นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของ

บริษัท ซีเค พาวเวอร์ จำกัด (มหาชน) และบริษัทในเครือ

สารบัญ

การควบคุมเอกสาร **1**

1. วัตถุประสงค์ **2**

2. ขอบข่าย **2**

3. คำนิยาม **2**

4. คำแถลงนโยบาย **3**

4.1 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 3

4.2. องค์กรภายใน 3

4.3. การรักษาความมั่นคงปลอดภัยด้านทรัพยากรมนุษย์ 4

4.4. การบริหารจัดการสินทรัพย์ 5

4.5. การควบคุมการเข้าถึง 6

4.6. วิทยาการเข้ารหัสลับ (CRYPTOGRAPHY) 8

4.7. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม 8

4.8. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน 9

4.9. ความมั่นคงปลอดภัยในการติดต่อสื่อสาร 10

4.10. การจัดหา การพัฒนา และการบำรุงรักษาระบบ 10

4.11. ความสัมพันธ์กับผู้จัดหา 11

4.12. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ 11

4.13. ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ 11

4.14. การปฏิบัติตามข้อกำหนด 11

5. เอกสารประกอบ **12**

การควบคุมเอกสาร

การอนุมัติเอกสาร

เอกสารนี้ได้รับการสอบทานและอนุมัติโดย:

จัดทำโดย	สอบทานโดย	สอบทานโดย
(นายอนุชา ประภาสนิรัติศัย) วันที่ (01/09/2565)	(นายอำนาจ ชื่นเจริญ) วันที่ (01/09/2565)	(นายบูรฮาน มะแด) วันที่ (01/09/2565)
Document Control	ISMA	ISMR

ประวัติการแก้ไขเอกสาร

รายละเอียดการแก้ไขเอกสารฉบับนี้:

แก้ไขครั้งที่	รายละเอียด	มีผลบังคับใช้วันที่
1.0	**จัดทำเอกสารครั้งแรก**	

1. วัตถุประสงค์

- จุดมุ่งหมายของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ คือ เพื่อกำหนดทิศทางและสนับสนุนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่ผู้บริหาร และกำหนดกฎเกณฑ์พื้นฐานทั่วไปสำหรับการดำเนินการตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับพนักงานทุกคนในองค์กรและบุคคลภายนอกที่ติดต่อธุรกิจกับองค์กร

2. ขอบข่าย

นโยบายฉบับนี้สำหรับใช้กับ:

- ทรัพยากรและสินทรัพย์ทั้งปวงที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของ ซีเค พาวเวอร์

3. คำนิยาม

- **บริษัท:** หมายถึง บริษัท ซีเค พาวเวอร์ จำกัด (มหาชน)
- **ผู้ใช้งาน:** หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหารจัดการ หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
- **สินทรัพย์:** หมายถึง สินทรัพย์ของบริษัทซึ่งประกอบด้วย เครื่องแม่ข่าย (เซิร์ฟเวอร์) ลูกค้า โครงสร้างเครือข่ายพื้นฐาน ระบบและซอฟต์แวร์ประยุกต์ ข้อมูล ตลอดจนระบบย่อยและส่วนประกอบคอมพิวเตอร์อื่นๆ ที่องค์กรเป็นเจ้าของหรือใช้งาน หรืออยู่ภายใต้ความรับผิดชอบขององค์กร นอกจากนี้ การใช้ระบบสารสนเทศหมายรวมถึงการใช้บริการต่างๆ ทั้งหมด ทั้งภายในและภายนอก เช่น การเข้าใช้อินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ เป็นต้น
- **การควบคุมการเข้าถึง:** หมายถึง การควบคุมและการจำกัดสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทที่เกี่ยวข้องกับการให้บริการและข้อมูลที่จำเป็นต่อการใช้งาน โดยมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากบุคคลทั้งภายในและภายนอก
- **การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ:** หมายถึง การดำรงรักษาไว้ซึ่งความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูลในระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
- **เหตุการณ์:** หมายถึง เหตุการณ์ที่ทำให้เกิดการขัดจังหวะที่อยู่นอกเหนือแผนที่วางไว้หรืออาจเป็นภัยคุกคามต่อการรักษาความลับ บูรณภาพ และความพร้อมใช้งานของสินทรัพย์ด้านเทคโนโลยีสารสนเทศขององค์กร

- **แผนกเทคโนโลยีสารสนเทศ:** หมายถึง หน่วยงานที่ดำเนินการเกี่ยวกับระบบสารสนเทศและระบบงานคอมพิวเตอร์และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศของบริษัท โดยมีหน้าที่ศึกษาวิเคราะห์เพื่อพัฒนาระบบสารสนเทศและระบบงานคอมพิวเตอร์ของบริษัท และปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง
- **รหัสผ่าน:** หมายถึง ตัวอักษร อักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูล เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศและการสื่อสาร

4. คำแถลงนโยบาย

4.1 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4.1.1. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- นโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจะต้องกำหนดและอนุมัติโดยคณะกรรมการอำนวยการ (steering committee) และจะต้องเผยแพร่และสื่อสารให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องทุกคนได้รับทราบ หลังจากได้รับการอนุมัติแล้ว

4.1.2. การสอบทานนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- การรักษาความมั่นคงปลอดภัยด้านสารสนเทศจะต้องได้รับการสอบทานเป็นประจำทุกปี หรือหากมีการแก้ไขเปลี่ยนแปลงที่เป็นสาระสำคัญ จะต้องได้รับการอนุมัติจากผู้บริหาร

4.2. องค์กรภายใน

4.2.1. บทบาทและความรับผิดชอบในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- ต้องกำหนดบทบาทและความรับผิดชอบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับแต่ละตำแหน่งงานในองค์กร

4.2.2. การแบ่งแยกหน้าที่

- ต้องกำหนดบทบาทและหน้าที่ความรับผิดชอบที่กำหนดดังกล่าวแยกออกจากกัน เพื่อไม่ให้เกิดความขัดแย้งเกี่ยวกับบทบาทและหน้าที่ความรับผิดชอบเช่นว่านั้น

4.2.3. การติดต่อกับหน่วยงานที่เกี่ยวข้อง

- ต้องติดต่อกับหน่วยงานที่เกี่ยวข้องอย่างเหมาะสม

4.2.4. การติดต่อกับกลุ่มที่มีความสนใจพิเศษ

- ต้องติดต่อกับกลุ่มที่มีความสนใจพิเศษของสมาคมผู้เชี่ยวชาญด้านความปลอดภัยอื่นๆ อย่างเหมาะสม

4.2.5. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารโครงการ

- ต้องกำหนดให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารโครงการ โดยการบริหารโครงการจะต้องมีวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งถือเป็นส่วนหนึ่งในทุกขั้นตอนของวิธีการบริหารโครงการที่ใช้

4.2.6. อุปกรณ์เคลื่อนที่และการทำงานจากระยะทางไกล

- ห้ามใช้อุปกรณ์เคลื่อนที่ ซึ่งรวมถึงสมาร์ทโฟนและแท็บเล็ต โดยไม่ได้รับอนุญาต
- อนุญาตให้พนักงานขององค์กรเข้าใช้งานจากระยะทางไกลผ่านแล็ปท็อปหรือโน้ตบุ๊กที่องค์กรจัดเตรียมไว้ให้เท่านั้น

4.3. การรักษาความมั่นคงปลอดภัยด้านทรัพยากรมนุษย์

4.3.1. ก่อนการจ้างงาน

- **การคัดกรอง:** การตรวจสอบประวัติของผู้สมัครงานทุกคนจะต้องดำเนินการตามกฎหมาย ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และเป็นไปตามเงื่อนไขความต้องการทางธุรกิจ
- **ข้อกำหนดและเงื่อนไขการจ้างงาน:** ในสัญญาหรือข้อตกลงที่ทำกับพนักงานและผู้รับจ้าง จะต้องระบุหน้าที่ความรับผิดชอบของพนักงานและผู้รับจ้างในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการปกป้องคุ้มครองสารสนเทศขององค์กรไว้ด้วย

4.3.2. ระหว่างการจ้างงาน

- **หน้าที่ความรับผิดชอบของผู้บริหาร:** ผู้บริหารต้องดำเนินการเพื่อให้พนักงาน ผู้รับจ้าง และบุคคลภายนอกตระหนักถึงหน้าที่ความรับผิดชอบของตนตามที่กำหนดไว้ในนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- **การตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การศึกษา และการฝึกอบรม:** ต้องสร้างจิตสำนึกและจัดให้มีการฝึกอบรมแก่พนักงานทุกคนอย่างน้อยปีละ 1 ครั้ง อาทิ ส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาเกี่ยวกับการสร้างจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยให้แก่พนักงาน เป็นต้น
- **กระบวนการทางวินัย:** กำหนดให้มีกระบวนการลงโทษทางวินัยอย่างเป็นทางการ

4.3.3. การสิ้นสุดการจ้างงานและการเปลี่ยนลักษณะการจ้างงาน

- จะต้องกำหนดและดำเนินการตามกระบวนการสิ้นสุดการจ้างงานและการเปลี่ยนลักษณะการจ้างงานอย่างเป็นทางการ ซึ่งรวมถึงกระบวนการส่งคืนสินทรัพย์และการตรวจสอบสิทธิ์การเข้าถึงสินทรัพย์ของผู้ใช้งานด้วย

4.4. การบริหารจัดการสินทรัพย์

4.4.1. ความรับผิดชอบต่อสินทรัพย์

- **ทะเบียนสินทรัพย์:** ต้องกำหนดรายชื่อและจัดทำเอกสารทะเบียนสินทรัพย์ โดยจะต้องมีการสอบทานอย่างน้อยปีละ 1 ครั้ง เพื่อรักษาความถูกต้องของทะเบียนสินทรัพย์
- **กรรมสิทธิ์ในสินทรัพย์:** ต้องกำหนดและจัดทำเอกสารรายชื่อผู้เป็นเจ้าของสินทรัพย์ทั้งหมด
- **การใช้งานสินทรัพย์อย่างเหมาะสม:** ต้องกำหนดให้มีการใช้งานสินทรัพย์ขององค์กรอย่างเหมาะสม
- **การส่งคืนสินทรัพย์:** เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนลักษณะการจ้างงาน พนักงานจะต้องส่งคืนสินทรัพย์ขององค์กรทั้งหมดที่อยู่ในความครอบครองของตน

4.4.2. การจัดลำดับชั้นสารสนเทศ

- **การจัดลำดับชั้นสารสนเทศ:** ต้องจัดลำดับชั้นสารสนเทศโดยจำแนกตามคุณค่า ข้อกำหนดทางกฎหมาย ความอ่อนไหว และความสำคัญต่อองค์กร
- **การติดป้ายชื่อสารสนเทศ:** ต้องติดป้ายชื่อสารสนเทศอย่างเหมาะสมตามที่ได้จัดลำดับชั้นความลับไว้
- **การจัดการสินทรัพย์:** ต้องดำเนินการจัดการสารสนเทศอย่างเหมาะสมตามการจัดลำดับชั้นสารสนเทศ

4.4.3. การจัดการสื่อที่ใช้ในการบันทึกข้อมูล

- **การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้:** จะต้องมีการบริหารจัดการและควบคุมสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ซึ่งรวมถึงอุปกรณ์ที่สามารถเก็บข้อมูล ใส่และถอดออกจากระบบได้
- **การกำจัดสื่อบันทึกข้อมูล:** ต้องมีการกำจัดสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไป ด้วยวิธีการที่ปลอดภัย อาทิ การล้างข้อมูลด้วยวิธีการที่ปลอดภัย

