นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

1. บทนำ

1.1. วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยให้แก่ทรัพย์สินของบริษัท โดยเฉพาะอย่างยิ่งทรัพย์สินที่เป็นข้อมูลสารสนเทศสำคัญที่ใช้ในการดำเนินธุรกิจ โดยการปกป้องให้พ้นภัยคุกคามและความเสี่ยง ทั้งจากภายในและภายนอกบริษัท ไม่ว่าจะเกิดขึ้นโดยเจตนาหรือไม่เจตนาก็ตาม รวมถึงเพื่อลดความเสียหายต่างๆ ที่อาจเกิดขึ้นจากเหตุละเมิดความมั่นคงปลอดภัย และเพื่อรักษาไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง

1.2. ขอบเขต

- ข้อมูลทั้งหมด (ทั้งที่อยู่ในรูปเอกสาร และอิเล็กทรอนิกส์ไฟล์) ที่ได้รับการจัดเก็บ ได้รับการใช้งาน หรือใช้ในการสื่อสารเพื่อดำเนินกิจการของบริษัท
- บุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบสารสนเทศของบริษัทซึ่งได้แก่ ผู้บริหาร พนักงานประจำ พนักงานชั่วคราว หุ้นส่วน ตัวแทนธุรกิจ บุคคลภายนอกที่ถูกว่าจ้างโดยบริษัท บริษัทคู่ค้า บริษัทหรือบุคคลที่เป็นคู่สัญญา และผู้ให้บริการ
- ทรัพย์สินทั้งหมดที่เกี่ยวข้องกับข้อมูล และที่ใช้ในการจัดเก็บ ส่งผ่าน หรือประมวลผลข้อมูล ซึ่งได้แก่ เครื่องเซิร์ฟเวอร์ ซอฟต์แวร์ โปรแกรม อิเล็กทรอนิกส์ไฟล์ เอกสารตีพิมพ์ เครื่องมือ สิ่งอำนวยความสะดวก ตลอดจนบริการที่ได้รับ

1.3. คำจำกัดความ

- MR หมายถึง ตัวแทนฝ่ายบริหารระบบมาตรฐาน (Management Representative) ในที่นี้ได้แก่ ISMR หรือ ISMA (อ้างอิง ISMS-PL-09 ISMS Manual)

2. นโยบาย

2.1. นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

1) ปกป้องข้อมูล (ไม่ว่าจะถูกเก็บในรูปแบบใดก็ตาม) ให้พ้นจากเหตุละเมิดต่างๆ ซึ่งอาจส่งผลกระทบต่อความลับของข้อมูล (Confidentiality) ความถูกต้องและสมบูรณ์ครบถ้วนของข้อมูล (Integrity) และความพร้อมใช้ของข้อมูล (Availability)
2) ปฏิบัติตามมาตรฐาน ISO/IEC 27001 และมาตรฐานอื่นๆ ตลอดจนนโยบายด้านความมั่นคงปลอดภัยที่บริษัทกำหนด เพื่อความมั่นคงปลอดภัยของข้อมูล
3) ปฏิบัติตามข้อกฎหมายอื่นๆ ที่เกี่ยวข้องทั้งหมด

