

**MFEC Public Company Limited**  
**เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**

โดยที่เป็นการสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ MFEC public company limited ให้มีแนวทางปฏิบัติ (Guideline) ข้อกำหนด (Standard) และขั้นตอนปฏิบัติ (Procedure) ของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ชัดเจนและเหมาะสมยิ่งขึ้น

MFEC Public Company Limited จึงกำหนดนโยบายการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของ MFEC Public Company Limited ดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศ MFEC Public Company Limited เรื่อง นโยบายการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 3 ให้มีนโยบาย (Policy) แนวทางปฏิบัติ (Guideline) ข้อกำหนด (Standard) และขั้นตอนปฏิบัติ (Procedure) ของการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศแบบท้ายประกาศนี้

ข้อ 4 ให้ผู้บริหารทุกระดับมีหน้าที่ส่งเสริมสนับสนุนและกำกับดูแลให้เกิดความมั่นคงปลอดภัยด้านสารสนเทศในสายงานที่อยู่ภายใต้ความรับผิดชอบดูแล

ข้อ 5 ให้เจ้าหน้าที่ทุกคนมีหน้าที่ดูแลรักษาข้อมูลสารสนเทศให้มีความมั่นคงปลอดภัย และใช้งานระบบสารสนเทศภายใต้ ข้อบังคับ ของกฎหมาย นโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติที่กำหนด

ข้อ 6 ให้ยึดถือว่า ความมั่นคงปลอดภัยด้านสารสนเทศ เป็นหน้าที่ของผู้บริหารและเจ้าหน้าที่ทุกคน โดยต้องให้ความร่วมมือ และ ปฏิบัติตามนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติอย่างเคร่งครัด

ข้อ 7 ให้ผู้จัดการเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ 1 Jan 2022

ลงชื่อ.....  
.....

(นายธนกร ชาลี)

ประธานเจ้าหน้าที่ฝ่ายปฏิบัติการ



## สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ .....	1
1. 政策的施行範例 (Access control) .....	8
1.1 แนวทางปฏิบัติในการควบคุมการเข้าถึงข้อมูลและการใช้งานสารสนเทศ .....	10
1.2 แนวทางปฏิบัติในการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ.....	12
วัตถุประสงค์ .....	12
1.3 แนวทางปฏิบัติในการบริหารจัดการการเข้าถึงและการใช้งานระบบสารสนเทศ .....	12
1.4 แนวทางปฏิบัติในการบริหารจัดการและการใช้งานรหัสผ่าน (User Password Management and Password Use) ....	14
1.5 แนวทางปฏิบัติในการเข้าถึงระบบเครือข่าย (Network Access Control) .....	16
1.6 แนวทางปฏิบัติในการยืนยันตัวบุคคล (User Identification and Authentication).....	18
1.7 แนวทางปฏิบัติในการเข้าถึงระบบปฏิบัติการ (Operating System Access Control).....	20
1.8 แนวทางปฏิบัติในการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์ .....	22
2. 政策的施行範例 (Data Classification).....	24
2.1 แนวทางปฏิบัติการจัดระดับข้อมูลและสินทรัพย์สารสนเทศ (Information Classification Guidelines).....	25
2.2 แนวทางปฏิบัติการจัดทำป้ายชื่อและการจัดการสารสนเทศ (Information Labeling and Handling) .....	25
2.3 แนวทางปฏิบัติการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Computer Media).....	26
2.4 แนวทางปฏิบัติการนำร่องข้อมูลและสื่อบันทึกข้อมูล (Disposal of Media) .....	26
2.5 แนวทางปฏิบัติในการเข้ารหัสสำหรับข้อมูลที่เป็นความลับ .....	27
2.6 แนวทางปฏิบัติสำหรับระบบที่ไม่ต้องการรับทราบ .....	29
2.7 แนวทางปฏิบัติสำหรับการโอนถ่ายข้อมูล .....	30
3. 政策的施行範例 (Operation Security) .....	31
3.1 แนวทางปฏิบัติในการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Information Asset Management) .....	32
3.2 แนวทางปฏิบัติในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ .....	35
3.3 แนวทางปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน .....	36
3.4. แนวทางปฏิบัติการป้องกันโคลด์มูร์รัย.....	37

3.5 แนวปฏิบัติการจัดการแพดซ์ .....	38
3.6 แนวปฏิบัติการบันทึกจัดเก็บล็อก.....	38
3.7 แนวปฏิบัติการเฝ้าดูความพร้อมใช้อุปกรณ์/ระบบ .....	39
3.8 แนวปฏิบัติการเฝ้าดูประสิทธิภาพอุปกรณ์/ระบบ .....	39
3.9 แนวปฏิบัติการค้นหาช่องโหว่ของอุปกรณ์/ระบบ.....	40
3.10 แนวปฏิบัติการรับเหตุขัดข้อง.....	41
<b>4. นโยบายย่ออยความปลอดภัยในการสื่อสาร (Communication Security).....</b>	<b>42</b>
4.1 แนวทางปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection).....	43
4.2 แนวทางปฏิบัติในการควบคุมการเข้ามายังต่อทางเครือข่าย .....	44
4.3 แนวทางปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control).....	45
4.4 แนวทางปฏิบัติในการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ .....	47
<b>5. นโยบายย่ออยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ.....</b>	<b>48</b>
ขอบเขตของนโยบายย่ออยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ .....	49
แนวทางปฏิบัติในการฟื้นคืนสภาพจากภัยพิบัติ (Disaster Recovery Plan Guideline).....	51
5.1 แนวทางของวงจรการบริหารงานคุณภาพ (PDCA) .....	51
5.2 แนวทางการวิเคราะห์ผลผลกระทบในการดำเนินงาน (BIA) .....	52
5.3 แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Assessment) .....	52
5.4 แนวทางในการสำรองข้อมูล .....	53
5.5 แนวทางในการกู้คืนระบบ .....	57
5.6 แนวทางในการซ้อมแผนการบริหารความต่อเนื่องของระบบสารสนเทศ .....	57
<b>6. นโยบายย่ออยการบริหารความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ.....</b>	<b>58</b>
6.1 แนวทางปฏิบัติในการประเมินความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ .....	60
<b>7. นโยบายย่ออยการบริหารจัดการผู้ให้บริการ (Supplier Management) .....</b>	<b>61</b>
7.1 แนวปฏิบัติการบริหารงานผู้ให้บริการภายใน .....	63
7.2 แนวปฏิบัติการบริหารงานผู้ให้บริการภายนอก .....	63

8. นโยบายย่ออย่างบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ (System acquisition and Development) .....	64
9. นโยบายย่ออย่างในบริหารทรัพยากรบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ.....	66
9.1 แนวทางปฏิบัติในการบริหารทรัพยากรบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ .....	67
ภาคผนวก ก.....	69
ข้อกำหนดการตั้งและเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยของ MFEC .....	69

## นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เนื่องจาก MFEC Public Company Limited (MFEC) ได้นำระบบสารสนเทศ มาใช้ในการดำเนินงานและให้บริการ ผู้เข้างาน พั้งภายในและภายนอกองค์กร ดังนั้นเพื่อให้การใช้สารสนเทศและระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานในลักษณะที่ไม่เหมาะสม หรือถูกคุกคามจากภัยต่างๆ ซึ่งจะช่วยลดความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน และบุคลากร

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การรักษาความมั่นคงปลอดภัยในการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของ MFEC ที่ต้องไม่เปิดเผยข้อมูลสารสนเทศ หรือระบบงานต่อบุคคลที่ไม่ได้รับสิทธิ์ (Confidentiality) การรักษาไว้ซึ่งความถูกต้องและความครบถ้วนของข้อมูลสารสนเทศ (Integrity) และความสามารถในการเข้าถึงและการใช้งานได้ตามความต้องการของผู้ที่ได้รับสิทธิ์ (Availability)

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

ทั้งนี้ รายละเอียดและโครงสร้างเอกสารนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สามารถดูได้ในเอกสารแนบท้าย องค์ประกอบและโครงสร้างของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

### **วัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ**

- เพื่อกำหนดและประกาศนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ทราบถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติตามอย่างเหมาะสม
- เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของ MFEC ว่า สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)
- เพื่อพัฒนาระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศดำเนินการอย่างเป็นระบบ และมีการพัฒนาปรับปรุงอย่างสม่ำเสมอ
- เพื่อปฏิบัติตามระเบียบ ข้อบังคับ สัญญา และกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

### **แนวทาง**

#### **แนวปฏิบัติด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ (อ้างอิงเอกสาร MFEC-ISMS-PO-002)**

- จัดทำกรศึกษา พัฒนา และจัดทำรายละเอียดการดำเนินการบริบทองค์กร ความต้องการผู้มีส่วนได้ส่วนเสีย และการกำหนดขอบเขตการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อเป็นแนวทางในการดำเนินการ
- จัดทำกรอบดำเนินการมาตรฐานด้านความมั่นคงปลอดภัยเพื่อเป็นต้นแบบการดำเนินการที่ชัดเจน

3. กำหนดให้ผู้บริหารระดับสูงเข้ามีส่วนร่วม พร้อมจัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และการกำหนดบทบาท หน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศให้ชัดเจน
4. กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และพิจารณาภาระการประเมินความเสี่ยง เพื่อใช้จัดทำแผนด้าน ความมั่นคงปลอดภัยสารสนเทศประจำปี
5. กำหนดให้การสนับสนุนด้านทรัพยากร การพัฒนาความรู้ความสามารถ ความตระหนักของบุคลากรที่เกี่ยวข้อง การสื่อสาร ตลอดกระบวนการ และการจัดทำเอกสารเพื่อให้บรรลุต่อวัตถุประสงค์ของความมั่นคงปลอดภัยสารสนเทศ
6. ติดตามโครงการ กระบวนการด้านความมั่นคงปลอดภัยเพื่อให้บรรลุต่อการดำเนินการตามแผนที่วางไว้
7. จัดทำการวัดประสิทธิภาพการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศในมิติต่างๆทั้งด้านนโยบาย ความเข้าใจของ บุคลากร กระบวนการดำเนินการ กฎหมายที่เกี่ยวข้อง และเทคโนโลยีสารสนเทศ
8. การติดตามการปฏิบัติจากหน่วยงานอิสระด้านความมั่นคงปลอดภัยสารสนเทศเพื่อให้เกิดความโปร่งใส และมีประสิทธิภาพใน การดำเนินการ
9. การจัดทำรายงานผลการดำเนินการเสนอให้กับผู้บริหารเพื่อรับทราบ และตัดสินใจในการดำเนินการเพื่อปรับปรุง ประสิทธิภาพ ประสิทธิผลการ ดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ

### **บทบาทและหน้าที่**

IT Governance เป็นผู้รับผิดชอบในการพิจารณาหรือกำหนดนโยบายและทิศทางของการรักษาความมั่นคงปลอดภัย ด้าน สารสนเทศ

Chief Operating Officer (COO) เป็นผู้รับผิดชอบในการพิจารณาข้อกำหนดและแนวทางปฏิบัติ กำกับดูแลการดำเนินการ ให้เป็นไปตามนโยบายและแนวทาง ปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวทางนโยบายดังกล่าว

ผู้บริหาร/ผู้บังคับบัญชา เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ใช้บริการภายใต้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ และเอกสารใดๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย แนวทางปฏิบัติ ข้อกำหนด ขั้นตอน ปฏิบัติ และเอกสารใดๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

เจ้าหน้าที่สารสนเทศ/ผู้ใช้งาน จะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของด้านสารสนเทศ รวมทั้ง ข้อกำหนด แนวทาง ปฏิบัติ ขั้นตอนปฏิบัติ และเอกสารใดๆที่เกี่ยวข้องกับนโยบายดังกล่าว การลงทะเบียนหรือฝ่าฝืนการปฏิบัติตาม จะต้องได้รับโทษทางวินัยตาม ระเบียบข้อบังคับที่ MFEC กำหนด

## ระยะเวลาทบทวน

เพื่อให้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ และเอกสาร ใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง MFEC จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนการปฏิบัติ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย ที่มีผลกระทบกับองค์กร

## นิยาม

1. “MFEC” หมายถึง MFEC Public Company Limited
2. “องค์กร” หรือ “สำนักงาน” หมายถึง MFEC Public Company Limited (MFEC)
3. “ผู้บริหาร” หมายถึง บุคคลที่ได้รับการแต่งตั้งอย่างเป็นทางการ เพื่อให้มีหน้าที่ในการกำหนดนโยบาย และดำเนินการบริหาร จัดการ MFEC ซึ่งประกอบด้วย
  - 3.1. ประธานเจ้าหน้าที่ฝ่าย / ผู้อำนวยการฝ่าย
  - 3.2. รองผู้อำนวยการ / ผู้จัดการแผนก (BU Head)
  - 3.3. ผู้จัดการส่วนงาน
4. “คณะกรรมการ” หมายถึง บุคคลที่ได้รับการแต่งตั้งอย่างเป็นทางการ เพื่อให้มีหน้าที่ในการกำกับ ดูแล หรือให้คำปรึกษา MFEC ในลักษณะที่มีการดำเนินการร่วมกันเป็นหมู่คณะ ซึ่งแบ่งออกได้ดังนี้
  - 4.1. คณะกรรมการบริหาร
  - 4.2. คณะกรรมการประเมินผล
  - 4.3. คณะกรรมการฝ่ายต่างๆที่เข่น IT Governance เป็นต้น
5. “ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ MFEC
6. “การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การรักษาไว้ซึ่งความลับ ความถูกต้องครบถ้วน และความพร้อมใช้ ตามความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศนั้นๆ รวมถึงความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และการ สื่อสารของ MFEC
7. “แนวทางปฏิบัติ” (Guideline) หมายถึง แนวทางที่ควรปฏิบัติตาม เพื่อให้สามารถบรรลุวัตถุประสงค์ได้ง่ายขึ้น
8. “ข้อกำหนด” (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์
9. “ขั้นตอนปฏิบัติ” (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้บรรลุตาม วัตถุประสงค์ที่ได้กำหนดไว้
10. “ผู้ใช้งาน” (IT User) หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศและ การ สื่อสารของ MFEC ตามสิทธิ์และหน้าที่ซึ่ง MFEC กำหนดไว้โดยแบ่งออกได้ดังนี้
  - 10.1. ผู้บริหาร และผู้บังคับบัญชา

- 10.2. คณะกรรมการ
- 10.3. เจ้าหน้าที่และลูกจ้างของ MFEC
- 10.4. บุคคลภายนอกที่ได้รับอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ MFEC
11. “สิทธิ์ของผู้ใช้งาน” หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน MFEC
12. “เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ” หรือ “เจ้าหน้าที่สารสนเทศ” หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้สามารถเข้าใช้งาน และบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของ MFEC โดยแบ่งออกได้ดังนี้
13. “ผู้ดูแลระบบ” (System Administrator) หมายถึง บุคคลที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษา ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านฮาร์ดแวร์และซอฟต์แวร์ ซึ่งสามารถเข้าถึงระบบงานหรือระบบจัดการ ฐานข้อมูลของ MFEC เช่น การกำหนดสิทธิ์ของผู้ใช้ เป็นต้น
14. “ผู้พัฒนาระบบ” (System Developer) หมายถึง บุคคลที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนา ระบบเทคโนโลยีสารสนเทศและการสื่อสาร
15. “บุคคลภายนอก” ที่มาดำเนินการติดตั้ง หรือบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวม ทั้งให้คำปรึกษาหรือปฏิบัติตามสัญญาจ้าง
16. “ภาคี” หมายถึง บุคคลหรือองค์กรภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของ MFEC โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
17. “ข้อมูลคอมพิวเตอร์” (Data) หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุกรรมทางอิเล็กทรอนิกส์
18. “ข้อมูลประจำทางคอมพิวเตอร์” (Log) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง วันที่ เวลา ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการสื่อสารของระบบคอมพิวเตอร์นั้น
19. “สารสนเทศ” (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมานำการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ โดยหมายรวมถึงสารสนเทศที่อยู่ในรูปแบบของอิเล็กทรอนิกส์และไม่ใช้อิเล็กทรอนิกส์
20. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน และหน่วยงานภายนอก เข้าถึงหรือใช้งานระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบเครือข่าย ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ
21. “ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนด

- คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่ทำให้อุปกรณ์หรือชุดอุปกรณ์ทำงานที่ประมวลผลข้อมูลและจัดเก็บข้อมูลโดยอัตโนมัติ
22. “ระบบเครือข่าย” (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่าง ระบบเทคโนโลยีสารสนเทศต่างๆของ MFEC เช่น ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
- 22.1. “ระบบอินทราเน็ต” (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆภายในหน่วยงาน ของ MFEC เข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
- 22.2. “ระบบอินเทอร์เน็ต” (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของ MFEC เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
23. “ระบบเทคโนโลยีสารสนเทศ” (Information Technology System) หมายถึง ระบบงานของ MFEC ที่นำเอatechnology สารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่ MFEC สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
24. “ห้องควบคุมระบบคอมพิวเตอร์” หรือ “ห้องเครื่องแม่ข่าย” หมายถึง ห้องที่จัดเตรียมพื้นที่ไว้สำหรับการติดตั้งเครื่องมือที่เป็น อุปกรณ์หลัก ของระบบคอมพิวเตอร์และระบบการสื่อสารของ MFEC อาทิเช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องจัดเก็บ ข้อมูลคอมพิวเตอร์ (Data Storage) อุปกรณ์เครือข่าย เป็นต้น
25. “เจ้าของข้อมูล” หมายถึง บุคคลหรือหน่วยงานที่รับผิดชอบในสินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดย ตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
26. “เจ้าของระบบ” หมายถึง บุคคลหรือหน่วยงานที่รับผิดชอบในระบบ (System Owner) โดยเจ้าของระบบเป็นผู้รับผิดชอบ ระบบงาน นั้นๆ หรือได้รับผลกระทบโดยตรงหากระบบนั้นเสียหาย
27. “สินทรัพย์สารสนเทศ” หมายถึง สินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ และ โปรแกรมประยุกต์ (Software and Application Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) ที่เกี่ยวข้องกับงานสารสนเทศ
28. “จดหมายอิเล็กทรอนิกส์” (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์ และ เครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นไฟล์ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถ ส่ง ข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail Box) ที่กำหนดไว้สำหรับ ผู้ใช้ในเครือข่าย ผู้รับสามารถเปิดอ่านข่าวสาร พิมพ์ลงกระดาษ หรือลบทิ้งได้
29. “ชื่อผู้ใช้งาน” (Username) หมายถึง ชุดตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นมาเพื่อใช้ในการเข้าใช้งานในระบบสารสนเทศที่กำหนดศิทธิ์การใช้งานไว้
30. “รหัสผ่าน” (Password) หมายถึง ตัวอักษรหรืออักษรหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อ

ควบคุม การเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

31. “โปรแกรมไม่พึงประสงค์” หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมอื่นเกิดความเสียหาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
32. “เหตุการณ์ด้านความมั่นคงปลอดภัย” (IT Security Event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืน นโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือ สถานการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย
33. “เหตุการณ์ที่ละเอียดความมั่นคงปลอดภัย” (IT Security Incident) หมายถึง เหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อ่อนโยน ซึ่งอาจทำให้ระบบสารสนเทศขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
34. “ระบบที่มีผลกระทบและมีความสำคัญสูงต่อองค์กร” ได้แก่ ระบบบริหารโครงการออนไลน์และ ระบบบัญชีการเงินและพัสดุ

องค์ประกอบและโครงสร้างของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- 1.นโยบายย่อยการควบคุมการเข้าถึงสารสนเทศ
  - 1.1. แนวทางปฏิบัติในการควบคุมการเข้าถึงข้อมูลและการใช้งานสารสนเทศ
  - 1.2. แนวทางปฏิบัติในการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ
  - 1.3. แนวทางปฏิบัติในการจัดการการเข้าถึงและการใช้งานระบบสารสนเทศ
  - 1.4. แนวทางปฏิบัติในการบริหารจัดการและการใช้งานรหัสผ่าน
  - 1.5. แนวทางปฏิบัติในการเข้าถึงระบบเครือข่าย
  - 1.6. แนวทางปฏิบัติในการยืนยันตัวบุคคล
  - 1.7. แนวทางปฏิบัติในการเข้าถึงระบบปฏิบัติการ
  - 1.8. แนวทางปฏิบัติในการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์
- 2.นโยบายย่อยการแบ่งขั้นความลับ
  - 2.1. แนวทางปฏิบัติการจัดระดับขั้นความลับของข้อมูลและสินทรัพย์สารสนเทศ (Information Classification Guidelines)
  - 2.2. แนวทางปฏิบัติการจัดทำป้ายชื่อและการจัดการสารสนเทศ (Information Labeling and Handling)
  - 2.3. แนวทางปฏิบัติการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Computer Media)
  - 2.4. แนวทางปฏิบัติการชำระล้างข้อมูลและสื่อบันทึกข้อมูล (Disposal of Media)
  - 2.5. แนวทางปฏิบัติในการเข้ารหัสสำหรับข้อมูลที่เป็นความลับ
  - 2.6. แนวทางปฏิบัติสำหรับระบบที่ไวต่อการรบกวน
- 3.นโยบายย่อยการดำเนินการอย่างปลอดภัย (Operation Security)

- 3.1. แนวทางปฏิบัติในการควบคุมทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Information Asset Management)
- 3.2. แนวทางปฏิบัติในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานท่ออุปกรณ์
- 3.3. แนวทางปฏิบัติในการปฎิบัติงานจากภายนอกสำนักงาน
- 3.4. แนวทางปฏิบัติการป้องกันโศดมุ่งร้าย
- 3.5. แนวทางปฏิบัติการจัดการแพตช์
- 3.6. แนวทางปฏิบัติการบันทึกจัดเก็บล็อก
- 3.7. แนวทางปฏิบัติการเฝ้าดูความพร้อมใช้อุปกรณ์/ระบบ
- 3.8. แนวทางปฏิบัติการเฝ้าดูประสิทธิภาพอุปกรณ์/ระบบ
- 3.9. แนวทางปฏิบัติการค้นหาช่องโหว่ของอุปกรณ์/ระบบ
- 3.10. แนวทางปฏิบัติการรับเหตุขัดข้อง
- 4.นโยบายย่อyleย่อความปลอดภัยในการสื่อสาร (Communication Security)
  - 4.1. แนวทางปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ
  - 4.2. แนวทางปฏิบัติในการควบคุมการเข้ามือต่อทางเครือข่าย
  - 4.3. แนวทางปฏิบัติในการควบคุมการจัดเดินทางบนเครือข่าย
- 5.นโยบายย่อการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ
  - 5.1. แนวทางของวงจรการบริหารงานคุณภาพ (PDCA)
  - 5.2. แนวทางการวิเคราะห์ผลกระทบในการดำเนินงาน (BIA)
  - 5.3. แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Assessment)
  - 5.4. แนวทางในการสำรองข้อมูล
  - 5.5. แนวทางในการกู้คืนระบบ
  - 5.6. แนวทางในการซ้อมแผนการบริหารความต่อเนื่องของระบบสารสนเทศ
- 6.นโยบายย่อการบริหารความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ
  - 6.1. แนวทางปฏิบัติในการประเมินความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ
- 7.นโยบายย่อการบริหารจัดการผู้ให้บริการ (Supplier Management)
  - 7.1 แนวทางปฏิบัติการบริหารงานผู้ให้บริการภายใน
  - 7.2 แนวทางปฏิบัติการบริหารงานผู้ให้บริการภายนอก
- 8.นโยบายย่อการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ (System acquisition and Development)
- 9.นโยบายย่อในการบริหารทรัพยากรบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
  - 9.1. แนวทางปฏิบัติในการบริหารทรัพยากรบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

## 1.นโยบายการควบคุมการเข้าถึงสารสนเทศ (Access control)

MFEC Public Company Limited (MFEC) มีการควบคุมการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เพื่อ กำหนด มาตรการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต ป้องกันการบุกรุกทั้งด้านกายภาพ ผ่านระบบเครือข่าย และจากโปรแกรม ที่จะสร้างความเสียหายแก่ข้อมูลหรือทำให้ระบบหยุดชะงัก และสามารถตรวจสอบติดตามการพิสูจน์ตัวบุคคลที่ใช้งาน ข้อมูลหรือระบบสารสนเทศขององค์การได้อย่างถูกต้องโดยยึดหลักดังนี้

1. การรักษาความลับ (Confidentiality) ให้บุคคลผู้มีสิทธิ์เท่านั้น เข้าถึงข้อมูลได้ และมีการควบคุมการเข้าถึงโดยข้อมูลที่เป็นความลับ จะได้ไม่ถูกเปิดเผยแก่ผู้ไม่มีสิทธิ์
2. ความถูกต้องครบถ้วน (Integrity) ให้มีการรักษาความถูกต้องครบถ้วนของข้อมูล และควบคุมความผิดพลาด ไม่ให้ข้อมูลถูกแก้ไข ลบทั้ง เป็นลี่นแปลงโดยผู้ไม่มีสิทธิ์
3. ความสามารถในการเข้าถึงและใช้งานได้ (Availability) ให้ผู้มีสิทธิ์ใช้ข้อมูลเท่านั้นสามารถที่จะเข้าถึงข้อมูลได้ตามเวลาที่ตกล่วงไป ผู้รับผิดชอบต้องควบคุมไม่ให้ระบบหยุดชะงัก มีสมรรถภาพในการทำงานต่อเนื่อง และมีการป้องกันไม่ให้มีสิ่งใดทำให้ระบบหยุด ทำงาน

### วัตถุประสงค์ของการควบคุมการเข้าถึงสารสนเทศ

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ MFEC ตระหนักถึงความสำคัญของการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของ MFEC ว่า สามารถเข้าถึงได้เฉพาะผู้มีสิทธิ์ (Confidentiality) มี ความครบถ้วนสมบูรณ์ (Integrity) และมีความพร้อมใช้งาน (Availability)
3. เพื่อให้สามารถตรวจสอบย้อนหลังการเข้าถึงระบบสารสนเทศต่างๆ ของผู้ใช้งานได้

### แนวทาง

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติต้านการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. จัดให้มีข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยวข้องกับสารสนเทศ การพัฒนาและบำรุงรักษาระบบสารสนเทศ และสิ่งใดๆที่เกี่ยวข้องกับสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่าง เหมาะสมและเพียงพอ และมีการกำหนดการควบคุมการใช้งานและการเข้าถึงที่อย่างชัดเจนตามหลักการของความต้องการในการ ใช้งานที่เหมาะสมและมั่นคงปลอดภัย
3. จัดให้มีแนวทางปฏิบัติในการพัฒนาการซอฟต์แวร์ ที่ต้องควบคุมการเข้าถึงและสิทธิ์ในการใช้ข้อมูลในระบบ ไปจนกระทั่งการควบคุมการเข้าถึงด้วยระบบปฏิบัติการ ซึ่งรวมถึงการใช้ข้อมูลในส่วนต่างๆภายในคอมพิวเตอร์ของผู้ใช้งาน
4. จัดให้มีแนวทางปฏิบัติในการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ และอุปกรณ์สารสนเทศ
5. จัดให้มีแนวทางปฏิบัติในการตรวจสอบความถูกต้องของข้อมูลบนอินเทอร์เน็ต รวมทั้งอุปกรณ์สารสนเทศให้ เข้าได้เฉพาะผู้มีสิทธิ์เท่านั้น

6. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งานข้อมูลและระบบ สารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

#### ขอบเขตของนโยบายย่อการควบคุมการเข้าถึงสารสนเทศ

ขอบเขตของนโยบายย่อการควบคุมการเข้าถึงสารสนเทศ หมายถึง การเข้าถึงสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ ห้องเครื่องแม่ข่าย ระบบเครือข่าย อุปกรณ์เทคโนโลยีสารสนเทศ โดยสารสนเทศหมายรวมถึงสารสนเทศที่อยู่ในรูปแบบของ อิเล็กทรอนิกส์และไม่ใช้อิเล็กทรอนิกส์

#### บทบาทและหน้าที่

**Chief Operating Officer (COO)** ทำหน้าที่กำกับดูแลให้เป็นไปตามนโยบายและแนวทางปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

**ผู้บริหาร/ผู้บังคับบัญชา** เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ที่เกี่ยวข้องภายในได้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการควบคุมการเข้าถึงสารสนเทศ

**ฝ่ายอำนวยการ** เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการควบคุมการเข้าถึงและการใช้งานสารสนเทศและระบบสารสนเทศ

**ฝ่ายเทคโนโลยีสารสนเทศ** เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ ห้องเครื่องแม่ข่าย ระบบเครือข่าย อุปกรณ์เทคโนโลยีสารสนเทศ และอื่นๆที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

**เจ้าหน้าที่สารสนเทศ/ผู้ใช้งาน** ต้องปฏิบัติตามนโยบายการควบคุมการเข้าถึงสารสนเทศ รวมทั้งข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับต่างๆที่เกี่ยวข้อง

#### ระยะเวลาทบทวน

เพื่อให้นโยบายการเข้าถึงสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง MFEC จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนการปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลง กระบวนการทำงาน วิธีการเข้าถึงสารสนเทศที่สำคัญที่กระทบกับนโยบาย

## 1.1 แนวทางปฏิบัติในการควบคุมการเข้าถึงข้อมูลและการใช้งานสารสนเทศ

### วัตถุประสงค์

เพื่อให้ผู้ใช้งานและผู้ดูแลระบบได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการเข้าถึงข้อมูลและการใช้งานสารสนเทศ โดยต้อง มีการป้องกันและควบคุมการเข้าถึงข้อมูลและการใช้งานระบบเทคโนโลยีสารสนเทศจากผู้ไม่มีสิทธิ์ ทั้งนี้เพื่อให้เกิดความ มั่นคงปลอดภัยทั้งต่อ ข้อมูลและระบบเทคโนโลยีสารสนเทศของ MFEC

### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

### นิยาม (ส่วนรวมกันในตอนต้น)

“ข้อตกลงการรักษาความลับ” (Non-Disclosure Agreement) หมายถึง เอกสารที่กล่าวถึงรายละเอียดของข้อมูลทางด้าน การเงิน/ธุรกิจ/ เทคโนโลยี รวมถึงข้อมูลของงานบริการทั้งที่ได้ทำขึ้นเป็นลายลักษณ์อักษรหรือโดยวาจา หรือบนสื่ออิเล็กทรอนิกส์อื่นๆ ที่ผู้ทำข้อตกลง ได้ตกลง กันว่าจะไม่เปิดเผยข้อมูลใดๆที่เป็นความลับนี้เพื่อใช้ในการดำเนินการอื่นใดนอกเหนือไปจากที่ได้ตกลงกัน ไว้

### แนวทางปฏิบัติ

1. อนุญาตให้ผู้ใช้งานเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจาก ผู้บังคับบัญชา/ เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น
2. ป้องกันการเข้าถึงคอมพิวเตอร์ เครือข่าย อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์ต่อพ่วง ไม่ให้เข้าถึงได้โดยไม่ได้รับ อนุญาต โดยมีการทำหนัดขั้นตอนและแบบฟอร์มในการขออนุญาตเข้าถึง ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อ ผู้ใช้งาน เหตุผลในการขอใช้ ระยะเวลาในการใช้บริการ
3. ควบคุมการเข้าถึงระบบสารสนเทศต่างๆ ของสำนักงานโดยจัดทำเป็นแบบฟอร์มขอใช้งานระบบที่มีการอนุมัติจาก ผู้บังคับบัญชา/ เจ้าของข้อมูล/เจ้าของระบบ
4. กำหนดสิทธิ์ผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องตามความจำเป็นต่อการใช้งานขั้นต่ำ (Least Privilege) โดยต้องได้รับอนุญาตจาก ผู้บังคับบัญชา/เจ้าของข้อมูล/เจ้าของระบบ เช่น
  - 4.1. เข้าถึง
  - 4.2. อ่านอย่างเดียว
  - 4.3. สร้างข้อมูล
  - 4.4. แก้ไข
  - 4.5. ลบข้อมูล
  - 4.6. อนุมัติ
  - 4.7. “ไม่มีสิทธิ์”

- โดยจัดให้มีการทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง หรือเมื่อจำเป็น
5. ให้ถือว่าการอนุมัติการเข้าถึงระบบสารสนเทศโดยผู้บังคับบัญชา/เจ้าของข้อมูล/เจ้าของระบบ เป็นการมอบอำนาจของหน่วยงานให้ ผู้ใช้งานเข้าถึงระบบสารสนเทศ
  6. ข้อมูลภายใน MFEC แบ่งเป็นประเภทต่าง ๆ ดังนี้
    - 6.1. ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ นโยบาย ยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
    - 6.2. ข้อมูลสารสนเทศด้านการดำเนินงาน ได้แก่ กฎหมาย ระเบียบ ผลการดำเนินงาน การใช้จ่ายงบประมาณ เป็นต้น
    - 6.3. ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลความรู้ด้านสุขภาวะ ข้อมูลประชาสัมพันธ์ เป็นต้น
  7. ข้อมูลภายใน MFEC จัดระดับขั้นความลับ ดังนี้
    - 7.1. ระดับ 1 ขั้นทั่วไป เปิดเผยแพร่สู่สาธารณะได้ตลอดเวลา
    - 7.2. ระดับ 2 ขั้นลับ เปิดเผยแพร่สู่บุคลภายนอกหรือสาธารณะได้เมื่อร้องขอ
    - 7.3. ระดับ 3 ขั้นลับมาก เปิดเผยแพร่สู่บุคลภายนอกหรือสาธารณะได้เมื่อได้รับการอนุมัติจากผู้จัดการ , BU Head หรือ ผู้ที่ได้รับมอบหมาย
    - 7.4. ระดับ 4 ขั้นลับที่สุด เปิดเผยแพร่สู่บุคลภายนอกหรือสาธารณะไม่ได้
  8. MFEC กำหนดช่องทางและเวลาสำหรับการเข้าถึงข้อมูล ดังนี้
    - 8.1. ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาทำการ)
    - 8.2. โทรศัพท์ (เข้าถึงได้ในเวลาทำการ)
    - 8.3. โทรสาร หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาทำการ)
    - 8.4. ระบบเครือข่ายภายใน (เข้าถึงได้ทุกช่วงเวลา)
    - 8.5. ระบบอินเตอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)
    - 8.6. ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)
    - 8.7. เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา)
  9. การเข้าใช้งานระบบที่มีผลกระทบและมีความสำคัญสูงต่อองค์กร ให้เข้าผ่านเครือข่ายภายใน MFEC หรือผ่านระบบ VPN เท่านั้น
  10. กำหนดให้มีการเข้ารหัสสำหรับข้อมูลสำคัญหรือข้อมูลลับแต่ละประเภท โดยข้อมูลที่มีระดับขั้นความลับระดับที่ 3 ขึ้นไปต้องมีการเข้ารหัสในการจัดเก็บ และต้องส่งผ่านช่องทางที่มีการเข้ารหัส เช่น SSL เป็นต้น
  11. จัดทำข้อตกลงการรักษาความลับ (Non-Disclosure Agreement) ระหว่าง MFEC กับหน่วยงานผู้ที่ได้รับการว่าจ้างหรือผู้ที่จำเป็นต้องเข้าถึงข้อมูล

## 1.2 แนวทางปฏิบัติในการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

### วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศเพื่อใช้งานตามภารกิจที่ได้รับมอบหมาย

### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

### แนวทางปฏิบัติ

1. จัดให้มีกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ ทั้งนี้ผู้ปฏิบัติงานจะได้รับอนุญาตจากผู้บังคับบัญชา ผู้อำนวยการฝ่ายบริหารงานบุคคล และผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศตามความจำเป็นในการใช้งาน
2. จัดให้มีการ trab ทวนสิทธิ์การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง
3. การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศของ MFEC จะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชา ผู้อำนวยการฝ่ายบริหารงานบุคคล และผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ โดยจะสามารถเข้าใช้ข้อมูลและระบบที่เกี่ยวข้องกับงานในหน้าที่ ความรับผิดชอบของบุคคลนั้นๆ เท่านั้น ความมั่นคงปลอดภัยของข้อมูลและกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งของนโยบายและแนวทางปฏิบัติที่ผู้ปฏิบัติงานต้องปฏิบัติตามอย่างเคร่งครัด

## 1.3 แนวทางปฏิบัติในการบริหารจัดการการเข้าถึงและการใช้งานระบบสารสนเทศ

### วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการบริหารจัดการการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศโดยต้องมีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ทั้งนี้เพื่อให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศของ MFEC

### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

### แนวทางปฏิบัติ

1. จัดให้มีการอบรมการใช้งานระบบเทคโนโลยีสารสนเทศให้กับผู้ใช้งานใหม่ ร่วมกับทางฝ่ายทรัพยากรบุคคล และมอบเอกสารรับรอง สิทธิ์การเข้าถึงแก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์ และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้ผู้ใช้งานลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเป็นลายลักษณ์อักษร
2. จัดให้มีมาตรการเชิงป้องกันภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ เช่น ติดตั้งโปรแกรม Antivirus ที่

เครื่อง ผู้ใช้งานทุกเครื่อง มีการติดตั้ง Firewall และ IPS (Intrusion Prevention System) เป็นต้น

### 3. การลงทะเบียนผู้ใช้งาน (User Registration)

- 3.1. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน โดยต้องระบุข้อมูลพื้นฐานเป็นอย่างน้อย ดังนี้ ชื่อและนามสกุล ตำแหน่งหน่วยงาน ระยะเวลาในการใช้งาน
- 3.2. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานว่าไม่มีการลงทะเบียนผู้ใช้งานมาก่อน
- 3.3. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
- 3.4. ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์และหน้าที่ ความรับผิดชอบของผู้ใช้งาน รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว
4. ตัดผู้ใช้งานออกจากทะเบียนโดยปฏิบัติตามขั้นตอนปฏิบัติของการตัดผู้ใช้งาน เมื่อมีการเพิกถอนสิทธิ์ตามกรณีต่อไปนี้
  - 4.1. สิ้นสุดหน้าที่ตามงานที่รับผิดชอบ เช่น การโอนย้ายงาน การลาออก
  - 4.2. ผู้บังคับบัญชาแจ้งเป็นลายลักษณ์อักษรว่าให้เพิกถอนสิทธิ์
5. กำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิ์การใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) สิทธิ์ การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่ และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่านั้น จำเป็นแก่การ ปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
6. ควบคุมการใช้ชื่อผู้ใช้งาน (Username) ที่มีสิทธิ์พิเศษ ให้ใช้ได้กรณีมีความจำเป็นและต้องใช้งานอย่างรัดกุม ทั้งนี้ในการพิจารณา ว่าการควบคุมชื่อผู้ใช้งาน ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น MFEC จะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาใน ภาพรวม
  - 6.1. ต้องได้รับความเห็นชอบจากผู้มีอำนาจ
  - 6.2. กรณีจำเป็นต้องมีการควบคุมขั้นสูง ต้องควบคุมการใช้งานชื่อผู้ใช้งาน ที่มีสิทธิ์พิเศษอย่างเข้มงวด และจำกัดการใช้งานเฉพาะ กรณีจำเป็นเท่านั้น
  - 6.3. ต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือสิ้นสุดการใช้งาน
  - 6.4. ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็น ระยะเวลาหนึ่ง เปิดใช้งานระบบ 2 Fa
7. ห้ามผู้ดูแลระบบ ใช้ชื่อผู้ใช้งานที่มีสิทธิ์ระดับสูงในการปฏิบัติงานทั่วไป
8. ต้องให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น กรณีมีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิ์ผู้ใช้งานรายอื่น ให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การแบ่งปันแฟ้มข้อมูล (Share Files) รวมถึง กำหนดระยะเวลา การใช้งานและยกเลิกการให้สิทธิ์ดังกล่าวทันทีที่ไม่มีความจำเป็นแล้วหรือพ้นระยะเวลาที่กำหนด
9. แบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ให้มีการสอบบันการปฏิบัติงานระหว่างผู้ใช้งานในฝ่ายเทคโนโลยีสารสนเทศ

### ดังนี้

- 9.1. ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment)
- 9.2. ต้องจัดให้มีคำบรรยายลักษณะงาน (Job description) ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายใต้ฝ่ายเทคโนโลยีสารสนเทศอย่างชัดเจนเป็นลายลักษณ์อักษร
- 9.3. ควรจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น
- 9.4. กำหนดให้ผู้ที่ทำหน้าที่ในการตรวจสอบประเมินความมั่นคงปลอดภัยของระบบต้องไม่เป็นผู้ดูแลระบบของระบบที่ตนตรวจสอบประเมิน
10. ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานดังนี้
  - 10.1. ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง
  - 10.2. ทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ของผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป
  - 10.3. ทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน
  - 10.4. กำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิ์ในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง
  - 10.5. ตรวจสอบสิทธิ์และติดตามการใช้งานตามสิทธิ์ที่ได้รับของแต่ละระบบ
  - 10.6. กำหนดให้มีการเพิกถอนสิทธิ์หรือระงับการใช้งานของแต่ละสิทธิ์หากต่างกันไป ตามหน้าที่ที่รับผิดชอบในแต่ละระบบ

### 1.4 แนวทางปฏิบัติในการบริหารจัดการและการใช้งานรหัสผ่าน (User Password Management and Password Use)

#### วัตถุประสงค์

1. เพื่อให้ผู้ใช้งานและผู้ดูแลระบบได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการบริหารจัดการและการใช้งานรหัสผ่าน เพื่อ การระบุตัวตน และสร้างความมั่นคงปลอดภัยจากบุคคลที่ไม่ได้รับอนุญาตเข้ามาล่วงรู้รหัสผ่าน อันส่งผลกระทบต่อความมั่นคง ปลอดภัยในระบบเทคโนโลยีสารสนเทศของ MFEC
2. เพื่อช่วยป้องกันการเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาต โดยการใช้รหัสผ่านที่มีความรักกุมมาก เพื่อให้สามารถป้องกันอุปกรณ์ เทคโนโลยีสารสนเทศจากบุคคลและซอฟต์แวร์ที่ไม่ประสงค์ดีได้มากขึ้น ทั้งนี้เพื่อให้เกิดความมั่นคงปลอดภัยทั้งต่อระบบสารสนเทศ และข้อมูลของ MFEC หรืออุปกรณ์ส่วนบุคคลที่นำมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ MFEC

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### นิยาม

“การเข้ารหัส” (Encryption) หมายถึง การเปลี่ยนข้อความหรือเครื่องหมายธรรมด้า ให้เป็นข้อความหรือเครื่องหมายลับ ด้วยวิธีใดวิธีหนึ่ง

### แนวทางปฏิบัติ

#### การบริหารจัดการรหัสผ่าน

- กำหนดให้ผู้ใช้งานลงนามหรือยืนยัน ในการป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิ์ และ หน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบ
- กำหนดขั้นตอนปฏิบัติ สำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
- กำหนดรหัสผ่านขั้วรวมไม่ซ้ำกันในการใช้งานแต่ละครั้ง เช่นรหัสผ่านเริ่มต้นของเซิร์ฟเวอร์ที่ต้องตั้งกันทุกเครื่อง หรือ รหัสผ่านล็อกอินบัญชีพนักงานที่ต้องตั้งกันทุกคนแม้เป็นรหัสผ่านขั้วรวม โดยรหัสผ่านขั้วรวมต้องส่งถึงผู้รับผิดชอบต่อระบบโดยทันที โดยตรง
- ผู้ใช้ที่ได้รับบัญชีที่ตั้งรหัสผ่านขั้วรวมมีหน้าที่เปลี่ยนรหัสผ่านทันทีที่ทำได้
- จัดส่งรหัสผ่านให้ผู้ใช้งานโดยตรงกับผู้ที่จำเป็นต้องใช้งานเท่านั้น ไม่ส่งผ่านช่องทางที่มีผู้อื่นเข้าถึงได้ เช่น แฟกซ์กลุ่ม, อีเมลกลุ่ม, หรือการส่งอีเมลถึงผู้ใช้หลายคนตรวจสอบยืนยันตัวตน และกำหนดสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Authentication and Authorization) ก่อนการเข้าสู่ ระบบงานคอมพิวเตอร์ ที่รักษาความปลอดภัย โดยให้สอดคล้องกับข้อกำหนดเรื่องการตั้งและเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย ของ MFEC และกำหนดให้ผู้ใช้งานแต่ละรายมีชื่อผู้ใช้งาน (User Account) เป็นของตนเอง
- ใช้กระบวนการเข้ารหัสทางเดียว (one way hash) ที่มีความปลอดภัยสูงในการเก็บรหัสผ่านในระบบ ไม่เก็บรหัสผ่านเป็นข้อความรหัสผ่านโดยตรง (plaintext)
- ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบที่มีผลกรบทบและมีความสำคัญสูงต่อองค์กรอย่างสมำเสมอ และดำเนินการตรวจสอบบัญชี รายชื่อผู้ใช้งานที่มิได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของบุคลากรที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจสอบ ได้แก่ การระงับ (Disable) การใช้งาน, ลบออกจากระบบ หรือ เปลี่ยนรหัสผ่าน เป็นต้น

#### การใช้งานรหัสผ่าน

- ต้องเก็บรหัสผ่านไว้เป็นความลับ ไม่ใช้รหัสผ่านร่วมกับผู้อื่น ไม่ใช้รหัสผ่านซ้ำกันบนบริการคนละตัว
- ระมัดระวังการล่วงรู้รหัสผ่านผู้อื่น ไม่มองจอหรือคีย์บอร์ดของผู้อื่นขณะกำลังพิมพ์รหัสผ่าน หากรับรู้โดยบังเอิญให้แจ้งเจ้าของบัญชีเพื่อเปลี่ยนรหัสผ่านโดยทันที
- ห้ามบันทึกรหัสผ่านในจุดที่ไม่สามารถควบคุมผู้เข้าถึงได้ (เช่น การบันทึกลงกระดาษโน้ตที่มองเห็นหล่ายคน, บันทึกในคอมพิวเตอร์ที่ใช้งานร่วมกัน) สามารถใช้ระบบบันทึกรหัสผ่านที่มีการป้องกันการเข้าถึง เช่น ระบบบันทึกรหัสผ่านในเบราว์เซอร์ที่ต้องล็อกอินก่อนใช้งาน หรือซอฟต์แวร์จัดการรหัสผ่าน (password manager) ที่ต้องใส่รหัสผ่านเพื่อปลดล็อก
- ใช้รหัสผ่านที่คาดเดาได้ยาก ตั้งรหัสผ่านความยาวเกิน 8 ตัวอักษรขึ้นไปทุกครั้งหากระบบอนุญาต รหัสผ่านไม่มีความ

เกี่ยวข้องกับข้อมูลที่ค้นหาได้ เช่น ชื่อ-นามสกุล, วันเกิดของตัวเองหรือคนใกล้ชิด ไม่ใช้รหัสผ่านที่มีความเกี่ยวข้องกับรหัสผ่านเดิมที่เคยใช้งาน (เช่น ต่อท้ายด้วยตัวเลขที่เพิ่มขึ้นทุกครั้งที่เปลี่ยนรหัส) อาจใช้ซอฟต์แวร์ช่วยสร้างรหัสผ่าน เช่น pwgen ในลินุกซ์ หรือตัวสร้างรหัสผ่านในซอฟต์แวร์จัดการรหัสผ่านต่างๆ

5. เปลี่ยนรหัสผ่านทันทีที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจร้าวไหลได้ เช่น มีรายงานบริการที่ใช้งานถูกแยกหรือข้อมูลรั่วไหล มีผู้มองเห็นจากพนักงานกำลังพิมพ์รหัสผ่าน ใส่รหัสผ่านผิดเว็บหรือแอป ใส่รหัสผ่านในช่องอื่นๆ ที่ไม่ใช่ช่องรหัสผ่าน เช่น ช่อง username
6. เปิดใช้งานการล็อกอินหลายชั้นตอน (multi-factor authentication - MFA) บนทุกระบบที่เกี่ยวข้องกับ MFEC เช่นหากระบบบันทึก รองรับ MFA เปลี่ยนแปลงรหัสผ่านขั้วคราวทันทีที่เข้าใช้งานเป็นครั้งแรกต้องตรวจสอบว่ามีการกำหนดรหัสผ่านที่รัดกุมตามแนวทางปฏิบัติ ดังกล่าวสำหรับบัญชีผู้ใช้งานทั้งหมดบนทุกอุปกรณ์เทคโนโลยี สารสนเทศ

## 1.5 แนวทางปฏิบัติในการเข้าถึงระบบเครือข่าย (Network Access Control)

### วัตถุประสงค์

เพื่อเป็นแนวทางปฏิบัติทางด้านความมั่นคงปลอดภัยเครือข่ายคอมพิวเตอร์ เพื่อควบคุมการเข้าถึงระบบสารสนเทศโดยรวมด้วย การให้ผู้ใช้งานสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนโดยมีการจำแนกตามสิทธิ์ที่มีการอนุญาตให้เข้าถึงได้มีการจัดระบบ การกำหนด ขอบเขต และหลักเกณฑ์การใช้งานระบบเครือข่ายของ MFEC โดยมีฝ่ายเทคโนโลยีสารสนเทศ ทำหน้าที่ในการกำกับดูแลการใช้งานเครือข่าย ของ MFEC

### ผู้รับผิดชอบ

1. ฝ่ายเทคโนโลยีสารสนเทศ
2. ผู้ดูแลระบบ
3. ผู้ใช้งาน

### นิยาม

1. “ระบบเครือข่ายไร้สาย” (WLAN: Wireless Local Area Network) หมายถึง ระบบการสื่อสารข้อมูลที่นำมาใช้ทดแทนหรือเพิ่ม ต่อกับระบบเครือข่ายใช้สายแบบดั้งเดิมโดยใช้การส่งคลื่นความถี่วิทยุในย่านวิทยุ RF และคลื่นอินฟราเรดในการรับและส่งข้อมูล ระหว่างคอมพิวเตอร์แต่ละเครื่องผ่านทางอากาศ ทะลุกำแพง เพดาน หรือสิ่งก่อสร้างอื่นๆ โดยปราศจากความต้องการของการเดินสาย
2. “Bring Your Own Device” (BYOD) หมายถึง แนวโน้มทางการใช้งานอุปกรณ์ทางเทคโนโลยี ที่บุคคลได้ตามนำอุปกรณ์ของตัวเองมาใช้ระบบสารสนเทศของ MFEC เช่น อีเมล ไฟล์เซิร์ฟเวอร์ และฐานข้อมูล เป็นต้น
3. “Peer-to-Peer” หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์ ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียม กัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูล ของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องเรียกใช้จากไฟล์เซิร์ฟเวอร์ เท่านั้น

## แนวทางปฏิบัติ

1. จัดระบบเครือข่ายเพื่อให้บริการแก่บุคลากรของ MFEC และผู้ที่ได้รับอนุญาตเท่านั้น
2. ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่า หากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของ MFEC
3. ไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประ韶เจ็งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร
4. ห้ามผู้ใช้งานละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่ไม่ใช่ของตน การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่องค์ความใดๆ ที่ก่อให้เกิดความเสียหายเลื่อมใสผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว MFEC ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว
5. ห้ามผู้ใช้งานโดยไม่ได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหัวห้ามของทางราชการ
6. ห้ามผู้ใช้งานกระทำการโอนหรือจ่ายเงินบัญชีผู้ใช้งานนี้ให้กับผู้อื่น เนื่องจากบัญชีผู้ใช้งาน (User Account) เป็นการมอบให้เฉพาะบุคคลเท่านั้น
7. กำหนดให้ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ ที่อาจจะเกิดขึ้น รวมถึงผลเสียหายที่เกิดจากการใช้บัญชีผู้ใช้งาน (User Account) ที่ MFEC มอบให้ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำการของผู้อื่น โดยไม่ได้เกิดจากความประมาท เลินเล่อของผู้ใช้งาน
8. กำหนดให้ผู้ใช้งานระบบเครือข่าย MFEC ต้องผ่านพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการ
9. กำหนดให้ผู้ใช้งานระบบเครือข่ายไร้สาย MFEC ใช้งานด้วยชื่อเครือข่าย หรือ SSID (Sub Station Identifier) และ มีระยะเวลาการใช้งาน ตามสถานภาพ สิทธิ์หรือประเภทของผู้ใช้งาน
10. การนำอุปกรณ์เทคโนโลยีสารสนเทศส่วนตัวมาใช้งาน (BYOD : Bring Your Own Device) และเชื่อมต่อกับระบบเครือข่าย MFEC ต้องผ่านการตรวจสอบความปลอดภัยบนอุปกรณ์นั้นๆ และยินยอมให้ MFEC ติดตั้งซอฟต์แวร์ตรวจสอบความปลอดภัยของอุปกรณ์ จึงสามารถถอนอนุญาตให้เข้าใช้บริการเชื่อมต่อกับระบบเครือข่าย MFEC ได้
11. กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายเพื่อใช้สารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
12. ห้ามเปิดหรือใช้งานโปรแกรมที่ใช้ทรัพยากรเครือข่ายอย่างหนัก หรือให้บริการบุคคลภายนอกโดยไม่ได้รับอนุญาต เช่น ซอฟต์แวร์ peer-to-peer, Tor node เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ
13. ระมัดระวังการใช้โปรแกรมเพื่อความบันเทิง ไม่ให้กระทบต่อทรัพยากรบริษัท ทั้งเน็ตเวิร์ค และเวลาทำงาน เลิกใช้งานทันที เมื่อได้รับการแจ้งจากฝ่ายไอทีหรือหัวหน้างาน
14. จัดทำและประกาศใช้ มาตรการดำเนินการสำหรับผู้กระทำผิด

## แนวทางปฏิบัติผู้ดูแลระบบ

1. ดูแลรักษาและปรับปรุงเครือข่ายให้สามารถใช้งานได้ดีอยู่เสมอ
2. ต้องดูแลการใช้งานเครือข่ายคอมพิวเตอร์ให้เป็นไปตามระเบียบนี้ กรณีที่พบว่ามีการกระทำหรือการใช้งานที่ไม่ถูกต้องให้รายงาน ต่อผู้บังคับบัญชาทราบโดยเร็ว และหากมีความจำเป็นเพื่อป้องกันความเสียหาย หรือผลกระทบที่อาจเกิดขึ้นต่อผู้อื่น หรือผลกระทบต่อการใช้งานระบบเครือข่ายโดยส่วนรวม ให้ผู้ดูแลระบบเครือข่ายรับงบการใช้งานได้
3. ต้องเก็บรักษาความลับของข้อมูลอันเนื่องมาจากการปฏิบัติหน้าที่
4. ต้องไม่ใช้อำนาจหน้าที่ในการเข้าถึงข้อมูลใดที่ตนไม่มีสิทธิ์เข้าถึง นอกจากรางวัลในหน้าที่