- **การถ่ายโอนสื่อบันทึกข้อมูล:** ต้องมีการป้องกันสื่อบันทึกข้อมูลที่มีข้อมูล มิให้มีการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานผิดวัตถุประสงค์ และการทุจริต ในระหว่างการถ่ายโอนข้อมูลตามที่มีการจัดลำดับชั้น

4.5. การควบคุมการเข้าถึง

4.5.1. การควบคุมการเข้าถึงตามความต้องการทางธุรกิจ

- **นโยบายการควบคุมการเข้าถึง**
  - ต้องกำหนดสิทธิในการเข้าถึงสารสนเทศ ระบบประมวลผลสารสนเทศ และสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ ตามวัตถุประสงค์ทางธุรกิจ และภายใต้หลักความจำเป็นต้องรู้ (need-to-know) และความจำเป็นต้องใช้งาน (need-to-use)
  - ต้องจำกัดสิทธิในการเข้าถึงสารสนเทศ ระบบประมวลผลสารสนเทศ และสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ สำหรับบัญชีผู้ใช้งานโดยได้รับอนุญาตน้อยที่สุดเท่าที่เป็นไปได้ตามความจำเป็นในการปฏิบัติงานของผู้ใช้งาน
  - ต้องกำหนดสิทธิในการเข้าถึงสารสนเทศ ระบบประมวลผลสารสนเทศ และสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ ให้เป็นไปตามการจัดลำดับชั้นสารสนเทศ
  - ต้องจำแนกบัญชีผู้ใช้งานที่ใช้สิทธิในการเข้าถึงสารสนเทศ ระบบประมวลผลสารสนเทศ และสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ ออกจากบัญชีผู้ใช้งานอื่น และระบุชื่อผู้เป็นเจ้าของบัญชีได้
  - ต้องใช้กระบวนการพิสูจน์ตัวตนและการอนุญาตที่มั่นคงปลอดภัย โดยกระบวนการที่นำมาใช้ดังกล่าวต้องมีความเหมาะสมกับความสำคัญของสารสนเทศ การจัดลำดับชั้นสารสนเทศ ระบบประมวลผลสารสนเทศ และสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ
  - กำหนดให้มีบัญชีผู้ใช้งานที่มีสิทธิ์สูงเฉพาะเมื่อมีความจำเป็นต้องใช้งานและต้องได้รับการอนุมัติจากเจ้าของสินทรัพย์หรือผู้มีอำนาจ
  - ต้องจัดการบัญชีผู้ใช้งานและสารสนเทศด้านการพิสูจน์ตัวตนที่เป็นความลับที่ได้รับจากองค์กร ด้วยความระมัดระวัง
  - ต้องมีการลงบันทึกรายละเอียดของกิจกรรมทั้งหมดที่ดำเนินการระหว่างการเข้าถึงสารสนเทศ ระบบประมวลผลสารสนเทศ และสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ ซึ่งการลงบันทึกดังกล่าวอย่างน้อยต้องประกอบด้วยสารสนเทศที่สามารถใช้เพื่อระบุตัวบุคคล การประทับเวลา และกิจกรรมที่ดำเนินการได้
  - ต้องลบบัญชีผู้ใช้งานที่ไม่ต้องใช้งานอีกต่อไปออกจากระบบ

- กำหนดบัญชีผู้ใช้งานให้เป็นรายบุคคล ซึ่งบัญชีดังกล่าวไม่อาจใช้ร่วมกับบุคคลอื่นได้
- ต้องมีการสอบทานบัญชีผู้ใช้งานและสิทธิ์ในการเข้าถึงอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน การลาหยุดของพนักงาน หรือสถานการณ์อื่นๆ ที่อาจส่งผลกระทบต่อสิทธิ์ในการเข้าถึงสารสนเทศ ระบบประมวลผลสารสนเทศ หรือสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ เพื่อปรับปรุงให้ทันสมัยและมีความถูกต้อง

