



นโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศและไซเบอร์

ของสำนักงานปลัดกระทรวงการพัฒนาสังคม
และความมั่นคงของมนุษย์



คำนำ

ในปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญ เพราะเข้ามาช่วยอำนวยความสะดวกในการทำงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ แต่ในขณะเดียวกันก็ทำให้เกิดความเสี่ยงเพิ่มขึ้น อันเนื่องมาจากภัยคุกคามของระบบเทคโนโลยีสารสนเทศ ซึ่งอาจสร้างความเสียหายต่อการปฏิบัติราชการได้ เนื่องจากระบบเทคโนโลยีสารสนเทศมีการเชื่อมโยงข้อมูลไปยังส่วนงานต่างๆ ส่งผลให้ช่องทางในการถูกบุกรุกเปิดกว้างขึ้น และอาจก่อให้เกิดเหตุอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อวินาศกรรมให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ส่งผลให้หน่วยงานสูญเสียชื่อเสียงหรือภาพพจน์ได้ ดังนั้น ผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์เป็นอย่างดี

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ขึ้น เพื่อให้หน่วยงานมีการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยและเชื่อถือได้ มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มีมาตรฐานเป็นที่ยอมรับในระดับสากล ตลอดจนเพื่อให้การดำเนินงานของหน่วยงานภายในเป็นไปในทิศทางเดียวกัน สอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ทั้งนี้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์นั้น ต้องได้รับความร่วมมือในการปฏิบัติตามอย่างเคร่งครัดและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว จึงหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ฉบับนี้ จะเป็นเครื่องมือในการดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ต่อไป

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ตุลาคม 2568

สารบัญ

	หน้า
บทนำ	
1. วัตถุประสงค์และขอบเขต	1
2. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์	1
3. คำนิยาม	3
4. ข้อตกลงและเงื่อนไข	8
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์	9
ส่วนที่ 1 การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	
1. การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ	13
2. การจัดการทรัพย์สิน (Asset Management)	20
3. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์	22
4. การตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	25
5. การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)	27
6. การจัดการผู้ให้บริการภายนอก (Third Party Management)	30
ส่วนที่ 2 การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	
1. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม	35
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน	39
3. การรักษาความมั่นคงปลอดภัยบนเครือข่าย	42
4. การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)	48
5. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)	52
6. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	57
7. การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)	60
8. การควบคุมการเข้าถึงของหน่วยงานภายนอก (Outsource Control)	63
9. การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	65
10. การเชื่อมต่อระยะไกล (Remote Connection)	67
11. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Bring Your Own Device)	69

สารบัญ (ต่อ)

	หน้า
ส่วนที่ 2 การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect) (ต่อ)	
12. การเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)	72
13. การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์	74
14. การใช้งานระบบเครือข่ายไร้สาย	77
15. การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.	79
16. การใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)	84
17. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	87
18. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)	92
19. การแบ่งปันข้อมูล (Information Sharing)	93
20. การบริหารจัดการข้อมูลองค์กร และป้องกันข้อมูลส่วนบุคคลหรือข้อมูลที่มีความสำคัญรั่วไหล	95
21. การบริหารจัดการการเข้ารหัสลับ (Encryption)	98
22. การกำหนดการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร	100
ส่วนที่ 3 การกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	
1. การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	104
ส่วนที่ 4 การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	
1. การรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response)	107
2. การสื่อสารในภาวะวิกฤต (Crisis Communication)	109
3. การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Exercise)	111
ส่วนที่ 5 การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	
1. การสำรองและทดสอบกู้คืนข้อมูล	114
2. การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	118

บทนำ

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ หรือต่อไปนี้จะเรียกว่า “สป.พม.” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ สป.พม. จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1) การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของ สป.พม. ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

2) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2549 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. 2562

3) เผยแพร่ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ฉบับนี้ ให้เจ้าหน้าที่ทุกระดับใน สป.พม. ได้รับทราบและถือปฏิบัติอย่างเคร่งครัด

4) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคล ภายนอกที่ปฏิบัติงานให้กับ สป.พม. ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

5) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ฉบับนี้ ต้องมี การดำเนินการตรวจสอบและประเมินตามระยะเวลาอย่างน้อย 1 ครั้งต่อปี

2. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

ส่วนที่ 1 การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify) แนวปฏิบัติ ที่เกี่ยวข้อง มีดังนี้

- 1) การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ
- 2) การจัดการทรัพย์สิน (Asset Management)
- 3) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์

- 4) การตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
- 5) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)
- 6) การจัดการผู้ให้บริการภายนอก (Third Party Management)

ส่วนที่ 2 การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect) แนวปฏิบัติที่เกี่ยวข้อง มีดังนี้

- 1) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
- 2) การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- 3) การรักษาความมั่นคงปลอดภัยบนเครือข่าย
- 4) การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)
- 5) การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)
- 6) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
- 7) การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)
- 8) การควบคุมการเข้าถึงของหน่วยงานภายนอก (Outsource Control)
- 9) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)
- 10) การเชื่อมต่อระยะไกล (Remote Connection)
- 11) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Bring Your Own Device)
- 12) การเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)
- 13) การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์
- 14) การใช้งานระบบเครือข่ายไร้สาย
- 15) การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.
- 16) การใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)
- 17) การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)
- 18) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)
- 19) การแบ่งปันข้อมูล (Information Sharing)
- 20) การบริหารจัดการข้อมูลองค์กร และป้องกันข้อมูลส่วนบุคคลหรือข้อมูลที่มีความสำคัญรั่วไหล
- 21) การบริหารจัดการการเข้ารหัสลับ (Encryption)
- 22) การกำหนดการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ 3 การกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) แนวปฏิบัติที่เกี่ยวข้อง มีดังนี้

- 1) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

ส่วนที่ 4 การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)
แนวปฏิบัติที่เกี่ยวข้อง มีดังนี้

- 1) การรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response)
- 2) การสื่อสารในภาวะวิกฤต (Crisis Communication)
- 3) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Exercise)

ส่วนที่ 5 การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)
แนวปฏิบัติที่เกี่ยวข้อง มีดังนี้

- 1) การสำรองและทดสอบกู้คืนข้อมูล
- 2) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ ผู้รับผิดชอบและผู้เกี่ยวข้อง และแนวปฏิบัติ โดยจะแสดงรายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ สป.พม. เพื่อให้ สป.พม. มีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และบุคลากรของ สป.พม. ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ฉบับนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. ซึ่งเจ้าหน้าที่ของ สป.พม. หน่วยงานภายนอก และผู้เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

3. คำนิยาม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ประกอบด้วย คำนิยาม ดังนี้

- 1) **สป.พม.** หมายความว่า สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
- 2) **ศทส.** หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- 3) **ผู้ใช้งาน** หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้าง และบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานเครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต หรือ e-Mail ที่ สป.พม. จัดสรรให้
- 4) **ผู้ดูแลระบบ** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศ หรือระบบเครือข่าย หรือระบบคอมพิวเตอร์
- 5) **เจ้าหน้าที่** หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของ สป.พม. ผู้รับบริการ ผู้ใช้งานทั่วไป
- 6) **สิทธิ์ของผู้ใช้งาน** หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของ สป.พม.

7) **สินทรัพย์/สินทรัพย์สารสนเทศ** หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับ สป.พม. เช่น เอกสาร สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง ระบบเครือข่าย และระบบสารสนเทศ

8) **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้อีกได้

9) **ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)** หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธ ความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

10) **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนข้อปฏิบัติด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความปลอดภัย

11) **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของ สป.พม. ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

12) **ระบบเครือข่าย** หมายความว่า กลุ่มของคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และสื่อสัญญาณ ที่ถูกนำมาเชื่อมต่อกัน ผ่านอุปกรณ์ด้านการสื่อสารหรือสื่ออื่นใด ซึ่งทาง ศทส. เป็นผู้กำหนด และทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนและใช้อุปกรณ์หรือทรัพยากรต่างๆ ของเครือข่าย ร่วมกันได้ โดยเครือข่ายคอมพิวเตอร์จะครอบคลุมทั้งเครือข่ายภายในหรือแลน (Local Area Network : LAN) แลนไร้สายหรือไวเลสแลน (Wireless LAN , WLAN) และเครือข่ายวงกว้างหรือแวน (Wide Area Network : WAN) ของ สป.พม. ผ่านการใช้บริการเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN)

13) **ระบบสารสนเทศ** หมายความว่า ระบบที่ประกอบด้วยส่วนต่างๆ ได้แก่ Hardware, Software, User, Data และ Procedure ซึ่งทุกองค์ประกอบนี้ทำงานร่วมกัน เพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งาน เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์ และติดตามผลการดำเนินงานของ สป.พม.

14) **การใช้งานอินเทอร์เน็ต** หมายความว่า การใช้บริการต่างๆ ผ่านเครือข่ายอินเทอร์เน็ตของ สป.พม.

15) **คอมพิวเตอร์** หมายความว่า คอมพิวเตอร์ที่มีการเชื่อมต่อเพื่อใช้งานเครือข่ายคอมพิวเตอร์ และอินเทอร์เน็ต ที่ สป.พม.

16) **ข้อมูล** หมายความว่า สิ่งที่ป้อนเข้าไปในคอมพิวเตอร์ ไม่ว่าจะเป็นตัวเลข ข้อความ คำสั่ง ชุดคำสั่ง ซอฟต์แวร์ แฟ้มข้อมูล หรือรายละเอียดซึ่งอาจอยู่ในรูปแบบประเภทต่างๆ

17) **รหัสผ่าน (Password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

18) **จดหมายอิเล็กทรอนิกส์ (e-Mail)** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

19) **ชุดคำสั่งไม่พึงประสงค์** หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

20) **หน่วยงานภายนอก** หมายความว่า องค์กรหรือหน่วยงานที่ สป.พม. อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของ สป.พม. โดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล หรือหน่วยงานที่ สป.พม. ดำเนินการส่งหรือเข้าถึงข้อมูลสารสนเทศ

21) **การจัดการทรัพย์สิน (Asset Management)** หมายความว่า การจัดการทรัพย์สิน เช่น ข้อมูล บุคลากร อุปกรณ์ ระบบ และสิ่งอำนวยความสะดวก ที่ช่วยให้หน่วยงานบรรลุวัตถุประสงค์ การระบุและจัดการให้สอดคล้องกับความสัมพันธ์กับวัตถุประสงค์และกลยุทธ์ความเสี่ยงของหน่วยงาน

22) **บริการที่สำคัญ** หมายความว่า บริการที่สำคัญตามภารกิจของ สป.พม. ที่อยู่ในรูปแบบเทคโนโลยีดิจิทัล เพื่อสนับสนุนและอำนวยความสะดวกแก่ประชาชน บุคลากร และหน่วยงานทั้งภายในและภายนอก

23) **Malware** ย่อมาจาก “Malicious Software” หมายความว่า โปรแกรมหรือซอฟต์แวร์ที่ถูกออกแบบมาเพื่อทำลาย ก่อวินระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต สามารถแฝงตัวมาในรูปแบบต่างๆ ได้ เช่น

Virus (ไวรัส) : แพร่กระจายผ่านไฟล์หรือโปรแกรมที่ดูเหมือนปลอดภัย เมื่อลงมือทำงาน จะทำลายข้อมูลหรือทำให้ระบบทำงานผิดปกติ

Worm (เวิร์ม) : แพร่กระจายตัวเองผ่านเครือข่ายโดยไม่ต้องพึ่งพาไฟล์ ทำให้ระบบช้าลงหรือหยุดทำงาน

Trojan (โทรจัน) : แฝงตัวมาในรูปของโปรแกรมที่ดูปลอดภัย แต่เมื่อถูกติดตั้งหรือเปิดใช้งาน จะทำงานในลักษณะที่เป็นอันตราย เช่น เปิดช่องทางให้ hacker ขโมยข้อมูลสำคัญ