### 1.6 แนวทางปฏิบัติในการยืนยันตัวบุคคล (User Identification and Authentication)

#### วัตถุประสงค์

1. เพื่อให้เป็นไปตามข้อบังคับพระราชบัญญัติว่าด้วยการกระทำการผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
2. เพื่อให้สามารถระบุตัวตนในการใช้งานระบบสารสนเทศ
3. เพื่อเป็นการกำหนดการควบคุมบุคคลที่มีสิทธิ์เข้าสู่ระบบสารสนเทศของ MFEC. และสามารถระบุให้บุคคลนั้นกระทำการได้ในระบบสารสนเทศได้ดีบ้าง รวมถึงการอนุญาตให้ใช้สารสนเทศตามระดับชั้นความลับ และจัดเก็บข้อมูลการใช้งานระบบของบุคคลนั้น

เพื่อไม่ให้ผู้ใช้งานสารสนเทศปฏิเสธความรับผิดชอบ (Non-Repudiation) ในการใช้งานระบบสารสนเทศของ MFEC. ได้ในภายหลัง

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### นิยาม

1. “การยืนยันตัวบุคคล” หมายถึง ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง
2. “ห้องปฏิบัติการเครือข่าย” หมายถึง ห้องที่ติดตั้งอุปกรณ์เครือข่ายหลัก แนวทางปฏิบัติ
3. ส่วนประกอบของการยืนยันตัวตนอย่างสมบูรณ์ ประกอบด้วย
4. การแสดงตัวตน (Identification)
5. การยืนยันตัวตน (Authentication)
6. การกำหนดสิทธิ์ (Authorization)
7. การบันทึกการใช้งาน (Accountability)

และมีแนวทางปฏิบัติในการยืนยันตัวบุคคล ดังต่อไปนี้

1. ตั้งชื่อผู้ใช้งานแต่ละบุคคลให้แยกออกจากกันเพื่อใช้ในการแสดงตัวตนและพิสูจน์ตัวตนที่แตกต่างกัน

2. แสดงตัวตนและพิสูจน์ตัวตนทุกรั้ง ก่อนใช้ระบบเทคโนโลยีสารสนเทศของ MFEC โดยใช้ชื่อบัญชีผู้ใช้งาน (User account) ร่วมกับการยืนยันตัวตน เช่น รหัสผ่าน (password), รหัสผ่านใช้ครั้งเดียว (OTP), หรือโทเคนยืนยันตัวตนแบบต่างๆ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไขในทันที
3. กำหนดให้ผู้ใช้งานที่เข้าระบบงานที่มีความสำคัญสูง ต้องทำการพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคงปลอดภัยสูง เช่น เปิดใช้งานการยืนยันตัวตนหลายขั้นตอน (multi factor authentication – MFA) กำหนดให้ผู้ใช้งานที่เป็นเจ้าของชื่อบัญชีผู้ใช้งาน ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ (Account) ของ เครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น โดยไม่ได้เกิดจากความประมาทเลินเล่อของผู้ใช้งาน
4. กำหนดให้ผู้ใช้งานต้องเก็บรักษารหัสผ่านของบัญชีผู้ใช้งาน ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือ จ่ายแจกให้ผู้อื่น
5. กำหนดให้ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (Logout) ทุกรั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว
6. กำหนดให้ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เข้ามาปฏิบัติงานที่ห้องปฏิบัติการเครือข่าย ต้องแจ้งให้ผู้ดูแลระบบรับทราบทุกรั้ง
7. กำหนดให้ผู้ใช้งานที่ต้องการเข้าถึงระบบสารสนเทศของ MFEC จากภายนอก ต้องได้รับอนุญาตจากผู้มีอำนาจก่อน และเป็นผู้ที่ได้รับ สิทธิในการเข้าใช้บริการแล้วเท่านั้น การเข้าสู่ระบบที่มีผลกระทบและมีความสำคัญสูงต้องคัดกรองเข้มต่อตามแนวทางปฏิบัติงานจากภายนอกสำนักงาน

## 1.7 แนวทางปฏิบัติในการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

### วัตถุประสงค์

- เพื่อเป็นแนวทางปฏิบัติทางด้านความมั่นคงปลอดภัยในการควบคุมผู้ใช้งานไม่ให้สามารถเข้าถึงการปรับแต่งการตั้งค่าต่างๆ ตลอดจนซอฟต์แวร์หรือรหัสประจำของระบบปฏิบัติการโดยไม่ได้รับอนุญาต
- เพื่อกำหนดขอบเขตและหลักเกณฑ์การใช้งานระบบปฏิบัติการ โดยมีผู้ดูแลระบบ ทำหน้าที่ในการควบคุม ดูแล ระบบปฏิบัติการ

### ผู้รับผิดชอบ

- ฝ่ายเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบ
- ผู้ใช้งาน

### นิยาม

“ระบบปฏิบัติการ” (Operating System) หมายถึง ซอฟต์แวร์ระบบ (systems software) ที่ทำหน้าที่ควบคุมการทำงานของ ฮาร์ดแวร์ทั้งหมด รวมทั้งการปฏิบัติงานของโปรแกรมด้วย เพื่อให้โปรแกรมและฮาร์ดแวร์ต่าง ๆ ทำงานประสานกัน แนวทางปฏิบัติ

- จัดให้มีระบบปฏิบัติการ (Operating System) ไว้เพื่อรับการปฏิบัติงานที่เกี่ยวข้องกับ MFEC เท่านั้น
- ควบคุมการแก้ไขหรือปรับแต่งค่าในระบบปฏิบัติการ ต้องผ่านการอนุมัติจากผู้บังคับบัญชาและผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร
- กำหนดให้ผู้ใช้งานแต่ละบุคคลมี ชื่อผู้ใช้ และ รหัสผ่าน ในการใช้งานระบบปฏิบัติการหรือเครื่องคอมพิวเตอร์ตามบทบาทหน้าที่ที่ บุคคลนั้นได้รับเท่านั้น
- ต้องยืนยันตัวตนทุกครั้งก่อนเข้าใช้ระบบปฏิบัติการ
- ตั้งค่าให้ระบบล็อกการใช้งานเพื่อไม่มีการใช้งานเป็นเวลานาน และยืนยันตัวตนใหม่หากต้องการใช้งานอีกครั้ง
- มีแนวทางการป้องกันการคาดเดารหัสผ่านไปเรื่อยๆ (brute force attack) เช่น การประวิงเวลาหลังผู้ใช้ใส่รหัสผ่านผิดกันจำนวนครั้งที่กำหนด หรือล็อกบัญชีใช้งานเพื่อให้ผู้ดูแลระบบปลดล็อก
- ควบคุมการนำ ชื่อผู้ใช้ และ รหัสผ่าน ของผู้ใช้คนหนึ่งฯ ไปเพิ่มสิทธิ์ให้เข้าใช้งานกับระบบปฏิบัติการของเครื่องคอมพิวเตอร์ เครื่อง อื่นให้ดำเนินการโดยผู้ดูแลระบบเท่านั้น โดยกำหนดสภาพแวดล้อมพื้นฐานของระบบปฏิบัติการเครื่องนั้นฯ แยกบัญชีผู้ใช้จากผู้ใช้ รายอื่น (Multi-User/Multi-identity Profiles) และกำหนดสิทธิ์ตามบทบาทหน้าที่สำหรับระบบปฏิบัติการนั้น
- ควบคุมการติดตั้งซอฟต์แวร์คอมพิวเตอร์ที่มีลิขสิทธิ์ของ MFEC ลงบนระบบปฏิบัติการ โดยผู้ใช้งานขออนุมัติต่อผู้บังคับบัญชา และ ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อขอใช้งานเพิ่มเติมได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดลิขสิทธิ์ลงบนระบบปฏิบัติการที่ MFEC ใช้งาน หากตรวจพบให้ผู้ดูแลระบบลบทิ้ง และนับเป็นความผิด ที่ผู้ใช้งานผู้นั้นต้องรับผิดชอบต่อความผิด

9. ควบคุมการติดตั้งโปรแกรมประยุกต์สำหรับการใช้งานทั่วไป โดยผู้ใช้งานของนัมติดต่อผู้บังคับบัญชาและผู้อำนวยการฝ่ายเทคโนโลยี สารสนเทศ เพื่อขอใช้งานเพิ่มเติมได้ตามความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งโปรแกรมประยุกต์อื่นใด ที่ไม่มีสิทธิ์ ลงบนระบบปฏิบัติการที่ MFEC ใช้งาน ด้วยตนเอง หากตรวจสอบให้ผู้ดูแลระบบทั้งและนับเป็นความผิดที่ผู้ใช้งานผู้นั้นต้องรับผิดชอบต่อความผิด
  10. ควบคุมการติดตั้ง ถอนการติดตั้ง หรือปรับเปลี่ยนการกำหนดค่าการทำงานของซอฟต์แวร์หรือโปรแกรมประยุกต์ โดยให้ผู้ดูแล ระบบพิจารณาผลผลกระทบกับระบบปฏิบัติการก่อนการดำเนินการ
  11. ห้ามใช้ซอฟต์แวร์ระบบปฏิบัติการของ MFEC เพื่อประโยชน์ทางการค้าใดๆ หรือเพื่อผลประโยชน์ส่วนตัว
  12. ห้ามผู้ใช้งานระบบปฏิบัติการ กระทำการใดๆ เพื่อควบคุมคอมพิวเตอร์เครื่องอื่น โดยเข้มต่อทึ้งจากภายในไปสู่ภายนอก หรือจากภายนอกเข้ามาสู่ระบบปฏิบัติการภายนอก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
  13. ควบคุมโดยตัดการใช้งานเมื่อไม่ได้มีการใช้งานเกินกว่าระยะเวลาที่กำหนด และล็อกหน้าจอสำหรับระบบปฏิบัติการที่มีความสำคัญ
  14. ควบคุมระยะเวลาการเข้มต่อเพื่อเข้าถึงระบบปฏิบัติการที่มีความสำคัญหรือมีความเสี่ยงสูง ให้เข้าถึงได้ในระยะเวลาที่กำหนด หรือเป็นไปตามที่ผู้ดูแลระบบกำหนดไว้
  15. จัดให้มีระบบบันทึกการเข้าใช้งานระบบปฏิบัติการ ที่ระบุถึงชื่อผู้ใช้ วันที่และเวลาที่เข้า/ออกระบบปฏิบัติการ
  16. ห้ามมิให้ผู้ใช้งานกระทำการติดตั้ง ถอนการติดตั้ง เปลี่ยนแปลง แก้ไขระบบปฏิบัติการหรือทำสำเนา เพื่อนำไปใช้งานที่อื่นโดยไม่ได้รับอนุญาต เนื่องจากระบบปฏิบัติการที่ MFEC จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นและสำคัญ
  17. ห้ามทำการปรับแต่ง BIOS โดยมิได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ เนื่องจากส่งผลกระทบกับการทำงานของคอมพิวเตอร์และระบบปฏิบัติการ
  18. กำหนดให้มีการจัดทำและประกาศใช้มาตรการดำเนินการสำหรับผู้กระทำการผิด
- แนวทางปฏิบัติสำหรับผู้ดูแลระบบ**
1. ดูแลรักษาและปรับปรุงระบบปฏิบัติการให้สามารถใช้งานได้ด้วยเสมอ
  2. ต้องดูแลการใช้งานระบบปฏิบัติการบนอุปกรณ์เทคโนโลยีสารสนเทศให้เป็นไปตามระเบียบนี้ กรณีที่พบว่า มีการกระทำการใดๆ ที่ไม่ถูกต้องให้รายงานต่อผู้บังคับบัญชาทราบโดยเร็ว และหากมีความจำเป็นเพื่อป้องกันความเสี่ยงหาย หรือผลกระทบที่อาจเกิดขึ้นต่อผู้อื่น หรือต่อการใช้งานระบบสารสนเทศโดยส่วนรวม ให้ผู้ดูแลระบบรับงบการใช้งานดังกล่าว
  3. ต้องเก็บรักษาความลับของข้อมูลอันเนื่องมาจากการปฏิบัติหน้าที่
  4. ต้องไม่ใช้อำนาจหน้าที่ในการเข้าถึงข้อมูลใดที่ตนไม่มีสิทธิ์เข้าถึง นอกจากงานในหน้าที่
  5. ต้องดำเนินการติดตั้งซอฟต์แวร์ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ โดยดำเนินการตามรายการตรวจสอบ (checklist) สำหรับ การติดตั้งเครื่องคอมพิวเตอร์ และปรับปรุงรายการตรวจสอบนั้นอย่างน้อยปีละ 1 ครั้ง โดยให้ระบุเวอร์ชันของรายการตรวจสอบ เพื่อป้องกันความสับสน มีแนวปฏิบัติซึ่งครอบคลุมประเด็นดังนี้
- 5.1. ใน bios (BIOS: Basic Input/Output System) เป็นชื่อโปรแกรมชุดหนึ่งซึ่งจะควบคุมการทำงานของคอมพิวเตอร์ใน

- ส่วนที่เกี่ยวข้องกับการนำข้อมูลเข้าไปเก็บและ การแสดงผล
- 5.2. ติดตั้งระบบปฏิบัติการ และซอฟต์แวร์ควบคุมการทำงานของชิ้นส่วนอุปกรณ์ (driver)
  - 5.3. กำหนดค่าเครื่อข่ายและการเข้าถึงทรัพยากรบนเครือข่าย
  - 5.4. ติดตั้งโปรแกรมป้องกันไวรัสหรือมัลแวร์ที่จัดการได้แบบรวมศูนย์ หรือแบบคลาวด์
  - 5.5. ติดตั้งโปรแกรมปรับปรุงการปิดช่องให้ของระบบปฏิบัติการโดยการดำเนินการอย่างสม่ำเสมอ
  - 5.6. ติดตั้งซอฟต์แวร์และโปรแกรมประยุกต์ รวมถึงซอฟต์แวร์ที่ใช้งานผ่านบริการคลาวด์ ตามที่จำเป็นต่อการปฏิบัติงาน เท่านั้น
  6. ต้องจัดทำบัญชีผู้ใช้ บัญชีเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่ระบุในระบบปฏิบัติการ ซอฟต์แวร์ที่ติดตั้ง และผู้มีสิทธิ์ใช้งาน พร้อมปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ

### 1.8 แนวทางปฏิบัติในการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์

#### วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์โดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อความมั่นคง ปลอดภัยของระบบสารสนเทศของ MFEC

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้พัฒนาระบบ
3. ผู้ใช้งาน

#### แนวทางปฏิบัติ

1. กำหนดให้ผู้ดูแลระบบต้องควบคุม จำกัด หรือให้สิทธิ์การเข้าถึงสารสนเทศ ข้อมูลและฟังก์ชันต่าง ๆ ของระบบสารสนเทศ และโปรแกรมประยุกต์ ดังนี้
  - 1.1. ต้องลงทะเบียนการเข้าใช้งานเพื่อทำการระบุตัวตน
  - 1.2. ให้เข้าถึงได้เฉพาะส่วนระบบงานและฟังก์ชันที่จำเป็นต่อการทำงานและที่ได้รับอนุญาตเท่านั้น
  - 1.3. ให้เข้าถึงได้เฉพาะข้อมูลที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น
  - 1.4. ห้ามไม่ให้กระทำการโอนย้ายสิทธิ์แก่ผู้อื่นโดยสิทธิ์การเข้าใช้งานให้เป็นสิทธิ์เฉพาะบุคคลเท่านั้น
  - 1.5. ให้ทำการยกเลิกสิทธิ์การเข้าใช้ทันทีที่ผู้ได้รับสิทธินั้นไม่ได้รับสิทธิ์การเข้าใช้งานอีกต่อไป
  - 1.6. กำหนดให้มีข้อความแสดงเตือนถึงผู้ไม่มีสิทธิ์เข้าถึงหรือใช้งานสารสนเทศ ระบบงาน ข้อมูลและฟังก์ชันต่าง ๆ ของระบบงาน
2. กำหนดให้ผู้ดูแลระบบต้องทำการควบคุมหรือจำกัดสิทธิ์การเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่ง ดังนี้
  - 2.1. ให้เข้าถึงได้เฉพาะส่วนฟังก์ชันที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น

- 2.2. ให้เข้าถึงได้เฉพาะข้อมูลที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น
- 2.3. กำหนดให้มีการพิสูจน์ตัวตน (Authentication) ก่อนการเข้าถึงระบบงานทุกครั้ง
- 2.4. กำหนดให้มีการจำกัดเส้นทางและวิธีการในการเข้าถึงระบบงานจากอีกรอบบงานหนึ่ง
- 2.5. กำหนดให้มีการลบหานสิทธิ์ในการเข้าถึงอย่างน้อยปีละ 1 ครั้ง
3. กำหนดให้ผู้ดูแลระบบต้องทำการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงานหนึ่ง โดยให้นำข้อมูลออกได้เฉพาะที่เกี่ยวข้อง และจำเป็นสำหรับการนำไปใช้งานเท่านั้น
4. กำหนดให้ระบบที่ใช้งานต้องมีการแสดงเฉพาะข้อมูลพื้นฐานเพื่อให้ผู้ใช้งานได้รับทราบข้อมูลเฉพาะที่จำเป็น และตามสิทธิ์การใช้งานเท่านั้น
5. กำหนดให้ระบบที่ใช้งานต้องมีข้อจำกัดไม่ให้ระบบแสดงความช่วยเหลือใด ๆ กรณีที่มีเหตุการณ์ไม่สงบส่งค์เกิดขึ้นในระบบ
6. กำหนดให้ระบบที่ใช้งานต้องมีฟังก์ชันที่สามารถทำการตรวจสอบและควบคุมการลงบันทึกเข้า (Login) ดังนี้
  - 6.1. แสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ลงบันทึกเข้า (Login) เสร็จแล้ว
  - 6.2. ตรวจสอบข้อมูลการลงบันทึกเข้า (Login) หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว
7. จำกัดไม่ให้ระบบแสดงข้อมูลภายนอกที่เปิดเผยข้อมูลภายใต้ชื่อของระบบ
8. จำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการลงบันทึกเข้า (Login) ผิด
9. กำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเข้ามายังระบบงานได้ภายหลังจากที่ใส่ข้อมูลการลงบันทึกเข้า
10. (Login) ผิดเกินกว่าจำนวนครั้งที่กำหนด
11. กำหนดให้มีฟังก์ชันที่สามารถส่งข้อมูลเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามลงบันทึกเข้า (Login) แต่ผิดพลาดเป็นจำนวนหลายครั้ง
12. กำหนดให้มีการบันทึกข้อมูลลงบันทึกเข้า (Login) ทั้งที่สำเร็จและไม่สำเร็จ
13. จำกัดช่วงเวลาที่นานที่สุดที่ผู้ใช้งานจะลงบันทึกเข้า (Login) ให้สำเร็จ
14. แสดงวันที่/เวลาที่ลงบันทึกเข้า (Login) ครั้งที่แล้ว (ทั้งที่สำเร็จและไม่สำเร็จ)

## 2. นโยบายย่อของการแบ่งชั้นความลับ (Data Classification)

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

### วัตถุประสงค์ของการควบคุมการเข้าถึงสารสนเทศ

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

### แนวทาง

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติต้านการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งานข้อมูลและระบบสารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

### ขอบเขตของนโยบายย่อของการแบ่งชั้นความลับ

ขอบเขตของนโยบายย่อของการแบ่งชั้นความลับ หมายถึงการกำหนดแนวทางปฏิบัติต่อชนิดของข้อมูลสารสนเทศตั้งแต่เริ่มจัดทำหรือได้มา การใช้งาน การสำเนา การกระจาย จนถึงการยกเลิกการใช้หรือการทำลาย ครอบคลุมสารสนเทศที่อยู่ในรูปแบบของ อิเล็กทรอนิกส์และไม่ใช้อิเล็กทรอนิกส์

### บทบาทและหน้าที่

Chief Operating Officer (COO) ทำหน้าที่กำกับดูแลให้เป็นไปตามนโยบายและแนวทางปฏิบัติในการแบ่งชั้นความลับ ผู้บริหาร/ผู้บังคับบัญชา เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ที่เกี่ยวข้องภายใต้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการแบ่งชั้นความลับ

ฝ่ายอำนวยการ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการแบ่งชั้นความลับและการใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการแบ่งชั้นความลับและการใช้งานข้อมูลสารสนเทศ

**เจ้าหน้าที่สารสนเทศ/ผู้ใช้งาน ต้องปฏิบัติตามนโยบายการควบคุมการเข้าถึงสารสนเทศ รวมทั้งข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับต่างๆที่เกี่ยวข้อง**

#### **ระยะเวลาทบทวน**

เพื่อให้นโยบายการเข้าถึงสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง MFEC จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนการปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลง กระบวนการทำงาน วิธีการเข้าถึงสารสนเทศที่สำคัญที่ระบุกับนโยบายนี้

#### **2.1 แนวทางปฏิบัติการจัดระดับขั้นความลับของข้อมูลและสินทรัพย์สารสนเทศ (Information Classification Guidelines)**

1. กำหนดให้บุคคลหรือหน่วยงานผู้รับผิดชอบสินทรัพย์สารสนเทศกำหนดขั้นความลับของข้อมูลและเอกสารให้เป็นไปตามข้อกำหนด ในการจัดระดับขั้นความลับของสารสนเทศของ MFEC เพื่อป้องกันสารสนเทศให้มีความมั่นคงปลอดภัยด้วยวิธีการที่เหมาะสมตามนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2. จัดให้มีการทบทวนระดับขั้นความลับอย่างน้อยปีละ 1 ครั้ง
3. เอกสารหรือสิ่งพิมพ์ที่พิมพ์หรือทำขึ้นมาจากต้นฉบับที่มีการกำหนดขั้นความลับไว้ทั้งในกรณีทั้งหมดหรือบางส่วนให้ถือว่า มี ขั้นความลับเดียวกันกับต้นฉบับ

#### **2.2 แนวทางปฏิบัติการจัดทำป้ายชื่อและการจัดการสารสนเทศ (Information Labeling and Handling)**

1. จัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์สินทรัพย์สารสนเทศที่เกี่ยวข้อง ให้เป็นไปตามข้อกำหนดในการ จัดทำป้ายชื่อและการจัดการสารสนเทศของ MFEC
2. ต้องควบคุมและรักษาความมั่นคงปลอดภัยข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้น อย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การ จัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย โดยต้องกำหนดเป็นขั้นตอนปฏิบัติให้ผู้ใช้งาน ต้องปฏิบัติ ตามอย่างเคร่งครัด เพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัย
3. ต้องทำลายเอกสารและสื่อบันทึกข้อมูลที่ไม่ใช้งานแล้ว ตามแนวทางของการชำรุดข้อมูลและสื่อบันทึกข้อมูล เพื่อให้มั่นใจ ว่า ข้อมูลที่มีระดับขั้นความลับตั้งแต่ “ลับ” ขึ้นไปของ MFEC จะไม่ถูกคืนโดยผู้ไม่มีสิทธิ
4. ผู้ใช้งานต้องทราบถึงการรักษาข้อมูลลับที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่อง คอมพิวเตอร์ที่มี การใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดย วิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม
5. ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลที่มีระดับขั้นความลับตั้งแต่ “ลับ” ขึ้นไป ไว้ในตู้ที่สามารถปิดล็อกได้ เมื่อไม่ได้ใช้งาน หรือเมื่อต้องวางเอกสารหรือสื่อบันทึกไว้โดยเฉพาะอย่างยิ่งเมื่ออุปนภัยทำการ

6. ข้อมูลที่มีระดับขั้นความลับตั้งแต่ “ลับ” ขึ้นไป ต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ (เช่น เครื่องพิมพ์ เครื่องโทรศัพท์ เครื่องถ่ายเอกสาร เป็นต้น) โดยทันที
7. ต้องไม่เปิดเผยข้อมูลที่มีระดับขั้นความลับตั้งแต่ “ลับ” ขึ้นไป ต่อบุคคลภายนอก เว้นแต่มีความจำเป็นในการปฏิบัติงานและการ เปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล
8. ต้องไม่พูดคุยหรือใช้งานข้อมูลลับในพื้นที่สาธารณะ เช่น รถโดยสาร ร้านอาหาร ฯลฯ
9. สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น Thumb-Drive, CD-ROM, External hard disk เป็นต้น) ที่มี ข้อมูล ลับบันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง
10. ข้อมูลที่เกี่ยวข้องกับการดำเนินงานของ MFEC ทั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเครื่อง คอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ดูแลระบบ ต้องได้รับการสำรองข้อมูลอย่างล้ำม้ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมี ปัญหา ใด ๆ เกิดขึ้น ด้วยอย่างเช่น การติดไวรัส ยาาร์ดติดสก์เสีย เป็นต้น
11. ข้อมูลที่มีระดับขั้นความลับตั้งแต่ “ลับ” ขึ้นไป ต้องถูกนำออกจากอุปกรณ์เทคโนโลยีสารสนเทศ อุปกรณ์ประมวลผลต่างๆ และสื่อบันทึกข้อมูล เมื่อมีการนำอุปกรณ์นั้นไปซ่อมบำรุงรักษา หรือตัดจำหน่าย โดยต้องเป็นการนำข้อมูลออกจากอย่างไม่ สามารถถูกกลับคืน มาใช้ได้อีก

### 2.3 แนวทางปฏิบัติการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Computer Media)

1. สื่อบันทึกข้อมูลทั้งหมดต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูลตามข้อกำหนด ของ ผู้ผลิตสื่อบันทึกข้อมูล
2. นำข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูล ต้องจัดเก็บข้อมูลไว้ที่แหล่งอื่นด้วย เพื่อ ป้องกันการสูญหายของข้อมูล
3. ข้อมูลที่มีระดับขั้นความลับตั้งแต่ “ลับ” ขึ้นไป ที่บันทึกอยู่ในสื่อบันทึกข้อมูล ต้องจัดเก็บแบบเข้ารหัส (Encrypt) เพื่อป้องกัน การ เข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ
4. ผู้ใช้งานต้องระมัดระวังในการใช้งานสื่อบันทึกข้อมูล โดยต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล และต้องมีการ ชำรุด ข้อมูลตามแนวทางของการชำรุดข้อมูลและสื่อบันทึกข้อมูล

### 2.4 แนวทางปฏิบัติการชำรุดข้อมูลและสื่อบันทึกข้อมูล (Disposal of Media)

1. ต้องกำหนดให้มีการชำรุดข้อมูลที่บันทึกอยู่ในสื่อบันทึกข้อมูล เมื่อไม่มีการใช้งานแล้ว โดยคำนึงถึงระดับขั้นความลับ การ นำสื่อบันทึกข้อมูลกลับมาใช้ใหม่ ประเภทของสื่อบันทึกข้อมูล ตามข้อกำหนดในการชำรุดข้อมูลและสื่อบันทึกข้อมูลของ MFEC
2. กรณีที่สื่อบันทึกข้อมูลมีข้อมูลที่มีระดับขั้นความลับต่างกันให้ดำเนินการชำรุดข้อมูลและสื่อบันทึกข้อมูลด้วยรูปแบบและ