- **การเข้าถึงเครือข่ายและการบริการเครือข่าย:** ต้องได้รับการอนุญาตให้เข้าถึงเครือข่ายและการบริการเครือข่ายขององค์กร อย่างเหมาะสมตามความจำเป็นในการใช้งาน

4.5.2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน

- **การลงทะเบียนและการเพิกถอนทะเบียนผู้ใช้งาน:** ต้องกำหนดให้มีขั้นตอนการลงทะเบียนและการเพิกถอนทะเบียนผู้ใช้งานและต้องนำไปปฏิบัติตาม
- **การจัดการสิทธิการเข้าถึงของผู้ใช้งาน:** ต้องกำหนดสิทธิ์ในการเข้าถึงที่แตกต่างกันไปสำหรับผู้ใช้งานแต่ละประเภทตามความจำเป็นในการใช้งาน
- **การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิพิเศษ:** ต้องมีการจำกัดและควบคุมสิทธิ์ในการเข้าถึงตามระดับสิทธิพิเศษ
- **การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนผู้ใช้งาน:** ต้องส่งรหัสผ่านและข้อมูลความลับสำหรับการพิสูจน์ตัวตนอื่นๆ ให้แก่ผู้ใช้งานด้วยวิธีการที่ปลอดภัยและให้ดำเนินการจัดการเสมือนข้อมูลที่มีความอ่อนไหว
- **การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน:** ต้องมีการทบทวนสิทธิในการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง
- **การเพิกถอนหรือเปลี่ยนแปลงสิทธิการเข้าถึงของผู้ใช้งาน:** ต้องมีการเพิกถอนสิทธิในการเข้าถึงของผู้ใช้งานเมื่อสัญญาหรือข้อตกลงของผู้ใช้งานสิ้นสุดลง หรือมีการปรับเปลี่ยนสิทธิในการเข้าถึงดังกล่าวเมื่อมีการเปลี่ยนแปลงสถานะการจ้างงานของผู้ใช้งาน

4.5.3. ความรับผิดชอบของผู้ใช้งาน

- **การใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตน:** พนักงานและบุคคลใดๆ ก็ตามที่อาจมีรหัสผ่านหรือข้อมูลความสำหรับการพิสูจน์ตัวตนอื่นๆ ขององค์กร จะต้องปฏิบัติตามแนวทางปฏิบัติขององค์กร

4.5.4. การควบคุมการเข้าถึงระบบและแอปพลิเคชัน

- **การจำกัดสิทธิในการเข้าถึงสารสนเทศ:** ต้องกำหนดให้มีการเข้าถึงสารสนเทศตามหลักความจำเป็นต้องรู้ (need-to-know)
- **ขั้นตอนในการเข้าใช้งาน (log-on) อย่างปลอดภัย:** ต้องกำหนดให้มีกระบวนการพิสูจน์ตัวตนในการเข้าถึงแต่ละระบบและแต่ละแอปพลิเคชันขององค์กร
- **ระบบบริหารจัดการรหัสผ่าน:** ต้องกำหนดและจัดทำเอกสารการบริหารจัดการรหัสผ่านและข้อกำหนดความซับซ้อนของรหัสผ่าน
- **การใช้งานโปรแกรมอรรถประโยชน์ระดับสิทธิพิเศษ:** ต้องมีการจำกัดและควบคุมโปรแกรมอรรถประโยชน์ โดยจะอนุญาตให้เฉพาะสิทธิ์ในการเข้าถึงระดับผู้ดูแลระบบเท่านั้น

4.6. วิทยาการเข้ารหัสลับ (cryptography)

4.6.1. ต้องมีการควบคุมและใช้วิทยาการเข้ารหัสลับที่เหมาะสมกับสารสนเทศที่ได้จัดลำดับชั้นความลับไว้ และต้องมีการควบคุมการเข้ารหัสคีย์ที่ใช้สำหรับการเข้ารหัสลับเพื่อปกป้องข้อมูลจากการเข้าถึงหรือการจัดการโดยผู้ที่ไม่ได้รับอนุญาต

4.7. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

4.7.1. การควบคุมการเข้าออกพื้นที่

- ต้องจัดให้มีการควบคุมการเข้าออกพื้นที่เพื่อให้แน่ใจได้ว่า เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงพื้นที่นั้นได้ ทั้งนี้ จะต้องจัดให้มีพนักงานคอยดูแลติดตามผู้เยี่ยมชมที่มีความจำเป็นต้องเข้าออกพื้นที่ขององค์กร โดยจะต้องมีการสอบทานการลงบันทึกการเข้าออกพื้นที่เป็นประจำอย่างสม่ำเสมอ

4.7.2. การรักษาความมั่นคงปลอดภัยของอุปกรณ์

- **การนำสินทรัพย์ออกนอกสถานที่:** ห้ามนำอุปกรณ์ออกนอกสถานที่โดยไม่ได้รับการอนุญาตและความเห็นชอบล่วงหน้าจากผู้มีอำนาจหรือเจ้าของสินทรัพย์
- **การทำลายอุปกรณ์ด้วยวิธีการที่ปลอดภัยหรือการนำอุปกรณ์กลับมาใช้งาน:** ต้องมีการทำลายอุปกรณ์ด้วยวิธีการที่ปลอดภัย
- **นโยบายโต๊ะทำงานปลอดข้อมูลสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy):** ต้องไม่วางทิ้งสารสนเทศทั้งปวงไว้บนโต๊ะทำงาน

4.8. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

4.8.1. ขั้นตอนและความรับผิดชอบในการดำเนินงาน

- **เอกสารการดำเนินงานและความรับผิดชอบ:** ต้องจัดทำเอกสาร เก็บรักษา และจัดเตรียมขั้นตอนการดำเนินงานให้พร้อมใช้งานแก่ผู้ใช้งานทุกรายที่มีความจำเป็นต้องใช้
- **การบริหารจัดการการเปลี่ยนแปลงด้านสารสนเทศ:** ต้องมีการควบคุมการเปลี่ยนแปลงขององค์กรที่อาจกระทบต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร
- **การบริหารจัดการความต้องการทรัพยากรสารสนเทศ:** ต้องเฝ้าติดตามและวางแผนการใช้ทรัพยากรสารสนเทศเป็นประจำอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่า มีทรัพยากรสารสนเทศเพียงพอต่อความต้องการใช้งานในอนาคต
- **การแยกเครื่องมือในการประมวลผลสารสนเทศสำหรับการพัฒนา การทดสอบ และการปฏิบัติงานจริงออกจากกัน:** ต้องแยกเครื่องมือในการประมวลผลสารสนเทศที่ใช้ในการพัฒนา การทดสอบ และปฏิบัติงานจริงออกจากกัน

4.8.2. การป้องกันซอฟต์แวร์ที่ไม่พึงประสงค์ (malware)

- **การป้องกันจากการถูกทำลายจากซอฟต์แวร์ที่ไม่พึงประสงค์:** ต้องดำเนินการควบคุมการตรวจหา การป้องกัน และการกู้คืนเพื่อป้องกันมิให้ถูกทำลายจากซอฟต์แวร์ที่ไม่พึงประสงค์ และต้องปรับปรุงให้ทันสมัยอยู่เสมอ

4.8.3. การสำรองข้อมูล

- **การสำรองข้อมูล:** ต้องสำรองข้อมูลเป็นประจำอย่างสม่ำเสมอ และต้องทดสอบการสำรองข้อมูลเป็นประจำอย่างสม่ำเสมอ

