

ประกาศที่ 011/2568

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน)

บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน) ให้ความสำคัญสูงสุดกับการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ ซึ่งเป็นรากฐานสำคัญต่อความสำเร็จและการดำเนินธุรกิจของบริษัท เพื่อให้การปฏิบัติงานสอดคล้องกับกฎหมายและมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงข้อบังคับอื่น ๆ ที่เกี่ยวข้อง จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ขึ้น โดยมีวัตถุประสงค์เพื่อกำหนดหลักการและแนวปฏิบัติพื้นฐานที่เกี่ยวข้องกับการปกป้องทรัพย์สินสารสนเทศของบริษัท

1. วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อ

- แสดงให้เห็นถึงความสำคัญที่บริษัทให้การรักษาความมั่นคงปลอดภัยไซเบอร์
- สร้างความมั่นใจแก่ลูกค้า คู่ค้า และสาธารณะว่าข้อมูลของท่านจะได้รับการดูแลปกป้องอย่างเหมาะสม
- กำหนดหลักการและแนวปฏิบัติพื้นฐานที่บุคคลภายนอกและผู้มีส่วนเกี่ยวข้องควรทราบเมื่อต้อง มีปฏิสัมพันธ์กับระบบหรือข้อมูลของบริษัท
- เป็นไปตามข้อกำหนดของกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

2. ขอบเขต

นโยบายนี้มีผลบังคับใช้กับ

- **ทรัพย์สินสารสนเทศของบริษัท** ครอบคลุมข้อมูล ระบบคอมพิวเตอร์ และอุปกรณ์ประมวลผลสารสนเทศทั้งหมดของบริษัท ไม่ว่าจะอยู่ในสถานที่ตั้งของบริษัท หรือบนแพลตฟอร์มคลาวด์ที่บริษัทใช้งาน
- **บุคคลภายนอก** บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการแก่บริษัท และได้รับสิทธิ์ในการเข้าถึงข้อมูลหรือระบบของบริษัท เช่น
 - ลูกค้า (Customer)
 - บริษัทคู่ค้า (Business Partners)
 - ผู้รับจ้างปฏิบัติงาน (Outsource)
 - ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ (Suppliers)
 - ผู้ให้บริการ (Service Providers)
 - ที่ปรึกษา (Consultants)
- **ผู้ใช้งานเว็บไซต์/แพลตฟอร์ม** ผู้ที่เข้ามาใช้งานเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มดิจิทัลของบริษัท

3. คำนิยาม

- บริษัท หมายถึง บริษัท จัสมิน เทคโนโลยี โซลูชัน จำกัด (มหาชน)
- ข้อมูล (Data) หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ที่บริษัทครอบครองหรือจัดการ
- ข้อมูลที่เป็นความลับ (Confidential Information) หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัทมีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณ ในการประกอบธุรกิจ หรือสัญญา ซึ่งบริษัทไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์ อย่างอื่นนอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท
- ระบบคอมพิวเตอร์ (Computer System) หมายถึง เครื่องมือหรืออุปกรณ์คอมพิวเตอร์ทุกชนิด ทั้งฮาร์ดแวร์และซอฟต์แวร์ อุปกรณ์เครือข่าย วัสดุ อุปกรณ์การจัดเก็บและถ่ายโอนข้อมูล รวมถึง ระบบอินเทอร์เน็ต อินทราเน็ต และอุปกรณ์สื่อสารโทรคมนาคมที่เกี่ยวข้องกับบริษัท
- บุคคลภายนอก (External Party) หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการ กับบริษัท และได้รับสิทธิในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัท

4. หลักการพื้นฐานในการรักษาความมั่นคงปลอดภัย (Security Principles)

บริษัทยึดมั่นในหลักการพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศดังนี้

- การรักษาความลับ (Confidentiality) ปกป้องข้อมูลไม่ให้เข้าถึงหรือเปิดเผยแก่ผู้ที่ไม่ได้รับอนุญาต เพื่อรักษาความเป็นส่วนตัวและข้อมูลเชิงพาณิชย์ที่เป็นความลับ
- ความสมบูรณ์ (Integrity) ทำให้มั่นใจว่าข้อมูลถูกต้อง ครบถ้วน ไม่ถูกแก้ไข ดัดแปลง หรือทำลาย โดยไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) ทำให้มั่นใจว่าระบบและข้อมูลพร้อมใช้งานเมื่อผู้ที่ได้รับอนุญาต ต้องการ เพื่อสนับสนุนการดำเนินธุรกิจอย่างต่อเนื่อง
- ความรับผิดชอบ (Accountability) กลไกที่สามารถตรวจสอบย้อนหลังการเข้าถึงและการกระทำ บนระบบและข้อมูล เพื่อให้สามารถระบุผู้รับผิดชอบได้
- การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) ไม่สามารถปฏิเสธการกระทำของตนเอง บนระบบหรือข้อมูลได้
- การปฏิบัติตามกฎหมาย (Compliance) ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และมาตรฐานสากล ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลอย่างเคร่งครัด