- วิธีการ ที่กำหนดให้สำหรับข้อมูลที่มีระดับขั้นความลับสูงสุด
3. ต้องชำระข้อมูลก่อนบริจาก ส่งซ่อน จำหน่าย รวมถึงส่งมอบให้บุคคลภายนอกถือครองสือบันทึกข้อมูล โดยปฏิบัติตาม รูปแบบ และวิธีการที่เหมาะสม
  4. กรณีการเข้าสือบันทึกข้อมูล หรือการใช้บริการคลาวด์หรือศูนย์ข้อมูล กับหน่วยงานภายนอก ต้องทำข้อตกลงเกี่ยวกับการ ชำระล้าง ข้อมูลและสือบันทึกข้อมูล โดยสามารถกำหนดให้เป็นหน้าที่ของผู้ให้บริการได้ และต้องสามารถตรวจสอบได้ว่ามี การดำเนินการ ตามข้อตกลงแล้ว
  5. ในการทำลายสือบันทึกข้อมูล ต้องมีการบันทึกรายละเอียดและเหตุผลของการทำลายข้อมูลและสือบันทึกข้อมูลดังกล่าว เพื่อ ใช้ใน การตรวจสอบ

## 2.5 แนวทางปฏิบัติในการเข้ารหัสสำหรับข้อมูลที่เป็นความลับ

### **วัตถุประสงค์**

เพื่อรักษาความลับของข้อมูลให้ข้อมูลนั้นเข้าถึงหรือเข้าชมได้โดยบุคคลที่ได้รับอนุญาตเท่านั้นโดยอาศัยกระบวนการทำงาน ด้วย คอมพิวเตอร์ที่ซับซ้อนเพื่อเข้ารหัส (Encrypt) ไปอยู่ในรูปของข้อมูลที่ไม่สามารถอ่านได้โดยตรง และข้อมูลนั้นจะถูกถอดรหัส (Decrypt) ใน รูปแบบและวิธีการที่ถูกต้องตรงกัน

### **ผู้รับผิดชอบ**

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

### **นิยาม**

1. “การเข้ารหัส” (Encryption) หมายถึง การเปลี่ยนข้อความหรือเครื่องหมายธรรมด้า ให้เป็นข้อความหรือเครื่องหมายลับ ด้วยวิธี ใดวิธีหนึ่ง
2. “การถอดรหัส” (Decryption) หมายถึง การเปลี่ยนข้อความหรือเครื่องหมายที่ถูกเข้ารหัส ให้เป็นข้อความหรือเครื่องหมาย ธรรมด้า ด้วยวิธีใดวิธีหนึ่ง
3. “เว็บแอปพลิเคชัน” (Web Application) หมายถึง โปรแกรมประยุกต์ที่เข้าถึงได้ด้วยโปรแกรมเว็บเบราว์เซอร์ผ่านระบบ เครือข่าย
4. “เว็บเบราว์เซอร์” (Web Browser) หมายถึง โปรแกรมคอมพิวเตอร์ที่ผู้ใช้งานสามารถใช้เพื่อคุ้มครองข้อมูลและตัดอับกับข้อมูล สารสนเทศที่จัดเก็บในเว็บแอปพลิเคชันที่สร้างขึ้นด้วยภาษาเฉพาะ เช่น ภาษา HTML
5. “เว็บเซิร์ฟเวอร์” (Web Server) หมายถึง เครื่องคอมพิวเตอร์ที่ให้บริการเว็บเพจ เมื่อผู้ใช้งานร้องขอเว็บเพจผ่านเว็บ เบราร์เซอร์ เรียกใช้โดยการระบุตำแหน่งของเว็บเพจ (URL) เว็บเซิร์ฟเวอร์จะส่งเว็บเพจที่ค้นหาได้กลับไปแสดงผลผ่านเว็บ เบราร์เซอร์ของผู้ใช้งาน
6. “กุญแจรหัส” (Key) หมายถึง ชุดตัวอักษรที่ซับซ้อนและยากต่อการคาดเดา ใช้สำหรับเข้ารหัสและถอดรหัส

7. “มัลแวร์” (Malware) ย่อมาจากคำว่า Malicious Software หมายถึง โปรแกรมคอมพิวเตอร์ประสงค์ร้ายต่างๆ ทำงานในลักษณะ ที่เป็นการโจมตีระบบ ทำให้ระบบเสียหาย รวมไปถึงการโจมตีข้อมูล
8. “ช่องโหว่ของซอฟต์แวร์” หมายถึง จุดอ่อนประการหนึ่งที่ทำให้ผู้โจมตีสามารถใช้เพื่อลดTHONหรือหลีกเลี่ยงการป้องกันความปลอดภัยเทคโนโลยีสารสนเทศ

#### แนวทางปฏิบัติ

1. ประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสม สำหรับข้อมูลที่จำเป็นต้องป้องกัน
2. กำหนดหลักการที่ไว้ป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล
3. จัดเก็บ ชื่อบัญชีผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ของระบบสารสนเทศลงในฐานข้อมูลใดๆ ต้องเข้ารหัสในส่วน ของรหัสผ่านก่อนบันทึกลงในฐานข้อมูลทุกรั้ง
4. ส่งต่อข้อมูลผ่านเน็ตเวิร์คโดยใช้โปรโตคอลที่มีการเข้ารหัสลับมั่นคง เช่น TLS, SSH มีการยืนยันว่าเซิร์ฟเวอร์ที่กำลังใช้งานเป็นเซิร์ฟเวอร์จริง เช่น การตรวจสอบกุญแจสาธารณะ (public key) ของเว็บต่างๆ
5. กำหนดช่องทางรับ - ส่งข้อมูลที่มีขั้นความลับตั้งแต่ “ลับ” ขึ้นไปที่เหมาะสมกับ MFEC ดังต่อไปนี้
  - 5.1. ระบบการสื่อสารข้อมูลที่เปิดให้ใช้งาน ซึ่งรวมทั้งเครือข่ายภายใน (Local Area Network) เครือข่ายไร้สาย (Wireless LAN) และอินเทอร์เน็ต
  - 5.2. อุปกรณ์เครือข่ายไร้สายที่อนุญาตให้ใช้ได้
  - 5.3. สื่อบันทึกข้อมูลที่สามารถถอดแยกจากตัวเครื่องคอมพิวเตอร์ได้
6. กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจรหัส (Key) สำหรับการเข้ารหัสข้อมูล ดังนี้
  - 6.1. วิธีการป้องกันกุญแจรหัสที่ใช้สำหรับการเข้ารหัสข้อมูล
  - 6.2. วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจรหัสเกิดการสูญหายหรือถูกทำให้เสียหาย
  - 6.3. บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล ประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจรหัส ผู้สร้าง กุญแจรหัส ผู้ทำหน้าที่ทำลาย ผู้ใช้งาน ผู้ทำหน้าที่จัดการกรณีกุญแจรหัสเกิดการสูญหาย
7. ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับ หรือวิธีการรักษาความลับของข้อมูล ดังนี้
  - 7.1. ต้องแสดงขั้นความลับบนไฟล์ข้อมูลลับ และแสดงขั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
  - 7.2. ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานที่ MFEC กำหนด
  - 7.3. ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการกำหนดรหัสผ่านเพื่อเปิดใช้ไฟล์
8. ห้ามเผยแพร่ไฟล์ข้อมูลลับของ MFEC โดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรโดยเด็ดขาด
9. ตรวจสอบการทำงานของระบบป้องกันมัลแวร์ (Malware) อย่างสม่ำเสมอ ในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล ว่า มีการทำงานของระบบป้องกันมัลแวร์ตามปกติหรือไม่
10. ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติ หรือไม่

11. สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอตามความจำเป็น

## 2.6 แนวทางปฏิบัติสำหรับระบบที่ไว้ต่อการรบกวน

### วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับระบบที่ไว้ต่อการรบกวน อันจะเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบที่ไว้ต่อการรบกวน

### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

### แนวปฏิบัติ

1. ระบบซึ่งไว้ต่อการรบกวนคือระบบที่มีผลกระทบและมีความสำคัญสูงต่อองค์กรได้แก่ ระบบบริหารโครงการออนไลน์ และระบบบัญชีการเงินและพัสดุ
2. แยกระบบซึ่งไว้ต่อการรบกวนออกจากระบบอื่น ๆ และควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ
3. ประเมินความเสี่ยงสำหรับการใช้งานทรัพยากร่วมกันระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่น ๆ ที่มีความสำคัญน้อยกว่า รวมทั้งมีการ trab ห่วงความเสี่ยงสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
4. ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ สำหรับระบบซึ่งไว้ต่อการรบกวน ดังนี้
  - 4.1. ต้องมีการร้องขอการเข้าใช้งาน พร้อมทั้งระบุเหตุผลในการเข้าใช้งานสำหรับอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องการเข้าใช้งานระบบซึ่งไว้ต่อการรบกวน
  - 4.2. การร้องขอการเข้าใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชา เจ้าของระบบ และผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ
  - 4.3. การเข้าใช้งานระบบซึ่งไว้ต่อการรบกวน ต้องใช้งานได้หลังจากที่ผ่าน การพิสูจน์ตัวตน (Authentication) และเท่านั้น
  - 4.4. ผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องจัดให้มีโปรแกรมป้องกันโปรแกรมที่ไม่ประสงค์ดี และต้องปรับปรุงให้โปรแกรมดังกล่าวทันสมัยอยู่เสมอ
  - 4.5. ผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่จะต้องไม่กระทำการใด ๆ อันจะก่อให้เกิดความเสี่ยงต่อการใช้งาน ระบบซึ่งไว้ต่อการรบกวน อาทิ การส่งรหัสผ่าน (Password) โดยมิได้ทำการเข้ารหัส
  - 4.6. ต้องทำการจำกัดสิทธิ์การเข้าใช้งานระบบซึ่งไว้ต่อการรบกวน และจะต้องเป็นสิทธิ์เฉพาะบุคคลเท่านั้น ห้ามมิให้โอนย้ายสิทธิ์ แก่ผู้อื่นโดยเด็ดขาด
  - 4.7. ต้องมีการตรวจสอบการเข้าใช้งานอยู่สม่ำเสมอสำหรับระบบซึ่งไว้ต่อการรบกวน หากมีการเข้าใช้งานระบบแต่มิได้กระทำการใด ๆ เกินกว่า 30 นาที ให้ตัดการเข้าใช้งานทันที
5. ควบคุมการเข้าใช้งานระบบซึ่งไว้ต่อการรบกวนจากภายนอกองค์กร โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึง

## สารสนเทศที่ได้กำหนดไว้

### 2.7 แนวทางปฏิบัติสำหรับการโอนถ่ายข้อมูล

#### วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศให้กับหน่วยงานภายนอกทั้งในรูปแบบภาษาไทย และอังกฤษ

#### ผู้รับผิดชอบ

- ผู้ใช้งาน

#### แนวทางปฏิบัติ

- การจัดทำขั้นตอนปฏิบัติในการป้องกันการโอนถ่ายข้อมูลจากการถูกดักจับ สำเนา แก้ไข ปรับเส้นทาง และทำลาย
- ระบบงานต่างๆที่มีการติดต่อสู่ภายนอกต้องมีการระบุเป็นกันโดยมุ่งร้ายผ่านการสื่อสารทางอิเล็กทรอนิกส์
- ต้องมีการจัดทำขั้นตอนป้องกันการสื่อสารข้อมูลที่มีระดับความสำคัญในข้อมูลอิเล็กทรอนิกส์ที่อยู่ในรูปแบบไฟล์แนบ
- การสื่อสารสู่ภายนอกผู้รับข้อมูลต้องรับทราบถึงนโยบายการยอมรับการใช้งานสารสนเทศองค์กร (Acceptable Use Policy)
- ผู้ที่รับข่าวสารข้อมูลจากภายนอก จะต้องรับผิดชอบต่อข้อมูลข่าวสารที่ได้รับ โดยไม่ไปทำการใดๆที่ทำให้เสื่อมเสียเชื่อเสียง ศุภภาพ ละเมิดความเป็นส่วนตัว ส่งต่ออย่างเป็นลูกโซ่
- ข้อมูลที่ติดต่อต้องมีการเข้ารหัสข้อมูลสารสนเทศทั้งการปกปิด การตรวจสอบความถูกต้อง การพิสูจน์การเข้าถึงข้อมูลสารสนเทศ
- ต้องรับผิดชอบต่อการเก็บรักษา ทำลายทั้งข้อมูล ที่เกี่ยวข้องให้สอดคล้องกับกฎระเบียบ กฎหมาย ข้อปฏิบัติท้องถิ่นนั้นๆ
- กำหนดให้มีการควบคุมการสื่อสารต่างๆ เช่นการส่งต่ออีเมลทาง E-mail สู่ E-mail ภายนอก
- ให้คำแนะนำกับบุคคลที่ได้รับข้อมูลสารสนเทศโดยห้ามไม่ให้เปิดเผยข้อมูลขั้นความลับออกสู่ภายนอก
- ไม่ทิ้งข้อมูลสารสนเทศที่มีความสำคัญ หรือส่งต่อไปยังบุคคลอื่นที่ไม่เกี่ยวข้องในระบบจัดเก็บที่ไม่ถูกต้อง
- ให้คำแนะนำเกี่ยวกับปัญหาการดำเนินการส่งข้อมูลแบบต่างๆ
  - วิธีการพิมพ์เอกสารทางเครื่องพิมพ์ต้องพิมพ์ในเครื่องพิมพ์ที่สามารถเห็นได้จากผู้สั่งพิมพ์
  - วิธีการรับแฟกซ์ จะต้องให้ผู้รับข่าวสารไปรอรับเอกสารก่อนที่จะส่งเอกสารไป
  - การพูดคุยข้อมูลความลับต้องไม่ดำเนินการในพื้นที่สาธารณะ หรือที่บุคคลอื่นสามารถรับข้อมูลได้
- การดำเนินการโอนถ่ายข้อมูลสารสนเทศจะต้องปฏิบัติตามข้อกำหนดที่สอดคล้องกับกฎหมาย

### 3. นโยบายย่ออย่างย่อด้านการดำเนินการอย่างปลอดภัย (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 และการกู้คืนกรณีที่พบปัญหาเกี่ยวกับข้อมูลสารสนเทศ หรือระบบงานสารสนเทศ
3. เพื่อให้ผู้บริหารได้รับรายงานที่เหมาะสม เพียงพอต่อการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ

#### **แนวทาง**

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

#### **ขอบเขตของนโยบายย่ออย่างย่อการดำเนินการอย่างปลอดภัย**

ขอบเขตของนโยบายย่ออย่างย่อการดำเนินการอย่างปลอดภัย หมายถึงการกำหนดแนวทางปฏิบัติต่อการดำเนินงานต่างๆ ที่จำเป็นเพื่อสร้างความมั่นใจในการใช้งานข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศ

#### **บทบาทและหน้าที่**

Chief Operating Officer (COO) ทำหน้าที่กำกับดูแลให้เป็นไปตามนโยบายและแนวทางปฏิบัติการดำเนินการอย่างปลอดภัย

ผู้บริหาร/ผู้บังคับบัญชา เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ที่เกี่ยวข้องภายใต้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการดำเนินการอย่างปลอดภัย

ฝ่ายอำนวยการ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการดำเนินการอย่างปลอดภัย

ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการดำเนินการอย่างปลอดภัย

เจ้าหน้าที่สารสนเทศ/ผู้ใช้งาน ต้องปฏิบัติตามนโยบายการดำเนินการอย่างปลอดภัย รวมทั้งข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้อง

## ระยะเวลาทบทวน

เพื่อให้นโยบายการเข้าถึงสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารได้ฯ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง MFEC จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนการปฏิบัติ ระเบียบข้อบังคับ และเอกสารได้ฯ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลง กระบวนการการทำงาน วิธีการเข้าถึงสารสนเทศที่สำคัญที่กระทบกับนโยบายนี้

### 3.1 แนวทางปฏิบัติในการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Information Asset Management)

#### วัตถุประสงค์

เพื่อควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบสารสนเทศให้ได้รับการป้องกันและปกป้องให้มีความมั่นคงปลอดภัยจากการ เข้าถึงและนำไปใช้งานของผู้ไม่มีสิทธิ ในระดับที่เหมาะสมตามระดับขั้นความลับ

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### คำนิยาม

1. “สินทรัพย์สารสนเทศ” หมายถึง สินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ และ โปรแกรมประยุกต์ (Software and Application Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) ที่เกี่ยวข้องกับงานสารสนเทศ
2. “สื่อบันทึกข้อมูล” หมายถึง สื่อบันทึกข้อมูลใดๆ ที่ใช้วิธีการทำงานอิเล็กทรอนิกส์

#### แนวทางปฏิบัติ

##### ทะเบียนสินทรัพย์ (Inventory of Assets)

1. จัดทำและเก็บทะเบียนสินทรัพย์สารสนเทศ เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและ บริหาร จัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ของ MFEC
2. ตรวจสอบสินทรัพย์ (inventory check) ทุกประเภทตามระยะเวลาที่กำหนดไว้
3. ประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่หรือมีการเปลี่ยนแปลงสินทรัพย์ที่สำคัญ เกิดขึ้น

##### ความเป็นเจ้าของสินทรัพย์ (Ownership for Assets)

1. กำหนดคุณลักษณะหรือหน่วยงานผู้รับผิดชอบสินทรัพย์สารสนเทศ โดยแยกตามประเภท บัญชี และรายการ อย่างชัดเจน
2. กำหนดหน้าที่และความรับผิดชอบที่มีต่อสินทรัพย์สารสนเทศ ดังนี้
3. ผู้รับผิดชอบสินทรัพย์ข้อมูลและเอกสาร (เจ้าของข้อมูล)

- 1.3.1. บริหารจัดการสิทธิ์ของผู้ใช้งานให้เป็นไปอย่างถูกต้องเหมาะสม
- 1.3.2. กำหนดระดับชั้นความลับให้กับข้อมูล
- 1.3.3. บริหารจัดการระดับชั้นความลับของข้อมูลให้เป็นไปตามความต้องการของการปฏิบัติงานให้มีความเหมาะสมและสอดคล้องกับระดับชั้นความลับนั้นๆ
- 1.3.4. มีการระบุหรือแสดงระดับชั้นความลับตามที่ได้จัดระดับไว้อย่างถูกต้องและเหมาะสม ไม่ว่าจะอยู่ในรูปแบบหรือสื่อประเภทใดก็ตาม
- 1.3.5. กำหนดพื้นฐานการรักษาความมั่นคงปลอดภัยของข้อมูล
- 1.3.6. ดำเนินการหรือมีการจัดการในเรื่องของการลงทะเบียนข้อมูลสารสนเทศย่างเหมาะสม
- 1.3.7. กำหนดความต้องการในการสำรองข้อมูล
- 1.3.8. ผู้รับผิดชอบสินทรัพย์ซอฟต์แวร์และโปรแกรมประยุกต์ (เจ้าของระบบ)
- 1.3.9. จัดให้มีการตรวจสอบระบบเทคโนโลยีสารสนเทศ ซอฟต์แวร์และโปรแกรมประยุกต์ ให้เป็นไปตามความต้องการใน ปัจจุบันอย่างสม่ำเสมอ
- 1.3.10. จัดให้มีการควบคุมดูแลข้อมูลให้มีความมั่นคงปลอดภัยในการเข้าใช้งาน
- 1.3.11. จัดให้มีการอนุมัติ ตรวจทาน และรับรองสิทธิ์การเข้าใช้ระบบเทคโนโลยีสารสนเทศ ซอฟต์แวร์และโปรแกรมประยุกต์ ที่ เหมาะกับระดับความสำคัญของข้อมูล
- 1.3.12. ระบุความต้องการในการสำรองข้อมูลและรหัสต้นฉบับ (Source Code) ของระบบเทคโนโลยีสารสนเทศ ซอฟต์แวร์และ โปรแกรมประยุกต์
- 1.3.13. จัดให้มีการตรวจสอบยืนยันรหัสต้นฉบับ (Source Code Authentication) เพื่อป้องกันการแก้ไขและความคุ้ม รุน (Version) ของซอฟต์แวร์ เช่น การทำ hashing ด้วยกระบวนการ MD5 หรือ SHA-1 เป็นต้น หรือวิธีการอื่น ได้ที่สามารถ นำมาใช้ยืนยันได้ว่าเป็นรหัสต้นฉบับที่ไม่ถูกเปลี่ยนแปลงแก้ไข
- 1.3.14. จัดให้มีการบริหารจัดการเรื่องสิทธิ์ในการใช้ซอฟต์แวร์ (License Management) อย่างเหมาะสม เพื่อไม่ให้มี เกิดการ ละเมิดลิขสิทธิ์การใช้ซอฟต์แวร์ หากมีการลงทะเบียนลิขสิทธิ์เกิดขึ้น เจ้าของระบบต้องเป็นผู้รับผิดชอบ
- 1.3.15. ดำเนินการหรือมีการจัดการในเรื่องของการลงทะเบียนความมั่นคงปลอดภัยอย่างเหมาะสม
- 1.3.16. สามารถมอบหมายหน้าที่และความรับผิดชอบดังกล่าวข้างต้น ให้แก่บุคคลอื่นที่เหมาะสม แต่เจ้าของระบบ ยังคงมีหน้าที่ และความรับผิดชอบต่อระบบเทคโนโลยีสารสนเทศ ซอฟต์แวร์และโปรแกรมประยุกต์ ดังกล่าวโดย สมบูรณ์

#### การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use of Assets)

- 1.1. จัดทำแนวทางและขั้นตอนปฏิบัติของการอนุญาตให้ใช้ข้อมูลและสินทรัพย์
- 1.2. อนุญาตให้ใช้งานสินทรัพย์ด้านเทคโนโลยีสารสนเทศ ดังนี้
  - 1.2.1. ระบบเทคโนโลยีสารสนเทศ ซอฟต์แวร์ โปรแกรมประยุกต์ และอุปกรณ์เทคโนโลยีสารสนเทศของ MFEC มี

วัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของ MFEC การใช้งานเพื่อกิจธุรส่วนตัวนี้ อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของผู้ใช้งาน และต้องไม่ทำให้เกิดความเสียหายหรือขัดแย้งกับการดำเนินงานและการกิจของ MFEC

- 1.2.2. ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ด้านเทคโนโลยีสารสนเทศที่ได้รับมอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลสินทรัพย์เหล่านี้ให้มีความมั่นคงปลอดภัยและคงความถูกต้อง โดย สินทรัพย์ด้านเทคโนโลยีสารสนเทศ หมายรวมถึง ข้อมูล ระบบเทคโนโลยีสารสนเทศ ซอฟต์แวร์ โปรแกรมประยุกต์ และอุปกรณ์เทคโนโลยีสารสนเทศในกรณีที่สินทรัพย์ด้านเทคโนโลยีสารสนเทศที่ได้รับมอบไว้ให้ใช้งานชำรุดหรือสูญหาย อันเกิดจากความประมาทของผู้ใช้งาน ผู้ใช้งานต้องรับผิดชอบค่าเสียหายตามมูลค่า สินทรัพย์นั้น
- 1.2.3. ผู้ใช้งานต้องรับผิดชอบในการใช้งานอุปกรณ์เทคโนโลยีสารสนเทศของ MFEC อย่างระมัดระวัง
- 1.2.4. ผู้ใช้งานสามารถนำอุปกรณ์เทคโนโลยีสารสนเทศแบบพกพาที่ได้รับมอบไว้ให้ใช้งานออกจากสำนักงาน เพื่อไปใช้งานนอกสถานที่ได้ โดยผู้ใช้งานต้องปฏิบัติตามแนวทางปฏิบัติในการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ส่วนอุปกรณ์ เทคโนโลยีสารสนเทศอื่นๆ ต้องแจ้งคำร้องขอ พร้อมได้รับการอนุมัติจากผู้มีอำนาจก่อน
- 1.2.5. อุปกรณ์เทคโนโลยีสารสนเทศทั้งหมดของ MFEC ต้องได้รับการปกป้องด้วยรหัสผ่านทุกครั้งเมื่อต้องการเข้าใช้งาน และเครื่องคอมพิวเตอร์ทั้งหมดต้องยืนยันตัวตนผู้ใช้ใหญ่ทุกครั้ง เมื่อไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง
- 1.2.6. ผู้ใช้งานต้องไม่เข้ามต่ออุปกรณ์เทคโนโลยีสารสนเทศส่วนตัวเข้าระบบเครือข่ายของ MFEC รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในอุปกรณ์เทคโนโลยีสารสนเทศของ MFEC ก่อนได้รับอนุญาต
- 1.2.7. อุปกรณ์เทคโนโลยีสารสนเทศของ MFEC ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาต จาก MFEC และ การติดตั้งชาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนอุปกรณ์เทคโนโลยีสารสนเทศของ MFEC ต้องกระทำโดยผู้ดูแลระบบที่มีหน้าที่ เกี่ยวข้องเท่านั้น
- 1.2.8. ห้ามติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของ MFEC
- 1.2.9. ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลที่มีขั้นความลับตั้งแต่ “ลับ” ขึ้นไปของ MFEC ห้ามได้มาจากการ พัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงาน เจ้าของระบบหรือเจ้าของข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของ MFEC
- 1.2.10. ระบบเทคโนโลยีสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีคุณสมบัติสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งาน ทั่วไปมีความเข้าใจและสามารถใช้งานระบบได้
- 1.2.11. จัดทำเอกสารรายชื่อซอฟต์แวร์ และระบบเทคโนโลยีสารสนเทศ ที่ถูกติดตั้งในอุปกรณ์เทคโนโลยีสารสนเทศของผู้ใช้งาน และ การติดตั้งต้องได้รับการอนุมัติโดยผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่า ซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้อง ครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของ MFEC เท่านั้น
- 1.2.12. จัดให้มีการควบคุมการเข้า-ออกพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย ดังนี้

- 1.2.12.1. การเข้า-ออกพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย กำหนดให้เข้า-ออกได้เฉพาะบุคคลที่ได้รับสิทธิ์เท่านั้น
- 1.2.12.2. บุคคลอื่นที่ไม่ได้รับสิทธิ์ หากมีความจำเป็นต้องเข้าพื้นที่ให้แจ้งเหตุผล พร้อมขออนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ และต้องให้บุคคลที่ได้รับสิทธิ์ เป็นผู้รับผิดชอบพาเข้าไปและอยู่ด้วยตลอดเวลา
- 1.2.12.3. บันทึกการเข้า-ออกพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย ซึ่งต้องระบุรายละเอียดอย่างน้อย ดังนี้ ชื่อ-นามสกุล ตำแหน่ง หน่วยงาน เวลาเข้า-ออก
- 1.2.12.4. ติดตั้งระบบป้องกันและตรวจสอบการเข้า-ออกพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย เช่น การใช้ระบบชี้ภาพ (Biometric) หรือ สมาร์ทการ์ด (Smartcard) และติดตั้งกล้องโทรทัศน์วงจรปิด เป็นต้น
- 1.2.13. ผู้ใช้งานต้องปฏิบัติตามนโยบาย แนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ คู่มือ คำแนะนำ และเอกสารใดๆ ที่เกี่ยวข้องกับการใช้งานสินทรัพย์ด้านเทคโนโลยีสารสนเทศ อย่างเคร่งครัด

### 3.2 แนวทางปฏิบัติในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

#### วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้อุปกรณ์เทคโนโลยีสารสนเทศ โดยต้องมีการป้องกัน การเข้าถึงอุปกรณ์เทคโนโลยีสารสนเทศ โดยไม่ได้รับอนุญาตจากบุคคลอื่น ในขณะที่ไม่มีผู้ใช้งานอยู่ที่อุปกรณ์ ทั้งนี้เพื่อให้ปลอดภัยทั้งต่อระบบสารสนเทศของ MFEC ข้อมูล และอุปกรณ์ส่วนบุคคลที่นำมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ MFEC ผู้รับผิดชอบ

1. ผู้ดูแลระบบ

2. ผู้ใช้งาน

#### แนวทางปฏิบัติ

- ผู้ใช้งานควรออกจากระบบเทคโนโลยีสารสนเทศของ MFEC โดยทันที เมื่อเสร็จสิ้นการใช้งาน เช่น ออกจากระบบงาน ออก จาก เครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้งาน (Logout)
- ผู้ใช้งานควรล็อก (Lock) อุปกรณ์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลช่วงเวลา เช่น การล็อกหน้าจอด้วยรหัสผ่าน และการล็อกคอมพิวเตอร์แบบพกพาเข้ากับสายล็อกเพื่อป้องกันการถูกขโมยเครื่องเป็นต้น
- ผู้ใช้งานควรป้องกันไม่ให้ผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศ โดยการกำหนดให้ต้องใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์
- ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอ หลังจากที่ไม่ได้ใช้งานมาช่วงระยะเวลาหนึ่งโดยอัตโนมัติ เช่น 15 นาที หลังจากที่ มีการล็อกหน้าจอแล้วนั้น ต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้
- ผู้ใช้งานควรปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือไม่มีการใช้

- งานนานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ซึ่งต้องใช้งานตลอด 24 ชั่วโมง ให้ผู้ดูแลระบบของจากระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายหรือล็อกหน้าจอ
6. ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจในมาตรการป้องกันที่ได้กำหนดไว้

### 3.3 แนวทางปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน

เพื่อให้ระบบสารสนเทศยังคงมีความมั่นคงปลอดภัยเมื่อมีการปฏิบัติงานจากภายนอกสำนักงาน

#### **ผู้รับผิดชอบ**

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### **แนวทางปฏิบัติ**

1. อนุญาตให้ผู้ใช้งานสามารถปฏิบัติงานจากภายนอกสำนักงานได้ 24 ชั่วโมง โดยสามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ผ่านทางช่องทางที่ MFEC กำหนดไว้
2. เมื่อปฏิบัติงานจากภายนอกสำนักงาน ต้องเข้าถึงระบบเทคโนโลยีสารสนเทศตามที่เจ้าของระบบ/เจ้าของข้อมูล กำหนดไว้
3. กำหนดให้ผู้ใช้งานต้องขออนุมัติจากผู้บังคับบัญชา และเจ้าของระบบ ในกรณีที่มีความจำเป็นต้องปฏิบัติงานจากภายนอกสำนักงาน ผ่านทางช่องทางที่ MFEC ไม่ได้กำหนดไว้ ประกอบด้วยรายละเอียดอย่างน้อยดังนี้ ชื่อผู้ใช้งาน เทคโนโลยีในการขอใช้ระยะเวลาในการใช้บริการ
4. กำหนดให้ผู้บังคับบัญชาต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร ในกรณีที่ต้องยกเลิกการปฏิบัติงานจากภายนอก สำนักงานของผู้ใช้งานซึ่งอยู่ภายใต้บังคับบัญชา
5. กำหนดให้ผู้ใช้งานจากภายนอกสำนักงานทุกคนต้องผ่านการพิสูจน์ตัวตน เพื่อให้เกิดความมั่นคงปลอดภัย ด้วยการใช้ชื่อผู้ใช้งาน และรหัสผ่าน เป็นต้น
6. จัดให้มีการป้องกันการเปิดเผยข้อมูล และการเข้าถึงข้อมูลตามที่เจ้าของข้อมูลกำหนด
7. ให้ปฏิบัติต่อข้อมูลที่มีระดับขั้นความลับตามที่ได้มีการกำหนดไว้ในข้อกำหนดในการจัดระดับขั้นความลับของสารสนเทศของ MFEC
8. ห้ามบุคคลที่ไม่เกี่ยวข้องกับการปฏิบัติงาน เช่น เพื่อน ครอบครัว ญาติ ของผู้ใช้งานเข้าถึงระบบสารสนเทศของ MFEC
9. จัดให้มีการบำรุงรักษาและให้บริการสนับสนุนสำหรับซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่ใช้งานจากระยะไกล
10. การเชื่อมต่อระบบที่มีความสำคัญสูงต้องปฏิบัติตามเงื่อนไขของ MFEC เช่น ซอฟต์แวร์ VPN, ซอฟต์แวร์ตรวจสอบความปลอดภัยของอุปกรณ์
11. จัดให้มีการป้องกันทรัพย์สินทางปัญญาที่เกิดขึ้นจากการปฏิบัติงานจากภายนอกสำนักงานอย่างเหมาะสม
12. จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติงานจากระยะไกล ซึ่งรวมถึงอุปกรณ์สำหรับการจัดเก็บข้อมูล และอุปกรณ์สื่อสารอย่างเหมาะสม

13. กำหนดให้การใช้งานอุปกรณ์ที่เป็นส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ MFEC จากระยะไกล ต้องอยู่ภายใต้การควบคุมดูแลของฝ่ายเทคโนโลยีสารสนเทศ
14. กำหนดให้ผู้ใช้งานต้องประเมินความมั่นคงปลอดภัยของสภาพแวดล้อมที่ใช้ปฏิบัติงานจากภายนอกสำนักงานก่อนการปฏิบัติงาน ทุกครั้ง

### 3.4. แนวทางปฏิบัติการป้องกันโคล้มุ่งร้าย

เพื่อให้ระบบสารสนเทศยังคงมีความมั่นคงปลอดภัยเมื่อมีภัยคุกคามจากผู้ไม่ประสงค์ดี

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### แนวทางปฏิบัติ

1. เครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ของบริษัทฯ ต้องมีซอฟต์แวร์ป้องกันไวรัสที่ถูกกฎหมาย พร้อมทั้งปรับปรุงฐานข้อมูลของซอฟต์แวร์ป้องกันไวรัสให้เป็นปัจจุบันอยู่เสมอ
2. เมื่อพบสิ่งผิดปกติในระบบสารสนเทศของบริษัทฯ ให้แจ้งฝ่ายเทคโนโลยีสารสนเทศทราบทันที
3. เครื่องคอมพิวเตอร์ทุกเครื่องที่นำมาเชื่อมต่อกับเครือข่ายบริษัทฯ ต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสด้วยคอมพิวเตอร์ที่มีประสิทธิภาพ และต้องมีการปรับปรุงอัพเดตฐานข้อมูลที่ตรวจสอบโคล้มุ่งร้ายให้เป็นปัจจุบันอยู่เสมอ
4. เครื่องคอมพิวเตอร์ทุกเครื่องที่นำมาเชื่อมต่อกับเครือข่ายบริษัทฯ ต้องมีการติดตั้งไฟร์วอลล์ส่วนบุคคล (Personal Firewall) และมีการอัพเดตสถานะไฟล์ต่างๆของระบบปฏิบัติการ โดยการดำเนินการตั้งกล่าวต่อต้องไม่ส่งผลกระทบต่อระบบงานหลัก
5. ห้ามผู้ใช้งานคอมพิวเตอร์ทำการเชื่อมต่อกับเครือข่ายภายนอกบริษัทฯ ก่อนได้รับอนุญาตจากผู้มีอำนาจ
6. ต้องมีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และควรที่จะมีการสำรองเครื่องคอมพิวเตอร์/อุปกรณ์คอมพิวเตอร์สำหรับระบบงานสำคัญ เพื่อป้องกันปัญหาจากไวรัสด้วย
7. ต้องมีการจัดทำคู่มือในการป้องกันไวรัสด้วยคอมพิวเตอร์เพื่อใช้เป็นแนวทางปฏิบัติให้แก่ผู้ใช้งาน รวมถึงการเผยแพร่ข่าวสารเกี่ยวกับไวรัสด้วยนิติใหม่อยู่เสมอ
8. ผู้ใช้งานเครื่องคอมพิวเตอร์ต้องไม่ทำการติดตั้งโปรแกรมใดๆที่ไม่ทราบแหล่งที่มา หรือไม่ได้มาจากแหล่งที่ทางศูนย์เทคโนโลยีสารสนเทศรับรอง
9. ห้ามพัฒนาโปรแกรมไวรัสด้วยคอมพิวเตอร์ หรือนำโปรแกรมไวรัสด้วยคอมพิวเตอร์หรือไวรัสมาเผยแพร่
10. ต้องมีการเฝ้าระวังระบบเครือข่าย และคอมพิวเตอร์ เพื่อป้องกันปัญหาด้านไวรัสด้วยคอมพิวเตอร์ เมื่อพบเครื่องต้องสงสัยว่าติดไวรัสให้ปฏิบัติตามแนวทางปฏิบัติที่ทางศูนย์เทคโนโลยีสารสนเทศกำหนด
11. ไม่ถอนติดตั้ง (Remove/Uninstall) หรือปิดบริการซอฟต์แวร์ป้องกันไวรัสบนเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

### 3.5 แนวปฏิบัติการจัดการแพตช์

เพื่อให้ระบบ/อุปกรณ์มีการปรับปรุงระบบ/อุปกรณ์ให้มีความปลอดภัย และประสิทธิภาพต่อการดำเนินงาน

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### แนวทางปฏิบัติ

1. ระบบปฏิบัติการ และอุปกรณ์เทคโนโลยีสารสนเทศต้องมีการจัดซื้อให้ถูกต้องตามลิขสิทธิ์ เพื่อให้รองรับต่อการปรับปรุงแพตช์ของเครื่องให้ทันสมัยอยู่เสมอ
2. เครื่องแม่ข่าย และอุปกรณ์สนับสนุนที่มีนัยสำคัญต้องมีการตรวจสอบการลงแพตช์ก่อนการปล่อยเพื่อให้มั่นใจว่าไม่ส่งผลกระทบต่อการทำงานของระบบงานที่เกี่ยวข้อง
3. เครื่องลูกข่าย และอุปกรณ์สนับสนุนต่างๆ ต้องมีการกำหนดค่าปรับปรุงแพตช์ให้ทันสมัยอยู่เสมอ
4. หลีกเลี่ยงการติดตั้งแพตช์จากแหล่งที่มาที่ไม่ได้ชัดเจน
5. กำหนดรอบการติดตามการลงแพตช์ว่ามีความถูกต้องเหมาะสมกับมาตรการที่ระบุอย่างน้อยปีละ 1 ครั้ง

### 3.6 แนวปฏิบัติการบันทึกจัดเก็บล็อก

เพื่อให้ระบบสารสนเทศดำเนินการสอดคล้องกับด้านกฎหมาย และป้องกันไม่ให้ผู้ใช้ที่มีสิทธิพิเศษเข้าถึงระบบโดยที่ไม่ได้มีระบบติดตาม หรือสอบทานการดำเนินการ

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### แนวทางปฏิบัติ

1. การพิจารณากฎหมายที่เกี่ยวข้องกับการบันทึกจัดเก็บล็อก และให้ผู้รับผิดชอบออกแบบระบบงานเพื่อรองรับต่อการดำเนินการด้านกฎหมาย ทั้งระยะเวลาในการจัดเก็บ การกำหนดช่วงเวลาดำเนินการ
2. เครื่องแม่ข่าย และระบบสนับสนุนเครื่องแม่ข่ายที่เข้าใช้ด้วยผู้ใช้สิทธิพิเศษทั้งหมดต้องมีการจัดทำบันทึกกิจกรรมดำเนินการ และจัดเก็บไว้อย่างปลอดภัย
3. การบันทึกจัดเก็บล็อกต้องรองรับการจัดเก็บทั้งระบบปฏิบัติการ และอุปกรณ์สนับสนุนต่อระบบงานของบริษัท
4. ระบบจัดเก็บล็อกต้องรองรับต่อการป้องกันการแก้ไขจากผู้ดูแลระบบหรือผู้เกี่ยวข้อง โดยมีการดำเนินการแยกเครื่องที่จัดเก็บจากเครื่องที่บริหารงาน
5. การบันทึกจัดเก็บล็อกต้องรองรับต่อการนำมาใช้ประกอบกับหลักฐานในการสืบสวนของผู้ที่ใช้ระบบสารสนเทศที่ไม่เหมาะสม ทั้งภายใน และภายนอกองค์กร
6. ระบบจัดเก็บล็อกต้องมีการจัดเตรียมระบบการเข้าถึงข้อมูลเพื่อวิเคราะห์ และนำล็อกมาดำเนินการเพื่อจัดทำรายงาน หรือ

จัดเตรียมส่งให้กับหน่วยงานที่ร้องขอได้อย่างรวดเร็ว ถูกต้อง และง่ายต่อการใช้งาน

7. ต้องมั่นใจว่าระบบจัดส่งล็อกมีความปลอดภัยป้องกันการเข้าถึง หรือแก้ไขจากบุคคลที่ไม่เกี่ยวข้อง  
กำหนดครอบครองตรวจสอบล็อกกว่ามีความพร้อมใช้ สิทธิ์เหมาะสม และเข้าถึงได้หรือไม่อย่างน้อยปีละครั้ง

### 3.7 แนวทางปฏิบัติการเฝ้าดูความพร้อมใช้อุปกรณ์/ระบบ

การเฝ้าดูความพร้อมใช้อุปกรณ์/ระบบมีความจำเป็นอย่างยิ่งเพื่อให้ผู้ดูแลสามารถทราบปัญหา หรือเหตุขัดข้องก่อนที่ผู้ใช้งานระบบสารสนเทศจะแจ้งเข้ามา

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### แนวทางปฏิบัติ

1. กำหนดผู้รับผิดชอบด้านความพร้อมใช้ของระบบ/อุปกรณ์
2. ประเมินความพร้อมใช้งานประสิทธิภาพและความสามารถในการให้บริการและทรัพยากรเพื่อให้มั่นใจว่ามีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจ
3. ระบุบริการที่สำคัญสำหรับองค์กร จัดทำแผนที่บริการและทรัพยากรไปยังกระบวนการทางธุรกิจและระบุอุปกรณ์/ระบบที่สนับสนุนทางธุรกิจ ตรวจสอบให้แน่ใจว่าลูกค้าได้รับผลกระทบจากทรัพยากรที่ไม่พร้อมใช้งานอย่างสมบูรณ์ สำหรับฟังก์ชันธุรกิจที่สำคัญตรวจสอบให้แน่ใจว่าข้อกำหนดความพร้อมใช้งานนั้นเป็นไปตามข้อตกลงระดับการให้บริการ (SLA)
4. วางแผนและจัดลำดับความสำคัญด้านความพร้อมใช้งานประสิทธิภาพของการเปลี่ยนแปลงความต้องการทางธุรกิจและข้อกำหนดในการให้บริการ
5. ตรวจสอบวัดวิเคราะห์รายงานและตรวจสอบความพร้อมใช้งานประสิทธิภาพ ระบุการเบี่ยงเบนจากเส้นเขตแดนที่จัดตั้งขึ้น ตรวจสอบรายงานการวิเคราะห์แนวโน้มระบุปัญหาที่สำคัญและผลต่าง เริ่มต้นการดำเนินการตามความจำเป็นและสร้างความมั่นใจว่ามีการแก้ไขปัญหาที่ค้างอยู่ทั้งหมด
6. แก้ไขความเบี่ยงเบนโดยการตรวจสอบและแก้ไขปัญหาความพร้อมใช้งานประสิทธิภาพที่ระบุ

### 3.8 แนวทางปฏิบัติการเฝ้าดูประสิทธิภาพอุปกรณ์/ระบบ

ระบบเทคโนโลยีสารสนเทศจำเป็นต้องมีการเฝ้าดูกิจกรรม และการใช้ระบบเพื่อประเมินความพึงพอใจของการดำเนินการเพื่อนำไปสู่การเปลี่ยนแปลงระบบให้เกิดความพร้อมใช้อย่างต่อเนื่องสอดคล้องข้อตกลงในการให้บริการกับความต้องการของผู้มีส่วนได้ส่วนเสีย และธุรกิจ

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### แนวทางปฏิบัติ

1. กำหนดผู้รับผิดชอบในการเฝ้าดูชี้ด้วยความสามารถของระบบ/อุปกรณ์

2. ประเมินขีดความสามารถและประสิทธิภาพว่าคุ้มค่าใช้จ่ายเพื่อรองรับความต้องการทางธุรกิจและส่งมอบตามข้อตกลงระดับบริการ (SLA) พร้อมสร้างพื้นฐานขีดความสามารถสำหรับการเบรียบเทียบในอนาคต
3. ระบุบริการที่สำคัญสำหรับองค์กร จัดทำแผนที่บริการและทรัพยากรไปยังกระบวนการทางธุรกิจและระบบงานสารสนเทศที่สนับสนุนกับทางธุรกิจเพื่อนำมาสร้างข้อกำหนดขีดความสามารถ และค่าฝ่าคูขั้นต่ำ (Threshold) ให้เป็นไปตามข้อตกลงระดับการให้บริการ (SLA)
4. วางแผนและจัดลำดับความสำคัญด้านขีดความสามารถของระบบ/อุปกรณ์ เพื่อพิจารณาภัยการเปลี่ยนแปลงความต้องการทางธุรกิจและข้อกำหนดในการให้บริการ
5. ตรวจสอบวัดวิเคราะห์รายงานและตรวจสอบขีดความสามารถ ระบุการเบี่ยงเบนจากเส้นเขตแดนที่จัดตั้งขึ้น ตรวจสอบรายงานการวิเคราะห์แนวโน้มระบุปัญหาที่สำคัญและผลต่าง เริ่มต้นการดำเนินการตามความจำเป็นและสร้างความมั่นใจว่ามีการแก้ไขปัญหาที่ค้างอยู่ทั้งหมด
6. แก้ไขความเบี่ยงเบนโดยการตรวจสอบและแก้ไขปัญหาขีดความสามารถในการใช้งานที่ระบุ

### 3.9 แนวปฏิบัติการค้นหาช่องโหว่ของอุปกรณ์/ระบบ

ระบบ/อุปกรณ์เทคโนโลยีสารสนเทศจะมีการรายงานช่องโหว่ในแต่ละวัน ซึ่งเพื่อหลีกเลี่ยงจากช่องโหว่ที่ถูกค้นพบ และประกาศสู่สาธารณะบริษัทจำเป็นต้องกำหนดครอบครองตรวจสอบในแต่ละปี เพื่อดำเนินการอุดช่องโหว่ที่ค้นพบ

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### แนวทางปฏิบัติ

1. กำหนดผู้รับผิดชอบในการดำเนินการค้นหาช่องโหว่
2. กำหนดเกณฑ์ดำเนินการในการค้นหาช่องโหว่ และขอบเขตดำเนินการเพื่อประสิทธิภาพในการทำงาน และบริหารทรัพยากรให้ได้อย่างมีประสิทธิภาพ
3. การใช้เครื่องมือค้นหาช่องโหว่ของระบบให้มีการควบคุมระยะเวลา และบุคคลที่ใช้ ไม่อนุญาตให้ติดตั้ง หรือใช้งานโดยไม่ได้รับการอนุมัติ
4. เครื่องมือที่ใช้ในการค้นหาช่องโหว่ต้องมีการพิจารณา และตรวจสอบแหล่งที่มา และความเหมาะสมในการดำเนินการ
5. การค้นหาช่องโหว่จะต้องดำเนินการจัดทำบันทึกแจ้งเวียนวันเวลาที่ดำเนินการเพื่อหลีกเลี่ยงผลกระทบต่อการใช้งาน
6. จัดทำการสื่อสาร เพื่อให้พนักงานตระหนักรถoration แจ้งเตือนช่องโหว่ทางเทคนิคที่จะเกิดขึ้นได้
7. กรณีที่พบช่องโหว่ และดำเนินการแก้ไขหรืออุดช่องโหว่ให้พิจารณากระบวนการดำเนินการบันทึกการเปลี่ยนแปลงเทคโนโลยีสารสนเทศด้วย
8. ในการรับมือต่อเหตุการณ์ด้านความปลอดภัยข้อมูลสารสนเทศ เช่นการปิดบริการ หรือพอร์ตที่เกี่ยวข้อง หรือการปรับเพิ่มช่องทางการติดต่อ หรือบริการที่ให้ผ่านในไฟร์วอลล์ ให้มีการวิเคราะห์ระดับความเสี่ยงเพื่อหลีกเลี่ยงต่อความเสียหาย

หรือช่องโหว่ที่เกิดขึ้น

9. กำหนดครอบการดำเนินการตรวจสอบช่องโหว่ทางเทคนิคอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

### 3.10 แนวทางปฏิบัติการรับเหตุขัดข้อง

ระบบเทคโนโลยีสารสนเทศจำเป็นต้องมีการรับเหตุขัดข้อง เพื่อดำเนินการนำระบบกลับคืนมาได้อย่างรวดเร็ว ลดผลกระทบต่อธุรกิจ และจัดเก็บการแจ้งเหตุเพื่อนำมาวิเคราะห์ต้นเหตุของปัญหาเพื่อแก้ไขเหตุขัดข้องไม่ให้เกิดขึ้นอีก

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### แนวทางปฏิบัติผู้ใช้งาน

1. รายงานเหตุขัดข้องให้กับเจ้าหน้าที่ที่เกี่ยวข้องทราบเมื่อพบเหตุขัดข้องทันทีที่พบ
2. เหตุขัดข้อง หรือช่องโหว่ของระบบต้องไม่แจ้งให้กับบุคลภายนอกทราบ นอกเสียจากเป็นตัวแทนของบริษัทฯในการติดต่อสื่อสารกับกลุ่มงานภายนอกในระบบที่รับผิดชอบอยู่

#### แนวทางปฏิบัติผู้ดูแลเหตุขัดข้อง

1. กำหนดผู้รับผิดชอบในเหตุขัดข้องแต่ละประเภทอย่างชัดเจน
2. กำหนดขั้นตอนในการรับมือเหตุการณ์ต่างๆ โดยมีการตรวจสอบ และวิเคราะห์ทุกที่ไม่เกี่ยวข้องเข้ามาใช้งานระบบ
3. จัดทำบันทึกเหตุขัดข้องประกอบด้วยรายละเอียดไม่น้อยกว่า ประเภทเหตุการณ์, วันเวลา, สถานที่, ผลกระทบ, ความเร่งด่วน, ลำดับความสำคัญ, บุคคลที่ติดต่อ (คนที่แจ้ง)
4. มีการเลือกยุทธวิธีที่เหมาะสมกับสถานการณ์ต่างๆที่เกิดขึ้นทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้โจมตี เพื่อยุติปัญหาที่เกิดขึ้นได้อย่างทันเวลา และถูกต้อง
5. เหตุขัดข้องที่พบข้ามเกิดกว่าเกณฑ์ที่ระบุให้ดำเนินการค้นหาสาเหตุเพื่อยุติเหตุขัดข้องนั้นไม่ให้เกิดขึ้นอีก
6. ต้องมีการกำหนดขั้นตอนปฏิบัติการกู้คืนระบบงานต่างๆ
7. ระบบงานต่างๆที่มีความสำคัญต้องมีการเตรียมอุปกรณ์ และเครื่องมือสำหรับการสำรองเพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

#### 4. นโยบายย่อความปลอดภัยในการสื่อสาร (Communication Security)

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

##### **วัตถุประสงค์ของความปลอดภัยในการสื่อสาร**

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคลาภายนอก ที่ปฏิบัติงานให้กับ MFEC ทราบถึงกิจกรรมที่จำเป็นในการดำเนินการกับการสื่อสารสารสนเทศ
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นใจในการดำเนินการกับการแลกเปลี่ยนข้อมูลสารสนเทศในเชิงการป้องกัน
3. เพื่อให้ผู้ใช้งานระบบสารสนเทศมีความมั่นใจในการติดต่อข้อมูลสารสนเทศภายในระบบสื่อสารทั้งภายใน และภายนอก องค์กร

##### **แนวทาง**

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติต้านการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เป็นลายลักษณ์ อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งาน ข้อมูลและระบบสารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

##### **ขอบเขตของนโยบายย่อความปลอดภัยในการสื่อสาร**

ขอบเขตของนโยบายย่อความปลอดภัยในการสื่อสาร หมายถึงการกำหนดแนวทางปฏิบัติต่อการดำเนินงานต่างๆ ที่จำเป็น เพื่อสร้างความมั่นใจในการใช้งานข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศ

##### **บทบาทและหน้าที่**

Chief Operating Officer (COO) ทำหน้าที่กำกับดูแลให้เป็นไปตามนโยบายและแนวทางปฏิบัติการสื่อสารข้อมูลสารสนเทศอย่างปลอดภัย

ผู้บริหาร/ผู้บังคับบัญชา เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ที่เกี่ยวข้องภายใต้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการสื่อสารข้อมูลสารสนเทศอย่างปลอดภัย

ฝ่ายอำนวยการ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เพยแพร) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการสื่อสารข้อมูลสารสนเทศอย่างปลอดภัย

ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เพยแพร) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการสื่อสารข้อมูลสารสนเทศอย่างปลอดภัย

เจ้าหน้าที่สารสนเทศ/ผู้ใช้งาน ต้องปฏิบัติตามนโยบายความปลอดภัยในการสื่อสาร รวมทั้งข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้อง

## ระยะเวลาทบทวน

เพื่อให้นโยบายการเข้าถึงสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง MFEC จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนการปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลง กระบวนการทำงาน วิธีการเข้าถึงสารสนเทศที่สำคัญที่กระทบกับนโยบายนี้

### 4.1 แนวทางปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

#### วัตถุประสงค์

เพื่อเป็นแนวทางปฏิบัติให้กับผู้ดูแลระบบ ซึ่งปฏิบัติงานกับระบบคอมพิวเตอร์ และอุปกรณ์เครือข่าย ได้ดำเนินการป้องกันความมั่นคงปลอดภัยของพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบคอมพิวเตอร์ และอุปกรณ์เครือข่ายที่ให้บริการใน MFEC ผู้รับผิดชอบ

#### ผู้ดูแลระบบ

#### นิยาม

1. “พอร์ต” (Port) ในความหมายของ Physical Port หมายถึง ช่องสำหรับต่อเข้ากับอุปกรณ์ หน่วยรับเข้า หน่วยแสดงผล รวมทั้งอุปกรณ์สนับสนุน ในเครื่องคอมพิวเตอร์มีพอร์ตหลายชนิด ซึ่งมีความเร็วในการรับส่งข้อมูลต่างกันตามลักษณะการใช้งาน
2. “พอร์ต” (Port) ในความหมายของ Logical Port หมายถึง หมายเลขที่กำหนดขึ้นเป็นมาตรฐานโดย Internet Assigned Numbers Authority (IANA) ที่เป็นหน่วยงานกลางในการประสานการเลือกใช้หมายเลขพอร์ต ว่าหมายเลขใดควรหมายความสำหรับ บริการใด ของแอ��แพลิเคชันที่มีการติดต่อหรือมีการส่งข้อมูล