4.8.4. การเฝ้าระวังและการบันทึกเหตุการณ์

- **การบันทึกเหตุการณ์:** ต้องบันทึก เก็บรักษา และสอบทานกิจกรรมการใช้งานของผู้ใช้งานอย่างสม่ำเสมอ
- **การป้องกันข้อมูลบันทึกเหตุการณ์:** ต้องป้องกันข้อมูลบันทึกเหตุการณ์จากการเข้าถึงและการดัดแปลงโดยไม่ได้รับอนุญาต
- **การบันทึกข้อมูลของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ:** ต้องมีการบันทึกกิจกรรมของผู้ดูแลระบบ
- **การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน:** ต้องตั้งเวลาของระบบประมวลผลสารสนเทศขององค์กรให้ตรงกับแหล่งเวลาที่เชื่อถือได้

4.8.5. การควบคุมซอฟต์แวร์ที่ใช้ปฏิบัติงาน

- **การติดตั้งซอฟต์แวร์ในระบบปฏิบัติการ:** การติดตั้งซอฟต์แวร์ต้องได้รับการดำเนินการหรือได้รับการอนุมัติโดยคณะทำงานด้านเทคโนโลยีสารสนเทศ

4.8.6. การบริหารจัดการช่องโหว่ทางเทคนิค

- **การบริหารจัดการช่องโหว่ทางเทคนิค:** ต้องพิจารณาติดตั้งและปรับปรุงอุปกรณ์ทั้งหมดให้ทันสมัยหรือดำเนินการใดๆ เพื่อบริหารจัดการช่องโหว่ตามคำแนะนำที่ได้รับจากบุคคลภายนอกที่เกี่ยวข้อง เพื่อให้ไม่มีผลกระทบต่ออุปกรณ์หรือซอฟต์แวร์เป็นประจำอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง
- **การจำกัดสิทธิในการติดตั้งซอฟต์แวร์:** การติดตั้งซอฟต์แวร์ต้องได้รับการดำเนินการหรือได้รับการอนุมัติโดยคณะทำงานด้านเทคโนโลยีสารสนเทศ

4.8.7. การพิจารณาการตรวจสอบระบบสารสนเทศ

- **การควบคุมการตรวจสอบระบบสารสนเทศ:** ต้องมีการวางแผนเกี่ยวกับกิจกรรมการตรวจสอบอุปกรณ์ประมวลผลสารสนเทศอย่างรอบคอบ เพื่อลดความเสี่ยงที่อาจเกิดขึ้นระหว่างการตรวจสอบ

4.9. ความมั่นคงปลอดภัยในการติดต่อสื่อสาร

4.9.1. การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย

- ต้องป้องกันระบบเครือข่ายภายในให้ปลอดจากการเข้าถึงและการดัดแปลงโดยไม่ได้รับอนุญาต
- ต้องแยกระบบเครือข่ายภายในออกจากกันเพื่อควบคุมการเข้าถึงบริการ ระบบ หรือสารสนเทศภายในองค์กร

4.9.2. การถ่ายโอนสารสนเทศ

- ต้องมีการถ่ายโอนสารสนเทศด้วยวิธีการที่ปลอดภัยและเหมาะสมกับประเภทชั้นของสารสนเทศตามที่องค์กรกำหนด

4.10. การจัดหา การพัฒนา และการบำรุงรักษาระบบ

- ต้องมีการกำหนดเงื่อนไขด้านความปลอดภัยเมื่อสร้างระบบหรือโครงการประมวลผลสารสนเทศใหม่
- ต้องดำเนินการทดสอบการใช้งานเครื่องมือหรือซอฟต์แวร์ที่จัดหาให้แก่ลูกค้าขององค์กรโดยผู้ใช้งานจริง