5. แนวปฏิบัติสำหรับบุคคลภายนอกและผู้ใช้งาน

เพื่อส่งเสริมสภาพแวดล้อมที่ปลอดภัย บริษัทขอความร่วมมือจากบุคคลภายนอกและผู้ใช้งานทุกท่าน ในการปฏิบัติดังนี้

5.1 การปกป้องข้อมูลส่วนตัว

- ดูแลรักษารหัสผ่าน (Password) และข้อมูลส่วนตัวที่ใช้ในการเข้าถึงระบบ หรือบริการ ของบริษัทเป็นความลับสูงสุด ห้ามเปิดเผยให้ผู้อื่นทราบ
- ตั้งรหัสผ่านที่คาดเดาได้ยาก และเปลี่ยนรหัสผ่านตามคำแนะนำของบริษัท

- ต้องไม่อนุญาตให้ผู้อื่นใช้งานระบบคอมพิวเตอร์ผ่านบัญชีผู้ใช้งานของตนโดยเด็ดขาด มิฉะนั้นผู้ใช้งานอาจมีความผิดทางวินัยและต้องรับผิดชอบต่อปัญหาที่เกิดขึ้น เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เป็นต้น
- ต้องสำรองข้อมูลสำคัญเก็บไว้ในที่ปลอดภัย เช่น สื่อจัดเก็บข้อมูลแบบพกพา หรือพื้นที่บนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่บริษัทฯ จัดสรรไว้ให้ เพื่อลดความเสี่ยงจากการไม่สามารถกู้คืนข้อมูลที่ถูกทำลายโดยไวรัส

5.2 การใช้งานระบบอย่างปลอดภัย

- ใช้งานเว็บไซต์ แอปพลิเคชัน และระบบของบริษัท ตามวัตถุประสงค์ที่กำหนดไว้เท่านั้น
- หลีกเลี่ยงการคลิกลิงก์น่าสงสัย ดาวน์โหลดไฟล์จากแหล่งที่ไม่รู้จัก หรือติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตบนอุปกรณ์ที่ใช้เข้าถึงระบบของบริษัท
- ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) และอัปเดตระบบปฏิบัติการบนอุปกรณ์ของท่านให้ทันสมัยอยู่เสมอ
- ต้องใช้ระบบของบริษัทในลักษณะที่ต้องทำตามกฎหมาย ไม่ละเมิดสิทธิ และไม่ก่อความเดือดร้อนหรือความเสียหายแก่บุคคลหรือองค์กรอื่น

5.3 การแจ้งเหตุผิดปกติ

- แจ้งให้บริษัททราบทันทีหากพบเห็นกิจกรรมที่น่าสงสัย การเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล หรือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริษัท

5.4 การปฏิบัติตามกฎหมายและข้อตกลง

- ปฏิบัติตามกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมาย ระเบียบ ข้อบังคับอื่น ๆ ที่มีผลบังคับใช้อยู่ในปัจจุบันและที่จะมีผลบังคับใช้ในอนาคต
- ปฏิบัติตามข้อตกลงหรือสัญญาระหว่างท่านกับบริษัท ที่เกี่ยวข้องกับการรักษาความลับและการใช้งานข้อมูล

6. การบริหารจัดการความมั่นคงปลอดภัยของบริษัท

มีมาตรการและกระบวนการที่เข้มงวดในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึง

- การบริหารจัดการความเสี่ยง มีการระบุ ประเมิน และจัดการความเสี่ยงด้านไซเบอร์อย่างต่อเนื่อง
- การควบคุมการเข้าถึง กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบอย่างรัดกุมตามหลักการ "เท่าที่จำเป็น"
- การปกป้องข้อมูล มีการเข้ารหัสข้อมูล การสำรองข้อมูล และมาตรการป้องกันการรั่วไหลของข้อมูล
- การจัดการเหตุการณ์ มีแผนการตอบสนองและแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างรวดเร็ว
- การฝึกอบรม สร้างความตระหนักและให้ความรู้แก่พนักงานอย่างสม่ำเสมอ
- การตรวจสอบ มีการตรวจสอบและประเมินประสิทธิภาพของมาตรการความปลอดภัยอย่างสม่ำเสมอ

7. การละเมิดนโยบาย

การละเมิดนโยบายความมั่นคงปลอดภัยไซเบอร์ของบริษัท อาจส่งผลให้เกิดความเสียหายร้ายแรงต่อบริษัท และบุคคลที่เกี่ยวข้อง การไม่ปฏิบัติตามนโยบายนี้อาจนำไปสู่

- การถูกระงับสิทธิ์การเข้าถึงระบบหรือบริการของบริษัท
- การยุติสัญญาหรือความสัมพันธ์ทางธุรกิจ
- การดำเนินคดีตามกฎหมายที่เกี่ยวข้อง

บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน) ขอขอบคุณทุกท่านที่ให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อประโยชน์และความปลอดภัยของทุกฝ่าย

ประกาศ ณ วันที่ 1 กรกฎาคม 2568



(นายชิ่ง โต ลี)

กรรมการผู้จัดการ

บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน)