MFEC

นโยบายการบริหารจัดการ ด้านความมั่นคงปลอดภัยสารสนเทศ

(Information Security Policy)

Version 2.0

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เนื่องจาก MFEC Public Company Limited (MFEC) ได้นำระบบสารสนเทศ มาใช้ในการดำเนินงานและให้บริการ ผู้ใช้งานทั้งภายในและภายนอกองค์กร ดังนั้นเพื่อให้การใช้สารสนเทศและระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่เหมาะสม หรือถูกคุกคามจากภัยต่าง ๆ ซึ่งจะช่วยลดความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน และบุคลากร

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การรักษาความมั่นคงปลอดภัยในการใช้งานสารสนเทศและระบบ เทคโนโลยีสารสนเทศของ MFEC ไม่เปิดเผยข้อมูลสารสนเทศ หรือระบบงานต่อบุคคลที่ไม่ได้รับสิทธิ์ (Confidentiality) การรักษาไว้ซึ่งความถูกต้องและความครบถ้วนของข้อมูลสารสนเทศ (Integrity) และความสามารถในการเข้าถึงและการใช้งานได้ตามความต้องการของผู้ที่ได้รับสิทธิ์ (Availability)

MFEC จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีนโยบาย (Policy) แนวทางปฏิบัติ (Guideline) ข้อกำหนด (Standard) และขั้นตอนปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษร โดย สอดคล้องตามกฎหมาย มาตรฐาน และแนวปฏิบัติสากล ของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ทั้งนี้ รายละเอียดและโครงสร้างเอกสารนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สามารถดูได้ในเอกสารแนบท้าย องค์ประกอบและโครงสร้างของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ

1. เพื่อกำหนดและประกาศนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติ ตามอย่างเหมาะสม
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของ MFEC ว่า สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)
3. เพื่อพัฒนากระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศดำเนินการอย่างเป็นระบบ และมีการพัฒนาปรับปรุงอย่างสม่ำเสมอ
4. เพื่อปฏิบัติตามระเบียบ ข้อบังคับ สัญญา และกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

แนวทาง

แนวปฏิบัติด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ (อ้างอิงเอกสาร MFEC-ISMS-PO-002)

1. จัดทำการศึกษา พัฒนา และจัดทำรายละเอียดการดำเนินการบริบทองค์กร ความต้องการผู้มีส่วนได้ส่วนเสีย และการกำหนดขอบเขตการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นแนวทางในการดำเนินการ
2. จัดทำกรอบดำเนินการมาตรฐานด้านความมั่นคงปลอดภัยเพื่อเป็นต้นแบบการดำเนินการที่ชัดเจน

3. กำหนดให้ผู้บริหารระดับสูงเข้ามีส่วนร่วม พร้อมจัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และการกำหนดบทบาทหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศให้ชัดเจน
4. กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และพิจารณากับการประเมินความเสี่ยง เพื่อใช้จัดทำแผนด้านความมั่นคงปลอดภัยสารสนเทศประจำปี
5. กำหนดให้การสนับสนุนด้านทรัพยากร การพัฒนาความรู้ความสามารถ ความตระหนักของบุคลากรที่เกี่ยวข้อง การสื่อสารตลอดกระบวนการ และการจัดทำเอกสารเพื่อให้บรรลุต่อวัตถุประสงค์ของความมั่นคงปลอดภัยสารสนเทศ
6. ติดตามโครงการ กระบวนการด้านความมั่นคงปลอดภัยเพื่อให้บรรลุต่อการดำเนินการตามแผนที่วางไว้
7. จัดทำการวัตประสิทธิภาพการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศในมิติต่าง ๆ ทั้งด้านนโยบาย ความเข้าใจของบุคลากร กระบวนการดำเนินการ กฎหมายที่เกี่ยวข้อง และเทคโนโลยีสารสนเทศ
8. การติดตามการปฏิบัติจากหน่วยงานอิสระด้านความมั่นคงปลอดภัยสารสนเทศเพื่อให้เกิดความโปร่งใส และมีประสิทธิภาพในการดำเนินการ
9. การจัดทำรายงานผลการดำเนินการเสนอให้กับผู้บริหารเพื่อรับทราบ และตัดสินใจในการดำเนินการเพื่อปรับปรุงประสิทธิภาพ ประสิทธิผลการ ดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ

1. นโยบายย่อยการควบคุมการเข้าถึงสารสนเทศ (Access control)

MFEC Public Company Limited (MFEC) มีการควบคุมการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เพื่อ กำหนดมาตรการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต ป้องกันการบุกรุกทั้งด้านกายภาพ ผ่านระบบเครือข่าย และจากโปรแกรม ที่จะสร้างความเสียหายแก่ข้อมูลหรือทำให้ระบบหยุดชะงัก และสามารถตรวจสอบติดตามการพิสูจน์ตัวบุคคลที่ใช้งานข้อมูลหรือระบบสารสนเทศขององค์การได้อย่างถูกต้องโดยยึดหลักดังนี้

1. การรักษาความลับ (Confidentiality) ให้บุคคลผู้มีสิทธิ์เท่านั้น เข้าถึงข้อมูลได้ และมีการควบคุมการเข้าถึงโดยข้อมูลที่เป็นความลับ จะได้ไม่ถูกเปิดเผยกับผู้ไม่มีสิทธิ์
2. ความถูกต้องครบถ้วน (Integrity) ให้มีการรักษาความถูกต้องครบถ้วนของข้อมูล และควบคุมความผิดพลาด ไม่ให้ข้อมูลถูกแก้ไข ลบทิ้ง เปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์
3. ความสามารถในการเข้าถึงและใช้งานได้ (Availability) ให้ผู้มีสิทธิ์ใช้ข้อมูลเท่านั้นสามารถที่จะเข้าถึงข้อมูลได้ตามเวลาที่ตกลงไว้ ผู้รับผิดชอบต้องควบคุมไม่ให้ระบบหยุดชะงัก มีสมรรถภาพในการทำงานต่อเนื่อง และมีการป้องกันไม่ให้มีสิ่งใดทำให้ระบบหยุดทำงาน

วัตถุประสงค์ของการควบคุมการเข้าถึงสารสนเทศ

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ตระหนักถึงความสำคัญของการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของ MFEC ว่า สามารถเข้าถึงได้เฉพาะผู้มีสิทธิ์ (Confidentiality) มีความครบถ้วนสมบูรณ์ (Integrity) และมีความพร้อมใช้งาน (Availability)
3. เพื่อให้สามารถตรวจสอบย้อนหลังการเข้าถึงระบบสารสนเทศต่าง ๆ ของผู้ใช้งานได้

แนวทาง

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติด้านการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. จัดให้มีข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยวข้องกับ สารสนเทศ การพัฒนาและบำรุงรักษาระบบสารสนเทศ และสิ่งใด ๆ ที่เกี่ยวข้องกับสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่าง เหมาะสมและเพียงพอ และมีการกำหนดการควบคุมการใช้งานและการเข้าถึงที่อย่างชัดเจนตามหลักการของความต้องการในการ ใช้งานที่เหมาะสมและมั่นคงปลอดภัย
3. จัดให้มีแนวทางปฏิบัติในการพัฒนาการซอฟต์แวร์ ที่ต้องควบคุมการเข้าถึงและสิทธิ์ในการใช้ข้อมูลในระบบ ไปจนกระทั้งการควบคุมการเข้าถึงด้วยระบบปฏิบัติการ ซึ่งรวมถึงการใช้ข้อมูลในส่วนต่าง ๆ ภายในคอมพิวเตอร์ของผู้ใช้งาน
4. จัดให้มีแนวทางปฏิบัติในการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ และอุปกรณ์สารสนเทศ
5. จัดให้มีแนวทางปฏิบัติในการการควบคุมการเข้าถึงห้องเครื่องแม่ข่าย หรือศูนย์ข้อมูลบนอินเทอร์เน็ต รวมทั้งอุปกรณ์สารสนเทศให้ เข้าได้เฉพาะผู้มีสิทธิ์เท่านั้น
6. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งานข้อมูลและระบบ สารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

ขอบเขตของนโยบายย่อยการควบคุมการเข้าถึงสารสนเทศ

ขอบเขตของนโยบายย่อยการควบคุมการเข้าถึงสารสนเทศ หมายถึง การเข้าถึงสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยี สารสนเทศ ห้องเครื่องแม่ข่าย ระบบเครือข่าย อุปกรณ์เทคโนโลยีสารสนเทศ โดยสารสนเทศหมายรวมถึงสารสนเทศที่อยู่ในรูปแบบของ อิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

2. นโยบายย่อยการแบ่งชั้นความลับ (Data Classification)

MFEC Public Company Limited (MFEC) มีการแบ่งชั้นความลับ เพื่อให้ผู้ใช้ข้อมูลสารสนเทศและเจ้าของข้อมุลสารสนเทศตระหนักต่อวิธีปฏิบัติที่เหมาะสมถูกต้อง และช่วยให้ข้อมูลสารสนเทศดำเนินการตามวิธีการบริหารจัดการข้อมูลสารสนเทศที่เหมาะสมตามหลัก การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความสามารถในการเข้าถึงและใช้งานได้ (Availability)

วัตถุประสงค์ของการควบคุมการเข้าถึงสารสนเทศ

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ตระหนักถึงความสำคัญของการดูแล และบำรุงรักษาข้อมูลสารสนเทศ ตั้งแต่สร้าง ใช้งาน ถึงการเลิกใช้งาน
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของ MFEC ว่า สามารถเข้าถึงได้เฉพาะผู้มีสิทธิ์ (Confidentiality) มี ความครบถ้วนสมบูรณ์ (Integrity) และมีความพร้อมใช้งาน (Availability)
3. เพื่อให้พนักงานมีความตระหนักต่อความปลอดภัยของข้อมูลสารสนเทศ

แนวทาง

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติด้านการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งานข้อมูลและระบบ สารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

ขอบเขตของนโยบายย่อยการแบ่งชั้นความลับ

ขอบเขตของนโยบายย่อยการแบ่งชั้นความลับ หมายถึงการกำหนดแนวทางปฏิบัติต่อชนิดของข้อมูลสารสนเทศตั้งแต่เริ่มจัดทำหรือได้มา การใช้งาน การสำเนา การกระจาย จนถึงการยกเลิกการใช้หรือการทำลาย ครอบคลุมสารสนเทศที่อยู่ในรูปแบบของ อิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

3. นโยบายย่อยด้านการดำเนินการอย่างปลอดภัย (Operation Security)

MFEC Public Company Limited (MFEC) มีกำหนดนโยบายนี้เพื่อให้การดำเนินการประจำมีความเพียงพอ และดำเนินการได้อย่างถูกต้องเหมาะสม และปลอดภัยตามเกณฑ์มาตรฐานการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความสามารถในการเข้าถึงและใช้งานได้ (Availability)

วัตถุประสงค์ของการดำเนินการอย่างปลอดภัย

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ทราบถึงกิจกรรมที่จำเป็นในการดำเนินการกับข้อมูลสารสนเทศ
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นใจในการดำเนินการกับข้อมูลสารสนเทศ และระบบสารสนเทศในเชิงการป้องกัน และการกู้คืนกรณีที่พบปัญหากับข้อมูลสารสนเทศ หรือระบบงานสารสนเทศ
3. เพื่อให้ผู้บริหารได้รับรายงานที่เหมาะสม เพียงพอต่อการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ

แนวทาง

1. จัดให้มีแนวทางปฏิบัติและขั้นตอนปฏิบัติด้านการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งานข้อมูลและระบบ สารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

ขอบเขตของนโยบายย่อยการดำเนินการอย่างปลอดภัย

ขอบเขตของนโยบายย่อยการการดำเนินการอย่างปลอดภัย หมายถึงการกำหนดแนวทางปฏิบัติต่อการดำเนินงานต่าง ๆ ที่จำเป็นเพื่อสร้างความมั่นใจในการใช้งานข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศ

4. นโยบายย่อยความปลอดภัยในการสื่อสาร (Communication Security)

MFEC Public Company Limited (MFEC) มีกำหนดนโยบายนี้เพื่อให้เกิดความปลอดภัยในการสื่อสารทั้งภายใน แลภายนอกองค์กร ตามเกณฑ์มาตรฐานการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความสามารถในการเข้าถึงและใช้งานได้ (Availability)

วัตถุประสงค์ของความปลอดภัยในการสื่อสาร

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ทราบถึงกิจกรรมที่จำเป็นในการดำเนินการกับการสื่อสารสารสนเทศ
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นใจในการดำเนินการกับการแลกเปลี่ยนข้อมูลสารสนเทศในเชิงการป้องกัน
3. เพื่อให้ผู้ใช้งานระบบสารสนเทศมีความมั่นใจในการติดต่อข้อมูลสารสนเทศภายในระบบสื่อสารทั้งภายใน และภายนอกองค์กร

แนวทาง

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติด้านการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งานข้อมูลและระบบ สารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

ขอบเขตของนโยบายย่อยความปลอดภัยในการสื่อสาร

ขอบเขตของนโยบายย่อยการความปลอดภัยในการสื่อสาร หมายถึงการกำหนดแนวทางปฏิบัติต่อการดำเนินงานต่าง ๆ ที่จำเป็นเพื่อสร้างความมั่นใจในการใช้งานข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศ

5. นโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

เนื่องจาก MFEC Public Company Limited (MFEC) ได้กำหนดแนวทางการป้องกันและเตรียมความพร้อมในการ จัดการเมื่ออยู่ในภาวะวิกฤติ โดยต้องดำเนินการให้ MFEC ดำเนินภารกิจได้อย่างต่อเนื่อง จึงได้กำหนดให้มีนโยบายย่อยด้านการบริหารความ ต่อเนื่องของระบบเทคโนโลยีสารสนเทศ เพื่อการตอบสนองและบรรเทาผลกระทบต่อกระบวนการทำงานสำคัญที่มีการพึ่งพาระบบเทคโนโลยี สารสนเทศให้สามารถทำงานได้อย่างต่อเนื่องในระดับที่ได้มีการตกลงกันไว้กับผู้มีส่วนได้ส่วนเสีย

วัตถุประสงค์ของการบริหารจัดการความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

1. เพื่อให้มีการวิเคราะห์ วางแผน เตรียมการ ทบทวนและซักซ้อมกระบวนการต่าง ๆ ที่จำเป็น
2. เพื่อให้สามารถใช้งานระบบสารสนเทศได้อย่างต่อเนื่องในระดับที่ได้มีการตกลงกันไว้ในภาวะฉุกเฉิน
3. เพื่อให้ผู้มีส่วนได้ส่วนเสียได้เกิดความเข้าใจร่วมกัน และทราบถึงบทบาทหน้าที่ในการมีส่วนร่วมเมื่อเกิดเหตุฉุกเฉิน หรืออุบัติการณ์

แนวทาง

การบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ หมายถึง การจัดเตรียมกระบวนการหรือระบบสำรอง เพื่อให้สามารถใช้ งานทดแทนเมื่อระบบหลักเกิดการหยุดชะงักในภาวะฉุกเฉิน ในระดับที่ได้มีการตกลงกันไว้แล้ว ให้เป็นไปตามเงื่อนไขที่ได้มีการพิจารณา ผลกระทบทางธุรกิจ (BIA : Business Impact Analysis) ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (MTPD : Maximum Tolerable Period of Disruption) ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (RTO : Recovery Time Objective) เป้าหมายของการฟื้นคืนสภาพ (RPO : Recovery Point Objective) และทำการฟื้นฟูระบบหลักให้กลับคืนสู่สภาวะปกติให้ได้

MFEC จึงกำหนดนโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ให้มีนโยบาย (Policy), แนวทางปฏิบัติ (Guideline), ข้อกำหนด (Standard), และขั้นตอนปฏิบัติ (Procedure) ของการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ เป็น ลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย แนวปฏิบัติและมาตรฐานสากล ของการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ดังนี้

1. จัดให้มีคณะทำงานบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ที่สอดคล้องตามแนวทางการบริหารความต่อเนื่องในการ ดำเนินงานของ MFEC โดยมีการวางแผน การนำไปปฏิบัติ การฝึกซ้อม และการปรับปรุงแก้ไขอย่างต่อเนื่อง
2. จัดให้มีการทำงานร่วมกับคณะกรรมการบริหารความเสี่ยง และคณะอนุกรรมการควบคุมภายในที่มีหน้าที่กำกับดูแลการพัฒนา ระบบการบริหารความต่อเนื่องในการดำเนินงานของ MFEC ในภาพรวม
3. จัดให้มีการทำงานร่วมกับส่วนงานที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัย โดยประสานความเชื่อมโยงกันของแต่ละขอบข่าย ที่พึ่งพาระบบสารสนเทศ ในการจัดทำแผนป้องกัน / ระงับเหตุฉุกเฉิน รวมทั้งร่วมเป็นคณะทำงานในโครงสร้างศูนย์อำนวยการเหตุ ฉุกเฉิน และภาวะวิกฤต
4. จัดให้มีการพัฒนาระบบการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ตามขอบข่ายที่รับผิดชอบ โดยมีการวางแผน การ นำไปปฏิบัติ การฝึกซ้อม และปรับปรุงแก้ไขอย่างต่อเนื่อง รวมทั้งจัดทำและกำหนดผู้รับผิดชอบในการจัดทำแผนเพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญต่อการดำเนินงานของระบบเทคโนโลยีสารสนเทศ และรายงานผลการดำเนินงานต่อคณะ กรรมการบริหารความเสี่ยงและควบคุมภายใน ทราบเป็นระยะ ๆ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
5. จัดให้ผู้บริหาร/ผู้บังคับบัญชามีหน้าที่รับผิดชอบ ผลักดัน และสนับสนุนการดำเนินงานด้านต่าง ๆ ตามกระบวนการการบริหารความ ต่อเนื่องของระบบเทคโนโลยีสารสนเทศ รวมทั้งเสริมสร้าง และพัฒนาความรู้ ความสามารถของบุคลากรที่เกี่ยวข้องเพื่อให้มั่นใจว่า บุคลากรสามารถปฏิบัติงานได้อย่างมีประสิทธิผล

จัดให้ผู้บริหาร เจ้าหน้าที่ บุคลากร ลูกจ้าง และผู้เกี่ยวข้อง ได้รับความรู้และความตระหนักถึงการมีส่วนร่วมที่จะทำให้ การบริหาร ความต่อเนื่องของระบบเทคโนโลยีสารสนเทศบรรลุวัตถุประสงค์ของการบริหารความต่อเนื่องในการดำเนินงานของ MFEC

ขอบเขตของนโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

ขอบเขตของกระบวนการ การให้บริการ สถานที่ปฏิบัติงาน ความต้องการด้านความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ตลอดจนการให้บริการสารสนเทศ ที่ใช้สนับสนุนกระบวนการที่สำคัญที่จะ

ถูกรวมอยู่ในขอบเขตของนโยบายนี้ สามารถพิจารณาได้จากปัจจัย ที่มีความสำคัญ มีกระบวนการทำงานที่มีการพึ่งพาระบบสารสนเทศ

- กระบวนการทำงานที่มีการพึ่งพาระบบสารสนเทศ ที่สำคัญ ได้แก่ กระบวนงานใน ระบบบริหารโครงการ , ระบบบัญชี การเงิน เบิกจ่าย , ระบบจัดเก็บเอกสารและระบบสารบรรณอิเล็กทรอนิกส์ , เว็บไซต์หลักของสำนักงานฯ
- ระดับความสำคัญของการกู้คืนระบบเทคโนโลยีสารสนเทศ
- ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (MTPD) และระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (RTO)
- ข้อกำหนดเกี่ยวกับระยะเวลาในขั้นตอนการทำสัญญา, การเบิกจ่ายทางการเงินและบัญชี กับการทำโครงการต่าง ๆ
- ข้อกำหนดของฝ่ายเทคโนโลยีสารสนเทศ ในด้านที่เป็นผู้ทำหน้าที่เป็นผู้ให้บริการสารสนเทศพื้นฐานให้กับสำนักงานฯ ได้แก่ การ เป็นผู้ให้บริการระบบสารสนเทศ คอมพิวเตอร์ และอุปกรณ์เครือข่าย
- ความเสี่ยงสำคัญในสถานที่ปฏิบัติงานหลัก ซึ่งอาจก่อให้เกิดผลกระทบต่อการให้บริการระบบงานที่สำคัญ ได้แก่ ห้องปฏิบัติการ เครื่องแม่ข่ายและอุปกรณ์เครือข่ายในสำนักงานฯ
- ความเสี่ยงสำคัญในการพึ่งพาการบริการด้านเทคโนโลยีจากผู้ให้บริการรายหนึ่งรายใด

6. นโยบายย่อยการบริหารความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

ความเสี่ยงเกิดขึ้นได้จากหลายปัจจัย หลายรูปแบบ และการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการดำเนินงานก็อาจก่อให้เกิด ความเสี่ยงต่อองค์กร โดยความเสี่ยงที่ให้ความสำคัญ ได้แก่ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ (access risk) ความ เสี่ยงด้านการบริหารจัดการระบบคอมพิวเตอร์ บุคลากรด้านคอมพิวเตอร์ ที่ไม่เหมาะสมเพียงพอ (infrastructure risk) ซึ่งความเสี่ยง ดังกล่าว อาจก่อให้เกิดผลกระทบต่อองค์กรและภาคีได้ จึงต้องมีการประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อให้เกิดการจัดการความเสี่ยงอย่าง เหมาะสม ทำให้เกิดความมั่นคงของระบบสารสนเทศ อันเป็นหลักประกันว่า องค์กรจะมีระบบสารสนเทศให้ใช้งานได้อย่างต่อเนื่อง ไม่ หยุดชะงักและมีความมั่นคงปลอดภัย

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
2. เพื่อพิจารณาแนวทางป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ
3. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอัตรายต่อระบบสารสนเทศ
4. เพื่อรับรองว่าการจัดเก็บสารสนเทศขององค์กรเป็นไปตามนโยบายและกฎหมายด้านความมั่นคงปลอดภัยและความลับส่วนบุคคล
5. เพื่อให้สอดคล้องกับแนวทางการบริหารความเสี่ยงของ MFEC

แนวทาง

1. องค์กรต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง
   1.1 มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ

1.2 มีการตรวจสอบประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

1.3 ให้มีการตรวจสอบประเมินความเสี่ยง โดยผู้ตรวจสอบภายในของ MFEC (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้าน ความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง

2. ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

2.1 กำหนดให้มีการดำเนินการทบทวนปรับปรุงนโยบายระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ ว่าสอดคล้องกับนโยบายหรือไม่

3. อย่างน้อยปีละ 1 ครั้ง ให้ผู้จัดการกองทุนทราบพร้อมเสนอแนะแนวทางปรับปรุงแก้ไขในกรณีที่. พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง

3.1 ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบความปลอดภัยของระบบสารสนเทศอย่าง สม่ำเสมอ เช่น การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุม ด้านความมั่นคงปลอดภัย

3.2 ควรมีเครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ระบบงานและเอกสารที่จำเป็นสำหรับ งานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้องจากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุม จำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

4. กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ประมวลผลสารสนเทศจากบุคคลหรือหน่วยงานภายนอก

5. มีมาตรการสำหรับการตรวจประเมินระบบสารสนเทศ ดังนี้

5.1 มีการกำหนดข้อตกลงร่วมกันระหว่างผู้ตรวจสอบกับผู้ดูแลระบบและ/หรือเจ้าของระบบ

5.2 มีการทำสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบสามารถตรวจสอบได้จากข้อมูลสำเนา และมีการทำลายสำเนาทั้งทันทีที่การ ตรวจสอบเสร็จสิ้น หรือหากมิได้ทำลาย ต้องมีการจัดเก็บไว้อย่างปลอดภัยและมีมาตรการป้องกันที่เหมาะสม

5.3 มีการจำกัดสิทธิ์ให้ผู้ที่ทำการตรวจสอบให้สามารถเข้าถึงข้อมูลได้โดยการอ่านเพียงอย่างเดียว

5.4 มีการกำหนดวิธีการจัดเก็บหลักฐานการตรวจสอบข้อมูลที่ปลอดภัย

5.5 มีการกำหนดขั้นตอนการปฏิบัติและหน้าที่ความรับผิดชอบของผู้ตรวจสอบอย่างชัดเจน

6.บุคลากรที่ทำหน้าที่เป็นผู้ตรวจสอบต้องมีการกำหนดให้เป็นอิสระแยกจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการ ตรวจสอบ

7. ให้มีการแปลผลการประเมินความเสี่ยงให้อยู่ในรูปแบบ risk map ตามแนวทางบริหารความเสี่ยงของ MFEC

7. นโยบายย่อยการบริหารจัดการผู้ให้บริการ (Supplier Management)

MFEC Public Company Limited (MFEC) มีกำหนดนโยบายนี้เพื่อให้เกิดความมั่นใจต่อการบริหารทรัพยากรทั้งจากผู้ให้บริการภายใน และภายนอกตั้งแต่การวิเคราะห์ความเสี่ยง และการบริหารงานความเสี่ยงกับผู้ให้บริการที่จะเกิดขึ้นต่อข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์ของการดำเนินการอย่างปลอดภัย

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ทราบถึงกิจกรรมที่จำเป็นในการให้บริการจากผู้ให้บริการทั้งภายใน และภายนอก
2. เพื่อให้เกิดความเชื่อมั่นในการดำเนินการสนับสนุน และแก้ไขปัญหาของระบบเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอกที่เป็นผู้ขาย หรือผู้ผลิต
3. เพื่อให้เกิดความพร้อมในการดำเนินการลดความเสี่ยงที่จะเกิดขึ้นจากผู้ให้บริการภายใน และภายนอก

แนวทาง

1. ประเมินความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการภายใน และภายนอกทั้งหมดเพื่อหามาตรการในการแก้ไขปัญหาความเสี่ยง
2. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารจัดการผู้ให้บริการ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
3. ให้ผู้เกี่ยวข้องรับทราบถึงแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารจัดการผู้ให้บริการ และดำเนินการได้อย่างถูกต้องเหมาะสม
4. ดำเนินการตรวจสอบวิธีการปฏิบัติของผู้เกี่ยวข้องเพื่อให้เกิดความมั่นใจในการดำเนินการตามทิศทางที่ออกแบบไว้

ขอบเขตของนโยบายย่อยการบริหารจัดการผู้ให้บริการ

ขอบเขตของนโยบายย่อยการบริหารจัดการผู้ให้บริการ หมายถึงการบริหารจัดการผู้ให้บริการทั้งภายใน และภายนอก ในรูปแบบของข้อตกลง และสัญญาที่ลงนามจากตัวแทนของคู่สัญญาทั้งสองฝ่าย

8. นโยบายย่อยการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ (System acquisition and Development)

MFEC Public Company Limited (MFEC) มีกำหนดนโยบายนี้เพื่อให้เกิดความมั่นใจต่อการได้มาซึ่งระบบ และการพัฒนาระบบให้มีความปลอดภัย และทำงานได้อย่างราบรื่นเพื่อไม่ส่งผลกระทบต่อธุรกิจ

