ความรับผิดชอบของผู้ที่มีส่วนเกี่ยวข้องในการกำกับ ดูแล และปฏิบัติตามหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศให้จัดเจน และสื่อสารให้พนักงานหรือผู้มีส่วนเกี่ยวข้องได้รับทราบเพื่อการปฏิบัติตามนโยบาย ระเบียบ ข้อกำหนดต่าง ๆ ได้อย่างถูกต้อง

2. **การบริหารความมั่นคงปลอดภัยด้านบุคลากร** (Human Resource Security)

   บริษัทต้องกำหนดมาตรการสำหรับผู้ใช้งานหรือพนักงานให้มีเข้าใจในหน้าที่ บทบาท ความรับผิดชอบ ของตนเองที่ได้รับและส่งเสริมให้มีความตระหนักรู้และปฏิบัติหน้าที่ตามความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเองอย่างเคร่งครัด เพื่อนำมาซึ่งการปกป้องผลประโยชน์ของบริษัท

3. **การบริหารจัดการสินทรัพย์** (Assets Management)

บริษัทต้องมีมาตรการในการระบุทรัพย์สินสารสนเทศของบริษัท พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบในการใช้งานและการป้องกันทรัพย์สินสารสนเทศอย่างเหมาะสม พร้อมทั้งกำหนดระดับการปกป้องข้อมูลสารสนเทศของบริษัทที่เหมาะสม สอดคล้องกับความสำคัญของข้อมูลที่มีต่อบริษัท เพื่อเป็นการป้องกันการเปิดเผย การเปลี่ยนแปลง การโอนย้าย การลบ หรือการทำลายข้อมูลของบริษัท โดยไม่ได้รับอนุญาต

4. **การควบคุมการเข้าถึง** (Access Control)

บริษัทต้องกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของบริษัท ทั้งนี้ต้องสามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของบริษัทได้อย่างถูกต้อง รวมทั้งต้องสนับสนุนให้ผู้ใช้งานมีความรับผิดชอบในการร่วมกันป้องกันข้อมูลของบริษัท เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัยได้ประสิทธิภาพสูงสุด

5. **การเข้ารหัสข้อมูล** (Cryptography)

บริษัทต้องกำหนดมาตรการในการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

6. **การรักษาความมั่นคงปลอดภัยสถานที่และสภาพแวดล้อม** (Physical and Environment Security)

บริษัทต้องมีมาตรการในการป้องกัน ควบคุมการใช้งานและการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัท ให้อยู่ในสภาพที่มีความสมบูรณ์ พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

7. **การรักษาความมั่นคงปลอดภัยสำหรับการดำเนินงาน** (Operation Security)

บริษัทต้องกำหนดมาตรการเพื่อให้การปฏิบัติงานกับระบบสารสนเทศของบริษัทเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย รวมทั้งต้องมีมาตรการในการป้องกันการสูญหาย เข้าถึง ล่วงรู้ เปิดเผย แก้ไขเปลี่ยนแปลง ทำให้เสียหายหรือทำลาย ข้อมูลและระบบคอมพิวเตอร์

8. **ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล** (Communications Security)

บริษัทต้องกำหนดมาตรการควบคุมการบริหารจัดการเครือข่าย และการส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกบริษัทให้มีความมั่นคงปลอดภัย

9. **การจัดหา การพัฒนา และการบำรุงรักษาระบบ** (System Acquisition, Development and Maintenance)

บริษัทต้องกำหนดมาตรการเพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงมีมาตรการในการควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

10. **การบริหารความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอก** (IT Outsourcing)

บริษัทต้องจัดทำมาตรการและกรอบการปฏิบัติงานของผู้ให้บริการภายนอก ในการให้บริการหรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย และได้เป็นประโยชน์สูงสุดแก่บริษัท

11. **การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ** (Cyber Security Incident Management)

บริษัทต้องกำหนดแนวทางในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ การเรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้นและการปรับปรุงแก้ไข เพื่อเป็นการป้องกันไม่ให้เกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศซ้ำขึ้นอีก

12. **การบริหารความต่อเนื่องทางธุรกิจ** (Business Continuity Management)

บริษัทต้องจัดให้มีมาตรการในการป้องกันการติดขัด หรือหยุดชงักของการดำเนินธุรกิจของบริษัท และป้องกันกระบวนการทางธุรกิจที่สำคัญ ซึ่งเป็นผลมาจากการล้มเหลวในการทำงานของระบบสารสนเทศของบริษัท รวมทั้งขั้นตอนในการกู้คืนระบบสารสนเทศให้กลับมาทำงานได้เป็นปรกติ ในระยะเวลาที่เหมาะสม

13. **การบริหารจัดการความเสี่ยงด้านความมั่งคงปลอดภัยสารสนเทศ** (Information System Security Risk Management)

บริษัทต้องจัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง การจัดการและการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้ และการติดตามและทบทวนความเสี่ยง รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกบริหารจัดการอย่างเหมาะสม

14. **การปฏิบัติตามข้อกำหนด** (Regulatory and Compliance)

บริษัทต้องจัดให้มีมาตรการและแนวทางเพื่อให้การดำเนินงานต่างๆของบริษัทเป็นไปตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความปลอดภัยต่าง ๆ ที่บริษัทและบุคลากรของบริษัทต้องปฏิบัติตาม รวมทั้งมีมาตรการในการตรวจสอบการปฏิบัติตามนโยบายทางด้านความปลอดภัยสารสนเทศที่กำหนดไว้

15. การทบทวนนโยบาย (Information Security Reviews)

กำหนดให้มีการทบทวนนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ ทั้งนี้บริษัทต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลง

16. การเผยแพร่นโยบาย

ทุกหน่วยงานมีหน้าที่รับผิดชอบโดยการประกาศให้ทราบและเผยแพร่นโยบายเหล่านี้ รวมทั้งทำการสนับสนุน ตอบสนองนโยบายของบริษัท

17. บทบังคับใช้

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศนี้ให้ใช้บังคับกับ พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของ บริษัท ล็อกซเล่ย์ จำกัด (มหาชน) และบริษัทในเครือ (ตามเอกสารแนบ) รวมถึงบุคคลภายนอก และหน่วยงานภายนอกที่ให้บริการแก่บริษัท โดยมีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป