บริษัท ซันเวนดิ้ง เทคโนโลยี จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

วันที่บังคับใช้: 27 ตุลาคม 2568

บริษัท ซันเวนดิ้ง เทคโนโลยี จำกัด (มหาชน) 34 ถนนกรุงเทพกรีฑา แขวงหัวหมาก เขตบางกะปิ กรุงเทพมหานคร 10240 โทรศัพท์ 0-2295-4255 โทรสาร 0-2683-6548
SUN VENDING TECHNOLOGY PCL. 34 Krungthep Kreetha Road, Hua Mak, Bang Kapi, Bangkok 10240 Thailand Tel : 0-2295-4255 Fax : 0-2683-6548

สารบัญ

1. บทนำ

เอกสารนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information Security Policy) ฉบับนี้จัดทำขึ้นโดยสอดคล้องกับวัตถุประสงค์และกลยุทธ์ขององค์กร และเพื่อให้มีการกำกับดูแล การกำหนดทิศทาง การรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท ซันเวนดิ้ง เทคโนโลยี จำกัด (มหาชน) ให้มีความชัดเจนในการนำไปปฏิบัติ ตลอดจนเพื่อให้มีความเข้าใจถึงแนวทางที่ดี รวมทั้งสามารถปฏิบัติตามให้สอดคล้องกับ กฎหมาย นโยบาย ขั้นตอนปฏิบัติกฎระเบียบที่บริษัทกำหนดไว้ ได้อย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน

2. วัตถุประสงค์ (Objective)

นโยบายและมาตรฐานการปฏิบัติงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศฉบับนี้จัดทำขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

2.1 เพื่อกำหนดทิศทาง หลักการ และ กรอบของข้อกำหนดในการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

2.2 เพื่อให้มั่นใจว่าการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศสอดคล้องกับความต้องการทางธุรกิจ และมีการปฏิบัติสอดคล้องกับข้อกำหนดความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่อาจเกี่ยวข้อง

2.3 เพื่อสนับสนุนให้เกิดการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศตามแนวความเสี่ยง อันนำไปสู่การเกิดกระบวนการตรวจสอบและปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศสอดคล้องกับมาตรฐานสากล

2.4 เพื่อสร้างการตระหนักถึงความสำคัญของการจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภายในบริษัท

3. หน้าที่และความรับผิดชอบ (Role and Responsibility)

3.1 หน้าที่ของคณะผู้บริหาร กำหนดกลยุทธ์ในภาพรวม การวิเคราะห์ความเสี่ยงและบริหารความเสี่ยง การประเมินผลกระทบต่อการดำเนินธุรกิจของบริษัท รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้คืนระบบยามฉุกเฉิน

3.2 หน้าที่ของผู้ใช้งาน (User / พนักงาน) ศึกษาทำความเข้าใจ และปฏิบัติตามนโยบายการบริหารจัดการเทคโนโลยีสารสนเทศของบริษัท ให้ความร่วมมือกับบริษัท อย่างเต็มที่ในการป้องกันระบบงานคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลสารสนเทศของบริษัทให้มีความปลอดภัยสูงสุด

3.3 หน่วยงานดูแลรักษาความปลอดภัยระบบสารสนเทศและสนับสนุนด้านสารสนเทศ (ITSecurity and Support) จัดทำนโยบาย กำหนดมาตรการ วิธีปฏิบัติงานในการปกป้องข้อมูลสารสนเทศ รวมถึงระเบียบในการดำเนินการนโยบายการบริหารจัดการเทคโนโลยีสารสนเทศให้มีความปลอดภัย ควบคุมการปฏิบัติงาน การใช้งานระบบสารสนเทศของบริษัท ให้อยู่ภายใต้กรอบนโยบายการบริหารจัดการเทคโนโลยีสารสนเทศ

4. นิยามคำศัพท์ / คำย่อ (Glossary / Acronym)

นิยามคำศัพท์ / คำย่อ	คำอธิบาย
บริษัทฯ	บริษัท ซันเวนดิ้ง เทคโนโลยี จำกัด (มหาชน)
ผู้ใช้งาน	กรรมการ ผู้บริหาร หรือ พนักงาน และ/หรือบุคคลภายนอกซึ่งได้รับอนุญาต
เจ้าของข้อมูล	ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเสียหาย
ทรัพย์สินด้านสารสนเทศ	1. ประเภทระบบ ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2. ประเภทอุปกรณ์ ซึ่งได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใดที่เกี่ยวข้อง 3. ประเภทข้อมูล ซึ่งได้แก่ ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ และซอฟต์แวร์ลิขสิทธิ์
ระบบสารสนเทศ	ระบบของการจัดเก็บ ประมวลผลข้อมูลโดยอาศัยบุคคล และเทคโนโลยีสารสนเทศในการดำเนินการเพื่อให้ได้สารสนเทศที่เหมาะสมกับงาน หรือภารกิจของแต่ละหน่วยงานในบริษัท
โครงสร้างพื้นฐานด้านเทคโนโลยี สารสนเทศ (IT Infrastructure)	หมายถึง องค์ประกอบของคอมพิวเตอร์ ระบบ หรืออุปกรณ์ใดๆ ที่จะนำมาใช้กับระบบ สารสนเทศ เพื่อให้ทำงานมีประสิทธิภาพและสอดคล้องกับความต้องการ ซึ่งรวมถึง – อุปกรณ์ฮาร์ดแวร์ เช่น เครื่องแม่ข่าย อุปกรณ์หน่วยความจำ (Storage) เครื่องลูกข่าย (Client) และคอมพิวเตอร์ตั้งโต๊ะ (Desktop) เป็นต้น – ซอฟต์แวร์ระบบ เช่น ระบบปฏิบัติการคอมพิวเตอร์ โปรแกรมแก้ไข (Software Patch) ชุดโปรแกรม BIOS ไดรฟ์เวอร์ (Driver) รวมถึงซอฟต์แวร์สำเร็จรูป เช่น ซอฟต์แวร์ฐานข้อมูล SQL หรือ Oracle เป็นต้น – ระบบและอุปกรณ์เครือข่าย เช่น ระบบเครือข่าย เราเตอร์ (Router) ไฟร์วอล (Firewall) เป็นต้น
ซอฟต์แวร์สำเร็จรูป (Software Package)	หมายถึง ซอฟต์แวร์ซึ่งมาจากผู้ผลิต เช่น Microsoft Office, Adobe Acrobat
จุดอ่อนหรือช่องโหว่ (Vulnerability)	หมายถึง สาเหตุหรือข้อบกพร่องที่เป็นช่องทางที่ก่อให้เกิดภัยคุกคาม
ภัยคุกคาม (Threat)	หมายถึง เหตุการณ์หรือสิ่งที่เกิดขึ้นจากภายใน หรือภายนอก และส่งผลเสียต่อทรัพย์สินของบริษัท
พื้นที่ควบคุม (Secure Area)	หมายถึง พื้นที่หรือบริเวณที่ใช้ในการจัดตั้ง จัดเก็บและประมวลผลสารสนเทศสำคัญของบริษัท เช่น ศูนย์คอมพิวเตอร์ ห้องคอมพิวเตอร์ ห้องระบบสื่อสาร ห้อง