วัตถุประสงค์ของการดำเนินการอย่างปลอดภัย

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ทราบถึงกิจกรรมที่จำเป็นในการได้มาซึ่งระบบ และการพัฒนาระบบ

2. เพื่อให้เกิดความเชื่อมั่นต่อระบบงานที่ได้มา หรือพัฒนาขึ้นว่าสามารถดำเนินการได้อย่างมีประสิทธิภาพ
3. เพื่อลดจำนวนของการร้องเรียนเหตุขัดข้องที่เกิดขึ้นในระบบงานที่ไม่มีประสิทธิภาพ

แนวทาง

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ให้ผู้เกี่ยวข้องรับทราบถึงแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารจัดการการได้มาซึ่งระบบและการพัฒนาระบบ
3. ดำเนินการตามนโยบาย และแนวทางที่กำหนดเพื่อสร้างความเชื่อมั่นในการรับมอบระบบได้อย่างมีประสิทธิภาพ

ขอบเขตของนโยบายย่อยการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ

ขอบเขตของนโยบายย่อยการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบรองรับต่อการดูแลระบบเทคโนโลยีสารสนเทศที่มีอยู่ในศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง รวมถึงกระบวนการที่เกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียเกี่ยวกับการได้มาซึ่งระบบ และการพัฒนาระบบ

9. นโยบายย่อยในการบริหารทรัพยากรบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

MFEC Public Company Limited (MFEC) มีกำหนดนโยบายนี้เพื่อให้เจ้าหน้าที่บริษัทฯ เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตน และลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์อย่างผิดวัตถุประสงค์ภายในบริษัทฯ

วัตถุประสงค์ของการดำเนินการอย่างปลอดภัย

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ทราบถึงกิจกรรมที่จำเป็นในการได้มาซึ่งการบริหารทรัพยากรบุคคล
2. เพื่อให้ได้มาซึ่งบุคลากรที่มีความรู้ความสามารถ และพัฒนาบุคลากรที่มีอยู่ให้มีความสามารถต่อทิศทางดำเนินการของบริษัท
3. เพื่อลดความเสี่ยงที่เกิดขึ้นจากการรั่วไหลของข้อมูลสารสนเทศอันเกิดจากบุคลากรในบริษัท

แนวทาง

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารทรัพยากรบุคคลเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ให้ผู้เกี่ยวข้องรับทราบถึงแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารทรัพยากรบุคคล
3. ดำเนินการตามนโยบาย และแนวทางที่กำหนดเพื่อสร้างความมั่นใจในทรัพยากรบุคคลที่มีอยู่สามารถทำงานตอบรับต่อความต้องการทางธุรกิจ

ขอบเขตของนโยบายย่อยการบริหารทรัพยากรบุคคล

ขอบเขตของนโยบายย่อยการบริหารทรัพยากรบุคคลครอบคลุมทั้งบุคลากรภายในองค์กร และผู้มีส่วนได้ส่วนเสียภายนอก เช่น Outsource หรือ 3rd Party ที่ต้องปฏิบัติตามมาตรการด้านทรัพยากรบุคคลที่ระบุนี้

10. นโยบายการนำอุปกรณ์ส่วนตัวเข้ามาใช้งานในระบบเครือข่ายขององค์กร (BYOD Policy)

นโยบายนี้มีวัตถุประสงค์เพื่อสร้างความเข้าใจและเป็นแนวปฏิบัติที่เกี่ยวข้องกับการนำอุปกรณ์ส่วนตัวเข้ามาใช้งานในระบบเครือข่ายของ บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) ภายใต้การกำกับดูแลของส่วนงาน IT Support โดยมีรายละเอียดดังนี้

วัตถุประสงค์

1. เพื่อเพิ่มประสิทธิภาพในการทำงานจากการใช้อุปกรณ์ที่ตรงกับความต้องการของพนักงาน
2. เพื่อเพิ่มความยืดหยุ่นและความสะดวกสบายในการทำงาน
3. เพื่อลดค่าใช้จ่ายในการจัดหาอุปกรณ์ในการทำงานใหม่ให้กับพนักงาน