#### แนวทางปฏิบัติ

1. ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งการเข้าถึงทางกายภาพ และเข้าถึงการควบคุมพอร์ต ผ่านทางระบบเครือข่าย เช่น การยืนยันตัวตนก่อนการเข้าปฏิบัติงาน
2. ควบคุมสถานที่ติดตั้งอุปกรณ์เครือข่ายที่เป็นช่องทางที่สามารถใช้สำหรับการปรับแต่งการกำหนดค่าการทำงานของระบบเครือข่าย เพื่อป้องกันการเข้าถึงทางกายภาพด้วยการต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต
3. ยกเลิกหรือปิดหมายเลขพอร์ตที่ไม่มีความจำเป็นในการใช้งาน บนอุปกรณ์ที่ติดตั้งอยู่ร่วมกับระบบเครือข่าย รวมถึงมีการตรวจสอบ และปิดช่องทางเข้าถึงพอร์ตทางกายภาพ ของระบบหรืออุปกรณ์อย่างสม่ำเสมอ เช่น มีการตรวจสอบอย่างน้อยเดือนละ 1 ครั้ง สำหรับระบบที่มีผลกระทบและมีความสำคัญสูงต่อองค์กร และอย่างน้อยไตรมาสละ 1 ครั้งสำหรับระบบทั่วไป
4. ต้องเปลี่ยนรหัสผ่านเริมต้นที่ติดมากับระบบ (Default Password) โดยทันที
5. ติดตั้งอุปกรณ์ป้องกันพอร์ต เพื่อป้องกันการบุกรุกโดยผู้ไม่ประสงค์ดี หรือใช้งานผิดวัตถุประสงค์ของการบริการได้ฯ

6. กำหนดให้มีการเปิด - ปิดช่องทางติดต่อสื่อสารของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงของอุปกรณ์เครือข่ายต่างๆ โดยปิด ช่องทางติดต่อสื่อสารที่มีความเสี่ยง ไม่ปลอดภัย หรืออาจก่อให้เกิดความเสียหายต่อระบบเครือข่าย
7. กำหนดสิทธิบุคคล ในการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ โดยให้เฉพาะบุคคลที่ปฏิบัติหน้าที่ เกี่ยวข้องเท่านั้น หากมีความจำเป็นต้องเข้า ต้องให้ผู้ดูแลระบบเป็นผู้รับผิดชอบนำพาเข้าไป และต้องมีผู้ดูแลระบบอยู่กับบุคคลนั้น ตลอดเวลา
8. กำหนดให้บุคคลภายนอกที่เข้าดำเนินการบำรุงรักษา บริหารจัดการช่องทางติดต่อสื่อสารของอุปกรณ์เครือข่าย หรือ บริหารจัดการ ผ่านระบบเครือข่าย ต้องแจ้งให้ผู้ดูแลระบบรับทราบก่อนทุกครั้ง
9. ติดตั้งระบบป้องกันและตรวจสอบการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์อย่างปลอดภัย เช่น การใช้ ระบบชี้ภาพ (Biometric) หรือ สมาร์ตการ์ด(Smartcard) และติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรมรรภ เป็นต้น
10. กำหนดบุคคลรับผิดชอบในการกำหนดค่า แก้ไข หรือเปลี่ยนแปลงค่าการทำงานต่างๆ ของระบบเครือข่าย และอุปกรณ์ ต่างๆ ที่ เขื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และทบทวนการกำหนดค่าการทำงานต่างๆ อย่างน้อยปีละ 1 ครั้ง นอกจากนี้ การ กำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

## 4.2 แนวทางปฏิบัติในการควบคุมการเขื่อมต่อทางเครือข่าย

### วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของการเขื่อมต่อทางเครือข่าย ควบคุมการเขื่อมต่อทางเครือข่าย และ ป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ของ MFEC

### ผู้รับผิดชอบ

ผู้ดูแลระบบ

### แนวทางปฏิบัติ

1. ต้องทำการติดตั้งซอฟต์แวร์หรือฮาร์ดแวร์สำหรับป้องกันการบุกรุก ซึ่งมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี รวมถึง มีการตรวจสอบและจัดทำรายงานทุก ๆ สามเดือน
2. ต้องทำการป้องกันเลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายมิให้หน่วยงานภายนอกสามารถมองเห็นและเขื่อมต่อ ได้ โดยตรง
3. ต้องทำการติดตั้งซอฟต์แวร์หรือฮาร์ดแวร์ที่สามารถบันทึกการทำงานของระบบเครือข่าย การปฏิบัติงานของผู้ใช้งาน การบุก รุก การเข้าอุปกรณ์ การใช้งานและข้อมูลจากรคอมพิวเตอร์ และต้องมีการจัดเก็บข้อมูลเหล่านี้ไว้ไม่ต่ำกว่า 90 วัน รวมถึง มีการ ตรวจสอบและจัดทำรายงานทุก ๆ สามเดือน
4. ต้องทำการควบคุมและจำกัดสิทธิ์การเขื่อมต่อทางระบบเครือข่ายของผู้ใช้งานต่อระบบงานและการโอนย้ายไฟล์ ดังนี้
  - 4.1. ต้องมีการลงทะเบียนผู้ใช้งานเพื่อระบุตัวตนในการเข้าใช้งานระบบ

- 4.2. ต้องมีการจำกัดสิทธิ์ให้เข้าใช้งานได้เฉพาะระบบงานที่ได้รับอนุญาตเท่านั้น
- 4.3. ต้องมีการจำกัดสิทธิ์ให้สามารถโอนย้ายไฟล์ได้เฉพาะไฟล์ที่รับอนุญาตเท่านั้น
5. ต้องทำการควบคุมบุคคลหรือหน่วยงานภายนอกที่ทำการเข้าใช้หรือเชื่อมต่อกับระบบเครือข่ายของ MFEC ดังนี้
  - 5.1. บุคคลหรือหน่วยงานภายนอกที่ต้องการเชื่อมต่อกับระบบเครือข่ายของ MFEC ต้องมีการร้องขอเข้าใช้งาน พร้อมระบุเหตุผลใน การเข้าใช้งาน
  - 5.2. การร้องขอเข้าใช้งานต้องได้รับอนุญาตจากผู้บริหารที่มีอำนาจของฝ่ายเทคโนโลยีสารสนเทศ
  - 5.3. ต้องมีการควบคุมช่องทาง (Port) ที่เข้ามาใช้งานอย่างรอบคอบด้วย
  - 5.4. ต้องมีการกำหนดระยะเวลาในการเชื่อมต่อและต้องทำการปิดการเชื่อมต่อทันทีที่สิ่งกำหนดเวลา
  - 5.5. ต้องมีการจำกัดเส้นทางในการเชื่อมต่อรวมถึงควบคุมของฟอร์варดหรืออาร์ดแวร์ที่นำมาใช้
  - 5.6. ในการเชื่อมต่อให้เป็นไปตามที่ฝ่าย เทคโนโลยีสารสนเทศ กำหนดไว้เท่านั้น
6. ต้องทำการควบคุมการเชื่อมต่ออินเตอร์เน็ตและระบบงานต่าง ๆ ดังนี้
  - 6.1. ต้องจัดให้มีการลงทะเบียนเพื่อระบุตัวตนในการเข้าใช้งาน
  - 6.2. การลงทะเบียนต้องทำเฉพาะบุคคลเท่านั้น โดยห้ามกระทำการโอนสิทธินี้แก่ผู้อื่น
  - 6.3. ต้องมีการจำกัดสิทธิ์เพื่อควบคุมผู้ใช้งานให้สามารถเข้าใช้งานได้เฉพาะระบบเครือข่ายและระบบงานที่ได้รับอนุญาตเท่านั้น
  - 6.4. ต้องมีการตรวจสอบและทบทวนสิทธิ์อย่างสม่ำเสมอ

### 4.3 แนวทางปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

#### วัตถุประสงค์

เพื่อเป็นแนวทางปฏิบัติที่ใช้ในการเชื่อมโยงเครือข่ายหลายรายเครือข่ายเข้าด้วยกัน หรือเชื่อมโยงอุปกรณ์หลายอย่างเข้าด้วยกัน เป็นส่วนหนึ่งที่ทำให้อุปกรณ์เครือข่ายทั้งหลายสามารถใช้แบบเดียวกันในการสื่อสารรับส่งข้อมูลได้มีประสิทธิภาพ ทำงานถูกต้องแม่นยำ และมีความมั่นคงปลอดภัย

#### ผู้รับผิดชอบ

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

#### แนวทางปฏิบัติ

1. ใช้อุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์เครือข่ายคอมพิวเตอร์เพื่อตรวจสอบเลขที่อยู่ไอพี (IP Address) ของทั้งต้นทางและปลายทาง ทำให้เครือข่ายที่แตกต่างกันสามารถสื่อสารกันได้ และควบคุมการถ่ายโอนของข้อมูลผ่านเครือข่ายต่างๆ จากเครือข่าย หนึ่งไปสู่อีกเครือข่ายหนึ่ง
2. ควบคุมไม่ให้มีการเปิดเผยแผนการใช้งานเลขที่อยู่ไอพี

3. กำหนดให้มีการแบ่งเลขที่อยู่ไอพีและชื่อโดเมน เพื่อแยกเครือข่ายย่อย หรือแยกเครือข่ายภายในและภายนอก
4. จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์เครื่องหนึ่งเครื่องใด ไปยังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่าย โดยไม่ อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น
5. กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเข้ามาย้ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการ เข้าใช้บริการระบบเครือข่ายตามสิทธิ์ที่ได้รับ
6. “ไม่อนุญาตให้บุคคลใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใดๆ ต่ออุปกรณ์เครือข่ายส่วนกลาง” ได้แก่ อุปกรณ์จัด เส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เข้ามต่อ กับระบบเครือข่าย โดยไม่ได้รับอนุญาตจาก ผู้ดูแลระบบ (System Administrator)
7. “ไม่อนุญาตผู้ใช้งานทำการเปลี่ยนแปลงเลขที่อยู่ไอพี หรือกำหนดค่าเลขที่อยู่ไอพีของเครื่องคอมพิวเตอร์ภายในหน่วยงาน โดย ไม่ได้ รับอนุญาตจากผู้ดูแลระบบ
8. ต้องดำเนินการใดๆ เพื่อยุติการกระทำของผู้ใช้งานที่ไม่เป็นไปตามแนวทางปฏิบัตินี้ และในกรณีที่จำเป็นให้ระงับการใช้ระบบ เครือข่าย ของผู้ใช้งานดังกล่าว เพื่อป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นแก่ MFEC

#### แนวทางปฏิบัติสำหรับผู้ดูแลระบบ

1. ดูแลรักษาและปรับปรุงระบบควบคุมการจัดเส้นทางบนเครือข่ายให้สามารถใช้งานได้ดีอยู่เสมอ
2. ดูแลการใช้งานระบบควบคุมการจัดเส้นทางบนเครือข่าย ให้เป็นไปตามแนวทางนี้ กรณีที่พบว่ามีการกระทำหรือการใช้งานที่ ไม่ ถูกต้องให้รายงานต่อผู้บังคับบัญชาทราบโดยเร็ว และหากมีความจำเป็นเพื่อป้องกันความเสียหาย หรือ ผลกระทบที่อาจ เกิดขึ้นต่อ ผู้อื่นหรือต่อการใช้งานระบบสารสนเทศโดยส่วนรวม ให้ผู้ดูแลระบบระงับการใช้งานดังกล่าว
3. ต้องจัดทำบัญชีอุปกรณ์เครือข่าย บัญชีเครื่องคอมพิวเตอร์แม่ข่าย ที่ระบุถึงการเข้ามายิง การจัดสรรหมายเลขที่อยู่ไอพี และผู้ มีสิทธิ์ ใช้งาน พร้อมปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ
4. ทบทวนและตรวจสอบเส้นทางบนเครือข่ายให้เป็นไปตามที่กำหนดอย่างน้อยปีละ 1 ครั้งและปรับปรุงแก้ไขหรือยกเลิก เส้นทางที่ไม่มีความจำเป็นต้องใช้งาน

อุปกรณ์จัดเส้นทาง (Router) หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทาง เพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น โดยจะอ่านที่อยู่ของอุปกรณ์ปลายทาง ทำการจัดเส้นทางที่ต้องสุด สงข้อมูลไปยังเครือข่ายที่ แตกต่างกันได้หรือเข้ามต่อ กับเครือข่ายอื่นได้ เช่น เครือข่ายอินเทอร์เน็ต

เลขที่อยู่ไอพี (IP Address) หมายถึง ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต้องอยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่อง จะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของ ตัวเลข 4 ส่วนหรือ 6 ส่วน ที่คั่น ด้วยเครื่องหมายจุด (.)

อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ ที่ทำหน้าที่รับ-ส่งข้อมูล โดย จะลดปัญหาการชนกันของข้อมูล เพราะไม่ต้องกระจายข้อมูลไปทุกช่องทางที่เข้ามต่ออยู่ และป้องกันการตั้งรับข้อมูลที่กระจายไป ในเครือข่าย

#### 4.4 แนวทางปฏิบัติในการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

##### **วัตถุประสงค์**

1. เพื่อสนับสนุนนโยบายการปฏิบัติงานได้ในทุกสถานที่ MFEC ได้นำอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่มาใช้งาน ร่วมกับ การนำ เทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้กับการปฏิบัติงาน โดยการใช้เครื่องคอมพิวเตอร์และสื่อสาร เคลื่อนที่เป็น เครื่องมือ ทั้งแบบอฟไลน์และออนไลน์ จึงมีความจำเป็นที่ต้องมีการบริหารจัดการควบคุมและกำหนดสิทธิ์การ ใช้งานเครื่อง คอมพิวเตอร์และสื่อสารเคลื่อนที่
2. เพื่อควบคุม ดูแล กำหนดสิทธิ์การเข้าใช้งาน ลดความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่เกิดจากการใช้งานอุปกรณ์
3. เพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่ และความรับผิดชอบในการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และ ปฏิบัติตาม อย่างเคร่งครัด
4. เพื่อลดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ MFEC จากการใช้งานอุปกรณ์คอมพิวเตอร์และ สื่อสารเคลื่อนที่

##### **ผู้รับผิดชอบ**

1. ผู้ดูแลระบบ
2. ผู้ใช้งาน

##### **นิยาม**

“อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่มีหน่วยประมวลผล หน่วยความจำ หรือมี หน่วยเชื่อมต่อกับ อุปกรณ์อื่นๆ เช่น คอมพิวเตอร์ โน๊ตบุ๊คหรือแล็ปท็อป โทรศัพท์มือถือ สมาร์ตโฟน แท็บเล็ต เป็นต้น

##### **แนวทางปฏิบัติ**

1. กำหนดให้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ที่ MFEC อนุญาตให้บุคคลใดนำไปใช้งาน เป็นทรัพย์สินของ MFEC ดังนั้น ผู้ใช้งาน ต้องใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของ MFEC
2. จัดให้มีการวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อนำมา ทบทวนและ ปรับปรุงการใช้งาน
3. จัดให้มีระบบควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อบริหารจัดการและควบคุมการใช้งานที่ส่วนกลางและ บริหาร จัดการการควบคุม กำหนดสิทธิ์การใช้งาน จัดการกับข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ผ่าน เครือข่าย อินเทอร์เน็ต ตลอดจนสามารถติดตามตำแหน่งของอุปกรณ์เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ ที่อาจสูญหายได้
4. จัดให้มีมาตรการในการตรวจจับและป้องกันโปรแกรมไม่พึงประสงค์ต่างๆ (Anti-malware)
5. จัดให้มีมาตรการเพื่อสร้างความตระหนักรักษาความมั่นคงทางไซเบอร์ ป้องกันการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เช่น การใช้งานในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเข้ามายังเครือข่ายสาธารณะภายนอก MFEC เป็นต้น
6. ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัส

## ข้อมูล

7. "ไม่อนุญาตให้บุคคลอื่น หรือบุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่"
8. "จัดให้มีการสำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ อย่างสม่ำเสมอ"
9. ควบคุมการเข้าถึงระบบงานของ MFEC จากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ซึ่งเชื่อมต่อผ่านทาง เครือข่ายอินเทอร์เน็ตสาธารณะ โดยให้ปฏิบัติตามแนวทางปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน
10. ควบคุมการติดตั้งซอฟต์แวร์หรือโปรแกรมประยุกต์ ในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่โดยให้ปฏิบัติตามแนวทางปฏิบัติ ในการเข้าถึงระบบปฏิบัติการ

## แนวทางปฏิบัติสำหรับผู้ดูแลระบบ

1. ดูแลรักษาและปรับปรุงอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ของ MFEC ให้สามารถใช้งานได้อยู่เสมอ
2. ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้เป็นไปตามแนวทางปฏิบัตินี้ กรณีที่พบว่า มีการกระทำหรือการใช้งานที่ไม่ถูกต้อง ให้รายงานต่อผู้ดูแลบัญชาทราบโดยเร็ว และหากมีความจำเป็นเพื่อป้องกันความเสียหาย หรือผลกระทบที่อาจเกิดขึ้น ต่อผู้อื่น หรือผลกระทบต่อการใช้งานระบบเทคโนโลยีสารสนเทศโดยส่วนรวม ให้ผู้ดูแลระบบปรับเปลี่ยนการใช้งานอุปกรณ์คอมพิวเตอร์และ สื่อสารเคลื่อนที่ังกกล่าวไว้
3. ต้องเก็บรักษาความลับของข้อมูลอันเนื่องมาจากการปฏิบัติหน้าที่
4. ต้องไม่ใช้ชื่อเจ้าหน้าที่ในการเข้าถึงข้อมูลใดที่ตนไม่มีสิทธิเข้าถึง นอกเหนืองานในหน้าที่

## 5.นโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

เนื่องจาก MFEC Public Company Limited (MFEC) ได้กำหนดแนวทางการป้องกันและเตรียมความพร้อมในการจัดการเมื่ออยู่ในภาวะวิกฤติ โดยต้องดำเนินการให้ MFEC ดำเนินภารกิจได้อย่างต่อเนื่อง จึงได้กำหนดให้มีนโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ เพื่อการตอบสนองและบรรเทาผลกระทบต่อกระบวนการการทำงานสำคัญที่มีการพึ่งพาระบบเทคโนโลยีสารสนเทศให้สามารถทำงานได้อย่างต่อเนื่องในระดับที่ได้มีการตกลงกันไว้กับผู้มีส่วนได้ส่วนเสีย วัตถุประสงค์ของการบริหารจัดการความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

1. เพื่อให้มีการวิเคราะห์ วางแผน เตรียมการ ทบทวนและซักซ้อมกระบวนการต่างๆ ที่จำเป็น
2. เพื่อให้สามารถใช้งานระบบสารสนเทศได้อย่างต่อเนื่องในระดับที่ได้มีการตกลงกันไว้ในภาวะฉุกเฉิน
3. เพื่อให้ผู้มีส่วนได้ส่วนเสียได้เกิดความเข้าใจร่วมกัน และทราบถึงบทบาทหน้าที่ในการมีส่วนร่วมเมื่อเกิดเหตุฉุกเฉิน หรือ อุบัติภัย

## แนวทาง

การบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ หมายถึง การจัดเตรียมกระบวนการหรือระบบสำรอง เพื่อให้สามารถใช้งานทดแทนเมื่อระบบหลักเกิดการหยุดชะงักในภาวะฉุกเฉิน ในระดับที่ได้มีการตกลงกันไว้แล้ว ให้เป็นไปตามเงื่อนไขที่ได้มีการพิจารณา ผลกระทบทางธุรกิจ (BIA : Business Impact Analysis) ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (MTPD :

Maximum Tolerable Period of Disruption) ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (RTO : Recovery Time Objective) เป้าหมายของการฟื้นคืนสภาพ (RPO : Recovery Point Objective) และทำการฟื้นฟูระบบหลักให้กลับคืนสู่สภาวะปกติได้

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

1. จัดให้มีคณะกรรมการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ที่สอดคล้องตามแนวทางการบริหารความต่อเนื่องในการดำเนินงานของ MFEC โดยมีการวางแผน การนำไปปฏิบัติ การฝึกซ้อม และการปรับปรุงแก้ไขอย่างต่อเนื่อง
2. จัดให้มีการทำางานร่วมกับคณะกรรมการบริหารความเสี่ยง และคณะกรรมการควบคุมภัย ในที่มีหน้าที่กำกับดูแลการพัฒนาระบบการบริหารความต่อเนื่องในการดำเนินงานของ MFEC ในภาพรวม
3. จัดให้มีการทำางานร่วมกับส่วนงานที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัย โดยประสานความเขื่อมโยงกันของแต่ละขอบข่าย ที่พัฒนาระบบสารสนเทศ ในการจัดทำแผนป้องกัน / ระงับเหตุฉุกเฉิน รวมทั้งร่วมเป็นคณะกรรมการในโครงสร้างศูนย์อำนวยการเหตุฉุกเฉิน และภาวะวิกฤต
4. จัดให้มีการพัฒนาระบบการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ตามขอบข่ายที่รับผิดชอบ โดยมีการวางแผน การนำไปปฏิบัติ การฝึกซ้อม และปรับปรุงแก้ไขอย่างต่อเนื่อง รวมทั้งจัดทำและกำหนดผู้รับผิดชอบในการจัดทำแผนเพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญต่อการดำเนินงานของระบบเทคโนโลยีสารสนเทศ และรายงานผลการดำเนินงานต่อคณะกรรมการบริหารความเสี่ยงและควบคุมภัยใน ทราบเป็นระยะๆ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
5. จัดให้ผู้บริหาร/ผู้บังคับบัญชา มีหน้าที่รับผิดชอบ ผลักดัน และสนับสนุนการดำเนินงานด้านต่างๆ ตามกระบวนการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ รวมทั้งเสริมสร้าง และพัฒนาความรู้ ความสามารถของบุคลากรที่เกี่ยวข้อง เพื่อให้มั่นใจว่า บุคลากรสามารถปฏิบัติงานได้อย่างมีประสิทธิผล
6. จัดให้ผู้บริหาร เจ้าหน้าที่ บุคลากร ลูกจ้าง และผู้เกี่ยวข้อง ได้รับความรู้และความตระหนักรถึงการมีส่วนร่วมที่จะทำให้ การบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศบรรลุวัตถุประสงค์ของการบริหารความต่อเนื่องในการดำเนินงานของ MFEC

#### ขอบเขตของนโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

ขอบเขตของกระบวนการ การให้บริการ สถานที่ปฏิบัติงาน ความต้องการด้านความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ตลอดจนการให้บริการสารสนเทศ ที่ใช้สนับสนุนกระบวนการที่สำคัญที่จะถูกรวบอยู่ในขอบเขตของนโยบายนี้ สามารถพิจารณาได้จากปัจจัย ที่มีความสำคัญ มีกระบวนการทำงานที่มีการพึ่งพาระบบสารสนเทศ

- กระบวนการทำงานที่มีการพึ่งพาระบบสารสนเทศ ที่สำคัญ ได้แก่ กระบวนการใน ระบบบริหารโครงการ , ระบบบัญชี การเงิน เบิกจ่าย , ระบบจัดเก็บเอกสารและระบบสารบรรณอิเล็กทรอนิกส์ , เว็บไซต์หลักของสำนักงานฯ
- ระดับความสำคัญของการคืนระบบเทคโนโลยีสารสนเทศ

- ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (MTPD) และระยะเวลาเป้าหมายในการพื้นดินสภาพ (RTO)
- ข้อกำหนดเกี่ยวกับระยะเวลาในขั้นตอนการทำสัญญา, การเบิกจ่ายทางการเงินและบัญชี กับการทำโครงการต่าง ๆ
- ข้อกำหนดของฝ่ายเทคโนโลยีสารสนเทศ ในด้านที่เป็นผู้ทำหน้าที่เป็นผู้ให้บริการสารสนเทศพื้นฐานให้กับสำนักงานฯ ได้แก่ การ เป็นผู้ให้บริการระบบสารสนเทศ คอมพิวเตอร์ และอุปกรณ์เครือข่าย
- ความเสี่ยงสำคัญในสถานที่ปฏิบัติงานหลัก ซึ่งอาจก่อให้เกิดผลกระทบต่อการให้บริการระบบงานที่สำคัญ ได้แก่ ห้องปฏิบัติการ เครื่องแม่ข่ายและอุปกรณ์เครือข่ายในสำนักงานฯ
- ความเสี่ยงสำคัญในการพึงพาการบริการด้านเทคโนโลยีจากผู้ให้บริการรายหนึ่งรายใด

#### บทบาทและหน้าที่

Chief Operating Officer (COO) ทำหน้าที่กำกับดูแลให้เป็นไปตามนโยบายและแนวปฏิบัติในการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

ผู้บริหาร/ผู้บังคับบัญชา เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ที่เกี่ยวข้องภายใต้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด แนวปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

คณะกรรมการบริหารความเสี่ยง เป็นผู้รับผิดชอบในการวิเคราะห์และกำหนดกลยุทธ์ในการบริหารความเสี่ยง จัดทำแผนการบริหารความเสี่ยง กำกับดูแลและติดตามการดำเนินการที่เกี่ยวข้องด้านความเสี่ยงของ MFEC

คณะกรรมการควบคุมภายใน เป็นผู้รับผิดชอบในการกำหนดขอบเขตการจัดการระบบควบคุมภายใน ควบคุมกำกับดูแล ให้ถูกต้องได้ มาตรฐานการควบคุมภายใน รวมถึงการพัฒนา ปรับปรุงระบบควบคุมภายใน กระบวนการ การ เครื่องมือ คุณภาพและแนวปฏิบัติให้เหมาะสมสมกับ สภาพแวดล้อมและความเสี่ยงที่เปลี่ยนแปลงไป

ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ การเตรียมการเพื่อลดความเสี่ยง ในการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ และลดระยะเวลาในการเตรียมการของทรัพยากรในด้านต่างๆ เพื่อกอบกู้พื้นดินระบบ เทคโนโลยีสารสนเทศ

เจ้าหน้าที่สารสนเทศ/ผู้ใช้บริการ จะต้องปฏิบัติตามนโยบายอยู่ด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ รวมทั้งข้อกำหนด แนวปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ มีส่วนร่วมในการวิเคราะห์ จัดเตรียมและซักซ้อมให้เป็นไปตามแผนความต่อเนื่อง ของระบบเทคโนโลยีสารสนเทศ

#### ระยะเวลาทบทวน

เพื่อให้นโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ รวมทั้งข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายย่อยดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง MFEC จึงจัดให้มีการ ทบทวนนโยบาย ข้อกำหนด แนวปฏิบัติ และขั้นตอนการปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายย่อยนี้เป็นประจำ ทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญทางเทคโนโลยี, โครงสร้างองค์กรที่อาจมีผลกระทบ

กับนโยบายอย่างนี้

## แนวทางปฏิบัติในการฟื้นคืนสภาพจากภัยพิบัติ (Disaster Recovery Plan Guideline)

MFEC Public Company Limited (MFEC) มีการสำรองข้อมูลที่สำคัญ โดยกำหนดรูปแบบ และแนวทางปฏิบัติ รวมทั้งแผนสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของสารสนเทศ เพื่อป้องกันการสูญหายอันอาจเกิดขึ้นจากการควบคุม หรือจาก การเกิดภัยพิบัติ โดยมอบหมายผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบ แผนการ และแนวทางปฏิบัติที่กำหนดไว้ เพื่อกำหนดเป็น มาตรฐานในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย หรือเครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์หลักที่ทำหน้าที่ เชื่อมโยงระบบเครือข่าย การเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถถูกกลับคืน หรือฟื้นฟูสภาพ ได้ภายในระยะเวลาที่เหมาะสม