โดยบริษัทมีนโยบายดังต่อไปนี้

1) ข้อมูลที่สำคัญของบริษัทต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต
2) ข้อมูลที่สำคัญของบริษัทต้องได้รับการรักษาความลับอย่างเหมาะสม
3) ข้อมูลที่สำคัญของบริษัทต้องมีความถูกต้องและสมบูรณ์ครบถ้วน
4) ข้อมูลที่สำคัญของบริษัทต้องพร้อมใช้งานอยู่เสมอ
5) กฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้องต่างๆ ต้องได้รับการปฏิบัติตามอย่างถูกต้องครบถ้วน
6) ต้องมีการจัดทำรายการทรัพย์สินสารสนเทศที่สมบูรณ์และครบถ้วน ประกอบด้วยรายการทรัพย์สินที่เกี่ยวกับอุปกรณ์และเครื่องคอมพิวเตอร์ ระบบงานสารสนเทศ และข้อมูล
7) พนักงานทุกคนควรได้รับการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
8) พนักงานทุกคนจะต้องปฏิบัติงานโดยคำนึงถึงความมั่นคงปลอดภัยสารสนเทศเสมอ (Awareness)
9) จัดให้มีการบริหารจัดการความเสี่ยงด้านสารสนเทศ (IT Risk management) และการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและข้อมูลในบริษัท
10) จัดทำแผนการจัดการเพื่อให้ธุรกิจดำเนินได้อย่างต่อเนื่อง พร้อมทั้งทำการดูแลรักษา และทดสอบแผนอย่างเหมาะสม
11) จัดให้มีชุดเอกสารนโยบายด้านความมั่นคงปลอดภัยของข้อมูล และเอกสารสนับสนุนที่เกี่ยวข้อง เพื่อกำหนดระเบียบปฏิบัติ ตลอดจนแนวทางการปฏิบัติงานและการใช้งานข้อมูลอย่างมั่นคงปลอดภัย
12) จัดให้มีกระบวนการในการรายงาน สืบสวน รับมือ และจัดการกับเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม โดยเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศตลอดจนสิ่งผิดปกติ และเหตุการณ์ที่น่าสงสัยอื่นๆ ต้องได้รับการรายงานไปที่ MR เพื่อดำเนินการตรวจสอบ และแก้ไข รวมถึงการรายงานต่อคณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยและหน่วยงานภายนอกตามกฎหมายในกรณีที่เกิดเหตุการณ์ร้ายแรง

2.2. การปฏิบัติตามนโยบายและการตรวจสอบ

1) พนักงานและบุคคลที่เกี่ยวข้องทุกคนต้องลงนามใน “เอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement)” และ / หรือ เอกสารอื่นๆที่เกี่ยวข้อง เพื่อเป็นการยอมรับว่าข้อมูลต่างๆ ที่ได้รับทราบและใช้ระหว่างการจ้างงาน เป็นทรัพย์สินของบริษัท และไม่

สามารถนำไปใช้เพื่อการอื่นโดยไม่ได้รับอนุญาต ทั้งนี้ในการใช้งานข้อมูลทั้งหลายในบริษัท จะถือว่าทุกคนรับทราบและยินยอมปฏิบัติตามเงื่อนไขของนโยบายนี้ทุกประการ

2) การเจตนาเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การจงใจใส่ข้อมูลที่ผิดพลาด และการเจตนาเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ถือเป็นสิ่งที่ต้องห้ามทั้งสิ้น การไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศฉบับนี้ ถือว่ามีความผิดทางวินัย และเพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบายนี้อย่างเคร่งครัด บริษัทจึงจำเป็นต้องจัดให้มีการตรวจติดตามการปฏิบัติงานของพนักงาน ตลอดจนบุคคลอื่นที่เกี่ยวข้องเป็นระยะๆ ผ่านการตรวจสอบติดตามการปฏิบัติงานภายใน (Internal Audit) และการตรวจสอบ Security Logs / Audit Trails ที่เกี่ยวข้อง ทั้งนี้ บริษัทขอสงวนสิทธิ์ในการกระทำการใดๆ ที่เห็นว่าจำเป็นเพื่อจัดการและป้องกันความมั่นคงปลอดภัยให้แก่ข้อมูลและระบบสารสนเทศของบริษัท

2.3. การทบทวนและปรับปรุงนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศทั้งหมด รวมถึงระเบียบและคำสั่งต่างๆ ที่เกี่ยวข้อง ต้องได้รับการทบทวนและประเมินผลเพื่อปรับปรุงเนื้อหา หรือยืนยันเนื้อหาเดิมโดยผู้บริหารอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าเนื้อหาของนโยบายยังคงไว้ซึ่งความครบถ้วนสมบูรณ์ มีประสิทธิภาพ และสามารถนำไปใช้งานได้อย่างเหมาะสม

2.4. บทลงโทษ

การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบาย ตลอดจนวิธีการปฏิบัติงาน และเอกสารสนับสนุนต่างๆที่เกี่ยวข้อง ไม่ว่าโดยเจตนาหรือไม่ก็ตาม ถือเป็นความผิดทางวินัย ซึ่งจะต้องพิจารณาลงโทษทางวินัยตามกฎระเบียบของบริษัท และหากการละเมิดหรือฝ่าฝืนนโยบายนั้นเข้าข่ายการกระทำที่ผิดกฎหมาย ผู้ละเมิดต้องได้รับการดำเนินคดีตามที่กฎหมายระบุไว้

(มีผลใช้บังคับตั้งแต่วันที่ 22 สิงหาคม 2566 เป็นต้นไป)