หลักเกณฑ์ทั่วไป

1. อุปกรณ์ที่พนักงานนำมาใช้ต้องมีคุณสมบัติเทียบเท่าหรือดีกว่าคุณสมบัติตามที่ส่วนงาน IT Support กำหนด เพื่อรองรับการทำงานตามวัตถุประสงค์ของหน่วยงานอย่างมีประสิทธิภาพ
2. อุปกรณ์ที่พนักงานนำมาใช้ต้องติดตั้งระบบปฏิบัติการ (Operating System: OS) และซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย โดยพนักงานจะนำเป็นผู้รับผิดชอบค่าลิขสิทธิ์ซอฟต์แวร์ที่ขอโปรแกรมคอมพิวเตอร์ติดตั้งในอุปกรณ์ทั้งหมดแต่เพียงผู้เดียว
3. อุปกรณ์ที่พนักงานนำมาใช้จะต้องได้รับการตรวจสอบซอฟต์แวร์ด้านซอฟต์แวร์ความปลอดภัยของส่วนงาน IT Support อย่างน้อยปีละ 1 ครั้ง และหากพบว่ามีการทำสำเนาโปรแกรมเทคโนโลยีสารสนเทศ พนักงานต้องดำเนินการจัดซื้อซอฟต์แวร์และติดตั้งซอฟต์แวร์ใหม่ที่เป็นลิขสิทธิ์ถูกต้องโดยทันที พนักงานต้องปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศอย่างเคร่งครัด

11. นโยบายการใช้ปัญญาประดิษฐ์ (AI Policy)

นโยบายการใช้ปัญญาประดิษฐ์ (Artificial Intelligence Policy : AI Policy) ของบริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) ฉบับนี้ จัดทำขึ้นเพื่อกำหนดกรอบการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) อย่างปลอดภัย ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Management System Policy : ISMS Policy), มาตรฐาน ISO/IEC 27001: 2022 และแนวทางของ IT Governance Committee

วัตถุประสงค์

เพื่อให้กำหนดกรอบการใช้งานปัญญาประดิษฐ์ (AI) อย่างปลอดภัย ให้สอดคล้องกับ

1. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) ฉบับล่าสุด
2. มาตรฐาน ISO/IEC 27001:2022
3. แนวทาง IT Governance Committee 2025

แนวทางปฏิบัติ

1. ใช้เครื่องมือ AI ได้ในกรณีที่ใช้กับข้อมูลระดับ Public
2. กรณีที่ใช้เครื่องมือ AI กับข้อมูลระดับ Internal Use หรือระดับที่สูงกว่า ต้องได้รับอนุญาตจากผู้บังคับบัญชาเป็นรายกรณี
3. ไม่แชร์แชตหรือข้อความใด ๆ ออกสู่สาธารณะ ผ่านทางบริการ AI ต่าง ๆ เช่น Gemini หรือ ChatGPT
4. รายงานเหตุผิดปกติ (Incident) ตามแนวปฏิบัติการรับเหตุขัดข้องของ ISMS Policy
5. นโยบายการพัฒนาซอฟต์แวร์ (Development Policy)
6. วัตถุประสงค์
7. กำหนดมาตรฐานการพัฒนา: สร้างกรอบการพัฒนาซอฟต์แวร์ที่มีระเบียบและคุณภาพสูง
8. ลดความเสี่ยงและป้องกันข้อผิดพลาด: มุ่งเน้นที่การลดความเสี่ยงและป้องกันข้อผิดพลาดในกระบวนการพัฒนา
9. ส่งเสริมการทำงานร่วมกัน: ส่งเสริมการทำร่วมกันและการสื่อสารที่มีประสิทธิภาพระหว่างทีม
10. ปฏิบัติตามข้อกำหนดทางกฎหมายและมาตรฐานที่เกี่ยวข้อง: ตรวจสอบให้แน่ใจว่ากระบวนการพัฒนาปฏิบัติตามข้อกำหนดทางกฎหมายและมาตรฐานที่เกี่ยวข้อง

แนวทางปฏิบัติ

1. การปฏิบัติตามนโยบาย: ทุกโครงการพัฒนาจะต้องปฏิบัติตามนโยบายและแนวทางที่กำหนดไว้ในเอกสารนี้
2. การใช้เครื่องมือและเทคโนโลยี: การพัฒนาจะต้องใช้เครื่องมือและเทคโนโลยีที่ได้รับการอนุมัติจาก ISMR หรือหัวหน้าส่วนงาน IT Support
3. การสื่อสารและการรายงาน: การสื่อสารและการรายงานความคืบหน้าจะต้องดำเนินการอย่างสม่ำเสมอ และให้ข้อมูลที่ชัดเจน

ด้านความปลอดภัย (Security)

วัตถุประสงค์

เพื่อรักษาความปลอดภัยของข้อมูลและระบบจากภัยคุกคามทางไซเบอร์

แนวทางปฏิบัติ

1. ทำการตั้งค่า Firewall และการป้องกันการบุกรุกเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
2. ทำการอัปเดตซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่อาจถูกใช้ในการโจมตี
3. ทำการฝึกอบรมพนักงานเกี่ยวกับความรู้ด้านความปลอดภัยไซเบอร์และการจัดการกับมัลแวร์

MFEC

Security
Our Responsibility