Adware (แอดแวร์) : แสดงโฆษณาบนเครื่องของผู้ใช้ บางครั้งติดตั้งโดยไม่ได้รับอนุญาต และติดตามพฤติกรรมเพื่อแสดงโฆษณาที่ตรงกับความสนใจ

Spyware (สปายแวร์) : สอดแนมและรวบรวมข้อมูลจากเครื่องของผู้ใช้โดยที่ผู้ใช้ไม่รู้ตัว เช่น การกดแป้นพิมพ์และการเข้าชมเว็บไซต์

24) **เครือข่ายสังคมออนไลน์ (Social Network)** หมายความว่า การเชื่อมโยง สื่อสารระหว่างบุคคลในเครือข่ายทางสังคมผ่านทางเว็บไซต์ หรือโปรแกรมประยุกต์ที่มีการเชื่อมต่อกับอินเทอร์เน็ตบนสื่อต่างๆ โดยมีการทำงานร่วมกันระหว่างผู้ส่งสารและผู้รับสารเพื่อสร้างเนื้อหาในรูปแบบของข้อมูล ภาพ และเสียง

25) **โพสต์ (Post)** หมายความว่า การส่งข้อความตัวอักษร ภาพ หรือวิดีโอคลิป เข้าสู่สื่อออนไลน์ เช่น เว็บไซต์ เพื่อแสดงความคิดเห็นหรือเผยแพร่ข้อมูลข่าวสาร

26) **บุคคลภายนอก (Third Party)** หมายความว่า บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงานหรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานหรือข้อมูลของลูกค้าที่ควบคุมโดยหน่วยงานได้

27) **การประเมินช่องโหว่ (Vulnerability Assessment)** หมายความว่า กระบวนการตรวจสอบและวิเคราะห์ระบบสารสนเทศ และโครงสร้างพื้นฐานด้านเทคโนโลยี เพื่อค้นหาจุดอ่อน/ช่องโหว่ที่อาจถูกโจมตี ทำให้สามารถป้องกันการโจมตีทางไซเบอร์ และปกป้องข้อมูลและทรัพย์สินของหน่วยงานได้อย่างมีประสิทธิภาพ

28) **การทดสอบเจาะระบบ (Penetration Testing)** หมายความว่า กระบวนการที่เจ้าหน้าที่ที่มีความเชี่ยวชาญด้านความปลอดภัยไซเบอร์ทำการจำลองการโจมตีในระบบ คอมพิวเตอร์ หรือเครือข่าย เพื่อค้นหาจุดอ่อนและช่องโหว่ที่อาจถูกโจมตี

29) **อินเทอร์เฟซ (Interface)** หมายความว่า การเชื่อมต่อกันระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์ สามารถถ่ายโอนข้อมูลซึ่งกันและกันได้

30) **ล็อก (Log)** หมายความว่า บันทึกหรือรายการข้อมูลที่เกิดขึ้นในระบบ คอมพิวเตอร์ หรือเครือข่าย ในการติดตามเหตุการณ์ต่างๆ เช่น การเข้าสู่ระบบ การเข้าถึงข้อมูล การทำงานของซอฟต์แวร์ และการดำเนินการต่างๆ ที่เกิดขึ้นในระบบ

31) **การทำให้ระบบมีความแข็งแกร่ง (System Hardening)** หมายความว่า การดำเนินการรักษาความปลอดภัยของระบบคอมพิวเตอร์ หรือเครือข่ายให้มีความปลอดภัยมากขึ้นโดยลดช่องโหว่ที่อาจจะถูกโจมตี หรือใช้ในการละเมิดความปลอดภัย กระบวนการนี้จะครอบคลุมหลายด้าน เช่น การตั้งค่าและปิดฟังก์ชันที่ไม่จำเป็น การกำหนดนโยบายความปลอดภัย การติดตั้งอัปเดตและแพตช์ความปลอดภัยล่าสุดเพื่อป้องกันช่องโหว่ใหม่ๆ การตั้งค่ารหัสผ่านที่แข็งแกร่งและการยืนยันตัวตนแบบหลายชั้น (MFA) เพื่อเพิ่มความปลอดภัยในการเข้าถึงระบบ การตั้งค่าการอนุญาตจำกัดการเข้าถึงระบบหรือไฟล์ต่างๆ ให้เฉพาะผู้ที่มีสิทธิ์ที่จำเป็นเท่านั้น การตรวจสอบล็อก และการตรวจสอบเหตุการณ์ (Logs) การใช้ Firewall และการตั้งค่า Network Security เพื่อควบคุมการเข้าถึงเครือข่ายและป้องกันการโจมตีจากภายนอก และการเข้ารหัสเพื่อป้องกันการโจรกรรมข้อมูล

32) **มาตรฐานกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard)** หมายความว่า นโยบายและแนวทางปฏิบัติที่หน่วยงานหรือผู้ดูแลระบบใช้ในการควบคุม บริหารจัดการ และกำหนดการตั้งค่าระบบคอมพิวเตอร์หรือเครือข่ายให้อยู่ในระดับที่ปลอดภัยที่สุดในขั้นพื้นฐาน ซึ่งสอดคล้องกับนโยบายความปลอดภัย โดยมีการป้องกันความเสี่ยงและช่องโหว่ที่อาจเกิดขึ้น

33) **สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)** หมายความว่า หลักการด้านความปลอดภัยที่กำหนดให้ผู้ใช้หรือระบบใดๆ ได้รับสิทธิ์การเข้าถึงเฉพาะข้อมูล ทรัพยากร หรือฟังก์ชันที่จำเป็นต่อการทำงานของตนเท่านั้น โดยไม่มีการให้สิทธิ์เกินกว่าที่จำเป็น หลักการนี้ช่วยลดความเสี่ยงที่อาจเกิดจากการใช้งานหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตหรือการละเมิดความปลอดภัย

34) **การเชื่อมต่อระยะไกล (Remote Connection)** หมายความว่า กระบวนการที่ผู้ใช้สามารถเข้าถึงคอมพิวเตอร์หรือระบบเครือข่ายจากระยะไกล ผ่านอินเทอร์เน็ตหรือเครือข่ายอื่นๆ โดยไม่จำเป็นต้องอยู่ที่สถานที่เดียวกับเครื่องคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่ต้องการเข้าถึง การเชื่อมต่อระยะไกลมักถูกใช้เพื่อการทำงานจากที่บ้าน การสนับสนุนทางเทคนิค หรือการเข้าถึงข้อมูลและแอปพลิเคชันจากสถานที่ต่างๆ

35) **สื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)** หมายความว่า อุปกรณ์ที่ใช้ในการเก็บข้อมูลซึ่งสามารถนำออกจากอุปกรณ์หลักได้ โดยทั่วไปจะมีฟังก์ชันการอ่านและเขียนข้อมูลได้ และสามารถถ่ายโอนข้อมูลไปยังอุปกรณ์อื่นได้ง่าย สื่อบันทึกข้อมูลแบบถอดได้มีหลายประเภท ซึ่งแต่ละประเภทมีคุณสมบัติและการใช้งานที่แตกต่างกัน ประเภทสื่อบันทึกข้อมูลแบบถอดได้แบ่งได้ ดังนี้

USB Flash Drive: อุปกรณ์ที่ใช้การเชื่อมต่อผ่านพอร์ต USB มีขนาดเล็กและสามารถเก็บข้อมูลได้หลาย GB ถึง TB ใช้งานง่ายและสะดวกในการพกพา

External Hard Drive: ฮาร์ดดิสก์ภายนอกที่เชื่อมต่อผ่าน USB หรือ eSATA มักใช้สำหรับเก็บข้อมูลขนาดใหญ่และสำรองข้อมูล

CD/DVD/Blu-ray Disc: แผ่นซีดี, แผ่นดีวีดี หรือแผ่นบลูเรย์ที่ใช้ในการเก็บข้อมูล ข้อมูลจะถูกเขียนลงบนแผ่นซึ่งสามารถอ่านได้โดยใช้เครื่องอ่านที่เหมาะสม

Memory Cards: การ์ดหน่วยความจำที่ใช้กับอุปกรณ์ต่างๆ เช่น กล้องดิจิทัล สมาร์ทโฟน หรือแท็บเล็ต เช่น SD card, microSD card

Magnetic Tape: สื่อบันทึกข้อมูลแบบเทปแม่เหล็กมักใช้ในงานเก็บข้อมูลระยะยาวและการสำรองข้อมูลในองค์กรขนาดใหญ่

36) **การรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response)** หมายความว่า กระบวนการในการตอบสนองและจัดการกับเหตุการณ์หรือการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นต่อระบบคอมพิวเตอร์หรือเครือข่ายของหน่วยงาน เพื่อลดผลกระทบจากการโจมตี พื้นฟูระบบให้กลับมาใช้งานได้ตามปกติ และป้องกันไม่ให้เกิดเหตุการณ์ในลักษณะเดียวกันขึ้นอีกในอนาคต

37) **การสื่อสารในภาวะวิกฤต (Crisis Communication)** หมายความว่า กระบวนการสื่อสารที่หน่วยงานหรือบุคคลใช้ในการจัดการและตอบสนองต่อสถานการณ์วิกฤตหรือเหตุการณ์ที่ส่งผลกระทบต่อภาพลักษณ์ ความน่าเชื่อถือ หรือความปลอดภัยขององค์กรหรือชุมชน สามารถช่วยลดความตื่นตระหนก ปรับปรุงการเข้าใจสถานการณ์ และรักษาความไว้วางใจของผู้มีส่วนได้ส่วนเสีย

38) **การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)** หมายความว่า กระบวนการและขั้นตอนในการกู้คืนระบบ เทคโนโลยี และข้อมูลที่ได้รับผลกระทบจากการโจมตีทางไซเบอร์ หรือเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ให้กลับมาใช้งานได้ตามปกติ รวมถึงการตรวจสอบและปรับปรุงเพื่อป้องกันการเกิดเหตุการณ์ซ้ำในอนาคต

4. ข้อตกลงและเงื่อนไข

- 1) ผู้ใช้งานต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และไซเบอร์ของ สป.พม. อย่างเคร่งครัดโดยไม่มีเงื่อนไข และจะอ้างว่าไม่ทราบนโยบายและแนวปฏิบัติฯ ดังกล่าวมิได้
- 2) ห้ามผู้ใช้งานกระทำการใดๆ อันละเมิดหรือขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่า หากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของ สป.พม.
- 3) ผู้ใช้งานต้องรักษาบัญชีผู้ใช้งาน (Account) ของตนเองไว้เป็นความลับเฉพาะตัว และไม่อนุญาตให้ผู้อื่นเข้าถึงระบบด้วย Account ของตนเองในทุกกรณี เพื่อป้องกันการใช้งานโดยมิชอบ
- 4) ผู้ใช้งานต้องเป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้งานและการอนุญาตให้ผู้อื่นเข้าถึงระบบด้วย Account ในนามของตนเอง โดยไม่สามารถปฏิเสธความผิดนั้นได้ เว้นแต่จะพิสูจน์ได้ว่า ผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
- 5) ผู้ดูแลระบบมีสิทธิ์ระงับ เพิกถอน หรือกระทำการใดๆ ต่อการใช้งานระบบของผู้ใช้งาน เพื่อความมั่นคงปลอดภัยของระบบ โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครรัฐ พ.ศ. 2549 มาตรา 5 ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ตลอดจนพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 และมาตรา 45 ได้กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

ดังนั้น เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐดำเนินการ มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีการดำเนินมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์เป็นที่ยอมรับในระดับสากล สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ เพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ดังต่อไปนี้

นโยบายที่ 1 นโยบายการระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify) มีแนวปฏิบัติ ดังนี้

- 1) การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ
- 2) การจัดการทรัพย์สิน (Asset Management)
- 3) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์
- 4) การตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
- 5) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)
- 6) การจัดการผู้ให้บริการภายนอก (Third Party Management)

นโยบายที่ 2 นโยบายการวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)
มีแนวปฏิบัติ ดังนี้

- 1) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
- 2) การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- 3) การรักษาความมั่นคงปลอดภัยบนเครือข่าย
- 4) การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)
- 5) การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)
- 6) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
- 7) การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชัน และสารสนเทศ (Application and Information Access Control)
- 8) การควบคุมการเข้าถึงของหน่วยงานภายนอก (Outsource Control)
- 9) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)
- 10) การเชื่อมต่อระยะไกล (Remote Connection)
- 11) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Bring Your Own Device)
- 12) การเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)
- 13) การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์
- 14) การใช้งานระบบเครือข่ายไร้สาย
- 15) การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.
- 16) การใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)
- 17) การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)
- 18) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)
- 19) การแบ่งปันข้อมูล (Information Sharing)
- 20) การบริหารจัดการข้อมูลองค์กร และป้องกันข้อมูลส่วนบุคคล หรือข้อมูลที่มีความสำคัญรั่วไหล
- 21) การบริหารจัดการการเข้ารหัสลับ (Encryption)
- 22) การกำหนดการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร

นโยบายที่ 3 นโยบายการกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) มีแนวปฏิบัติ ดังนี้

- 1) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

นโยบายที่ 4 นโยบายการกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) มีแนวปฏิบัติ ดังนี้

- 1) การรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response)
- 2) การสื่อสารในภาวะวิกฤต (Crisis Communication)
- 3) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Exercise)

นโยบายที่ 5 นโยบายการกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) มีแนวปฏิบัติ ดังนี้

- 1) การสำรองและทดสอบกู้คืนข้อมูล
- 2) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

การกำหนดความรับผิดชอบ

1) ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ในฐานะผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) ของหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรือเป็นอันตรายใด ๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงาน

2) ผู้บริหารที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO) ของหน่วยงาน เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงาน

3) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ วิธีการ และแนวทางแก้ไขปัญหาแก่เจ้าหน้าที่ระดับปฏิบัติหรือผู้ที่ได้รับมอบหมาย ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงาน

4) ให้มีการแต่งตั้งคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ เพื่อปฏิบัติหน้าที่บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ กำหนด มาตรการ วิธีปฏิบัติ และบริการ ให้แก่ผู้ใช้งานและผู้มีส่วนได้ส่วนเสียปฏิบัติตาม

5) เพื่อให้การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบ ผู้รับผิดชอบระบบสารสนเทศ และผู้ที่ได้รับมอบหมาย เป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงานให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ 1 ครั้ง และหากมีการเปลี่ยนแปลงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงาน ให้ประกาศให้เจ้าหน้าที่ทุกระดับของหน่วยงานรับทราบทุกครั้ง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ จัดเป็นมาตรฐานด้านการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง จึงให้ใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่ของหน่วยงานและผู้เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์
สำนักงานปลัดกระทรวงการพัฒนากำลังคนและความมั่นคงของมนุษย์

ส่วนที่ 1

การระบุ และเข้าใจถึงบริบทต่างๆ
เพื่อการบริหารจัดการความเสี่ยง (Identify)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ	รหัสเอกสาร : IC-0101

การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดบทบาทและความรับผิดชอบของเจ้าหน้าที่ในสังกัด สป.พม. ให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่น และการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต รวมถึงกรณีที่ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. เกิดความเสียหาย หรืออันตรายใดๆ ต่อหน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. ผู้บริหาร

1.1 ปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ (Chief Executive Officer : CEO)

1.2 รองปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ ที่ได้รับมอบหมายให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO) สป.พม.

2. ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ดังนี้

2.1 ผู้บังคับบัญชา : ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2.2 ผู้ดูแลระบบ : เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ในสังกัด สป.พม. ทุกคน

แนวปฏิบัติ

1. ผู้บริหารมีหน้าที่ความรับผิดชอบ ดังนี้

1.1 ปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ (Chief Executive Officer : CEO)

1.1.1 ให้ความเห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.

1.1.2 รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

1.2 รองปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ ที่ได้รับมอบหมายให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO) สป.พม.

1.2.1 กำหนดให้มีการจัดทำและทบทวนหรือปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.

1.2.2 กำหนดให้ผู้รับผิดชอบและผู้เกี่ยวข้อง มีการดำเนินงานตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ	รหัสเอกสาร : IC-0101

1.2.3 กำหนดให้มีการตรวจสอบตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. โดยผู้ตรวจสอบภายในหน่วยงานของรัฐหรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก

1.2.4 กำหนดให้มีการบริหารจัดการทรัพยากรอย่างเพียงพอต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สป.พม. ในแต่ละปีงบประมาณ

2. ผู้ดูแลระบบมีหน้าที่ความรับผิดชอบ ดังนี้

2.1 ผู้บังคับบัญชา : ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2.1.1 กำกับดูแลการจัดทำและทบทวนหรือปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. และนโยบายสนับสนุนต่างๆ

2.1.2 กำหนดมาตรการและกำกับติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.

2.2 ผู้ดูแลระบบ : เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย

2.2.1 จัดทำบัญชีสินทรัพย์สารสนเทศของอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย และรายการระบบสารสนเทศให้ถูกต้อง และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.2.2 เก็บรักษาอุปกรณ์บริหารจัดการเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ในพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

2.2.3 ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่าย ช่องทางการสื่อสารของระบบเครือข่าย และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งาน

2.2.4 ดูแลรักษาและตรวจสอบการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย ให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้นในทันที ดังนี้

(1) กรณีเกิดจากการใช้งานของผู้ใช้งาน ที่ไม่เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ให้รีบแจ้งผู้ใช้งานนั้น ยุติการกระทำในทันที

(2) กรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อ สป.พม. ให้ผู้ดูแลระบบ พิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

2.2.5 ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย และโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดี (Malware) ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ	รหัสเอกสาร : IC-0101

- 2.2.6 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของ สป.พม. เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งาน นับตั้งแต่เริ่มใช้งาน และต้องเก็บรักษาไว้อย่างครบถ้วน ถูกต้อง ตามระยะเวลาที่กฎหมายกำหนด นับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย
- 2.2.7 กำหนดสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของผู้ใช้งาน ให้สามารถใช้งานได้ตามภารกิจและสิทธิ์ที่ได้รับ
- 2.2.8 ทบทวนและปรับปรุงบัญชีผู้ใช้งานตามสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ
- 2.2.9 ควบคุมและตรวจสอบการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของผู้ใช้งาน ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 2.2.10 ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งาน โดยไม่มีเหตุผลอันสมควร
- 2.2.11 ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร
- 2.2.12 ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร
- 2.2.13 คินสินทรัพย์สารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนโดยทันทีที่พ้นจากหน้าที่ ให้กับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย เพื่อตรวจสอบการคินสินทรัพย์สารสนเทศนั้น

3. ผู้ใช้งานมีหน้าที่ความรับผิดชอบ ดังนี้

เป็นผู้เข้าถึงและใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ ระบบเครือข่าย และระบบสารสนเทศของ สป.พม. ตามสิทธิ์ที่ได้รับอนุญาต โดยต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. อย่างเคร่งครัด ดังนี้

3.1 การใช้งานรหัสผ่าน (Password Use)

- 3.1.1 ควรตั้งรหัสผ่านโดยมีความยาวอย่างน้อย 12 ตัวอักษร
- 3.1.2 ควรตั้งรหัสผ่านที่ประกอบด้วย ตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ
- 3.1.3 ควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วย อักขระที่เรียงกัน เช่น 123, abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น 111, aaa เป็นต้น
- 3.1.4 ควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
- 3.1.5 ควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ
- 3.1.6 ไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ	รหัสเอกสาร : IC-0101

- 3.1.7 ควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีในครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบ
- 3.1.8 ควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น
- 3.1.9 ควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด หรืออย่างน้อยทุกๆ 3 เดือน
- 3.1.10 ควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว
- 3.1.11 ไม่ควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่ผู้อื่นมองเห็นได้ง่าย
- 3.1.12 ไม่เปิดเผยรหัสผ่านของตนเองกับผู้อื่น
- 3.1.13 ไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น
- 3.1.14 ไม่ควรกำหนดให้ทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเอง
เมื่อทำการล็อกอินในภายหลัง
- 3.1.15 ควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกัน สำหรับระบบงานต่างๆ ที่ใช้งาน

3.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

- 3.2.1 ควรป้องกันไม่ให้ผู้อื่นเข้าใช้ระบบงาน/เครื่องคอมพิวเตอร์/เครื่องโน้ตบุ๊กของตน โดยให้ใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งาน
- 3.2.2 ควรตั้งค่าให้มีการล็อก (Lock) หน้าจอของอุปกรณ์โดยอัตโนมัติ เมื่อไม่ได้ใช้งานนานเกินกว่า 15 นาที
- 3.2.3 ควรออกจากระบบงาน/เครื่องคอมพิวเตอร์/เครื่องโน้ตบุ๊กที่ใช้งาน โดยทันทีเมื่อเสร็จสิ้นงาน
- 3.2.4 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้น หรือไม่มีการใช้งานนานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องแม่ข่ายที่ให้บริการ

3.3 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

- 3.3.1 รับผิดชอบต่อสินทรัพย์ที่ สป.พม. มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของตนเอง โดยต้องบันทึกรายการสินทรัพย์ที่ผู้ใช้งานรับผิดชอบ และตรวจสอบทุกครั้งเมื่อมีการรับหรือคืนสินทรัพย์ โดยเจ้าหน้าที่ที่ได้รับมอบหมายของหน่วยงาน
- 3.3.2 มีสิทธิ์ใช้สินทรัพย์ที่ สป.พม. จัดเตรียมไว้ให้เพื่อการใช้งานเท่านั้น ห้ามนำไปใช้ในกิจกรรมที่ สป.พม. ไม่ได้กำหนด โดยหากเกิดความเสียหายต่อหน่วยงาน จากการละเมิดดังกล่าว ให้ถือว่าเป็นความผิดส่วนบุคคล และผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นนั้น
- 3.3.3 หากสินทรัพย์เกิดการชำรุดหรือสูญหายจากความประมาทของผู้ใช้งาน ผู้ใช้งานต้องชดเชยค่าเสียหายตามมูลค่าสินทรัพย์นั้น
- 3.3.4 กรณีที่ต้องทำงานนอกสถานที่ ผู้ใช้งานจะต้องดูแลและรับผิดชอบต่อสินทรัพย์ของ สป.พม. ที่อยู่ในความรับผิดชอบเป็นอย่างดี
- 3.3.5 ห้ามให้ผู้อื่นยืมสินทรัพย์ไม่ว่ากรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน
- 3.3.6 ห้ามติดตั้งซอฟต์แวร์คอมพิวเตอร์ใดๆ ลงบนเครื่องคอมพิวเตอร์ หากจำเป็นต้องติดตั้ง จะต้องแจ้งให้ ศทส. ทราบ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ	รหัสเอกสาร : IC-0101

3.3.7 ไม่คัดลอกหรือทำสำเนาเพิ่มข้อมูลที่มีลิขสิทธิ์ก่อนได้รับอนุญาต และต้องไม่ใช่หรือลบเพิ่มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

3.3.8 หากจะนำอุปกรณ์สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ไปให้ผู้อื่นใช้งานต่อ จะต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อน โดยใช้วิธีการลบหรือการเขียนทับข้อมูลเดิมหลายรอบ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

3.3.9 หากจำเป็นต้องทำลายอุปกรณ์สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ ให้ดำเนินการตามมาตรการ ดังนี้

มาตรการการทำลายข้อมูลและสื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์	
ประเภท	วิธีการทำลาย
กระดาษ	ใช้วิธีการย่อยทำลายด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ใช้วิธีการย่อยทำลายด้วยเครื่องทำลายเอกสาร
เทป DDS , DAT, LTO	1. ทำการลบข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป 2. ทำลายด้วยวิธีการทุบหรือบดให้เสียหาย
ฮาร์ดดิสก์ (Hard Disk) หรือ Memory Devices เช่น USB flash drive , SD cards	1. ทำลายข้อมูลโดยใช้เทคโนโลยีซอฟต์แวร์ Wiping ที่สอดคล้องกับมาตรฐาน DoD 5220-22M ของกระทรวงกลาโหม สหรัฐอเมริกา ว่าด้วยการลบข้อมูลในฮาร์ดดิสก์ ดังนี้ ● ใช้ซอฟต์แวร์ Disk Wipe (http://www.diskwipe.org) ในการทำลายข้อมูลทั้ง Hard Disk หรือ Memory Devices โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://www.diskwipe.org/download.php ● ใช้ซอฟต์แวร์ Eraser (http://eraser.heidi.ie) ในการลบเพิ่มข้อมูล/ไฟล์ข้อมูล โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php 2. ทำลายด้วยวิธีการทุบหรือบดให้เสียหาย