นิยามคำศัพท์ / คำย่อ	คำอธิบาย
	จัดเก็บสารสนเทศที่สำคัญ เป็นต้น ซึ่งต้องมีการควบคุมให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เท่านั้นที่สามารถผ่านเข้าออกได้
โปรแกรมที่ไม่ประสงค์ดี (Malicious Software)	หมายถึง โปรแกรมหรือชุดโปรแกรมที่ทำให้สารสนเทศ หรือระบบสารสนเทศเกิดความ เสียหายโดยตั้งใจ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แอดแวร์ (Adware) หรือสปายแวร์ (Spyware) เป็นต้น
การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	หมายถึง การปฏิบัติงานจากบ้าน (Work at Home) หรือสถานที่ภายนอกบริษัท
โปรแกรมประเภทยูทิลิตี้ (System Utilities)	หมายถึง โปรแกรมเพื่อใช้สำหรับงานบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของระบบ คอมพิวเตอร์ เฉพาะทาง เช่น Registry Editor และ Administrative Tools บนระบบปฏิบัติการ Microsoft Windows เป็นต้น
การเปลี่ยนแปลงที่มีลักษณะฉุกเฉิน หรือเร่งด่วน (Emergency Change)	หมายถึง การแก้ไขเปลี่ยนแปลงแบบฉุกเฉินที่ต้องดำเนินการโดยด่วน เพื่อแก้ไขปัญหา หรือป้องกันเหตุการณ์ที่อาจสร้างผลกระทบร้ายแรงต่อการดำเนินธุรกิจ หรือการให้บริการระบบงาน
ต้อง (Must)	หมายถึง ให้ปฏิบัติตามมาตรฐานการปฏิบัติงานอย่างเคร่งครัด
ควร (Should)	หมายถึง ให้เลือกปฏิบัติตามมาตรฐานการปฏิบัติงานตามความเหมาะสม

5. นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Policy Topics)

นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ประกอบด้วยไปด้วย 4 หัวข้อหลักดังต่อไปนี้

หัวข้อที่ 1 มาตรการขององค์กร (Organizational controls)

- การกำหนดนโยบายและโครงสร้าง: บริษัทต้องจัดทำนโยบายความมั่นคงปลอดภัยที่ชัดเจน โดยมีการตรวจสอบและปรับปรุงให้ทันสมัยทุกปีตามกฎหมายที่เกี่ยวข้อง พร้อมทั้งกำหนดบทบาทหน้าที่และความรับผิดชอบของพนักงานในการใช้อุปกรณ์คอมพิวเตอร์พกพาและการทำงานจากภายนอก
- การบริหารจัดการทรัพย์สิน: มีการกำหนดผู้รับผิดชอบทรัพย์สินทางสารสนเทศอย่างชัดเจน มีการแบ่งระดับความลับของข้อมูล และดูแลสื่อบันทึกข้อมูลอย่างเหมาะสม
- การควบคุมการเข้าถึง: กำหนดสิทธิ์ในการเข้าถึงและแก้ไขข้อมูล เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้งานระบบหรือแอปพลิเคชันโดยมิชอบ

หัวข้อที่ 2 มาตรการด้านบุคลากร (People controls)

- ความรับผิดชอบของพนักงาน: กำหนดหน้าที่ด้านความปลอดภัยให้พนักงานและบุคคลภายนอกรับทราบ ตั้งแต่ก่อนเริ่มงาน ระหว่างทำงาน ไปจนถึงเมื่อสิ้นสุดการจ้างงาน
- บทลงโทษ: มีการกำหนดบทลงโทษที่ชัดเจนหากมีการละเมิดกฎหรือข้อบังคับเกี่ยวกับความมั่นคงปลอดภัย

หัวข้อที่ 3 มาตรการทางกายภาพ (Physical controls)

- การป้องกันสถานที่และอุปกรณ์: เน้นการป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงพื้นที่ติดตั้งอุปกรณ์สารสนเทศ เพื่อป้องกันความเสียหาย การแทรกแซงการทำงาน หรือการถูกโจรกรรมทรัพย์สินของบริษัท

หัวข้อที่ 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

6. การไม่ปฏิบัติตามนโยบายและบทลงโทษ (Noncompliance and Penalties)

