บริษัท สหกิจบรรจุภัณฑ์ จำกัด

นโยบายและแนวทางปฏิบัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Policy)

รหัสเอกสาร:	IT-CP-01
ชื่อเอกสาร:	นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
หมายเลขปรับปรุงเอกสาร:	2566-001
วันที่เอกสารมีผลบังคับใช้:	19 มกราคม 2566

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุง เอกสาร:	**คำอธิบายและเหตุผลในการแก้ไข**
2566-001	เอกสารเผยแพร่ฉบับแรก

รายการบันทึก

ลำดับ	รายการบันทึก	ผู้รับผิดชอบ	อายุการจัดเก็บหลักฐาน	วิธีการจัดเก็บ หลักฐาน

สารบัญ

1. หลักการและเหตุผล

บริษัท สหกิจบรรจุภัณฑ์ จำกัด ได้จัดทำ “นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566” ขึ้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ และ เสถียรภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง อีกทั้งยังช่วยให้หน่วยงานสามารถลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือที่ไม่อาจคาดคิดไว้ ให้เกิดระบบความมั่นคง และ ปลอดภัยของหน่วยงาน ถ้าถูกบุกรุก หรือ ถูกโจมตีก็จะช่วยให้หน่วยงานสามารถฟื้นฟูระบบอย่างรวดเร็วภายหลังจากภัยคุกคามได้สิ้นสุดลง

2. วัตถุประสงค์

บริษัท สหกิจบรรจุภัณฑ์ จำกัด ได้จัดทำ “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566” โดยมีวัตถุประสงค์ดังนี้

2.1 เพื่อกำหนดนโยบาย และ แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้อง

2.2 เพื่อสร้างความเชื่อมั่นด้านความมั่นคงปลอดภัยไซเบอร์ และการดำเนินงานต่างๆ ภายในหน่วยงาน เป็นไปอย่างมีประสิทธิภาพ ประสิทธิผลและเสถียรภาพ

2.3 เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ ผู้บริหาร ผู้ดูแลระบบ และผู้ใช้งานภายในหน่วยงาน รวมทั้งบุคคลภายนอกที่ปฏิบัติงานภายในหน่วยงาน ให้มีความรู้ความเข้าใจ และ มีความตระหนักถึงความสำคัญในนโยบายและแนวทาง ปฏิบัติพร้อมทั้งปฏิบัติตามนโยบายแนวทางปฏิบัตินี้อย่างเคร่งครัด

3. องค์ประกอบและขอบเขตของนโยบาย

นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน จัดทำขึ้นเพื่อ กำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องตามพระราชบัญญัติการรักษา ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566 โดยขอบเขตมีผลบังคับใช้นโยบายและแนวทางปฏิบัติการรักษา ความมั่นคงปลอดภัยไซเบอร์ครอบคลุมหน่วยงานและการให้บริการภายในทั้งหมดของ บริษัท โดยมี รายละเอียดนโยบายและแนวทางปฏิบัติดังนี้

4. คำนิยาม

ลำดับ	คำศัพท์	ความหมาย
1	หน่วยงาน หรือ องค์กร หรือ บริษัท	บริษัท สหกิจบรรจุภัณฑ์ จำกัด
2	ผู้ใช้งาน (User)	พนักงาน ตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของบริษัท
3	สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

ลำดับ	คำศัพท์	ความหมาย
4	ผู้ดูแลระบบ (System Administrator)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบ คอมพิวเตอร์ ระบบเครือข่าย และระบบงาน
5	สินทรัพย์	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตน อันมีมูลค่า หรือ คุณค่าสำหรับหน่วยงาน
6	การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)	การอนุญาต การกำหนดสิทธิ หรือมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย
7	ความมั่นคงปลอดภัยด้านสารสนเทศ	การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ
8	เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	กรณีระบุการเกิดเหตุการณ์ สภาพของบริการ หรือ เครือข่าย ที่แสดงให้เห็นถึงความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์ อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
9	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
10	ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
11	ระบบอินทราเน็ต (Intranet)	ระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
12	ระบบสารสนเทศ	ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการ การพัฒนา และ ควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น
13	หน่วยงานภายนอก	องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึง และการใช้งานข้อมูล หรือทรัพย์สินต่างๆ ของหน่วยงานโดยจะได้รับ สิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษา ความลับข้อมูล

ลำดับ	คำศัพท์	ความหมาย
14	จดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail)	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่าน เครื่องคอมพิวเตอร์ และ ระบบเครือข่ายที่เชื่อมโยงกันข้อมูลที่ส่ง จะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้ มาตรฐานที่ใช้ ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
15	สื่อบันทึกพกพา	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น
16	ชื่อผู้ใช้ (Username)	ชุดของตัวอักษร หรือ ตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งาน ระบบคอมพิวเตอร์ และ ระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้
17	รหัสผ่าน (Password)	ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และ ระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และ ระบบเทคโนโลยีสารสนเทศ
18	การพิสูจน์ยืนยันตัวตน (Authentication)	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการ พิสูจน์โดยใช้ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
19	VPN (Virtual Private Network)	เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการ รับ-ส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ตทาให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
20	แผนผังระบบเครือข่าย (Network Diagram)	แผนผังซึ่งแสดงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน
21	เครื่องแม่ข่าย (Server)	เครื่องหรือโปรแกรมคอมพิวเตอร์ซึ่งทำงานให้บริการในระบบเครือข่ายแก่ลูกข่าย
22	อุปกรณ์กระจายสัญญาณ ข้อมูล (Switch)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ - ส่งข้อมูล
23	ไฟร์วอลล์ (Firewall)	เทคโนโลยีป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์จากบุคคลภายนอกเพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่ายโดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

ลำดับ	คำศัพท์	ความหมาย
24	อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)	อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย
25	อัปเดต (Update)	ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

5. นโยบายอุปกรณ์แบบพกพา (Mobile device policy)

นโยบายและมาตรการสนับสนุนสำหรับการใช้งานอุปกรณ์แบบพกพา เมื่อมีการนำมาใช้งานเพื่อบริหารจัดการความเสี่ยงจากการใช้อุปกรณ์แบบพกพาโดยจะต้องดำเนินการ ดังนี้

5.1 อุปกรณ์สื่อสารประเภทพกพาต้องได้รับการอนุญาต จากหน่วยงานที่ดูแลรับผิดชอบ จึงจะสามารถเข้าถึงข้อมูลสารสนเทศของบริษัท ได้

5.2 อุปกรณ์สื่อสารประเภทพกพาต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

5.3 ไม่ควรเก็บข้อมูลสำคัญของบริษัท ไว้บนอุปกรณ์สื่อสารประเภทพกพา แต่ถ้ามีความจำเป็นต้องจัดเก็บบนอุปกรณ์สื่อสารประเภทพกพา จะต้องมีการเข้ารหัสข้อมูลตามแนวทางการ เข้ารหัสของบริษัท

5.4 ต้องป้องกันข้อมูล และ สารสนเทศ ที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

5.5 ข้อมูลที่มีชั้นความลับซึ่งถูกจัดเก็บไว้บนอุปกรณ์สื่อสารประเภทพกพา หรือ ถูกส่งผ่านเครือข่ายไร้สายที่ต้องการส่งออกไปนอกบริษัท ต้องได้รับการอนุมัติจากเจ้าของข้อมูลและเข้ารหัสข้อมูล ก่อนเท่านั้น ไม่ควรเคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล และ จะต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

5.6 ระบบคอมพิวเตอร์อื่นของบุคคลภายนอก ที่ต้องการเชื่อมต่อกับระบบของบริษัท จะต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ

5.7 ต้องมีการรักษาความปลอดภัยทางกายภาพร่วมด้วย เช่น ผู้ใช้งานจะต้องออกจากระบบทุกครั้งเมื่อไม่ได้ใช้งานหรือช่วงที่ผู้ใช้งานไม่ได้อยู่ที่เครื่องของผู้ใช้งาน

5.8 กรณีที่อุปกรณ์สื่อสารประเภทพกพาเป็นสมบัติของ บริษัท การคืนเครื่องหรือส่งซ่อม ให้ผู้ใช้งานทำสำเนาข้อมูลจากอุปกรณ์สื่อสารประเภทพกพาเก็บไว้ทั้งหมด และลบข้อมูล ทั้งหมดที่มีอยู่บนอุปกรณ์สื่อสารประเภทพกพาก่อนส่งซ่อม

5.9 อุปกรณ์สื่อสารประเภทพกพา เช่น เครื่องคอมพิวเตอร์แบบพกพา (Laptop) หรือ Smart Device ควรมีกระบวนการเพื่ออัปเดตระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ ตามแนวปฏิบัติการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของ บริษัท

5.10 การเข้าถึงและใช้ข้อมูลสารสนเทศ ซึ่งรวมถึงชั้นความลับของผู้ใช้งานเป็นอันสิ้นสุดลงทันที เมื่อผู้ใช้งานพ้นสภาพตามสิทธิ์ของผู้ใช้งาน

5.11 บริษัท อาจดำเนินการทางวินัย แพ่ง หรืออาญา กับผู้ที่ล่วงละเมิดการเข้าถึง ล่วงละเมิดใช้งาน หรือล่วงละเมิดเผยแพร่ข้อมูลสารสนเทศที่เป็นความลับโดยที่ผู้นั้นไม่มีสิทธิ์อันชอบ

6. นโยบายการปฏิบัติงานจากระยะไกล (Teleworking Policy)

นโยบายและมาตรการสนับสนุนสำหรับการปฏิบัติงานจากภายนอกต้องมีการนำมาใช้งานเพื่อป้องกันข้อมูลที่มีการเข้าถึง การประมวลผลหรือการจัดเก็บจาก บริษัท โดยจะต้องดำเนินการดังนี้

6.1 ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอกบริษัท หน่วยงานที่รับผิดชอบต้องปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิ์ที่ได้รับและมีการตรวจสอบการใช้งานอย่างสม่ำเสมอ

6.2 ไม่อนุญาตให้ใช้งาน Remote Access สำหรับการปฏิบัติงานภายใต้ขอบเขตการดำเนินงาน ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เว้นแต่กรณีเกิดเหตุฉุกเฉินหรือเกิด เหตุการณ์ภัยพิบัติที่มีความจำเป็นต้องให้มีการปฏิบัติงานจากภายนอกเท่านั้น กรณีที่ต้องมี การเชื่อมต่อ Remote Access เพื่อปฏิบัติงานจากภายนอก ต้องได้รับการอนุมัติการเชื่อมต่อ ผ่านระบบ Virtual Private Network (VPN) ของบริษัท เท่านั้น

6.3 ห้ามนำซอฟต์แวร์การควบคุมจากระยะไกล เช่น PC-Anywhere หรือ Carbon copy มาใช้ กับคอมพิวเตอร์ของบริษัท การใช้ซอฟต์แวร์ที่ไม่เหมาะสมสามารถเป็นช่องทางให้ ผู้ที่ไม่ประสงค์ดีเข้ามายังเครือข่ายของบริษัท

7. นโยบายการควบคุมการเข้าถึง (Access control policy)

7.1 ความต้องการการให้บริการสำหรับการควบคุมการเข้าถึง

7.1.1 นโยบายควบคุมการเข้าถึง (Access control policy) นโยบายควบคุมการเข้าถึงต้องมีการ ดำเนินการดังนี้

7.1.1.1 กำหนดให้มีการควบคุมการเผยแพร่ข้อมูลและการให้สิทธิ์ เช่น หลักการความจำเป็นที่ต้องรู้ (Need to know), ระดับของความปลอดภัยและการจัดระดับชั้น การเข้าถึงข้อมูล

7.1.1.2 ควบคุมการจัดการสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญทุกระบบ

7.1.1.3 การแบ่งแยกการควบคุมการเข้าถึง เช่น การร้องขอเข้าถึงการให้สิทธิ์การเข้าถึง, หรือ การบริหารการเข้าถึง

7.1.1.4 ต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง ทุกระบบสารสนเทศที่มีความสำคัญ

7.1.1.5 ต้องถอดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ เมื่อบุคลากรพ้นสภาพ โยกย้ายเปลี่ยนผู้รับผิดชอบ หรือมีการปรับเปลี่ยนอย่างมีนัยสำคัญ

7.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ได้รับอนุมัติการ เข้าถึงเท่านั้น โดยจะต้องดำเนินการดังนี้

7.1.2.1 การกำหนดเครือข่าย และบริการเครือข่ายที่อนุญาตให้เข้าถึง

7.1.2.2 ขั้นตอนให้สิทธิ์ที่อนุญาตให้เข้าถึงเครือข่าย และบริการเครือข่าย

7.1.2.3 การควบคุมการจัดการ และขั้นตอนเพื่อป้องกันการเชื่อมต่อเครือข่าย และบริการ เครือข่าย

7.1.2.4 วิธีที่ใช้ในการเข้าถึงเครือข่าย และบริการเครือข่าย เช่น การใช้ Virtual Private Network (VPN) หรือ เครือข่ายไร้สาย

7.1.2.5 ระบบเครือข่ายที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอก ต้องมีการใช้อุปกรณ์ หรือ ซอฟต์แวร์ในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์ อื่น ๆ รวมทั้งต้องมี ความสามารถ ในการตรวจจับไวรัสด้วย

7.2 ความรับผิดชอบของผู้ใช้งาน

7.2.1 การใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตน (Use of secret authentication information)

ขั้นตอนการใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตนจะต้องดำเนินการดังนี้

7.2.1.1 ผู้ใช้งานต้องจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตนไว้เป็นความลับ ต้องมั่นใจว่าไม่ได้เปิดเผย ข้อมูลดังกล่าวต่อคนอื่น

7.2.1.2 หลีกเลี่ยงการการเก็บบันทึกข้อมูลความลับสำหรับการพิสูจน์ตัวตน (เช่น กระดาษซอฟต์แวร์ หรือ อุปกรณ์มือถือ ยกเว้นจะสามารถจัดเก็บได้อย่างปลอดภัย

7.2.1.3 เปลี่ยนข้อมูลความลับสำหรับการพิสูจน์ตัวตนเมื่อมีข้อบ่งชี้ว่ามีภัยคุกคาม

7.2.1.4 เมื่อรหัสผ่านถูกใช้สำหรับการพิสูจน์ตัวตน ให้เลือกรหัสผ่านที่มี คุณภาพตามข้อ 7.3.3

7.3 การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

7.3.1 ข้อกำหนดการเข้าถึงสารสนเทศ (Information Access Restriction)

ขั้นตอนสำหรับข้อกำหนดการเข้าถึงสารสนเทศจะต้องดำเนินการดังนี้

7.3.1.1 ต้องมีการจัดเตรียมหน้าจอหรือเมนูสำหรับควบคุมการเข้าถึงระบบ

7.3.1.2 ควบคุมสิทธิ์การเข้าถึงของผู้ใช้งาน เช่น อ่าน, เขียน และลบ

7.3.1.3 ควบคุมสิทธิ์การเข้าถึงของแอปพลิเคชัน

7.3.1.4 จัดเตรียมสิทธิ์การเข้าถึงทางกายภาพ และ ลอจิคัลสำหรับระบบ และ แอปพลิเคชันที่สำคัญ

7.3.2 ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัย (Secure log-on procedure)

ขั้นตอนในการเข้าสู่ ระบบอย่างปลอดภัยจะต้องดำเนินการ ดังนี้

7.3.2.1 ไม่แสดงข้อมูล เช่น ชื่อ, รุ่น, ไอพีแอดเดรสของระบบ หรือแอปพลิเคชันจนกว่า จะมีการเข้าสู่ระบบจะเสร็จสิ้นสมบูรณ์

7.3.2.2 ไม่ควรแสดงข้อความเพิ่มเติมระหว่างเข้าสู่ระบบซึ่งอาจช่วยให้ผู้ที่ไม่ได้รับอนุญาต เข้าสู่ระบบได้

7.3.2.4 จำกัดจำนวนครั้งของการพยายามเข้าสู่ระบบ เช่น ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง และหลังการเข้าสู่ระบบผิดพลาดให้บังคับระยะเวลาทิ้งช่วง เช่น 15 นาที ก่อนที่จะยอมให้เข้าสู่ระบบอีกครั้ง ขึ้นอยู่กับระบบสารสนเทศที่มีความสำคัญต่อ การให้บริการ

7.3.2.5 ตัดการใช้งานของผู้ใช้งานที่ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง เช่น 30 นาที โดยเฉพาะในพื้นที่ที่ความเสี่ยงสูง เช่น เครือข่ายสาธารณะ หรือ เครือข่ายภายนอก ของ บริษัท

7.3.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System)

ขั้นตอนในการเข้าสู่ระบบ อย่างปลอดภัยจะต้องดำเนินการดังนี้

7.3.3.1 บังคับการใช้รหัสผู้ใช้งาน และรหัสผ่านให้ใช้งานสำหรับแต่ละบุคคลเท่านั้น

7.3.3.2 บังคับใช้รหัสผ่านที่มีคุณภาพ รายละเอียดดังนี้

1) ต้องมีความยาวมากกว่าหรือเท่ากับ 8 ตัวอักษร เป็นอย่างน้อย
2) ต้องมีส่วนประกอบของอักษรตัวเล็ก ตัวใหญ่ อักขระพิเศษ และ ประกอบกัน
3) บังคับผู้ใช้งานให้เปลี่ยนรหัสผ่านในการเข้าสู่ระบบครั้งแรก
4) บังคับให้เปลี่ยนรหัสผ่านตามรอบ เช่น ทุก 1 ปี
5) ไม่แสดงรหัสผ่านบนหน้าจอที่ผู้ใช้งานกำลังป้อนข้อมูล
7) จัดเก็บไฟล์รหัสผ่านแยกจากข้อมูลทั่วไปของแอปพลิเคชัน
8) ต้องไม่บันทึกรหัสผ่านในระบบความจำของโปรแกรม

7.3.4 การควบคุมการเข้าถึงโปรแกรมซอร์สโค้ด (Access Control to Program Source Code)

ขั้นตอนในการควบคุมการเข้าถึงโปรแกรมซอร์สโค้ดจะต้องดำเนินการ ดังนี้

7.3.4.1 ต้องไม่เก็บ Source Code Library ไว้บนระบบที่ใช้งานจริง (Production System)

7.3.4.2 การเข้าถึง Source code ต้องจำกัดสิทธิ์ให้เฉพาะผู้ใช้งานที่จำเป็น เช่น โปรแกรมเมอร์ หรือผู้มีสิทธิ์เฉพาะหน้าที่ที่ได้รับมอบหมายเท่านั้น

7.3.4.3 ระหว่างการทดสอบต้องไม่เก็บ Source code ที่ใช้ทดสอบร่วมกับที่ใช้งานจริง

7.3.4.4 ต้องจัดเก็บ Source code ในสภาพแวดล้อมที่ปลอดภัย

7.3.4.5 การเปลี่ยนแปลงหรือแก้ไข Source code ต้องได้รับการอนุมัติจาก บริษัท ก่อนเสมอ

8. นโยบายการควบคุมการเข้าถึงทางกายภาพ (Physical Control Policy)

8.1 การกำหนดความปลอดภัยของพื้นที่

8.1.1 พื้นที่ใช้งานระบบสารสนเทศ (Physical Security Perimeter)

8.1.1.1 ต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศเพื่อการเฝ้าระวังควบคุม และรักษา ความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

8.1.1.2 ต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้อง กับความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

8.1.1.3 ไม่อนุญาตให้ถ่ายภาพ บันทึกวิดีโอหรือเสียง ภายในบริเวณที่ต้องมีความมั่นคง ปลอดภัยด้านสารสนเทศ (Secure Areas) เว้นแต่จะได้รับอนุญาต

8.1.2 การควบคุมการ เข้า - ออก (Physical entry controls)

8.1.2.1 ระบุตัวตนผู้ใช้งานและช่วงเวลาที่มีสิทธิ์ผ่าน เข้า - ออก ในแต่ละพื้นที่อย่างชัดเจน

8.1.2.2 ผู้ใช้งานจะได้รับสิทธิ์ให้ เข้า - ออก สถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนด เท่านั้น

8.1.3 ความปลอดภัยของสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

8.1.3.1 พื้นที่สำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์ หรือ ระบบที่มีความสำคัญ สูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่าน เข้า - ออก ของบุคคล ทั่วไป

8.1.3.2 พื้นที่สำนักงานจะต้องไม่มีป้าย หรือ สัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว

8.1.3.3 พื้นที่สำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ ควรมีความปลอดภัย เช่น กั้นพื้นที่ อย่างรอบด้าน ติดตั้งผนังติดตั้งเหล็กดัดล็อคประตูที่ใช้ดอกกุญแจหรือมี ระบบ Access Control

8.1.4 การป้องกันภัยคุกคามภายนอก และสิ่งแวดล้อม (Protecting against external and environmental threats)

8.1.4.1 พื้นที่สำนักงานที่มีระบบสำคัญจะต้องมีการควบคุมการ เข้า - ออก อย่างเข้มงวด และตั้งอยู่ในพื้นที่ที่ปลอดภัยจากภัยทางธรรมชาติ เช่น แผ่นดินไหว หรือน้ำท่วม