3.3.10 มีส่วนร่วมในการบำรุงรักษาโปรแกรมป้องกันไวรัสที่ใช้ โดยตรวจสอบว่า มีการ Update โปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ ศทส. ทราบ หากไม่สามารถ Update โปรแกรมป้องกันไวรัสให้ทันสมัยได้

3.3.11 สำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

3.3.12 ไม่ปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัส ที่ ศทส. ติดตั้งให้

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ	รหัสเอกสาร : IC-0101

- 3.3.13 แจ้งให้ ศทส. ทราบทันที เมื่อพบว่าคอมพิวเตอร์หรือโปรแกรมที่ใช้มีความผิดปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส
- 3.3.14 ตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นด้วยโปรแกรมป้องกันไวรัสทุกครั้ง เมื่อมีการนำมาติดตั้งหรือใช้งาน และหากตรวจพบไวรัสจะต้องจัดการทำลายไวรัสโดยเร็วที่สุด
- 3.3.15 หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมที่นำมาใช้งานได้ ห้ามผู้ใช้งานทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปในเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เด็ดขาด
- 3.3.16 หากต้องการนำเครื่องคอมพิวเตอร์มาใช้งานภายใต้ระบบเครือข่ายของ สป.พม. จะต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องคอมพิวเตอร์ก่อน โดยซอฟต์แวร์นั้น ต้องสามารถ Update ให้เป็นปัจจุบัน และตรวจจับ Malware อื่นๆ ได้ เช่น Spyware หากไม่มีต้องแจ้งให้ ศทส. ติดตั้งให้
- 3.3.17 การใช้งานระบบเครือข่ายของ สป.พม. ผู้ใช้งานจะต้องลงทะเบียนเพื่อขอใช้งานจากผู้ดูแลระบบก่อน โดยผู้ที่ได้รับสิทธิ์ให้เข้าใช้งานได้ จะได้รับบัญชีผู้ใช้งาน (Account) ซึ่งประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password)
- 3.3.18 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ก่อนเข้าใช้งานระบบเครือข่ายของ สป.พม. ทุกครั้ง ด้วยบัญชีผู้ใช้งาน (Account) ของตนเองเท่านั้น
- 3.3.19 ห้ามเข้าศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ซึ่งเป็นพื้นที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์บริหารจัดการเครือข่ายโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ
- 3.3.20 ไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ
- 3.3.21 ไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้ากับระบบเครือข่ายของ สป.พม. เพื่อเปิดใช้งานเองในหน่วยงาน หรือประกอบธุรกิจส่วนบุคคล
- 3.3.22 กรณีที่ผู้ใช้งานพยายามเข้าถึงระบบโดยมิชอบ หรือโจมตีระบบ หรือมีพฤติกรรมการใช้งานที่ละเมิดต่อแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. หรือกฎหมายที่เกี่ยวข้อง ผู้ใช้งานนั้นจะถูกระงับหรือยกเลิกการใช้งานระบบเครือข่ายของ สป.พม. ทันที
- 3.3.23 กรณีที่ผู้ใช้งานได้กระทำการใดๆ ที่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อหน่วยงานหรือผู้หนึ่งผู้ใด ผู้ใช้งานนั้นจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ	รหัสเอกสาร : IC-0101

3.4 นำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ

- 3.4.1 ประเมินข้อมูลที่ต้องป้องกัน โดยพิจารณาตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 เพื่อระบุระดับความสำคัญและระดับความลับที่เหมาะสม
- 3.4.2 เลือกรหัสการเข้ารหัสที่เป็นมาตรฐานสากล มาใช้กับข้อมูลที่ต้องป้องกัน
- 3.4.3 การจัดเก็บรหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของระบบสารสนเทศ ลงในฐานข้อมูลใดๆ จะต้องทำการเข้ารหัสด้วยอัลกอริทึม 3DES หรือ AES ใน field ของ Password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง
- 3.4.4 การเชื่อมต่อระบบสารสนเทศแบบ Web Application เพื่อส่งข้อมูลระหว่างเบราว์เซอร์ และเว็บเซิร์ฟเวอร์ จะต้องเชื่อมต่อโดยการเข้ารหัส (SSL) ผ่านโปรโตคอล HTTPS
- 3.4.5 กำหนดช่องทางที่เหมาะสม ในการรับ - ส่งข้อมูลสำคัญหรือข้อมูลลับ ดังนี้
 - (1) ระบบเครือข่ายแบบ LAN
 - (2) ระบบเครือข่ายแบบไร้สาย หรือ Wireless LAN
 - (3) สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ ที่สามารถถอดแยกจากตัวเครื่องคอมพิวเตอร์ได้
- 3.4.6 กำหนดวิธีการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัส ดังนี้
 - (1) กำหนดผู้รับผิดชอบเพื่อทำหน้าที่เกี่ยวกับการเข้ารหัส เช่น การสร้างกุญแจ การควบคุม และดูแลกุญแจ การทำลายกุญแจ การใช้งานกุญแจ และการจัดการกรณีกุญแจเกิดการสูญหาย
 - (2) กำหนดวิธีการป้องกันกุญแจที่ใช้สำหรับการเข้ารหัส
 - (3) กำหนดวิธีการกู้คืนข้อมูลที่ถูกรหัสไว้ ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย
- 3.4.7 ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับหรือวิธีการรักษาความลับของข้อมูล ดังนี้
 - (1) แสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
 - (2) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ ด้วยวิธีการเข้ารหัสตามมาตรฐาน ที่ สป.พม. กำหนด
 - (3) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ด้วยการกำหนดรหัสผ่าน ให้กับไฟล์ข้อมูลลับนั้น
- 3.4.8 ห้ามแชร์ไฟล์ข้อมูลลับบนระบบเครือข่ายของ สป.พม. เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้
- 3.4.9 ตรวจสอบการทำงานของระบบป้องกันไวรัสในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล อย่างสม่ำเสมอ เพื่อให้สามารถป้องกันไวรัสได้ตามปกติ
- 3.4.10 ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ ของซอฟต์แวร์หรือไม่
- 3.4.11 สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การจัดการทรัพย์สิน (Asset Management)	รหัสเอกสาร : IC-0102

การจัดการทรัพย์สิน (Asset Management)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการ และแนวปฏิบัติในการรวบรวม และบริหารจัดการทรัพย์สินด้านเทคโนโลยีดิจิทัล สำหรับการควบคุม ป้องกัน และรักษาความมั่นคงปลอดภัยแก่ทรัพย์สินด้านเทคโนโลยีดิจิทัล ของ สป.พม. ได้อย่างเหมาะสม รวมถึงปรับปรุงให้ทะเบียนทรัพย์สินด้านเทคโนโลยีดิจิทัล ของ สป.พม. มีความถูกต้อง และทันสมัยอยู่เสมอ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. ผู้บริหาร

- 1.1 ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (Chief Executive Officer : CEO)
- 1.2 รองปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ที่ได้รับมอบหมายให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO) สป.พม.

2. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)

3. เจ้าหน้าที่/ผู้ดูแลทรัพย์สิน หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย

4. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. จัดทำทะเบียนทรัพย์สิน (Inventory)

- 1.1 ให้เจ้าหน้าที่/ผู้ดูแลทรัพย์สินที่ได้รับมอบหมายจัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และทบทวนทะเบียนทรัพย์สินให้เป็นปัจจุบัน รวมถึงตรวจสอบว่ามีความชำรุดเสียหาย หรือไม่เหมาะสมที่จะนำมาใช้งาน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้
 - ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญ
 - ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญ
 - ตำแหน่งทางกายภาพของทรัพย์สิน ของบริการที่สำคัญ
 - การระบุและการจัดลำดับความสำคัญของทรัพย์สิน ของบริการที่สำคัญ
 - ระบุเจ้าของ และ/หรือผู้ดำเนินการของทรัพย์สิน ของบริการที่สำคัญ
 - การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญ บนระบบเครือข่ายภายใน และ/หรือภายนอก
- 1.2 ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรง และมีนัยสำคัญ (Direct and Significant Interface)
- 1.3 ต้องมีกระบวนการในการบริหารจัดการทรัพย์สินสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (End of Life) หรือสิ้นสุดการให้บริการ (End of Support) เพื่อป้องกันภัยคุกคามทางไซเบอร์
- 1.4 ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สิน อย่างน้อยปีละ 1 ครั้ง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การจัดการทรัพย์สิน (Asset Management)	รหัสเอกสาร : IC-0102

2. การปรับปรุงแก้ไขข้อมูล

ให้เจ้าหน้าที่/ผู้ดูแลทรัพย์สินทำการทบทวนและตรวจสอบทรัพย์สินเป็นประจำทุก 1 ปี เทียบกับทะเบียนทรัพย์สิน เพื่อตรวจสอบว่ามีการชำรุด เสียหาย หรือไม่เหมาะสมที่จะนำมาใช้งานหรือไม่ เพื่อไม่ให้เกิดผลต่อการทำงานและการให้บริการผู้ใช้งาน

3. กรณีทรัพย์สินชำรุดเสียหายหรือไม่สามารถใช้งานได้

กรณีเครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ ต้องมีการดำเนินการจ้างบำรุงรักษาพร้อมกำหนดให้มีการจัดหาระบบในการติดตามการทำงาน (Monitor) หากพบว่าคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ ไม่สามารถใช้งานได้ตามปกติ ต้องให้ระบบสามารถส่ง Line แจ้งเตือนไปยังโทรศัพท์มือถือของเจ้าหน้าที่ทราบ รวมถึงมีการกำหนดค่า SLA (Service Level Agreement) การบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ และอุปกรณ์ กับผู้รับจ้างในการดำเนินการอย่างเหมาะสมในเวลาที่กำหนดและไม่ส่งผลกระทบต่อการทำงานของระบบเครือข่าย และฐานข้อมูลของ สป.พม. หลังจากดำเนินการแล้ว เจ้าหน้าที่จะบันทึกรายละเอียดลงในประวัติการซ่อมทุกครั้ง

กรณีเครื่องคอมพิวเตอร์และอุปกรณ์ ชำรุด และโปรแกรมสำนักงานไม่สามารถใช้งานได้ปกติผู้ใช้งานแจ้งปัญหาจากการใช้งานผ่านโปรแกรมซ่อมบำรุงครุภัณฑ์ โดยเจ้าหน้าที่ ศทส. จะทำการรับเรื่อง เพื่อประเมินเบื้องต้นสำหรับการแก้ไข เช่น ทำการซ่อม เปลี่ยนอุปกรณ์ ลงโปรแกรม อัปเดตโปรแกรม เป็นต้น หลังจากดำเนินการแล้ว เจ้าหน้าที่จะบันทึกรายละเอียดลงในประวัติการซ่อมทุกครั้ง

4. กรณีที่ทรัพย์สินกำลังจะหมดอายุการใช้งาน ต่อสัญญาเช่า/บำรุงรักษา หรือต่อใบอนุญาต (License)

เจ้าหน้าที่/ผู้ดูแลทรัพย์สิน ต้องมีการจัดทำแผนและดำเนินการการทดแทนทรัพย์สินกำลังจะหมดอายุการใช้งาน การต่อสัญญาเช่า/บำรุงรักษา และการต่อใบอนุญาต (License) ตามเวลาที่กำหนดเพื่อไม่ให้ส่งผลกระทบต่อการทำงานของบริการ โดยต้องระบุคุณลักษณะ รายละเอียดของอุปกรณ์ ให้เหมาะสมกับการใช้งาน