วัดถุประสังค์

แนวทางปฏิบัติในการพื้นศีนสภาพจากภัยพิบัติน้ำที่เพื่อเป็นแนวทางในการดำเนินงานของการพื้นศีนสภาพด้วยวิธีการทางอิเล็กทรอนิกส์อย่างมีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามมาตรฐาน ข้อกำหนดและระเบียบปฏิบัติที่เกี่ยวข้อง รวมถึงสอดคล้อง กับนโยบายการบริหารความต่อเนื่องในการดำเนินงานของ MFEC โดยให้บุคลากรที่เกี่ยวข้องได้รับทราบและปฏิบัติตามอย่างเคร่งครัด

ជំនួយដាក់

ຜົດແລຮະບບ

แนวทางปฏิบัติ

แนวทางปฏิบัติการฟื้นคืนสภาพจากภัยพิบัติ ในเอกสารฉบับนี้ ประกอบไปด้วย

1. แนวทางของวงจรบริหารงานคุณภาพ (PDCA)
  2. แนวทางการวิเคราะห์ผลกระบวนการ (BIA)
  3. แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Assessment)
  4. แนวทางในการสำรองข้อมูล
  5. แนวทางในการกู้คืนระบบ
  6. แนวทางในการซ้อมแผนการบริหารความต่อเนื่องของระบบสารสนเทศ

### 5.1 แนวทางของวงจรการบริหารงานคุณภาพ (PDCA)

การบริหารความต่อเนื่องของระบบสารสนเทศนั้น จะต้องมีแพนกวงจร PDCA เข้ามาปรับปรุงและพัฒนาการดำเนินการให้มีประสิทธิภาพมากขึ้นด้วย

- จัดให้มีการวางแผนการล่วงหน้าในกรณีที่มีเหตุการณ์อันตรายเกิดขึ้น (Plan) จากจุดที่สำคัญของ MFEC ที่กล่าวว่า ระบบสารสนเทศ ได้ที่ต้องให้บริการต่อเนื่องแม้จะเกิดภัยพิบัติ เช่น ระบบบัญชีการเงิน ระบบบริหารโครงการ หรือฝ่ายเทคโนโลยี

สารสนเทศจะต้อง รักษาเครื่องคอมพิวเตอร์แม่ข่ายให้สามารถให้บริการได้ตลอดเวลา และวางแผนว่าทำอย่างไรจึงสามารถให้บริการได้จริง อาจจะ ต้องมีกระบวนการย้ายเครื่องคอมพิวเตอร์แม่ข่ายบางส่วนไปยังศูนย์ข้อมูลสำรองได้มีเกิดภัยพิบัติ

2. จัดให้มีการควบคุมให้มีการดำเนินการตามแผนที่วางไว้ (Do) มีการลงมือตามแผนที่วางไว้ ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายสำรอง และเตรียมพร้อมสำหรับการถ่ายโอนงานไปยังศูนย์ข้อมูลสำรองเมื่อจำเป็น
3. จัดให้มีการตรวจสอบและทบทวน (Check) มีการซักซ้อมเมื่อเกิดภัยพิบัติ ตรวจสอบว่าเมื่อย้ายข้อมูลแล้วสามารถทำงานต่อเนื่องได้ จริงหรือไม่ หรือเกิดปัญหาระหว่างการย้าย เช่น ใช้เวลาในการย้ายข้อมูลนานเกินไปจนกระทั่งกระทบกับการทำงาน
4. จัดให้มีการปรับปรุงแผนการอย่างต่อเนื่อง (Act) แผนการควรได้รับการปรับปรุงตามความเปลี่ยนแปลงของระบบงานและความต้องการที่เปลี่ยนแปลงไป MFEC จะจะมีระบบสารสนเทศใหม่เพิ่มขึ้นมา ที่มีความสำคัญสูง หรือมีความจำเป็นต้องให้บริหารความต่อเนื่องของระบบสารสนเทศเมื่อจำนวนผู้ใช้ระบบเพิ่มมากขึ้น

## 5.2 แนวทางการวิเคราะห์ผลกระทบในการดำเนินงาน (BIA)

1. จัดให้มีการระบุระบบเทคโนโลยีสารสนเทศซึ่งเป็นกระบวนการที่สำคัญในการให้บริการ และเป็นกระบวนการที่มีส่วนเกี่ยวข้องกับผู้ใช้บริการโดยตรง ซึ่งหากขาดกระบวนการนี้แล้วจะส่งผลให้ MFEC ไม่สามารถบรรลุวัตถุประสงค์หลักในการทำงานได้
2. จัดให้มีการกำหนดหลักเกณฑ์การวิเคราะห์ โดยจำแนกผลกระทบออกเป็น ด้านการเงิน ด้านชื่อเสียง และภาพลักษณ์ขององค์กร ด้านผู้มีส่วนได้ส่วนเสียขององค์กร และด้านการปฏิบัติตามกฎหมาย/ข้อบังคับ
3. จัดให้มีการรวบรวมข้อมูลด้วยวิธีการสัมภาษณ์ สำรวจ หรือประชุมเชิงปฏิบัติการ
4. จัดให้มีการระบุช่วงเวลาหยุดชะงักที่ยอมรับได้สูงสุด (MTPD : Maximum Tolerable Period of Disruption) โดยใช้หลักเกณฑ์ที่กำหนด และระดับที่ยอมรับได้ (Acceptance) ซึ่งเป็นที่ยอมรับ
5. จัดให้มีการระบุระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (RTO : Recovery Time Objective) โดยพิจารณาถึงระยะเวลาที่ใช้ในการฟื้นฟู และเริ่กคืนการดำเนินงาน ได้แก่ การเดินทางไปสถานที่ปฏิบัติงานสำรอง การรวบรวมบุคลากร การติดตั้งอุปกรณ์ สำนักงาน การจัดเตรียมข้อมูลต่าง ๆ และการประสานงานกับผู้รับจ้าง (Outsource) เป็นหลัก
6. จัดให้มีการกำหนดเป้าหมายของการฟื้นคืนสภาพ (RPO : Recovery Point Objective) โดยพิจารณาจากปริมาณข้อมูลสูญหาย ในเวลาที่ยอมรับได้ เพื่อให้กลับสู่การดำเนินงานตามปกติ
7. จัดให้มีการสรุปการวิเคราะห์ผลกระทบในการดำเนินงาน และจัดลำดับความสำคัญของระบบเทคโนโลยีสารสนเทศ โดยผ่านความเห็นชอบของคณะกรรมการบริหารความต่อเนื่องในการดำเนินงานของ MFEC

## 5.3 แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Assessment)

1. จัดให้มีการระบุภัยคุกคามที่สำคัญที่เกิดขึ้นในปัจจุบัน และอาจจะเกิดขึ้นในอนาคต โดยภัยคุกคามที่ถูกระบุ จะขึ้นอยู่กับ

ลักษณะ ของกระบวนการหลัก อาจคำนึงถึงความเสี่ยงโดยทั่วไปด้านความต่อเนื่องในการดำเนินงานที่ร่วบรวมโดยสถาบันอันเป็นที่ยอมรับ ในระดับสากล เช่น Business Continuity Institute (BCI) เป็นต้น

2. จัดให้มีคุณภาพทำงานบริหารความเสี่ยง ทำหน้าที่ร่วมกันระบุภัยคุกคาม โดยพิจารณาปัจจัยจากภายนอกองค์กร เช่น บุคลากร ระบบ โครงสร้างพื้นฐานของอาคาร ปัจจัยจากภายนอกองค์กร เช่น การสื่อสารและการโทรศัพท์ ภัยธรรมชาติ การโจมตีระบบโดยผู้ไม่ประสงค์ดี เป็นต้น
3. จัดให้มีการประเมินและวัดระดับความเสี่ยงเป็นขั้นตอน ที่ช่วยในการจัดลำดับความเสี่ยง โดยเรียงลำดับความเสี่ยงสูงสุดไปจนถึง ความเสี่ยงต่ำสุด การประเมินระดับความเสี่ยงจะอาศัยพื้นฐานในการพิจารณาความสัมพันธ์ของผลกระทบ (Impact) และโอกาสที่ จะเกิด (Probability) ตามหลักเกณฑ์การประเมินความเสี่ยงที่ได้ตกลงร่วมกัน และสามารถคำนวณได้จาก ระดับความเสี่ยง = โอกาสที่จะเกิด X ผลกระทบ
4. จัดให้มีการกำหนดเงื่อนไขที่ใช้ในการจัดลำดับความเสี่ยง และจัดลำดับความเสี่ยงจากมากไปหาน้อย เพื่อใช้ประโยชน์ในการพิจารณาเลือกวัสดุที่สำคัญ และจัดทำแผนตอบสนองอุบัติการณ์
5. จัดให้มีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และอาจส่งผลกระทบต่องค์กร เช่น ระบบ เทคโนโลยีสารสนเทศเกิดความเสียหาย หรือการเกิดความเสียหายจากภัยธรรมชาติต่าง ๆ เป็นต้น
6. จัดให้มีการจัดทำแผนตอบสนองอุบัติการณ์โดยพิจารณาเลือกจากภัยคุกคามที่มีผลกระทบอยู่ในระดับสูง แต่มีโอกาสที่จะเกิดภัยคุกคามอยู่ในระดับต่ำ ซึ่งอ้างอิงตาม แนวทางอันเป็นที่ยอมรับในระดับสากลคือ Good Practice Guideline 2008 ของสถาบัน Business Continuity Institute (BCD)
7. จัดให้มีการจัดทำรายงานผลการประเมินความเสี่ยงด้านสารสนเทศ และข้อเสนอแนะ เพื่อนำเสนอต่อกองการทำงานบริหารความเสี่ยง

#### 5.4 แนวทางในการสำรองข้อมูล

จัดให้มีการกำหนดระบบเทคโนโลยีสารสนเทศในการสำรองข้อมูล ที่สอดคล้องกับความเสี่ยงต่างๆ ที่จะเกิดขึ้นกับระบบสารสนเทศ อาจได้แก่ การโจมตีระบบโดยผู้ไม่ประสงค์ดี การเกิดอัคคีภัย อุทกภัย และอุบัติภัยต่างๆ โดยคำนึงถึงผลกระทบของความเสี่ยงการยอมรับได้ ของการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ และงบประมาณของฝ่ายเทคโนโลยีสารสนเทศ ให้ได้ข้อสรุปว่าจะทำการสำรองและการกู้คืนระบบในรูปแบบเทคโนโลยีได โดย MFEC จะจัดการเข้าสถานที่สำรองไว้ที่ Data center ที่มีมาตรฐานสำหรับการทำ Disaster Recovery Site และจัดซื้อหรือเช่าอุปกรณ์ที่จำเป็นในการปฏิบัติการของ การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายและอินเทอร์เน็ตและมี Private link เชื่อมโยงจากสถานที่หลักไปยังสถานที่สำรองดังกล่าว ตามข้อกำหนดที่ได้ตกลงกันไว้และให้ใช้งานระบบสำรองได้ภายในระยะเวลาที่ยอมรับ ได้

การทำ Disaster Recovery Site มี 5 รูปแบบ ดังต่อไปนี้

1. Hot Site คือ สามารถทำงานได้ทันทีโดยที่อุปกรณ์ในสถานที่หลักและสถานที่สำรอง ทำงานควบคู่กันไป เมื่อเกิดเหตุอุบัติภัย

ขึ้น สามารถที่จะดำเนินงานตามปกติได้ทันที

2. Warm Site คือ สามารถทำงานได้ต่อเมื่อ เมื่อเกิดเหตุอุบัติภัยขึ้นจะต้องทำการ ติดตั้งอุปกรณ์ต่างๆ ก่อนจึงจะสามารถ ดำเนินงาน ได้ตามปกติ
3. Cold Site คือ เมื่อเกิดเหตุอุบัติภัยขึ้น จึงทำการซื้อหรือเช่าอุปกรณ์ต่างๆ ใหม่ เช่น เครื่องคอมพิวเตอร์แม่ข่าย และจะต้องทำ การ ติดตั้งระบบสารสนเทศใหม่ทั้งหมด ใช้เวลานานพอสมควรในการขับระบบเทคโนโลยีสารสนเทศ
4. Standby site คือ จัดการสรรหาสถานที่ ยังมีได้ดำเนินการได้ ๆ ทั้งสิ้น
5. Nothing คือ ไม่มีการดำเนินการทำระบบสำรองใดๆทั้งสิ้น

**รูปแบบเทคโนโลยีที่ใช้การสำรองและกู้คืนระบบแบ่งออกได้เป็น 3 แบบ ดังต่อไปนี้**

1. Automation ใช้เวลาในการกู้คืนระบบเป็นระยะเวลาที่ สามารถทำการสำรองข้อมูลทันที
2. Replication ใช้เวลาในการกู้คืนระบบเป็นระยะเวลาช่วงโมง จะทำการคัดลอกสำเนาข้อมูลไปเก็บไว้ที่ปลายทางและทำการขับ ระบบแบบ Manual
3. Restore ใช้เวลาในการกู้คืนระบบ เป็นระยะเวลาเป็นวันหรือสัปดาห์ เป็นการกู้ข้อมูลจากสื่อบันทึกประเภทต่างๆ เช่น เทป หรือ ดิสก์

**เครื่องมือหรือโปรแกรมในการสำรองและกู้คืนระบบสารสนเทศ**

ผู้ดูแลระบบและพัฒนาแผนกู้คืนระบบเทคโนโลยีสารสนเทศ มีหน้าที่จัดหาเครื่องมือในการใช้สำรองและกู้คืนระบบสารสนเทศ ตามงบประมาณที่ได้รับการจัดสรรในการทำการสำรองข้อมูลในองค์กรที่สำคัญ รวมถึงซอฟต์แวร์ที่ใช้ประกอบในการสำรองข้อมูล สำคัญใน องค์กร มีขั้นตอนการปฏิบัติการดังนี้

**การสำรองข้อมูล**

1. ต้องสำรองข้อมูลสำคัญในการดำเนินกิจการ รวมถึงซอฟต์แวร์ระบบปฏิบัติการ (Operating System) โปรแกรมระบบงาน คอมพิวเตอร์ (Application System) ชุดคำสั่งที่ใช้ทำงาน และข้อมูลสำคัญ ให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่าง ต่อเนื่อง
2. มีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อยควรมีรายละเอียด ดังนี้
  - 2.1. ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
  - 2.1.2. ประเภทสื่อบันทึก
  - 2.1.3. จำนวนและความถี่ที่ต้องสำรอง
  - 2.1.4. ขั้นตอนและวิธีการสำรองข้อมูลโดยละเอียด
  - 2.1.5. สถานที่และวิธีการเก็บรักษาสื่อบันทึก
3. มีการบันทึกการปฏิบัติงานเกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วนและควรมีการตรวจสอบ

บันทึกดังกล่าวอย่างสม่ำเสมอ (Operator logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้น และ สิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

4. มีการรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้ง วิธีการที่ใช้แก้ไขด้วย
5. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของสำนักงานฯ จาก จำเป็นมากไปหาน้อย
6. ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
7. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งาน สารสนเทศได้ตามปกติอย่างต่อเนื่องโดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่าง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
8. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
9. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
10. ระบุความถี่ของการปฏิบัติในแต่ละข้อ ให้มีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้จากผู้เกี่ยวข้อง
11. จัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการจัดทำระบบสำรองข้อมูล และ สารสนเทศของ MFEC
12. พิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้ ตามลำดับความสำคัญ
13. จัดให้มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล
14. จัดให้มีการมอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้
15. มีขั้นตอนปฏิบัติในการสำรองข้อมูลและกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้องทั้งซอฟต์แวร์ โปรแกรม ประยุกต์ และข้อมูลในระบบสารสนเทศ
16. มีขั้นตอนปฏิบัติในการตรวจสอบปัญหา ในกรณีที่พบปัญหาในการสำรองข้อมูล จะเป็นเหตุให้ไม่สามารถดำเนินการได้อย่าง สมบูรณ์ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหาและรายงานต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ
17. กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสิ่งที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูล มี ส่องชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
18. จัดให้มีการเข้ารหัสข้อมูล (Encrypted backup) ในการสำรองข้อมูลที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อ ป้องกันมิให้ข้อมูลสำรองหล่อนั้นถูกเปิดเผย
19. ต้องปฏิบัติตามขั้นตอนปฏิบัติ (Backup Procedure) ตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) โดย เครื่องครดิ

20. ระบุความต้องการสำรองข้อมูลและระบบสารสนเทศ ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการ โดยจะใช้วิธีสำรองข้อมูล แบบ Full Backup ตามความต้องดังนี้
- 20.1.1. Web servers: สำรองข้อมูลเผยแพร่บนเว็บไซต์ 1 ครั้งต่อเดือน และสำรองข้อมูลแบบส่วนต่าง 1 ครั้งต่อวัน
  - 20.1.2. Database servers: สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ 1 ครั้งต่อสัปดาห์ และสำรองข้อมูลแบบส่วนต่าง 1 ครั้งต่อวัน
  - 20.1.3. Firewall server: สำรองข้อมูล Rule ของ Firewall 1 ครั้งต่อเดือน
  - 20.1.4. Server อื่นๆ: สำรองข้อมูลบนเซิร์ฟเวอร์อื่นๆ เช่น ระบบงานต่างๆ 1 ครั้งต่อเดือน

#### การเก็บรักษาข้อมูลสำรอง

1. ต้องจัดเก็บสือบันทึกข้อมูลสำรอง ในสถานที่จัดเก็บข้อมูลสำรองที่ได้มาตรฐาน ติดตั้งอยู่สถานที่อื่นหรือตามความจำเป็น
2. ดำเนินการสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดย สถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหาย (Physical Security)
3. ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคต ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน เช่น เมื่อจัดเก็บข้อมูลใน สือบันทึกประเภทใด ต้องเก็บอุปกรณ์ ซอฟต์แวร์หรือโปรแกรมประยุกต์ที่เกี่ยวข้องสำหรับใช้อ่านสือบันทึกประเภทนั้นไว้ด้วย เช่นกัน เป็นต้น
4. จัดทำรายการหรือบัญชี ที่มีรายละเอียดชัดเจนไว้บนสือบันทึกข้อมูลสำรอง หรือบนระบบบันทึก เพื่อให้สามารถค้นหาได้โดยเร็ว และป้องกันการใช้งานข้อมูลสำรองผิดพลาด
5. จัดทำทะเบียนคุณภาพรับและส่งมอบข้อมูลสำรอง โดยมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูลและเวลา การขอใช้งานข้อมูลสำรอง ต้องได้รับอนุมัติจากผู้มีอำนาจ
6. จัดทำขั้นตอนการทำลายข้อมูลสำคัญและสือบันทึกที่ไม่ได้ใช้งานแล้ว รวมถึงข้อมูลลับต่างๆ ที่อาจยังคงอยู่ในสือบันทึก เช่น ใน Recycle bin ของระบบปฏิบัติการ เป็นต้น

#### การทดสอบข้อมูลสำรอง

1. กำหนดขั้นตอนการปฏิบัติของการทดสอบข้อมูลสำรอง ทั้งซอฟต์แวร์ระบบปฏิบัติการ (Operating System) โปรแกรมระบบงาน คอมพิวเตอร์ (Application System) ชุดคำสั่งที่ใช้ทำงาน และข้อมูล โดยปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
2. กำหนดแผนการทดสอบ และปฏิบัติการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ โดยทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งซอฟต์แวร์และโปรแกรมระบบต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้
3. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จะเป็นเหตุทำให้ต้องกู้คืนระบบผู้ดูแล ระบบต้องดำเนินการแก้ไข พร้อมทั้งรายงานผลการแก้ไข บันทึกและสรุปผลการปฏิบัติงานต่อผู้อำนวยการฝ่าย

เทคโนโลยี สารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ

### 5.5 แนวทางในการกู้คืนระบบ

1. กำหนดให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม
2. แจ้งผู้ใช้ระบบทราบทันที เมื่อพบว่าความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย มีผลกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ และรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์
3. ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทำงานอิเล็กทรอนิกส์ให้คุณทำงงานบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ แจ้งเหตุไปยังคุณทำงานบริหารความต่อเนื่องในการดำเนินงานของ MFEC เพื่อดำเนินการต่อไป
4. บันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหา
5. กำหนดให้มีการทดสอบและปรับปรุงแผนการกู้คืนระบบ อย่างน้อยปีละ 1 ครั้ง

### 5.6 แนวทางในการซ้อมแผนการบริหารความต่อเนื่องของระบบสารสนเทศ

การเตรียมพร้อมกรณีฉุกเฉิน

1. จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบ หรือฟื้นฟูสภาพระบบและข้อมูลมาได้ภายในระยะเวลาที่เหมาะสม หรือจัดทำระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว เพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้
  - 1.1.1. จัดลำดับความสำคัญของระบบงาน ข้อมูล ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้ต่อไประบบงาน
  - 1.1.2. กำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
  - 1.1.3. มีขั้นตอนการกู้คืนระบบและข้อมูลโดยละเอียดในแต่ละสถานการณ์
  - 1.1.4. กำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้อง ทั้งหมด
  - 1.1.5. ระบุรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะ ของเครื่องคอมพิวเตอร์ (Specification) ขั้นต่ำ ค่ากำหนดการทำงาน (System configuration) ระบบเครือข่ายและอุปกรณ์ เครือข่ายที่ต้องใช้งาน เป็นต้น
  - 1.1.6. ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน ในกรณีที่มีศูนย์คอมพิวเตอร์สำรอง เช่น สถานที่ตั้ง แผนที่ การอนุญาตให้เข้าถึงสถานที่ เป็นต้น
  - 1.1.7. ปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินสำเนาไว้ในอุปกรณ์
2. จัดให้มีการทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง

- เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และบันทึกผลการทดสอบ หรือการรายงานผลด้วย
3. จัดให้มีมาตรการเพื่อการสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบ เนพาะเท่าที่จำเป็น
  4. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินของระบบเทคโนโลยีสารสนเทศเพื่อรับสถานการณ์ฉุกเฉินจากภัยพิบัติ
  5. ทดสอบ ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้ งานได้หากเกิดเหตุการณ์ขึ้นจริง
  6. บันทึกเหตุการณ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น โดยพิจารณาถึง ประเภท ปริมาณ และ หลักฐาน สำหรับข้องง เพื่อใช้กรณีที่เหตุการณ์มีความเกี่ยวข้องกับการทำเนินการทางกฎหมาย
  7. ระบุรายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉินนี้ รวมมีสาระครอบคลุมภัยพิบัติหรือสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของ MFEC โดยมีหัวข้อสำคัญ ดังนี้
    - 7.1.1. การเตรียมการเบื้องต้น
    - 7.1.2. ผู้รับผิดชอบ
    - 7.1.3. มาตรการความปลอดภัยและแผนดำเนินงานในการนำระบบคอมพิวเตอร์กลับสู่สภาพปกติ เมื่อเกิดความเสียหาย หรือหยุด ทำงาน

## 6.นโยบายอย่างการบริหารความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

ความเสี่ยงเกิดขึ้นได้จากหลายปัจจัย หลายรูปแบบ และการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการดำเนินงานก็อาจ ก่อให้เกิด ความเสี่ยงต่อองค์กร โดยความเสี่ยงที่ให้ความสำคัญ ได้แก่ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ (access risk) ความเสี่ยงด้านการบริหารจัดการระบบคอมพิวเตอร์ บุคลากรด้านคอมพิวเตอร์ ที่ไม่เหมาะสมเพียงพอ (infrastructure risk) ซึ่งความเสี่ยง ดังกล่าว อาจก่อให้เกิดผลกระทบต่อองค์กรและภาคีได้ จึงต้องมีการประเมินความเสี่ยง อย่างสม่ำเสมอ เพื่อให้เกิดการจัดการความเสี่ยงอย่าง เหมาะสม ทำให้เกิดความมั่นคงของระบบสารสนเทศ อันเป็นหลักประกันว่า องค์กรจะมีระบบสารสนเทศให้ใช้งานได้อย่างต่อเนื่อง ไม่ หยุดชะงักและมีความมั่นคงปลอดภัย

### **วัตถุประสงค์**

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดได้
2. เพื่อพิจารณาแนวทางป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ
3. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอัตราภัยต่อระบบสารสนเทศ
4. เพื่อรับรองว่าการจัดเก็บสารสนเทศขององค์กรเป็นไปตามนโยบายและกฎหมายด้านความมั่นคงปลอดภัยและความลับส่วน บุคคล
5. เพื่อให้สอดคล้องกับแนวทางการบริหารความเสี่ยงของ MFEC

## บทบาทและหน้าที่

ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่)นโยบาย ข้อกำหนด แนวปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ตรวจสอบภายใน (Internal Auditor)/ตรวจสอบภายนอก (External Auditor) เป็นผู้ตรวจสอบและประเมินความเสี่ยง 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) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน
  - 2.1. กำหนดให้มีการดำเนินการทบทวนปรับปรุงนโยบายระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติตาม ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ ว่าสอดคล้องกับนโยบายหรือไม่
  3. อย่างน้อยปีละ 1 ครั้ง ให้ผู้จัดการกองทุนทราบพร้อมเสนอแนะแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง
    - 3.1. ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบความปลอดภัยของระบบสารสนเทศ อย่าง สม่ำเสมอ เช่น การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของ การควบคุม ด้านความมั่นคงปลอดภัย
    - 3.2. ควรมีเครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ ระบบงานและเอกสารที่จำเป็น สำหรับ งานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้องจากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุม จำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น
  4. กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ประมวลผลสารสนเทศจากบุคคลหรือหน่วยงานภายนอก
  5. มีมาตรการสำหรับการตรวจสอบและประเมินระบบสารสนเทศ ดังนี้
    - 5.1. มีการกำหนดข้อตกลงร่วมกันระหว่างผู้ตรวจสอบกับผู้ดูแลระบบและ/หรือเจ้าของระบบ
    - 5.2. มีการทำสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบสามารถตรวจสอบได้จากข้อมูลสำเนา และมีการทำลายสำเนาทั้งทันทีที่การ

- ตรวจสอบเสร็จสิ้น หรือหากมีได้ทำลาย ต้องมีการจัดเก็บไว้อย่างปลอดภัยและมีมาตรการป้องกันที่เหมาะสม
- 5.3. มีการจำกัดสิทธิ์ให้ผู้ที่ทำการตรวจสอบให้สามารถเข้าถึงข้อมูลได้โดยการอ่านเพียงอย่างเดียว
  - 5.4. มีการกำหนดวิธีการจัดเก็บหลักฐานการตรวจสอบข้อมูลที่ปลอดภัย
  - 5.5. มีการกำหนดขั้นตอนการปฏิบัติและหน้าที่ความรับผิดชอบของผู้ตรวจสอบอย่างชัดเจน
  6. บุคลากรที่ทำหน้าที่เป็นผู้ตรวจสอบต้องมีการกำหนดให้เป็นอิสระแยกจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการ ตรวจสอบ
  7. ให้มีการแปลผลการประเมินความเสี่ยงให้อยู่ในรูปแบบ risk map ตามแนวทางบริหารความเสี่ยงของ MFEC

## 6.1 แนวทางปฏิบัติในการประเมินความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

### วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการประเมินความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ อันจะเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

### ผู้รับผิดชอบ

1. ฝ่ายเทคโนโลยีสารสนเทศ
2. ผู้ตรวจสอบภายในของ MFEC (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)
3. ผู้ดูแลระบบ

### แนวทางปฏิบัติ

1. จัดให้มีการตรวจสอบและประเมินความเสี่ยงเรื่องความมั่นคงปลอดภัยด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง
  - 1.1. มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
  - 1.2. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
  - 1.3. มีการกำหนดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายในของ MFEC (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง
2. ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้องค์กรได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศขององค์กร
  - 2.1. กำหนดให้มีการดำเนินการทบทวนปรับปรุงนโยบายระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ว่า สอดคล้องกับนโยบาย หรือไม่อย่างน้อยปีละ 1 ครั้ง และรายงานให้คณะกรรมการบริหารความเสี่ยงทราบ พร้อม

- เสนอแนะแนวทางปรับปรุงแก้ไขใน กรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยสารสนเทศมีจุดบกพร่อง
- 2.2. ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบความปลอดภัยของระบบสารสนเทศอย่าง สม่ำเสมอ เช่น การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุม ด้านความมั่นคงปลอดภัย
  - 2.3. ควรมีเครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ ระบบงานและเอกสารที่จำเป็นสำหรับ งานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้องจากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุม จำกัดการเข้าใช้งาน ให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น
  3. กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ประมวลผลสารสนเทศจากบุคคลหรือหน่วยงานภายนอก
  4. มีมาตรการสำหรับการตรวจสอบประเมินระบบสารสนเทศ ดังนี้
    - 4.1. มีการกำหนดชัดตอกย้ำว่าผู้ตรวจสอบกับผู้ดูแลระบบและ/หรือเจ้าของระบบ
    - 4.2. มีการกำหนดขอบเขตในการตรวจสอบประเมิน
    - 4.3. มีการกำหนดวิธีการในการตรวจสอบประเมินที่เหมาะสมกับขอบเขตที่ได้กำหนด
    - 4.4. มีการทำสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบสามารถตรวจสอบได้จากข้อมูลสำเนา และมีการทำลายสำเนาทั้งทันทีที่การตรวจสอบเสร็จสิ้น หรือหากมิได้ทำลาย ต้องมีการจัดเก็บไว้อย่างปลอดภัยและมีมาตรการป้องกันที่เหมาะสม
    - 4.5. มีการจำกัดสิทธิ์ให้ผู้ที่ทำการตรวจสอบให้สามารถเข้าถึงข้อมูลได้โดยการอ่านเพียงอย่างเดียว
    - 4.6. มีการกำหนดวิธีการจัดเก็บหลักฐานการตรวจสอบข้อมูลที่ปลอดภัย
    - 4.7. มีการกำหนดขั้นตอนการปฏิบัติและหน้าที่ความรับผิดชอบของผู้ตรวจสอบอย่างชัดเจน
  5. บุคลากรที่ทำหน้าที่เป็นผู้ตรวจสอบต้องมีการกำหนดให้เป็นอิสระแยกจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ และต้องเป็นผู้ที่มีความเชี่ยวชาญในการตรวจสอบประเมินเรื่องความมั่นคงปลอดภัยของระบบสารสนเทศ
  6. ให้มีการแปลผลการประเมินความเสี่ยงให้อยู่ในรูปแบบ risk map ตามแนวทางบริหารความเสี่ยงของ MFEC

## 7.นโยบาย>y อยการบริหารจัดการผู้ให้บริการ (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 และแก้ไขปัญหาของระบบเทคโนโลยีสารสนเทศจากผู้ให้บริการ ภายนอกที่เป็นผู้ขาย หรือผู้ผลิต
3. เพื่อให้เกิดความพร้อมในการดำเนินการลดความเสี่ยงที่จะเกิดขึ้นจากผู้ให้บริการภายใน และภายนอก

#### แนวทาง

1. ประเมินความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการภายใน และภายนอกทั้งหมดเพื่อหมายเหตุการในการแก้ไขปัญหาความเสี่ยง
2. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารจัดการผู้ให้บริการ เป็นลายลักษณ์อักษร โดยสอดคล้องตาม กฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ
3. ให้ผู้เกี่ยวข้องรับทราบถึงแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารจัดการผู้ให้บริการ และดำเนินการได้อย่างถูกต้อง เหมาะสม
4. ดำเนินการตรวจสอบวิธีการปฏิบัติของผู้เกี่ยวข้องเพื่อให้เกิดความมั่นใจในการดำเนินการตามทิศทางที่ออกแบบไว้ ขอบเขตของนโยบายอย่างการบริหารจัดการผู้ให้บริการ

ขอบเขตของนโยบายอย่างการบริหารจัดการผู้ให้บริการ หมายถึงการบริหารจัดการผู้ให้บริการทั้งภายใน และภายนอก ใน รูปแบบของข้อตกลง และสัญญาที่ลงนามจากตัวแทนของคู่สัญญาทั้งสองฝ่าย  
บทบาทและหน้าที่

Chief Operating Officer (COO) ทำหน้าที่กำกับดูแลให้เป็นไปตามนโยบายและแนวทางปฏิบัติการบริหารจัดการผู้ให้บริการ

ผู้บริหาร/ผู้บังคับบัญชา เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ที่เกี่ยวข้องภายใต้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารจัดการผู้ให้บริการ

ฝ่ายอำนวยการ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารจัดการผู้ให้บริการ

ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารจัดการผู้ให้บริการอย่างเหมาะสม

เจ้าหน้าที่สารสนเทศ/ผู้ใช้งาน ต้องปฏิบัติตามนโยบายการดำเนินการอย่างปลอดภัย รวมทั้งข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับต่างๆที่เกี่ยวข้อง

#### ระยะเวลาทบทวน

เพื่อให้นโยบายการเข้าถึงสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง Mfec จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนการปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลง กระบวนการทำงาน วิธีการเข้าถึงสารสนเทศที่สำคัญที่กระทำการบันนโยบายนี้

## 7.1 แนวปฏิบัติการบริหารงานผู้ให้บริการภายนอก

1. จัดทำข้อตกลงในการให้บริการระหว่างเจ้าของระบบกับผู้ให้บริการภายนอกในไฟล์เดียว
2. สื่อสารข้อตกลงระหว่างผู้ให้บริการภายนอกกับหน่วยงานที่เกี่ยวข้อง
3. บันทึก ติดตามผลดำเนินการตามข้อตกลง
4. วัดผลดำเนินการ และรายงานผลการดำเนินการให้กับผู้บริหารทราบ

## 7.2 แนวปฏิบัติการบริหารงานผู้ให้บริการภายนอก

1. กำหนดเงื่อนไขในการคัดเลือกผู้ให้บริการโดยพิจารณาจากฐานข้อมูลการคัดกรองของหน่วยงานกลาง และ/หรือเกณฑ์ที่บริษัทฯได้จัดทำขึ้นเพื่อใช้เป็นเงื่อนไขของการจัดซื้อจัดจ้างของงานพัสดุ
2. กรณีที่ผู้ให้บริการภายนอกเข้าถึงระบบงานสำคัญให้จัดทำสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Non-Disclosure Agreement) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน
3. กรณีที่ใช้บริการด้านการพัฒนาระบบงานต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Development environment) เท่านั้น หากให้เข้าใช้ระบบงานหลัก (Production environment) ต้องมีการควบคุม และการตรวจสอบผู้ให้บริการอย่างเข้มงวด
4. กำหนดให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ
5. ต้องมีการกำหนดให้ผู้ให้บริการรายงานปัญหาต่างๆ และแนวทางการแก้ไขในการปฏิบัติงานเมื่อมีการร้องขอ หรือมีการปรับปรุงเทคโนโลยีให้ทันสมัยที่เกี่ยวข้องกับระบบงาน และเข้ามามีส่วนร่วมกับการพัฒนาระบบธุรกิจต่อเนื่อง
6. ผู้ให้บริการภายนอกต้องรับทราบถึงมาตรการด้านความปลอดภัยที่บริษัทฯ ได้ระบุ และพร้อมปฏิบัติตามอย่างเคร่งครัด
7. ต้องมีการจัดทำขั้นตอนในการตรวจสอบของผู้ให้บริการ โดยมีรายละเอียดที่ระบุหนักต่อด้านความปลอดภัยสารสนเทศ
8. จัดเตรียมวิธีการรับมือกับข้อพิพาทที่เกิดขึ้นระหว่างผู้ให้บริการภายนอก และกำหนดหน่วยงานที่เข้ามาดำเนินการเมื่อเกิดข้อพิพาท

## 8. นโยบายย่อการบริหารจัดการการได้มาซึ่งระบบ 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 ของกรรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ให้ผู้เกี่ยวข้องรับทราบถึงแนวทางปฏิบัติ และขั้นตอนปฏิบัติการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ
3. ดำเนินการตามนโยบาย และแนวทางที่กำหนดเพื่อสร้างความเชื่อมั่นในการรับมอบระบบได้อย่างมีประสิทธิภาพ

### ขอบเขตของนโยบายย่อการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ

ขอบเขตของนโยบายย่อการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบรองรับต่อการดูแลระบบเทคโนโลยีสารสนเทศที่มีอยู่ในศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง รวมถึงกระบวนการที่เกี่ยวข้องกับผู้มีส่วนได้ส่วนเสีย เกี่ยวกับการได้มาซึ่งระบบ และการพัฒนาระบบ

### บทบาทและหน้าที่

Chief Operating Officer (COO) ทำหน้าที่กำกับดูแลให้เป็นไปตามนโยบายและแนวทางปฏิบัติการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ

ผู้บริหาร/ผู้บังคับบัญชา เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ที่เกี่ยวข้องภายใต้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ

ฝ่ายอำนวยการ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ

ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ ขั้นตอน ปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารจัดการการได้มาซึ่งระบบ และการพัฒนาระบบ อย่างเหมาะสม

เจ้าหน้าที่สารสนเทศ/ผู้ใช้งาน ต้องปฏิบัติตามนโยบายการดำเนินการอย่างปลอดภัย รวมทั้งข้อกำหนด แนวทางปฏิบัติ

## ขั้นตอนปฏิบัติ ระเบียบข้อบังคับต่างๆที่เกี่ยวข้อง

**ผู้ทดสอบระบบ** เป็นผู้รับผิดชอบในการทดสอบระบบที่พัฒนาขึ้นเพื่อตรวจสอบฟังก์ชันการทำงาน และความถูกต้องของกระบวนการ ข้อมูลสารสนเทศ

**นักพัฒนาระบบ** เป็นผู้รับผิดชอบในการพัฒนาระบบงานครอบคลุมทั้งพนักงานภายใน และการจัดจ้างภายนอกเข้ามาดำเนินการพัฒนาระบบ

### ระยะเวลาทบทวน

เพื่อให้แน่ใจว่าการเข้าถึงสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง MFEC จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนการปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลง กระบวนการทำงาน วิธีการเข้าถึงสารสนเทศที่สำคัญที่กระทบกับนโยบายนี้

### แนวปฏิบัติผู้ใช้งานระบบ/พนักงาน

- เข้าร่วมในการทดสอบระบบสารสนเทศที่มีการพัฒนา หรือจัดซื้อใหม่ เพื่อให้เหมาะสมกับผู้ใช้งานในระบบสารสนเทศนั้น
- ผู้ใช้ระบบลงนามยอมรับผลการทดสอบเมื่อพบว่าซอฟต์แวร์หรือระบบที่จัดซื้อใหม่มีความสามารถตรงกับที่ผู้ใช้ต้องการ

### แนวปฏิบัติเจ้าของระบบสารสนเทศ

- จัดทำขั้นตอนหรือวิธีปฏิบัติในการพัฒนา การแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน (กำหนดขอบเขต และให้ทุกคนส่งบันทึกมาที่สารสนเทศบริษัทฯเพื่อสรุปรายงาน)
- จัดทำขั้นตอน หรือวิธีปฏิบัติในการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และมีบันทึกเหตุผลความจำเป็น และการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกราย
- ซึ่งรายละเอียดของขั้นตอนในการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ให้กับผู้ใช้งาน และบุคคลที่เกี่ยวข้องให้ได้รับทราบอย่างทั่วถึง พร้อมทั้งมีกลไกการควบคุมในการปฏิบัติตาม (System Password Policy, Log, Monitoring)
- ระบบงานหลักต้องมีการแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Development environment) ออกจากส่วนที่ใช้งานจริง (Production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น
- การพัฒนา หรือการแก้ไขเปลี่ยนแปลงระบบงาน ต้องระบุก็งระบบรักษาความปลอดภัย และเตือนภัยการทำงานของระบบงาน ประกอบด้วย
  - การตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input Validation)
  - การตรวจสอบความถูกต้องของกระบวนการทำงานภายใน (Internal Process)

- การตรวจสอบความถูกต้องของข่าวสาร (Message Integrity)
  - การตรวจสอบความถูกต้องของการประมวลผลข้อมูล (Output Validation)
6. การร้องขอให้มีการพัฒนา หรือการเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำอย่างเป็นลายลักษณ์อักษรจากผู้มีอำนาจหน้าที่
  7. มีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานหลัก
  8. ต้องมีการสอบทานกฎหมายของทางการในการแก้ไขเปลี่ยนแปลงระบบงาน เพื่อให้สอดคล้องกับกฎหมายที่ระบุ
  9. ผู้ร้องขอและศูนย์เทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นๆ ที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ และประมวลผลได้ครบถ้วนถูกต้อง
  10. ในระบบงานสำคัญต้องมีหน่วยงาน หรือทีมงานเข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนา และการทดสอบระบบ ก่อนที่จะอนุญาตไปใช้งานจริง

#### **แนวปฏิบัติของนักพัฒนาระบบ และนักทดสอบระบบ**

1. ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ให้เป็นปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา(Versioning Control)
2. ต้องมีการปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้รับพัฒนา หรือแก้ไขเปลี่ยนแปลงให้ทันสมัยอยู่เสมอ
3. ต้องจัดเก็บโปรแกรมเวอร์ชันก่อนการพัฒนาไว้ใช้ในกรณีที่เวอร์ชันปัจจุบันทำงานผิดพลาด หรือไม่สามารถทำงานได้
4. ต้องเขียนรายละเอียดการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง
5. กำหนดให้มีการสอบทานระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน
6. ต้องจัดทำขั้นตอนการตรวจสอบการอนุญาตระบบงานให้ถูกต้องครบถ้วนเพื่อใช้ในการดำเนินการได้อย่างมีประสิทธิภาพ

#### **9. นโยบายอย่างยั่งในการบริหารทรัพยากรบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**

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

#### **วัตถุประสงค์ของการดำเนินการอย่างปลอดภัย**

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

## แนวทาง

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

### ขอบเขตของนโยบายย่อยการบริหารทรัพยากรบุคคล

ขอบเขตของนโยบายย่อยการบริหารทรัพยากรบุคคลครอบคลุมทั้งบุคลากรภายในองค์กร และผู้มีส่วนได้ส่วนเสียภายนอก  
เช่น Outsource หรือ 3<sup>rd</sup> Party ที่ต้องปฏิบัติตามมาตรการด้านทรัพยากรบุคคลที่ระบุนี้

#### บทบาทและหน้าที่

**Chief Operating Officer (COO)** ทำหน้าที่กำกับดูแลให้เป็นไปตามนโยบายและแนวทางปฏิบัติการบริหารทรัพยากรบุคคล  
ผู้บริหาร/ผู้บังคับบัญชา เป็นผู้รับผิดชอบในการสนับสนุนให้ผู้ที่เกี่ยวข้องภายใต้บังคับบัญชาปฏิบัติตามนโยบาย ข้อกำหนด  
แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารทรัพยากรบุคคล

**ฝ่ายอำนวยการ** เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทางปฏิบัติ  
ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารทรัพยากรบุคคล

**ฝ่ายเทคโนโลยีสารสนเทศ** เป็นผู้รับผิดชอบในการพัฒนา (จัดทำ ปรับปรุง ทบทวน เผยแพร่) นโยบาย ข้อกำหนด แนวทาง  
ปฏิบัติ ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับการบริหารทรัพยากรบุคคลอย่างเหมาะสม

**เจ้าหน้าที่สารสนเทศ/ผู้ใช้งาน** ต้องปฏิบัติตามนโยบายการดำเนินการอย่างปลอดภัย รวมทั้งข้อกำหนด แนวทางปฏิบัติ  
ขั้นตอนปฏิบัติ ระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้อง

#### ระยะเวลาทบทวน

เพื่อให้นโยบายการเข้าถึงสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่  
เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง MFEC จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ  
ข้อกำหนด และขั้นตอนการปฏิบัติ ระเบียบข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อมีการ  
เปลี่ยนแปลง กระบวนการทำงาน วิธีการเข้าถึงสารสนเทศที่สำคัญที่กระทบกับนโยบายนี้

### 9.1 แนวทางปฏิบัติในการบริหารทรัพยากรบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางปฏิบัติการสรรหาบุคลากร

1. จัดทำขั้นตอนปฏิบัติในการคัดเลือกเจ้าหน้าที่เพื่อเข้าใช้ระบบสารสนเทศอย่างรัดกุมโดยเฉพาะในตำแหน่งงานที่เกี่ยวข้องกับ  
ระดับข้อมูลสารสนเทศที่สำคัญ
2. แจ้งเงื่อนไขการว่าจ้างตั้งแต่ขั้นตอนการจัดหา หรือจัดจ้างรวมถึงระบุเงื่อนไขในการยกเลิก

3. แจ้งให้เจ้าหน้าที่ หรือบุคคลที่เกี่ยวข้องทราบถึงนโยบายการใช้ระบบสารสนเทศบริษัทฯ เพื่อปกป้องสารสนเทศ และข้อมูลสารสนเทศจากบุคคลที่ไม่เกี่ยวข้อง

#### **แนวปฏิบัติการพัฒนาบุคลากร**

1. เจ้าหน้าที่ หรือบุคคลที่เกี่ยวข้องต้องเข้ารับการอบรม และเข้าร่วมกับการให้ความรู้เกี่ยวกับกฎหมาย กฎระเบียบ และนโยบาย เพื่อให้ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศอย่างถูกต้องเหมาะสม
2. ดำเนินการตรวจสอบ และจัดทำรายงานผลด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง และกำหนดรอบดำเนินการที่ชัดเจน
3. กำหนดให้เจ้าหน้าที่ หรือบุคคลที่เกี่ยวข้องกับสารสนเทศ และเทคโนโลยีสารสนเทศเข้าร่วมฝึกอบรมการอพยพการรับมือกับเหตุฉุกเฉินหรือภัยพิบัติ

#### **แนวปฏิบัติการยุติการว่าจ้าง**

1. ดำเนินการยกเลิกสิทธิ์ด้านการใช้ทรัพย์สินบริษัทฯ และทรัพย์สินที่เป็นสารสนเทศองค์กรทันทีที่มีการยุติการว่าจ้าง หรือมีการเปลี่ยนความรับผิดชอบในหน่วยงาน
2. จัดทำขั้นตอนปฏิบัติในการยุติการว่าจ้างอย่างชัดเจน พร้อมทั้งกำหนดให้มีรอบการตรวจสอบสิทธิ์การเข้าถึงทรัพย์สินบริษัทฯ เป็นระยะ

## ภาคผนวก ก.

### ข้อกำหนดการตั้งและเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยของ MFEC

1. กำหนดรหัสผ่านให้มีความยาวไม่น้อยกว่า 8 ตัวอักษร
2. ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งานหรือสามารถคาดเดาได้จ่าย เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น
3. ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
4. ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านโดยทันที
5. ผู้ใช้งานต้องเก็บรหัสผ่านไว้เป็นความลับ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที
6. ผู้ใช้งานใส่รหัสผ่านผิดได้อาย่างมากไม่เกิน 5 ครั้ง ในกรณีที่เกินจะถูกระงับการเข้าใช้งาน และต้องร้องขอให้ผู้ดูแลระบบทำการยกเลิกการ ระงับการเข้าใช้งานข้อกำหนดการชำระล้างข้อมูลและสือบันทึกข้อมูลของ MFEC สารสนเทศของ MFEC ที่มีระดับขั้นความลับตั้งแต่ ระดับ 2 ขั้นลับ เปิดเผยได้ เมื่อร้องขอ ไปจนถึง ระดับ 4 ขั้นลับที่สุด เปิดเผย ไม่ได้ ต้องได้รับการปกป้องไม่ให้ถูกเปิดเผยอย่างไม่เหมาะสมหรือถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ์ในการเข้าถึงจากการเลิกใช้งานสือบันทึก ข้อมูล ต่างๆ จึงจัดให้มีข้อกำหนดในการชำระล้างข้อมูลและสือบันทึกข้อมูลของ MFEC ขึ้น โดยให้ดำเนินการตามประเภทของสือบันทึก ข้อมูล ดังนี้

ประเภท	การลบข้อมูล	การล้างข้อมูล	การทำลายสื่อบันทึกข้อมูล
Hard copy storage เช่น เอกสารกระดาษ, ไมโครฟอร์ม เป็นต้น	ไม่มี	ไม่มี	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้
อุปกรณ์เครือข่าย เช่น router, switch เป็นต้น	ตั้งค่าเริ่มต้นจากโรงงาน	ดำเนินการตามคู่มือการใช้งานอุปกรณ์	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละลาย
อุปกรณ์สื่อสารเคลื่อนที่ เช่น smartphone, tablet, PDA เป็นต้น	ดำเนินการตามคู่มือการใช้งานอุปกรณ์ เช่น factory reset, erase all, secure wipe	ดำเนินการตามคู่มือการใช้งานอุปกรณ์ ทั้งนี้ขึ้นอยู่กับความสามารถของอุปกรณ์ แต่ละรุ่น เช่น การทำ cryptographic erase	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละลาย
Optical Media เช่น CD, DVD, BD เป็นต้น	ไม่มี	ไม่มี	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละลาย ขุดพินผู้ด้านที่ใช้บันทึกข้อมูล
Flash memory-based storage devices ที่เป็น USB removable media	เขียนทับข้อมูลเดิมอย่างน้อย 2 ครั้ง	ดำเนินการตามคู่มือการใช้งานอุปกรณ์ ทั้งนี้ขึ้นอยู่กับความสามารถของอุปกรณ์	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละลาย
Flash memory-based storage devices ที่เป็น memory card	เขียนทับข้อมูลเดิมอย่างน้อย 2 ครั้ง	ไม่มี	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละลาย
Flash memory-based storage devices ที่เป็น embedded flash memory on board and device	ตั้งค่าเริ่มต้นจากโรงงาน (factory reset)	ไม่มี	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละลาย
RAM and ROM-based storage device เช่น DRAM	ปิดเครื่องนำแหล่งจ่ายไฟออก หรือนำ DRAM ออกโดยต้องไม่มีไฟเลี้ยง เป็นเวลาอย่างน้อย 5 นาที	ปิดเครื่องนำแหล่งจ่ายไฟออก หรือนำ DRAM ออกโดยต้องไม่มีไฟเลี้ยง เป็นเวลาอย่างน้อย 5 นาที	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ บดให้ละลาย

ประเภท	การลบข้อมูล	การล้างข้อมูล	การทำลายสื่อบันทึกข้อมูล
RAM and ROM-based storage device เช่น EEPROM	ดำเนินการตามคู่มือการใช้งาน	ดำเนินการตามคู่มือการใช้งาน	ทำลายทางกายภาพ จنمี สามารถนำข้อมูลกลับมาใช้ ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ บดให้ละเอียด
สื่อแม่เหล็ก เช่น ATA hard disk	เขียนทับข้อมูลเดิมด้วย 0 ทั้งหมดอย่างน้อย 1 ครั้ง	ดำเนินการตามคู่มือการใช้งานอุปกรณ์ ทั้งนี้ขึ้นอยู่กับความสามารถของอุปกรณ์ เช่น ใช้ชุดคำสั่ง ATA Sanitize device, security erase, cryptographic erase, หรือ ล้างด้วยสนามแม่เหล็ก (Degaussing)	ทำลายทางกายภาพ จnmี สามารถนำข้อมูลกลับมาใช้ ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละเอียด
Flash memory-based storage devices เช่น ATA solid state drive, SCSI SSD, NVM express SSD เป็นต้น	เขียนทับข้อมูลเดิมด้วย 0 ทั้งหมดอย่างน้อย 1 ครั้ง หรือ ใช้ชุดคำสั่ง secure erase	ดำเนินการตามคู่มือการใช้งานอุปกรณ์ ทั้งนี้ขึ้นอยู่กับความสามารถของอุปกรณ์ เช่น ใช้ชุดคำสั่ง SCSI Sanitize, cryptographic erase, หรือ ล้างด้วยสนามแม่เหล็ก	ทำลายทางกายภาพ จnmี สามารถนำข้อมูลกลับมาใช้ ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละเอียด
Peripherally attached storage เช่น external hard disk	เขียนทับข้อมูลเดิมด้วย 0 ทั้งหมดอย่างน้อย 1 ครั้ง	ดำเนินการตามคู่มือการใช้งานอุปกรณ์ ทั้งนี้ขึ้นอยู่กับความสามารถของอุปกรณ์ เช่น ใช้ชุดคำสั่ง block erase, cryptographic, erase	ทำลายทางกายภาพ จnmี สามารถนำข้อมูลกลับมาใช้ ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละเอียด
Flash memory-based storage devices เช่น ATA solid state drive, SCSI SSD, NVM express SSD เป็นต้น	เขียนทับข้อมูลเดิมด้วย 0 ทั้งหมดอย่างน้อย 1 ครั้ง หรือ ใช้ชุดคำสั่ง secure erase	ดำเนินการตามคู่มือการใช้งานอุปกรณ์ ทั้งนี้ขึ้นอยู่กับความสามารถของอุปกรณ์ เช่น ใช้ชุดคำสั่ง ATA Sanitize, SCSI Sanitize, NVM Express format, block erase, security erase, cryptographic erase	ทำลายทางกายภาพ จnmี สามารถนำข้อมูลกลับมาใช้ ใหม่ได้ เช่น ตัดเป็นชิ้นเล็กๆ เผาจนไหม้ บดให้ละเอียด

## นิยาม

1. การชำระล้างข้อมูลและสีอับนทึกข้อมูล (Sanitization) หมายความว่า รูปแบบในการลบข้อมูล การล้างข้อมูล การทำลายสีอับนทึก ข้อมูลด้วยวิธีการที่ทำให้ไม่สามารถถูกกลับคืนมาใช้ได้อีก
2. การลบข้อมูล (Clear) หมายความว่า การทำให้ข้อมูลไม่สามารถถูกกลับคืนมาใช้ได้ แต่สีอับนทึกข้อมูลยังคงรูปและสามารถนำกลับมาใช้ได้อีก
3. การล้างข้อมูล (Purge) หมายความว่า การทำให้ข้อมูลไม่สามารถถูกคืนกลับมาใช้ได้อีก แม้วิธีการในห้องปฏิบัติการ
4. การทำลายสีอับนทึกข้อมูล (Destroy) หมายความว่า การทำให้ข้อมูลและสีอับนทึกข้อมูลไม่สามารถนำกลับมาใช้ได้อีก แม้วิธีการในห้องปฏิบัติการ