8.1.4.2 ต้องจะมีอุปกรณ์ดับเพลิงอย่างเพียงพอและเหมาะสม ทั้งนี้ในพื้นที่ที่ต้องมีการ รักษาความปลอดภัย ควรพิจารณาติดตั้งระบบดับเพลิงอัตโนมัติ

8.1.4.3 ต้องดูแลเรื่องความสะอาดของพื้นที่โดยทั่วไปอย่างสม่ำเสมอ เพื่อไม่ให้มีวัสดุที่เป็นเชื้อเพลิงอยู่ในพื้นที่ดังกล่าว

8.1.5 การปฏิบัติงานในพื้นที่ควบคุม (Working in Control Areas)

8.1.5.1 ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพ หรือ วิดีโอในบริเวณควบคุม เป็นต้น

8.1.5.2 ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือ วิดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

8.1.6 การจัดเตรียมพื้นที่สำหรับส่งมอบ (Delivery and loading areas)

8.1.6.1 ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ควรจัดเป็น บริเวณแยกออกมา

8.1.6.2 ต้องจัดให้มีขั้นตอนการลงทะเบียนเพื่อบริหารจัดการทรัพย์สินที่ถูกส่งมอบ

8.2 การกำหนดความปลอดภัยของอุปกรณ์

8.2.1 การจัดวางและป้องกันอุปกรณ์ (Equipment siting and protection)

8.2.1.1 ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรือ อันตรายที่อาจจะเกิดขึ้นกับอุปกรณ์เหล่านั้น

8.2.1.2 มีการจัดเตรียมพื้นที่จัดเก็บอุปกรณ์ที่ปลอดภัย และไม่สามารถเข้าถึงได้โดยง่าย เช่น ตู้ หรือลิ้นชักที่มีกุญแจล็อค

8.2.1.3 ห้ามมิให้มีการสูบบุหรี่ รับประทานอาหาร และ น้ำดื่ม ในพื้นที่จัดวางอุปกรณ์ของ ศูนย์เทคโนโลยีสารสนเทศ

8.2.1.4 ห้ามนำสารเคมี และเครื่องมือที่อาจก่อให้เกิดอันตรายกับอุปกรณ์เข้ามาในบริเวณ พื้นที่ปฏิบัติงานนอกจากได้รับการพิจารณาอนุญาต และ ตรวจสอบความเหมาะสมแล้ว เท่านั้น

8.2.1.5 ทำการติดตั้งระบบป้องกันฟ้าผ่ากับอาคารอย่างเหมาะสม

8.2.2 ระบบสาธารณูปโภคพื้นฐาน (Supporting utilities)

8.2.2.1 ต้องมีระบบไฟฟ้าสำรองอัตโนมัติเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่องและต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาตามความเหมาะสม

8.2.2.2 ต้องจัดให้มีระบบเตือนภัย / ป้องกันภัย เช่น ระบบดับเพลิง ระบบเตือนอัคคีภัย

8.2.2.3 ต้องมีการวางแผน และซักซ้อมการปฏิบัติรับมือกับภัยพิบัติ เช่น อัคคีภัย อย่าง น้อยปีละ 1 ครั้ง

8.2.2.4 ระบบที่สำคัญจะต้องมีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ เพื่อลดความสูญเสียที่อาจเกิดขึ้น จากผลกระทบจากเหตุการณ์ภัยพิบัติ หรือ เหตุการณ์ไม่คาดคิด

8.2.3 การทำลายอย่างปลอดภัยหรือนำกลับมาใช้งานของอุปกรณ์ (Secure disposal or re-use of equipment)

8.2.3.1 ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ทั้งนี้เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว

8.2.3.2 การทำลายหรือการนำอุปกรณ์กลับมาใช้ใหม่จะต้องถูกกำหนดขั้นตอนการดำเนินงานในการทำลายหรือการนำอุปกรณ์อิเล็กทรอนิกส์กลับมาใช้ใหม่เพื่อให้ แน่ใจได้ว่าข้อมูลใด ๆ ที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งโดยที่ไม่สามารถ กู้คืนกลับมาใช้ได้อีก

8.2.4 อุปกรณ์ที่ไม่อยู่ระหว่างการใช้งาน (Unattended user equipment)

8.2.4.1 ต้องใช้งานซอฟต์แวร์พักหน้าจอ โดยตั้งเวลาให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน

8.2.4.2 ต้องทำการออกจากโปรแกรม หรือบริการระบบเครือข่ายเมื่อไม่ใช้งาน

8.2.5 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and Clear screen policy)

8.2.5.1 ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็นข้อมูลความลับ หรือ ลับมาก ไว้ในที่สามารถพบเห็นได้ง่าย โดยจัดเก็บไว้ในที่ที่ปลอดภัย นอกจากนี้ ตู้จ่ายเอกสาร หรือ จดหมาย และ เครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

8.2.5.2 เมื่อสั่งพิมพ์งานเอกสารที่มีข้อมูลสำคัญ ผู้สั่งพิมพ์ต้องทำการจัดเก็บเอกสาร โดยทันที

9. นโยบายการสำรองข้อมูล (Backup Policy)

9.1 ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

9.2 กรณีที่เกิดการผิดพลาดในการสำรองข้อมูล ผู้สำรองข้อมูลต้องบันทึกรายละเอียดของข้อผิดพลาดที่เกิดขึ้น พร้อมแนวทางแก้ไข

9.3 ต้องมีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสม เพื่อให้สามารถกู้ข้อมูลกลับคืนได้

9.4 ต้องควบคุมความปลอดภัยของข้อมูลที่สำรองตามชั้นความลับ โดยใช้เทคโนโลยีที่เหมาะสมเพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

9.5 ต้องจัดให้มีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ และ การทดสอบควรดำเนินการบนสื่อที่จัดเตรียมไว้แยกจากสื่อที่ใช้สำหรับสำรองข้อมูลตามปกติ เพื่อป้องกันกรณีการทดสอบการกู้คืนข้อมูลไม่สำเร็จซึ่งอาจจะทำให้ข้อมูลที่สำรองไว้เสียหายและไม่สามารถนำกลับมาใช้งานได้

10. นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling policy)

10.1 การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้

10.1.1 บริษัทไม่อนุญาต ให้ใช้งานสื่อบันทึกข้อมูลพกพา ทุกชนิด

10.1.2 ในกรณีที่จำเป็นต้องใช้งานสื่อบันทึกข้อมูลพกพา จะต้องได้รับการอนุมัติจากผู้บริหารเป็นลายลักษณ์อักษร

10.1.3 ต้องใช้สื่อบันทึกพกพาของบริษัทเท่านั้น ไม่อนุญาตให้ใช้สื่อบันทึกพกพาของส่วนตัว

10.1.4 หลังการใช้งานทุกวัน ต้องจัดเก็บสื่อบันทึกพกพาไว้ที่แผนกบุคคล ห้ามนำสื่อบันทึกพกพาออกนอกบริษัท

10.1.5 มีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน

10.1.6 ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เพื่อลดโอกาสการสูญหายของข้อมูล

10.2 การทำลายสื่อบันทึกข้อมูล

10.2.1 สื่อที่บันทึกข้อมูลที่มีความสำคัญมาก จะต้องมีการทำลายด้วยวิธีการที่ปลอดภัย เช่น การเผา หรือแยกชิ้นส่วนเป็นชิ้นเล็ก ๆ หรือลบข้อมูลด้วยซอฟต์แวร์อื่น ๆ ที่มีใช้ใน บริษัท

10.2.2 กระบวนการต่าง ๆ ต้องระบุวิธีการกำจัดสื่อบันทึกข้อมูลอย่างชัดเจนเพื่อความปลอดภัย ของข้อมูล

10.2.3 เพื่อความสะดวกควรรวบรวมสื่อทั้งหมดที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

10.2.4 ในกรณีที่เลือกใช้บริการกำจัดสื่อและเอกสารรวมทั้งอุปกรณ์ต่าง ๆ จากหน่วยงานภายนอก ควรระมัดระวังในการเลือกใช้บริการต้องเลือกหน่วยงานภายนอกที่มีการควบคุมที่ดี มีมาตรฐานและมีประสบการณ์

10.2.5 ในการกำจัดสื่อบันทึกข้อมูลจะต้องมีการบันทึกเพื่อใช้ในการตรวจสอบ

ภาคผนวก

ลายเซ็นรบรองเอกสาร

หน้าที่	ชื่อ - นามสกุล	ตำแหน่ง	ลายมือชื่อ	วันที่
จัดทำโดย	นายอภิสร จันทรศร	หัวหน้าแผนกไอที		19 ม.ค. 2566
ทบทวน				
อนุมัติ				