5. การขออนุญาตนำทรัพย์สินออกนอกพื้นที่

ผู้ที่จะนำทรัพย์สินออกนอกพื้นที่ของหน่วยงานหรือมีการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกหน่วยงาน จะต้องมีการขออนุญาตเป็นลายลักษณ์อักษรเท่านั้น

6. หน้าที่รับผิดชอบของผู้ใช้งาน

ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของหน่วยงาน ต้องเป็นผู้รับผิดชอบทรัพย์สินที่ใช้งาน ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน เพื่อประกอบธุรกิจการค้าหรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบที่เกี่ยวข้อง ห้ามดัดแปลง แก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0103

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์

วัตถุประสงค์

เพื่อเป็นแนวทางในการวางกรอบและกระบวนการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ของหน่วยงาน และต้องมีการตรวจสอบและปรับปรุงอย่างต่อเนื่อง เพื่อให้เหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไปและภัยคุกคามใหม่ๆ ที่เกิดขึ้น

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. คณะกรรมการ หมายถึง คณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
3. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
4. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การดำเนินงาน

- 1.1 แต่งตั้งคณะกรรมการภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนา ระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นประธาน
- 1.2 ประชุมคณะกรรมการฯ เพื่อจัดทำแผนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 1.3 นำเสนอร่างแผนฯ ต่อปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ เพื่อขอความเห็นชอบ
- 1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน และเตรียมความพร้อมเพื่อรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผนฯ
- 1.6 ทบทวน/ปรับปรุงแผนฯ ปีละ 1 ครั้ง

2. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์

2.1 การประเมินความเสี่ยง (Risk Assessment)

- 2.1.1 การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากรหรือปัจจัยภายนอก

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0103

2.1.2 การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

2.1.3 การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินงานของหน่วยงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

2.2 ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการฯ ประกาศกำหนด

2.3 ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- วันที่ระบุความเสี่ยง (Date the Risk is Identified)
- คำอธิบายของความเสี่ยง (Description of the Risk)
- โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- การจัดการความเสี่ยง (Risk Treatment)
- เจ้าของความเสี่ยง (Risk Owner)
- สถานะของการจัดการความเสี่ยง (Status of the Treatment)
- ความเสี่ยงที่เหลือ (Residual Risk)

2.4 การจัดการความเสี่ยง (Risk Treatment) ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสม สอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินงาน ให้สอดคล้องกับสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

2.5 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

2.6 การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยงและผลกระทบการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการกำกับและดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0103

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 4 : การตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0104

การตรวจประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

วัตถุประสงค์

เพื่อให้หน่วยงานมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ที่อาจเกิดขึ้น ทำให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงาน โดยการตรวจสอบและประเมินความเสี่ยงนั้น จะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **คณะทำงาน** หมายถึง คณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
3. **ผู้รับการตรวจประเมิน** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
4. **ผู้ตรวจสอบภายในหน่วยงานของรัฐ** (Internal Auditor) หมายถึง เจ้าหน้าที่ของกลุ่มตรวจสอบภายใน สป.พม. ที่ได้รับมอบหมาย

แนวปฏิบัติ

1. การดำเนินงาน

- 1.1 แต่งตั้งคณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนาระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นประธาน
- 1.2 ประชุมคณะทำงานฯ เพื่อจัดทำแผนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 1.3 นำเสนอร่างแผนฯ ต่อปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เพื่อขอความเห็นชอบ
- 1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน และเตรียมความพร้อมเพื่อรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผนฯ
- 1.6 ทบทวน/ปรับปรุงแผนฯ ปีละ 1 ครั้ง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 4 : การตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0104

2. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์

- 2.1 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม. ปีละ 1 ครั้ง โดยดำเนินการให้สอดคล้องตามแผนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 2.2 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม. ให้ดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor)
- 2.3 กำหนดขอบเขตและขั้นตอนปฏิบัติสำหรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 2.4 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม. ที่มีความสำคัญหรือเป็นข้อมูลส่วนบุคคล มีข้อจำกัด ดังนี้
 - 2.4.1 ผู้ตรวจสอบภายในหน่วยงานของรัฐ สามารถเข้าถึงข้อมูลที่ต้องตรวจสอบในลักษณะที่อ่านได้เพียงอย่างเดียว
 - 2.4.2 ในกรณีที่ผู้ตรวจสอบภายในหน่วยงานของรัฐจำเป็นต้องเข้าถึงข้อมูลชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้ จะต้องดำเนินการด้วยวิธีการที่ปลอดภัย
 - 2.4.3 มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบภายในหน่วยงานของรัฐทำงานบนข้อมูลสำเนา
 - 2.4.4 มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ
 - 2.4.5 มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ
- 2.5 ผู้ตรวจสอบภายในหน่วยงานของรัฐ สรุปรายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม. เสนอต่อ ปพม. และ ศทส. เพื่อรับทราบ
- 2.6 ทบทวน/ปรับปรุงการดำเนินงานตามที่ผู้ตรวจสอบภายในหน่วยงานของรัฐให้ข้อเสนอแนะต่อไป

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 5 : การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)	รหัสเอกสาร : IC-0105

การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

วัตถุประสงค์

เพื่อให้หน่วยงานมีการประเมินช่องโหว่เพื่อค้นหาและระบุช่องโหว่ในระบบบริการที่สำคัญซึ่งอาจถูกโจมตีได้ เช่น การตั้งค่าที่ไม่ปลอดภัย ซอฟต์แวร์ที่ไม่อัปเดต หรือจุดอ่อนอื่นๆ ที่อาจถูกใช้เพื่อเจาะเข้าระบบ และมีการทดสอบเจาะระบบเพื่อดูว่าจุดอ่อนจากช่องโหว่สามารถถูกใช้ในการเข้าถึงข้อมูลหรือทำลายระบบบริการที่สำคัญได้อย่างไร ซึ่งจะช่วยให้ทราบจุดแข็งและจุดอ่อนของระบบ เพื่อป้องกันการโจมตีในอนาคต โดยการหาช่องโหว่และปิดช่องโหว่ทันทีที่พบ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **คณะทำงาน** หมายถึง คณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
3. **เจ้าหน้าที่** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
4. **ผู้ประเมินช่องโหว่และทดสอบเจาะระบบ** หมายถึง ผู้ให้บริการภายนอก ที่ได้รับการว่าจ้างจาก ศทส. ให้ดำเนินการประเมินช่องโหว่และทดสอบเจาะระบบของ สป.พม.
5. **เจ้าของระบบ** หมายถึง หน่วยงานที่เป็นเจ้าของกระบวนการงานในการพัฒนาระบบสารสนเทศของบริการที่สำคัญของ สป.พม.

แนวปฏิบัติ

1. การประเมินช่องโหว่

- 1.1 ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ อ้างอิงตามหลักการบริหารความเสี่ยงเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยไซเบอร์และการควบคุม โดยครอบคลุมบริการที่สำคัญ
 - Information Technology System
 - Industrial Control System
- 1.2 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย
 - Host Security Assessment
 - Network Security Assessment
 - Architecture Security Assessment

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 5 : การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)	รหัสเอกสาร : IC-0105

- 1.3 ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและความคุ้มครอง ก่อนที่จะทำการทดสอบระบบใหม่ใดๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใดๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

2. การทดสอบเจาะระบบ

- 2.1 ควรดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบ เทคโนโลยีสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ต ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

- 2.2 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) ครอบคลุมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยต้องมีการกำหนดรายละเอียดและข้อจำกัดต่างๆ ที่ใช้ในการทดสอบเจาะระบบ เพื่อให้ทราบถึงสิ่งที่ต้องทำและสิ่งที่ต้องหลีกเลี่ยง และหลีกเลี่ยงความเข้าใจผิดระหว่างผู้ทดสอบและเจ้าของระบบ องค์ประกอบของขอบเขตการทดสอบเจาะระบบ ได้แก่

- ระบุทรัพย์สินที่จะทดสอบ (Assets to be Tested) โดยระบุระบบสารสนเทศและองค์ประกอบที่ต้องการทดสอบ เช่น เซิร์ฟเวอร์, แอปพลิเคชัน/เว็บ, ฐานข้อมูล, หรืออุปกรณ์เครือข่าย
- ระบุประเภทของการทดสอบ (Types of Testing) ซึ่งประกอบด้วย
 - การทดสอบภายนอก (External Testing) เป็นการเจาะระบบจากภายนอกเครือข่ายหรือหน่วยงาน
 - การทดสอบภายใน (Internal Testing) เป็นการเจาะระบบจากภายในหน่วยงาน เช่น การทดสอบในลักษณะที่ว่าบุคคลภายนอกละเมิดการเข้าถึง โดยเข้ามาสู่ในเครือข่ายภายในแล้วสามารถทำอะไรได้บ้าง
 - การทดสอบแบบ Black-box หรือ White-box หรือ Gray-box ซึ่งเลือกรูปแบบกำหนดตามระดับของข้อมูลที่มีผู้ทดสอบมี
- ข้อจำกัดและข้อยกเว้น (Constraints and Exclusions) โดยระบุข้อจำกัด เช่น บางส่วนของระบบที่ไม่ควรถูกทดสอบเพราะอาจส่งผลเสียต่อการทำงาน เช่น เซิร์ฟเวอร์ที่ให้บริการอยู่ตลอดเวลา หรือข้อมูลที่เป็นความลับสูง
- เป้าหมายของการทดสอบ (Testing Objectives) ระบุวัตถุประสงค์เฉพาะ เช่น การหาช่องโหว่ด้านความปลอดภัย การประเมินการป้องกันการโจมตี หรือการทดสอบความสามารถในการกู้คืนระบบเมื่อถูกโจมตี

- 2.3 ต้องดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบความถูกต้องของระบบ โครงสร้างพื้นฐาน และระบบสารสนเทศ โดยผู้ทดสอบที่มีการรับรองและได้รับประกาศนียบัตร ที่เป็น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 5 : การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)	รหัสเอกสาร : IC-0105

ที่ยอมรับและเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

- 2.4 ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน
- 2.5 ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

3. การวิเคราะห์ผลการประเมินช่องโหว่และทดสอบเจาะระบบ และการแก้ไขช่องโหว่

- 3.1 ต้องนำรายงานสรุปผลการประเมินช่องโหว่และการทดสอบเจาะระบบ มาวิเคราะห์เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สป.พม.
- 3.2 การประเมินและแก้ไขช่องโหว่ของบริการที่สำคัญต้องปฏิบัติตามแนวทางดังต่อไปนี้
 - กำหนดกระบวนการหรือเครื่องมือเพื่อใช้ในการระบุ จัดลำดับความสำคัญ และติดตามแพตช์ (หรือโปรแกรมแก้ไขช่องโหว่) ของบริการสำคัญ
 - กำหนดกระบวนการทดสอบและติดตั้งแพตช์ตามระดับความสำคัญ
 - กำหนดให้มีการปรับปรุงแพตช์ของระบบปฏิบัติการ (Operation System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication) ในระยะเวลาที่เหมาะสมตามระดับความเสี่ยง
 - ทดสอบแพตช์ที่ออกใหม่ทุกครั้ง ก่อนนำไปติดตั้งบนระบบงานจริง
 - ทดสอบและติดตั้งแพตช์สำหรับช่องโหว่ที่มีความเสี่ยงสูงทันทีที่แพตช์ได้ถูกเผยแพร่ออกมา
 - ติดตามช่องโหว่ที่ยังไม่ถูกแพตช์หรือที่ยังอยู่ระหว่างดำเนินการ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 6 : การจัดการผู้ให้บริการภายนอก (Third Party Management)	รหัสเอกสาร : IC-0106

การจัดการผู้ให้บริการภายนอก (Third Party Management)

วัตถุประสงค์

เพื่อให้หน่วยงานมีการควบคุม ตรวจสอบ และบริหารจัดการผู้ให้บริการภายนอกที่มีส่วนเกี่ยวข้องในการให้บริการ หรือการดำเนินการของ สป.พม. เพื่อให้ สป.พม. สามารถดำเนินการได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัย สามารถลดความเสี่ยงและปกป้องข้อมูลของหน่วยงาน รวมถึงการปฏิบัติตามกฎหมาย และระเบียบข้อบังคับต่างๆ ตามมาตรการของภาครัฐ และที่ สป.พม. กำหนดไว้ได้

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ให้บริการภายนอก หมายถึง ผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT Outsourcing) หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศ และการเข้าถึงข้อมูลสำคัญของ สป.พม.