การกระทำซึ่งถือเป็นการไม่ปฏิบัติตามนโยบายฉบับนี้ ได้แก่

- การฝ่าฝืนกฎเกณฑ์: ไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดที่เกี่ยวข้องขององค์กร,
- การละเมิดความลับ: การเข้าไปล่วงรู้หรือเปิดเผยข้อมูลสารสนเทศที่เป็นความลับโดยไม่ได้รับอนุญาต ซึ่งขัดต่อหลักการปกป้องข้อมูล,
- การใช้เครื่องมือผิดเงื่อนไข: ใช้อุปกรณ์คอมพิวเตอร์ โปรแกรม และเครือข่ายในลักษณะที่ผิดไปจากนโยบายที่บริษัทกำหนดไว้
- การสร้างความเสียหายต่อองค์กร: การเปิดเผยข้อมูลที่ส่งผลเสียต่อทรัพย์สิน ชื่อเสียง หรือภาพลักษณ์ของบริษัท ทั้งในปัจจุบันและอนาคต
- การลงโทษทางวินัย (Disciplinary Punishment) เมื่อมีการละเมิดหรือปฏิบัติไม่สอดคล้องกับมาตรฐานความมั่นคงปลอดภัย จะถือเป็น "โทษทางวินัยอย่างร้ายแรง" ซึ่งบริษัทจะดำเนินการทางวินัยตามข้อบังคับการทำงาน และ/หรือกฎหมายที่เกี่ยวข้อง

7. ข้อยกเว้นการไม่ปฏิบัติตามนโยบาย (Exceptions)

หากมีความจำเป็นทางธุรกิจหรือข้อจำกัดทางเทคโนโลยีจนไม่สามารถทำตามกฎปกติได้ องค์กรอนุญาตให้ทำเรื่องยกเว้นได้เป็นรายกรณีโดยมีเงื่อนไขคือ

- วิเคราะห์และบันทึกเหตุผล: เปรียบเทียบผลดีกับความเสี่ยงที่เกิดขึ้น และจัดทำเอกสารชี้แจงเหตุผลที่ไม่ปฏิบัติตามนโยบายให้ชัดเจนเป็นลายลักษณ์อักษร
- ใช้มาตรการทดแทนและขออนุมัติ: กำหนดวิธีป้องกันอื่น (Mitigating Control) เพื่อลดความเสี่ยง และต้องได้รับความเห็นชอบเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและหน่วยงาน IT Security ก่อนดำเนินการ

8. การปรับปรุงและพัฒนานโยบาย (Policy Review and Revision)

หน่วยงาน IT Security มีหน้าที่ทบทวนและปรับปรุงนโยบายความมั่นคงปลอดภัยอย่างน้อย ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้ระบบสอดคล้องกับความต้องการทางธุรกิจและก้าวทันภัยคุกคามใหม่ ๆ, ทั้งนี้ การแก้ไขใด ๆ จะต้องได้รับการ อนุมัติจากผู้บริหารสูงสุด และแจ้งให้ผู้เกี่ยวข้องทราบทุกครั้ง

9. มาตรฐานความมั่นคงปลออดภัยด้านสารสนเทศ (Information Security Standard)

1) หลักการพื้นฐาน (CIA Triad)
   มาตรฐานนี้ยึดหลักการสำคัญ 3 ประการคือ :
   - การรักษาความลับ (Confidentiality): ป้องกันการเปิดเผยข้อมูลแก่ผู้ที่ไม่ได้รับอนุญาต
   - ความถูกต้องครบถ้วน (Integrity): ป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
   - ความพร้อมใช้ (Availability): ข้อมูลและระบบต้องพร้อมใช้งานเมื่อต้องการ
2) การบริหารจัดการระดับองค์กรและบุคลากร
   - นโยบายและโครงสร้าง: ต้องมีนโยบายที่ผ่านการอนุมัติจากผู้บริหาร และมีการทบทวนอย่างสม่ำเสมอตามความเสี่ยงที่เปลี่ยนไป, มีการกำหนดหน้าที่ความรับผิดชอบด้านความปลอดภัยให้ชัดเจน และพนักงานทุกคนต้องลงนามข้อตกลงไม่เปิดเผยความลับ (NDA),
   - ความปลอดภัยด้านทรัพยากรบุคคล: ต้องมีการตรวจสอบประวัติก่อนจ้างงาน มีการอบรมสร้างความตระหนักด้านความปลอดภัย (Awareness Training) และเมื่อพ้นสภาพการจ้างงาน ต้องยกเลิกสิทธิ์เข้าถึงระบบและคืนทรัพย์สินทันที,
3) การจัดการสินทรัพย์และการควบคุมการเข้าถึง
   - การจัดการสินทรัพย์: ต้องจัดทำทะเบียนทรัพย์สิน (Inventory) ระบุเจ้าของ และกำหนดชั้นความลับของข้อมูล (Information Classification) เพื่อการป้องกันที่เหมาะสม,,
   - การควบคุมการเข้าถึง (Access Control): ยึดหลักให้สิทธิ์เฉพาะผู้ที่จำเป็นตามหน้าที่ (Need-to-do Basis), มีระบบพิสูจน์ตัวตนที่เข้มงวดและ
     มีการกำหนดมาตรการควบคุมการพิสูจน์ตัวตนที่เหมาะสม