4.11. ความสัมพันธ์กับผู้จัดหา

- ในข้อตกลงกับผู้จัดหา ต้องกำหนดให้มีข้อตกลงการรักษาความลับและการรักษาความมั่นคงปลอดภัยขององค์กร อาทิเช่น
  - ผู้จัดหาจะต้องปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องทั้งหมด
  - ผู้จัดหาจะต้องไม่นำพาองค์กรไปสู่การโจมตีทางไซเบอร์หรือการกระทำที่ขัดต่อกฎหมายหรือข้อบังคับใดๆ ทั้งสิ้น
  - จำเป็นต้องมีการแจ้งเตือนล่วงหน้าเมื่อมีการเปลี่ยนแปลงผู้จัดหาขององค์กรที่อาจส่งผลกระทบต่อองค์กร
- ให้ถือว่าข้อมูลก่อนทำสัญญาและหลังทำสัญญาเป็นข้อมูลลับ
- ผู้จัดหาจะต้องปฏิบัติตามนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงนโยบายอื่นๆ และจรรยาบรรณขององค์กร
- ต้องมีการทบทวนและประเมินผลการบริการและผลผลิตที่ต้องส่งมอบอื่นๆ ที่ได้รับจากผู้จัดหา เพื่อให้แน่ใจได้ว่า ผู้จัดหาจะไม่เกินข้อตกลงระดับในการให้บริการ (SLA) หรือข้อกำหนดอื่นใด
- ผู้จัดหาจะต้องปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องทั้งหมด

4.12. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

- ต้องมีการกำหนดแผนเผชิญเหตุ
- ต้องมีการกำหนดบทบาทและหน้าที่ความรับผิดชอบและสื่อสารให้แต่ละบุคคลรับทราบ พร้อมแผนเผชิญเหตุ
- ต้องบันทึกหลักฐานของเหตุการณ์ที่เกิดขึ้นไว้เป็นฐานความรู้

4.13. ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ

- องค์กรต้องวางแผนและจัดทำเอกสารเกี่ยวกับแผนความต่อเนื่องทางธุรกิจ โดยแผนดังกล่าวจะต้องได้รับการทดสอบและประเมินผลเพื่อปรับปรุงอย่างน้อยปีละ 1 ครั้ง

4.14. การปฏิบัติตามข้อกำหนด

4.14.1. การปฏิบัติตามข้อกำหนดทางสัญญาและกฎหมาย

- **การระบุข้อกำหนดทางสัญญาและกฎหมายที่บังคับใช้:** ต้องมีการระบุและดำเนินการให้เป็นไปตามกฎหมายและระเบียบที่บังคับใช้ โดยการดำเนินงานขององค์กรต้องไม่ขัดต่อกฎหมายและระเบียบที่ใช้บังคับดังกล่าว
- **สิทธิ์ในการใช้งานทรัพย์สินทางปัญญา:** พนักงานต้องตรวจสอบให้แน่ใจว่าการใช้ทรัพย์สินทางปัญญาไม่ขัดต่อสัญญาที่ทำกับเจ้าของสินทรัพย์ และกฎหมายที่บังคับใช้
- **การปกป้องคุ้มครองบันทึก:** บันทึกทั้งหมดขององค์กรจะต้องได้รับการรักษาความปลอดภัยด้วยมาตรการการควบคุมที่เหมาะสม
- **ความเป็นส่วนตัวและการปกป้องคุ้มครองข้อมูลที่ระบุตัวตนได้:** ข้อมูลที่ระบุตัวตนได้จะต้องได้รับการคุ้มครองอย่างน้อยตามที่กฎหมายและระเบียบที่บังคับใช้กำหนด
- **มาตรการควบคุมการเข้ารหัสลับ:** ต้องใช้และปฏิบัติตามมาตรการควบคุมการเข้ารหัสลบตามข้อตกลง กฎหมาย และระเบียบที่บังคับใช้

4.14.2. การสอบทานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- ต้องจัดให้มีการตรวจสอบภายใน เพื่อสอบทานการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติต่างๆ ขององค์กรอย่างน้อยปีละ 1 ครั้ง
- ต้องจัดให้มีการสอบทานสินทรัพย์ทางด้านเทคนิคภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) อย่างน้อยปีละ 1 ครั้ง

5. เอกสารประกอบ

- ไม่มี

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

-ลงลายมือชื่อ-

(ดร.ทนง พิทยะ)

ประธานกรรมการ