แนวปฏิบัติ

1. การคัดเลือกและการกำหนดความรับผิดชอบ

- 1.1 ต้องมีการกำหนดความรับผิดชอบ (Responsible) และมีการรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใดๆ ก็ตามในส่วนของการบริการที่สำคัญ
- 1.2 ต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของ สป.พม. เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงระบบสารสนเทศ ฐานข้อมูล การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางเทคโนโลยี โดยต้องมีการจัดทำข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดดังต่อไปนี้
 - ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญ ตามความต้องการ
 - ธุรกิจของหน่วยงานและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
 - ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของหน่วยงานจากภัยคุกคาม
 - ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทาน ผลิตภัณฑ์ สิทธิของหน่วยงาน ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก
- 1.3 ต้องมีการกำหนดแนวทางการคัดเลือกบุคคลภายนอกอย่างชัดเจนและเหมาะสมก่อนตัดสินใจใช้บริการ โดยพิจารณาประเมินให้ครอบคลุมตามระดับความมั่นคงปลอดภัยและความเสี่ยงที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ซึ่งครอบคลุมประเด็นสำคัญดังต่อไปนี้

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 6 : การจัดการผู้ให้บริการภายนอก (Third Party Management)	รหัสเอกสาร : IC-0106

- ความสามารถทางด้านเทคนิค ความเชี่ยวชาญ ประสบการณ์ และความพร้อมในการดำเนินงาน
- การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์
- การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่างๆ
- การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง
- การใช้เทคโนโลยีแบบเปิด (Open Technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยี รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง เช่น การใช้รูปแบบการรับส่งข้อมูล

2. การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

- 2.1 ต้องจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เป็นลายลักษณ์อักษร
- 2.2 ต้องระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญในสัญญาหรือข้อตกลงกับผู้ให้บริการภายนอก อย่างชัดเจน โดยพิจารณาให้ครอบคลุมตามระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก ดังนี้
 - ขอบเขตการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก
 - บทบาท หน้าที่ และความรับผิดชอบของผู้ให้บริการภายนอก
 - มาตรฐานการปฏิบัติงานขั้นต่ำของผู้ให้บริการภายนอก เช่น ความพร้อมใช้งานของระบบ เทคโนโลยีสารสนเทศ เป็นต้น
 - การติดตามและรายงานผลการปฏิบัติงานของผู้ให้บริการภายนอก
 - การรักษาความปลอดภัยของข้อมูล การรักษาความลับ และความเป็นส่วนตัวของ สป.พม.
 - การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก
 - สิทธิและหน้าที่ของ สป.พม. ในการเปลี่ยนแปลง แก้ไข ยุติ หรือยกเลิกสัญญาหรือข้อตกลง
 - ขอบเขตความรับผิดชอบในกรณีเกิดปัญหาหรือข้อขัดข้องในการให้บริการ เช่น การให้บริการล่าช้า หรือมีข้อผิดพลาดในการให้บริการ เป็นต้น รวมถึงแนวทางการแก้ไขปัญหาและการชดเชยค่าเสียหายที่อาจเกิดขึ้น
 - การกำหนดเงื่อนไขในสัญญา หรือข้อตกลงเกี่ยวกับการให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และเจ้าหน้าที่ผู้รับผิดชอบ มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก

3. การติดตามผลการปฏิบัติงานของผู้ให้บริการภายนอก

ต้องมีการติดตามผลการปฏิบัติงานของผู้ให้บริการภายนอกอย่างต่อเนื่อง โดยพิจารณาตามระดับความเสี่ยง และระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก รวมถึง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 6 : การจัดการผู้ให้บริการภายนอก (Third Party Management)	รหัสเอกสาร : IC-0106

การรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

4. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ในการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

ต้องมีการกำกับ ติดตามการใช้บริการจากผู้ให้บริการภายนอก การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ในการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล เป็นไปตามหลักการรักษาความลับของข้อมูล ความถูกต้องเชื่อถือได้ของระบบสารสนเทศ และการรักษาสภาพความพร้อมใช้งาน โดยมีรายละเอียด ดังต่อไปนี้

4.1 การจัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกและทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง โดยต้องบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การบำรุงรักษาทรัพย์สินอย่างสม่ำเสมอ การยกเลิกและเรียกคืนทรัพย์สิน โดยทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ต้องมีการระบุอุปกรณ์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูลที่ถือครอง รวมถึงการจัดประเภทและระดับความสำคัญของข้อมูล และเจ้าของทรัพย์สิน (Owner) เป็นอย่างน้อย และต้องมีการวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดอายุการใช้งาน (End of Life) หรือสิ้นสุดการให้บริการ (End of Support) จากผู้ผลิต

4.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security) ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at Endpoint) ข้อมูลที่อยู่ระหว่างการรับ - ส่ง ผ่านเครือข่าย (Data in Transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (Data at Rest) โดยครอบคลุม

- แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องตามระดับความสำคัญ ซึ่งครอบคลุมถึงการกำหนดสิทธิผู้เข้าถึงข้อมูล วิธีการรับส่ง การประมวลผล การจัดเก็บข้อมูล และการทำลายข้อมูล
- การเข้ารหัสลับข้อมูล (Cryptography) ตามระดับความสำคัญของข้อมูล รวมถึงวิธีการเข้ารหัสข้อมูล (Cryptographic Algorithm) และการบริหารจัดการกุญแจเข้ารหัสลับ (Key Management) โดยครอบคลุมทุกขั้นตอนของวงจรการบริหารจัดการกุญแจเข้ารหัสลับ (Lifecycle of Cryptographic Keys) กระบวนการสร้าง แจกจ่าย จัดเก็บ ใช้งาน การสำรอง เพิกถอน การต่ออายุ รวมถึงการบันทึกและตรวจสอบกิจกรรมที่สำคัญ

4.3 มีมาตรการควบคุมการเข้าถึงอย่างน้อย ดังนี้

- มีกระบวนการควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 6 : การจัดการผู้ให้บริการภายนอก (Third Party Management)	รหัสเอกสาร : IC-0106

- กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้มีสิทธิใช้งานระบบและผู้ใช้งานที่ได้รับสิทธิสูงให้ชัดเจน
- ควบคุมดูแลการให้สิทธิแก่ผู้ให้บริการภายนอก โดยจำกัดสิทธิตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน เพื่อไม่ให้บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ
- กำหนดวิธีการระบุและพิสูจน์ตัวตนผู้ใช้งานด้วยวิธีการที่รัดกุมเพียงพอ
- ในกรณีที่ผู้ให้บริการภายนอกเชื่อมต่อเพื่อเข้าถึงระบบงานของ สป.พม. ผ่านช่องทางการเข้าถึงระบบงานระยะไกล (System Remote Access) ควรมีกระบวนการบริหารจัดการการเข้าถึงระยะไกลด้วยวิธีการที่ปลอดภัย ดังนี้
 - ต้องมีการขออนุญาต และได้รับการอนุมัติก่อนการเข้าถึงระบบงานระยะไกล (System Remote Access) ของบัญชีผู้ใช้งาน โดยให้ใช้เฉพาะกรณีที่มีความจำเป็นเท่านั้น และจำกัดระยะเวลาในการเข้าถึงระบบงาน
 - มีการพิสูจน์ตัวตนผู้ใช้งานแบบ Two-Factors Authentication และการเชื่อมต่อผ่าน Virtual Private Network (VPN)
 - มีการควบคุมการเข้าใช้งาน โดยจำกัดการเข้าใช้งานได้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้น หรือใช้เทคโนโลยีบริหารจัดการเครื่องคอมพิวเตอร์แบบเสมือน (Virtual Desktops Infrastructure) เพื่อลดความเสี่ยงจากการติด Malware หรือการเข้าถึงระบบงานที่ไม่เหมาะสม
 - สามารถระบุและสอบทานแหล่งที่มาของอุปกรณ์หรือระบบปลายทางที่เข้าเชื่อมต่อกับระบบเครือข่ายของผู้รับใบอนุญาตแบบระยะไกล
 - มีการสอบทานการเข้าถึงระบบงานระยะไกล
- ดูแลให้ผู้ให้บริการภายนอกจัดเก็บบันทึกข้อมูลประวัติของการพิสูจน์ตัวตนและการเข้าถึง (Access Log) บันทึกการดำเนินงาน (Activity Log) ตามระยะเวลาที่กฎหมายกำหนด โดยมีการสอบทานข้อมูลการบันทึกเหตุการณ์ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยงและความสำคัญอย่างเป็นประจำ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์
สำนักงานปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์

ส่วนที่ 2

การวางมาตรฐานควบคุม
เพื่อปกป้องระบบของหน่วยงาน (Protect)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม	รหัสเอกสาร : IC-0201

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อเป็นมาตรการในการควบคุม ป้องกัน และรักษาความมั่นคงปลอดภัยเกี่ยวกับสถานที่ที่เป็นที่ตั้ง และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม. โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ปฏิบัติที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม.

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **เจ้าหน้าที่** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายหรือที่มีสิทธิ์ในการเข้าออกพื้นที่
3. **ผู้มาติดต่อ** หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มาติดต่อขอเข้าถึงหรือใช้ข้อมูล หรือทรัพย์สินต่างๆ ภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม.

แนวปฏิบัติ

1. ศทส. มีหน้าที่ความรับผิดชอบ ดังนี้

1.1 กำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

- 1.1.1 กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม. ให้ชัดเจน โดยสามารถแบ่งแยกได้เป็น พื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) และพื้นที่ติดตั้งอุปกรณ์กระจายสัญญาณเครือข่าย (Access Network Area) เป็นต้น
- 1.1.2 จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม. และประกาศให้รับทราบโดยทั่วกัน

1.2 ควบคุมสินทรัพย์สารสนเทศ

1.2.1 พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

- (1) มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม.
- (2) ผนังล้อมรอบศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ควรสร้างเป็นผนังทึบ
- (3) ประตูหรือทางเข้าพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม. ต้องออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ
- (4) ประตูหรือทางเข้าของศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ต้องมีระบบที่สามารถล็อกได้ เพื่อป้องกันการบุกรุกทางกายภาพ
- (5) ให้เจ้าหน้าที่ที่ปฏิบัติงานภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม. ต้องปิดประตูและหน้าต่างให้ล็อกอยู่เสมอ ภายหลังเลิกงาน และนอกเวลาราชการ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม	รหัสเอกสาร : IC-0201

1.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน

- (1) ติดตั้งระบบและอุปกรณ์สนับสนุนการทำงานที่เพียงพอต่อความต้องการใช้งาน ภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม. เช่น ระบบปรับอากาศ ระบบควบคุมอุณหภูมิและความชื้น ระบบไฟฟ้าสำรอง ระบบดับเพลิง ระบบควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control) หรืออุปกรณ์ที่สามารถป้องกันภัยคุกคามจากผู้บุกรุกและกล้องวงจรปิด (CCTV) เป็นต้น
- (2) มีการใช้ระบบไฟฟ้าสำรองกับระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า และต้องทดสอบระบบไฟฟ้าสำรองอย่างสม่ำเสมอ
- (3) มีการตรวจสอบหรือทดสอบระบบและอุปกรณ์สนับสนุนการทำงานอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานได้ตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
- (4) มีการดูแลและบำรุงรักษาระบบและอุปกรณ์สนับสนุนการทำงานอย่างถูกต้องและสม่ำเสมอ โดยจัดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ 1 ครั้ง

1.2.3 การป้องกันอุปกรณ์

- (1) แยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่ง เพื่อดูแลความมั่นคงปลอดภัย
- (2) มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอนหรือไฟฟ้ากระชาก
- (3) มีการตรวจสอบ สอดส่อง ระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. เพื่อป้องกันความเสียหายต่ออุปกรณ์
- (4) ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ ภายในบริเวณพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.
- (5) มีการกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศทุกครั้ง เมื่อว่างเว้นจากการใช้งาน

2. เจ้าหน้าที่มีหน้าที่ความรับผิดชอบ ดังนี้

2.1 ควบคุมการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม.