4) มาตรการทางกายภาพและเทคโนโลยี

- ความปลอดภัยทางกายภาพ: มีการกำหนดพื้นที่หวงห้าม (Secure Areas) ควบคุมการเข้า-ออก, และมีระบบสนับสนุน เช่น เครื่องสำรองไฟ (UPS) และระบบป้องกันอัคคีภัย,
- ความปลอดภัยทางเทคนิค:
  - การเข้ารหัสข้อมูล (Cryptography): เพื่อรักษาความลับและความถูกต้องของข้อมูลสำคัญ
  - การป้องกันมัลแวร์: ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตให้เป็นปัจจุบันเสมอ
  - การสำรองข้อมูล (Backup): ต้องมีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง
  - การจัดการช่องโหว่ (Vulnerability Management): ติดตามและติดตั้งซอฟต์แวร์แก้ไขช่องโหว่ (Patch) อย่างเป็นระบบ

5) การสื่อสารและการพัฒนาระบบ

- ความมั่นคงปลอดภัยของเครือข่าย: มีการแบ่งแยกเครือข่าย (Segmentation) และใช้โปรโตคอลที่ปลอดภัย เช่น SSL หรือ HTTPS ในการรับส่งข้อมูล,,
- การจัดหาและพัฒนาระบบ: ต้องกำหนดความต้องการด้านความปลอดภัยตั้งแต่ขั้นตอนการออกแบบ แยกสภาพแวดล้อมสำหรับการพัฒนา (UAT) ออกจากระบบที่ใช้งานจริง (Production) และทดสอบความปลอดภัยก่อนนำขึ้นใช้งาน,

6) การบริหารจัดการเหตุการณ์และความต่อเนื่องทางธุรกิจ

- การจัดการเหตุการณ์ (Incident Management): พนักงานต้องรายงานเหตุละเมิดความปลอดภัยทันที มีขั้นตอนการตอบสนอง การเก็บหลักฐานตามกฎหมาย และการเรียนรู้จากเหตุการณ์เพื่อป้องกันการเกิดซ้ำ
- ความต่อเนื่องทางธุรกิจ (BCM): ต้องมีแผนรองรับเหตุการณ์ฉุกเฉินเพื่อให้ธุรกิจดำเนินต่อไปได้แม้เกิดภัยพิบัติ และต้องมีการทดสอบแผนอย่างน้อยปีละ 1 ครั้ง,

7) การปฏิบัติตามข้อกำหนด (Compliance)
ต้องปฏิบัติตามกฎหมายที่เกี่ยวข้อง (เช่น พ.ร.บ. คอมพิวเตอร์, PDPA) และข้อกำหนดในสัญญาจ้างอย่างเคร่งครัด, รวมถึงจัดให้มีการตรวจสอบความสอดคล้องโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนด

(นายพิศณุ โชควัฒนา)

กรรมการผู้อำนวยการ

บริษัท ซันเวนดิ้ง เทคโนโลยี จำกัด (มหาชน) 34 ถนนกรุงเทพกรีฑา แขวงหัวหมาก เขตบางกะปิ กรุงเทพมหานคร 10240 โทรศัพท์ 0-2295-4255 โทรสาร 0-2683-6548
SUN VENDING TECHNOLOGY PCL. 34 Krungthep Kreetha Road, Hua Mak, Bang Kapi, Bangkok 10240 Thailand Tel : 0-2295-4255 Fax : 0-2683-6548