ความปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ

ในยุคที่ข้อมูลมีบทบาทสำคัญต่อการดำเนินธุรกิจ ความมั่นคงปลอดภัยด้านข้อมูลและเทคโนโลยีสารสนเทศถือเป็นพื้นฐานของการกำกับดูแลกิจการที่ดี บริษัท ซันเวนดิ้ง เทคโนโลยี จำกัด (มหาชน) (“SVT”) ให้ความสำคัญกับการคุ้มครองข้อมูลและความปลอดภัยของระบบสารสนเทศอย่างรอบด้าน เพื่อรักษาความเป็นส่วนตัวของข้อมูลลูกค้า พนักงาน และผู้มีส่วนได้เสีย รวมถึงสนับสนุนความต่อเนื่องและประสิทธิภาพในการดำเนินธุรกิจอย่างยั่งยืน

การสนับสนุนเป้าหมายการพัฒนาที่ยั่งยืน

ความสงบสุข ยุติธรรมและสถาบันที่เข้มแข็ง

ความร่วมมือเพื่อการพัฒนาที่ยั่งยืน

แนวทางการบริหารจัดการ

นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ จัดทำขึ้นให้สอดคล้องกับวัตถุประสงค์และกลยุทธ์ขององค์กร เพื่อกำหนดกรอบการกำกับดูแลและแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท ซันเวนดิ้ง เทคโนโลยี จำกัด (มหาชน) ให้สามารถนำไปปฏิบัติได้อย่างชัดเจน เป็นมาตรฐานเดียวกัน และเป็นไปตามกฎหมาย นโยบาย และระเบียบที่เกี่ยวข้องอย่างมีประสิทธิภาพ โดยประกอบไปด้วย 4 หัวข้อ ดังนี้

1. มาตรการขององค์กร (Organizational controls)

- การกำหนดนโยบายและโครงสร้าง: บริษัทต้องจัดทำนโยบายความมั่นคงปลอดภัยที่ชัดเจน โดยมีการตรวจสอบและปรับปรุงให้ทันสมัยทุกปีตามกฎหมายที่เกี่ยวข้อง พร้อมทั้งกำหนดบทบาทหน้าที่และความรับผิดชอบของพนักงานในการใช้อุปกรณ์คอมพิวเตอร์พกพาและการทำงานจากภายนอก

- การบริหารจัดการทรัพย์สิน: มีการกำหนดผู้รับผิดชอบทรัพย์สินทางสารสนเทศอย่างชัดเจน มีการแบ่งระดับความลับของข้อมูล และดูแลสื่อบันทึกข้อมูลอย่างเหมาะสม

- การควบคุมการเข้าถึง: กำหนดสิทธิ์ในการเข้าถึงและแก้ไขข้อมูล เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้งานระบบหรือแอปพลิเคชันโดยมิชอบ

2. มาตรการด้านบุคลากร (People controls)

- ความรับผิดชอบของพนักงาน: กำหนดหน้าที่ด้านความปลอดภัยให้พนักงานและบุคคลภายนอกรับทราบตั้งแต่ก่อนเริ่มงาน ระหว่างทำงาน ไปจนถึงเมื่อสิ้นสุดการจ้างงาน

- บทลงโทษ: มีการกำหนดบทลงโทษที่ชัดเจนหากมีการละเมิดกฎหรือข้อบังคับเกี่ยวกับความมั่นคงปลอดภัย

3. มาตรการทางกายภาพ (Physical controls)

- การป้องกันสถานที่และอุปกรณ์: เน้นการป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงพื้นที่ติดตั้งอุปกรณ์สารสนเทศ เพื่อป้องกันความเสียหาย การแทรกแซงการทำงาน หรือการถูกโจรกรรมทรัพย์สินของบริษัท

4. มาตรการทางเทคโนโลยี (Technological controls)

- การป้องกันข้อมูลและระบบ: ใช้เทคนิคการเข้ารหัส (Cryptography) เพื่อรักษาความลับและป้องกันข้อมูลรั่วไหล, รวมถึงมีการสำรองข้อมูล และป้องกันมัลแวร์หรือโปรแกรมไม่ประสงค์ดี

- การตรวจสอบช่องโหว่: มีการสแกนช่องโหว่ (VA Scan) และทดสอบเจาะระบบ (Pentest) เพื่อลดความเสี่ยงจากการถูกโจมตี

- การสื่อสารและผู้ให้บริการภายนอก: ดูแลความปลอดภัยของเครือข่ายและการแลกเปลี่ยนข้อมูล พร้อมทั้งกำกับดูแลผู้ให้บริการภายนอก (Suppliers) ให้ปฏิบัติตามข้อตกลงด้านความปลอดภัยอย่างเคร่งครัด

- การรับมือเหตุการณ์และความต่อเนื่อง: มีแผนรองรับเมื่อเกิดเหตุละเมิดความปลอดภัยเพื่อไม่ให้กระทบต่อการบริการ และเตรียมความพร้อมให้อุปกรณ์สามารถใช้งานได้อย่างต่อเนื่อง (Business Continuity)

- การปฏิบัติตามกฎหมาย: ตรวจสอบและปฏิบัติให้สอดคล้องกับข้อกำหนดทางกฎหมายและสัญญาอย่างสม่ำเสมอ

<u>ผู้มีส่วนได้เสียที่เกี่ยวข้อง</u>

1. พนักงาน/ผู้บริหาร

- ปฏิบัติตามนโยบายความปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศที่บริษัทกำหนดอย่างเคร่งครัด

2. ผู้ถือหุ้น

- ได้รับความคุ้มครองความปลอดภัยของระบบและความโปร่งใสด้านการจัดการข้อมูลเทคโนโลยีสารสนเทศ

3. คู่ค้า

- ได้รับความคุ้มครองความปลอดภัยของระบบและความโปร่งใสด้านการจัดการข้อมูลเทคโนโลยีสารสนเทศ

4. ภาครัฐ

- กำกับ ดูแล และกำหนดกฎระเบียบที่เกี่ยวข้องกับข้อมูลและเทคโนโลยีสารสนเทศ

ลิงก์แนบเอกสารที่เกี่ยวข้อง

- นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

  https://www.sunvending.co.th/storage/downloads/corporate-governance/corporate-policies/svt-it-security-policy-th.pdf