- 2.1.1 จัดทำคู่มือ/คำแนะนำ/วิธีปฏิบัติในการเข้าออกพื้นที่ และต้องประกาศให้รับทราบโดยทั่วกัน
- 2.1.2 จัดให้มีระบบจัดเก็บบันทึกการเข้าออกพื้นที่
- 2.1.3 จัดทำแบบบันทึกการเข้าออกพื้นที่ โดยต้องระบุรายละเอียดอย่างน้อย ดังนี้ ชื่อ - นามสกุล ตำแหน่ง หน่วยงาน ประเภทสิทธิ เครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับสิทธิ รายละเอียดกิจกรรม และระยะเวลาดำเนินการ
- 2.1.4 จัดทำบัตรผู้มาติดต่อ (Visitor) และให้ผู้มาติดต่อแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ หรือบัตรอนุญาตเข้าออกภายในอาคารที่ได้แลกมาก่อนหน้า เป็นต้น ในการเข้าออกพื้นที่

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม	รหัสเอกสาร : IC-0201

- 2.1.5 ให้ผู้มาติดต่อติดบัตรผู้มาติดต่อ (Visitor) ตรงจุดที่สามารถมองเห็นได้ชัดเจน ตลอดเวลาที่อยู่ภายในพื้นที่
- 2.1.6 รับคืนบัตรจากผู้มาติดต่อ (Visitor) โดยต้องตรวจสอบผู้มาติดต่อและอุปกรณ์ที่ได้รับสิทธิ์ทุกครั้ง หลังเลิกใช้งาน พร้อมลงบันทึกเวลาออกและรายการอุปกรณ์ ในแบบบันทึกการเข้าออกพื้นที่ให้ถูกต้อง รวมทั้งบันทึกลงในระบบจัดเก็บบันทึกการเข้าออกพื้นที่ไว้ด้วย
- 2.1.7 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้มาติดต่อ มีความจำเป็นต้องเข้าออกพื้นที่ หรือมิได้ขอสิทธิ์ในการเข้าออกพื้นที่ไว้ล่วงหน้า เจ้าหน้าที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนอนุญาต และจดบันทึกการเข้าออกพื้นที่ไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่ โดยเจ้าหน้าที่จะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลาและต้องควบคุมอย่างเข้มงวด
- 2.1.8 กำกับและดูแลให้ผู้มาติดต่อปฏิบัติตามคู่มือ/คำแนะนำ/วิธีปฏิบัติ ในการเข้าออกพื้นที่อย่างเคร่งครัด
- 2.1.9 ตรวจสอบแบบบันทึกการเข้าออกพื้นที่เป็นประจำทุกวันหรือทุกครั้งที่มีการเข้าออก
- 2.1.10 ตรวจสอบประวัติการเข้าออกพื้นที่เป็นประจำอย่างน้อยเดือนละ 1 ครั้ง

2.2 กำหนดสิทธิ์การเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.

- 2.2.1 กำหนดสิทธิ์ของแต่ละบุคคลตามลำดับความสำคัญ โดยสิทธิ์นั้นต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร
- 2.2.2 จัดทำแบบกำหนดสิทธิ์การเข้าออกพื้นที่ โดยต้องระบุรายละเอียดอย่างน้อย ดังนี้ ชื่อ - นามสกุล ตำแหน่ง หน่วยงาน หน้าที่และความรับผิดชอบ ระยะเวลาดำเนินการ และประเภทสิทธิ์
- 2.2.3 กำหนดสิทธิ์/ปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ทุกครั้งที่มีการเปลี่ยนแปลง และต้องทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง
- 2.2.4 จัดทำทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

3. ผู้มาติดต่อมีหน้าที่ความรับผิดชอบ ดังนี้

3.1 การเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ สป.พม.

- 3.1.1 แลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ หรือบัตรอนุญาตเข้าออกภายในอาคารที่ได้แลกมาก่อนหน้า เป็นต้น เพื่อรับบัตรผู้มาติดต่อ (Visitor) และบันทึกข้อมูลลงในแบบบันทึกการเข้าออกพื้นที่ทุกครั้งที่มีการเข้าออก
- 3.1.2 ติดบัตรผู้มาติดต่อ (Visitor) ตรงจุดที่สามารถมองเห็นได้ชัดเจน ตลอดเวลาที่อยู่ภายในพื้นที่
- 3.1.3 กรณีที่ต้องการนำอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่าย เข้ามาภายในบริเวณพื้นที่ จะต้องบันทึกรายการอุปกรณ์ที่นำเข้ามาลงในแบบบันทึกการเข้าออกพื้นที่ให้ถูกต้อง
- 3.1.4 คืนบัตรผู้มาติดต่อ (Visitor) กับเจ้าหน้าที่ โดยเจ้าหน้าที่จะตรวจสอบผู้มาติดต่อและอุปกรณ์ พร้อมลงบันทึกเวลาออกและรายการอุปกรณ์ในแบบบันทึกการเข้าออกพื้นที่ทุกครั้งที่มีการเข้าออก

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม	รหัสเอกสาร : IC-0201

3.1.5 ปฏิบัติตามคู่มือ/คำแนะนำ/วิธีปฏิบัติ ในการเข้าออกพื้นที่อย่างเคร่งครัด

3.2 การเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.

3.2.1 ขออนุญาตเข้าออกพื้นที่ล่วงหน้าก่อนวันที่จะเข้าพื้นที่ โดยต้องกรอกข้อมูลความต้องการ และรายละเอียดตามแบบกำหนดสิทธิ์การเข้าออกพื้นที่ที่ทาง ศทส. กำหนด

3.2.2 ต้องได้รับอนุมัติสิทธิ์ในการเข้าออกพื้นที่ จากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายก่อน จึงจะเข้าออกพื้นที่ได้

3.2.3 ผู้มาติดต่อจะถูกบันทึกรายละเอียดข้อมูลลงในทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การบริหารจัดการการเข้าถึงของผู้ใช้งาน	รหัสเอกสาร : IC-0202

การบริหารจัดการการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์

เพื่อให้เจ้าหน้าที่ใช้เป็นมาตรการในการควบคุมและบริหารจัดการการเข้าถึงของผู้ใช้งาน โดยอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. เท่านั้น

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน

- 1.1 เสริมเนื้อหาเพื่อสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ เข้ากับหลักสูตรฝึกอบรมต่างๆ ตามแผนการฝึกอบรมของ สป.พม.
- 1.2 เผยแพร่ประชาสัมพันธ์และให้ความรู้ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ อย่างสม่ำเสมอ ในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยให้มีการปรับเปลี่ยนเกร็ดความรู้ให้ทันสมัยอยู่เสมอ
- 1.3 จัดฝึกอบรมผู้ใช้งานเพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. ได้อย่างถูกต้อง รวมถึงให้ตระหนักและเข้าใจถึงภัยไซเบอร์และผลกระทบที่เกิดจากการใช้งานโดยไม่ระมัดระวัง

2. การลงทะเบียนผู้ใช้งาน (User Registration)

- 2.1 จัดเตรียมแบบฟอร์มลงทะเบียนผู้ใช้งาน ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. โดยต้องระบุข้อมูลพื้นฐานอย่างน้อย ดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน
- 2.2 ตรวจสอบและให้สิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. ที่เหมาะสมต่อหน้าที่ความรับผิดชอบของผู้ใช้งาน
- 2.3 ระงับหรือเพิกถอนสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. โดยทันที เมื่อผู้ใช้งานนั้นเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือลาออก

3. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

- 3.1 การแจ้งขอเปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. จะต้องจัดทำเป็นลายลักษณ์อักษร และระบุเหตุผลความจำเป็น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การบริหารจัดการการเข้าถึงของผู้ใช้งาน	รหัสเอกสาร : IC-0202

- 3.2 กำหนดสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. เฉพาะการปฏิบัติงานในหน้าที่เท่านั้น โดยต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
- 3.3 กำหนดระดับสิทธิ์ที่เหมาะสมในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.
- 3.4 พิจารณามอบหมายสิทธิ์ให้สอดคล้องตามแนวปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ
- 3.5 กรณีจำเป็นต้องให้สิทธิ์พิเศษหรือสิทธิ์สูงสุดกับผู้ใช้งาน พิจารณาดังนี้
 - 3.5.1 ผู้ใช้งานนั้นต้องได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
 - 3.5.2 กำหนดระดับการเข้าถึงและใช้งานระบบอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่เป็นที่จำเป็นเท่านั้น
 - 3.5.3 กำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง
 - 3.5.4 กำหนดรหัสผ่านให้ต่างจากรหัสผู้ใช้งานตามปกติ และให้เปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น เปลี่ยนรหัสผ่านทุกครั้งหลังจากหมดความจำเป็นในการใช้งาน หรือหากมีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น
- 3.6 ผู้ใช้งานต้องรับทราบสิทธิ์และปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. อย่างเคร่งครัด
- 3.7 หากตรวจพบว่าผู้ใช้งานมีการกระทำความผิดหรือละเมิดต่อแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. เจ้าหน้าที่ต้องทำการระงับหรือเพิกถอนสิทธิ์ของผู้ใช้งานนั้นทันที
- 3.8 เมื่อผู้ใช้งานมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ เจ้าหน้าที่ต้องทำการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งานนั้นทันที
- 3.9 การเพิกถอนสิทธิ์ของผู้ใช้งานออกจากระบบ
 - 3.9.1 กรณีเป็นเจ้าหน้าที่ของ สป.พม. ให้เพิกถอนเมื่อผู้ใช้งานนั้นมีการเปลี่ยนแปลงตำแหน่งหน้าที่ความรับผิดชอบหรือลาออกหรือพ้นสภาพจากการเป็นเจ้าหน้าที่ของ สป.พม. หรือเมื่อไม่มีการเข้าใช้งานเป็นระยะเวลาติดต่อกันเกิน 90 วัน
 - 3.9.2 กรณีเป็นบุคคลจากหน่วยงานภายนอก ให้เพิกถอนตามวันที่ระบุในแบบฟอร์มลงทะเบียนผู้ใช้งาน หรือเมื่อไม่มีการเข้าใช้งานเป็นระยะเวลาติดต่อกันเกิน 30 วัน

4. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

- 4.1 กำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการคาดเดาโดยผู้อื่นและแตกต่างกัน
- 4.2 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านให้มีความยากต่อการคาดเดาโดยผู้อื่น
- 4.3 ส่งมอบรหัสผ่านให้กับผู้ใช้งานด้วยวิธีที่มีความมั่นคงปลอดภัย โดยหลีกเลี่ยงการใช้อีเมลฟรีของเอกชนเป็นช่องทางในการส่งมอบ
- 4.4 กำหนดขั้นตอนปฏิบัติในการบริหารจัดการรหัสผ่านของผู้ใช้งานที่มีความมั่นคงปลอดภัย ดังนี้

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การบริหารจัดการการเข้าถึงของผู้ใช้งาน	รหัสเอกสาร : IC-0202

- 4.4.1 รหัสผ่านควรมีความยาวอย่างน้อย 12 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ
- 4.4.2 ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- 4.4.3 ผู้ใช้งานควรเปลี่ยนรหัสผ่านทุกๆ 6 เดือน หรือตามที่ผู้ดูแลระบบกำหนด
- 4.4.4 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานแฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านระบบเครือข่ายคอมพิวเตอร์
- 4.4.5 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- 4.4.6 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- 4.5 กรณีตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกระงับสิทธิ์การใช้งานชั่วคราว จนกว่าจะดำเนินการเปลี่ยนรหัสผ่านเป็นที่เรียบร้อยแล้ว

5. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

- 5.1 ทบทวนสิทธิ์และปรับปรุงบัญชีผู้ใช้งาน ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเปลี่ยนแปลงตำแหน่ง ย้ายหน่วยงาน ลาออก หรือสิ้นสุดการจ้างงาน
- 5.2 ทบทวนสิทธิ์และปรับปรุงบัญชีผู้ใช้งาน สำหรับผู้ใช้งานที่มีสิทธิ์ในระดับสูง ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น สิทธิ์ในระดับผู้ดูแลระบบ
- 5.3 ตรวจสอบและติดตามการใช้งานของผู้ใช้งานตามสิทธิ์ที่ได้รับในแต่ละระบบอย่างสม่ำเสมอ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การรักษาความมั่นคงปลอดภัยบนเครือข่าย	รหัสเอกสาร : IC-0203

การรักษาความมั่นคงปลอดภัยบนเครือข่าย

วัตถุประสงค์

เพื่อเป็นมาตรการในการติดตั้งและกำหนดค่าต่างๆ ของระบบเครือข่ายและอุปกรณ์เครือข่าย ได้แก่ ไฟร์วอลล์ (Firewall) ระบบตรวจจับและป้องกันการบุกรุก (IDPS) การป้องกันมัลแวร์และไวรัส (Anti-Malware/Anti-Virus) และระบบเครือข่ายไร้สาย (Wireless LAN) โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ปฏิบัติที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเครือข่ายของ สป.พม.

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเครือข่ายของ สป.พม.

แนวปฏิบัติ

1. ผู้ดูแลระบบมีหน้าที่ความรับผิดชอบ ดังนี้

1.1 การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

- 1.1.1 ติดตั้ง กำหนดค่า และบริหารจัดการไฟร์วอลล์ เพื่อกำหนดค่าต่างๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน และสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายภายในของ สป.พม.
- 1.1.2 ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น จึงจะสามารถเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ได้
- 1.1.3 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
- 1.1.4 ทุกเส้นทางที่เชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาต จะต้องถูกปฏิเสธโดยไฟร์วอลล์
- 1.1.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
- 1.1.6 สำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า
- 1.1.7 ระบบเครื่องคอมพิวเตอร์แม่ข่ายสารสนเทศที่เข้าถึงบริการได้จากทั้งภายในและภายนอกทั้งหมด ต้องถูกติดตั้งใน Demilitarized Zone (DMZ) และต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ
- 1.1.8 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การรักษาความมั่นคงปลอดภัยบนเครือข่าย	รหัสเอกสาร : IC-0203

- 1.1.9 ให้บริการเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย โดยอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น และจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง
- 1.1.10 ให้บริการเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์บนเครือข่าย ตามที่ได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยต้องระบุข้อมูล ดังนี้
 - (1) หมายเลข Port ที่ต้องการขอให้เปิด
 - (2) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร
 - (3) วัตถุประสงค์หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้นๆ
 - (4) วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้
 - (5) ผู้ดูแล/ผู้รับผิดชอบ/ผู้พัฒนาระบบ
- 1.1.11 ให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย โดยเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทาง ศทส. อนุญาตให้ใช้งานเท่านั้น หากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อ นอกเหนือจากที่กำหนด จะต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายก่อน
- 1.1.12 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในของ สป.พม. จะต้องดำเนินการผ่าน VPN เท่านั้น และต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายก่อน และต้องบันทึกรายการที่ได้ดำเนินการตามที่ขอไว้ด้วย
- 1.1.13 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยเป็นไปตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
- 1.1.14 ระวังการใช้งานระบบเครือข่ายและอินเทอร์เน็ต สป.พม. ของเครื่องคอมพิวเตอร์ลูกข่ายทันที หากพบว่า มีพฤติกรรมการใช้งานที่ขัดต่อประกาศหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ สป.พม. หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศของ สป.พม. จนกว่าจะได้รับการแก้ไข
- 1.1.15 ยกเลิกการให้บริการระบบเครือข่ายและอินเทอร์เน็ต สป.พม. ของผู้ใช้งานทันที หากพบว่า ผู้ใช้งานมีเจตนาใช้งานที่ขัดต่อประกาศหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ สป.พม. หรือกฎหมาย หรือการทำงานของโปรแกรมที่อาจทำให้เกิดความเสี่ยงต่อความปลอดภัยหรือทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของ สป.พม.

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การรักษาความมั่นคงปลอดภัยบนเครือข่าย	รหัสเอกสาร : IC-0203

1.2 การรักษาความมั่นคงปลอดภัยของระบบตรวจจับและป้องกันการบุกรุก (IDPS Policy)

- 1.2.1 ติดตั้ง กำหนดค่า และบริหารจัดการระบบตรวจจับและป้องกันการบุกรุก เพื่อตรวจสอบความปลอดภัยของระบบเครือข่าย และป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนระบบเครือข่ายภายใน ของ สป.พม. ให้มีความมั่นคงปลอดภัย
- 1.2.2 ตรวจสอบ และ Update Patch/Signature ของ IDPS เป็นประจำ
- 1.2.3 ตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้ง host-based IDPS เป็นประจำทุกวัน
- 1.2.4 ตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลที่มีการใช้งานระบบเครือข่าย เป็นประจำทุกวัน
- 1.2.5 บันทึกผลการตรวจสอบโฮสต์และระบบเครือข่ายทั้งหมดที่มีการส่งข้อมูลผ่าน IDPS
- 1.2.6 การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้นานอย่างน้อย 90 วัน
- 1.2.7 ทำการลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ เพื่อลดความเสียหายและป้องกันเหตุการณ์ที่อาจเกิดขึ้นอีกในอนาคต
- 1.2.8 จัดทำรายงานแสดงผลการตรวจสอบการบุกรุก เป็นประจำทุกเดือน
- 1.2.9 IDPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงระบบเครือข่ายของระบบสารสนเทศตามปกติ
- 1.2.10 IDPS Policy จะต้องครอบคลุมทุกโฮสต์ในระบบเครือข่ายและระบบเครือข่ายข้อมูลของ สป.พม. ทั้งหมด รวมถึงเส้นทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทางที่ข้อมูลอาจเดินทาง
- 1.2.11 ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะ จะต้องผ่านการตรวจสอบจาก IDPS
- 1.2.12 หากตรวจพบว่าระบบมีการทำงานผิดปกติ จะต้องรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายทราบ ทันทีที่ตรวจพบ
- 1.2.13 หากตรวจพบว่ามีพฤติกรรมการใช้งาน หรือกิจกรรม หรือเหตุการณ์ที่น่าสงสัย ซึ่งมีความเสี่ยงต่อการบุกรุกและการโจมตีระบบ หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายทราบ ทันทีที่ตรวจพบ
- 1.2.14 ยกเลิกการเชื่อมต่อระบบเครือข่ายของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

1.3 การป้องกันมัลแวร์และไวรัส (Anti-Malware/Anti-Virus Policy)

- 1.3.1 จัดหาโปรแกรมบริหารจัดการระบบป้องกันไวรัสจากส่วนกลาง และโปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การรักษาความมั่นคงปลอดภัยบนเครือข่าย	รหัสเอกสาร : IC-0203

- 1.3.2 ติดตั้ง กำหนดค่า และบริหารจัดการโปรแกรมป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย เพื่อป้องกันไม่ให้เกิดความเสียหายต่อข้อมูลในเครื่องคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตของ สป.พม. โดยโปรแกรมป้องกันไวรัสต้องมีคุณสมบัติตรวจจับและป้องกันไวรัส เวิร์ม โทรจัน สปายแวร์ ได้เป็นอย่างดี
- 1.3.3 ติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องที่มีการเชื่อมต่อกับระบบเครือข่ายของ สป.พม.
- 1.3.4 ปรับปรุงระบบฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์เสียหายจากไวรัสคอมพิวเตอร์
- 1.3.5 หากโปรแกรมป้องกันไวรัสมีการปรับเปลี่ยนรุ่น จะต้องดำเนินการปรับเปลี่ยนรุ่นตามโปรแกรมล่าสุดให้กับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายทั้งหมด
- 1.3.6 หากตรวจพบหรือมีปัญหาจากไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย จะต้องตัดการเชื่อมต่อกับระบบเครือข่ายทันที และดำเนินการตรวจสอบและแก้ไขปัญหาให้แล้วเสร็จ
- 1.3.7 จัดทำรายงานแสดงผลการป้องกันไวรัสของระบบคอมพิวเตอร์ สป.พม. เป็นประจำทุกเดือน

1.4 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless LAN Policy)

- 1.4.1 ติดตั้ง กำหนดค่า และบริหารจัดการระบบเครือข่ายไร้สาย เพื่อควบคุมการเข้าถึงและสร้างความมั่นคงปลอดภัยของการทำงานของระบบเครือข่ายไร้สายของ สป.พม.
- 1.4.2 การติดตั้งอุปกรณ์เครือข่ายไร้สายในพื้นที่ สป.พม. ต้องได้รับความเห็นชอบจาก ศทส. ก่อน
- 1.4.3 ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น จึงจะสามารถเข้าถึงฟังก์ชันที่ใช้ในการตั้งค่าของจุดเชื่อมต่อระบบเครือข่ายไร้สายได้
- 1.4.4 จุดเชื่อมต่อระบบเครือข่ายไร้สาย จะต้องมีการกำหนดค่า Gateway ที่เป็นค่าที่กำหนดไว้ของระบบเครือข่ายส่วนนั้นเท่านั้น
- 1.4.5 ทุกจุดเชื่อมต่อระบบเครือข่ายไร้สายและอุปกรณ์ที่เกี่ยวข้อง เช่น Access Point จุดเชื่อมต่อสายสัญญาณ Switch จะต้องมีความปลอดภัย และมีรูปแบบในการจัดเก็บและเข้าถึงอุปกรณ์
- 1.4.6 SSID (Service Set Identifier) ที่กำหนด จะต้องถูกต้องตามรูปแบบที่ ศทส. กำหนดไว้ และจะต้องไม่มีการบ่งบอกหรือแสดงตำแหน่งของสาย ที่จุดเชื่อม LAN หรือชื่ออื่นๆ
- 1.4.7 เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน
- 1.4.8 SSID ที่ Broadcast จะให้บริการเฉพาะระบบเครือข่ายภายนอก ยกเว้นจุดที่ ศทส. อนุญาตให้ใช้ระบบเครือข่ายภายใน สป.พม. จะต้องยกเลิกค่าการ Broadcast SSID

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การรักษาความมั่นคงปลอดภัยบนเครือข่าย	รหัสเอกสาร : IC-0203

- 1.4.9 อุปกรณ์ที่ ศทส. อนุญาตให้ใช้ระบบเครือข่ายภายใน สป.พม. จะต้องระบุ SSID ที่ถูกต้อง จึงจะสามารถใช้งานได้
- 1.4.10 SNMP จะต้องถูกยกเลิกหากไม่จำเป็นสำหรับการบริหารจัดการระบบเครือข่าย หรือหากมีความจำเป็นต้องใช้จะต้องมีการเปลี่ยนแปลงค่าเริ่มต้น (Default) ของ Community String
- 1.4.11 กำหนดให้มีการ Authentication ทุกครั้งก่อนการใช้งาน ด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User password)
- 1.4.12 กำหนดรายการ MAC Address ให้สามารถเข้าใช้ Access Point ได้ เฉพาะเครื่องคอมพิวเตอร์ ที่อนุญาตเท่านั้น และตามรหัสผู้ใช้ (User account) และรหัสผ่าน (User password) ที่กำหนดไว้เท่านั้น
- 1.4.13 ยกเลิกการเชื่อมต่อระบบเครือข่ายไร้สายของอุปกรณ์ทุกชนิด ที่ไม่เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ สป.พม. หรือมีความเสี่ยงต่อระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้ทราบล่วงหน้า
- 1.4.14 ห้ามไม่ให้ผู้ดูแลระบบ บอกค่าติดตั้งของระบบเครือข่ายไร้สายกับผู้ใช้งานหรือบุคคลภายนอก
- 1.4.15 ระบบเครือข่ายไร้สายสำหรับให้บริการระบบอินเทอร์เน็ต จะต้องติดตั้งโดยแยกระบบเครือข่ายไร้สาย ออกจากระบบเครือข่ายภายใน LAN เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก
- 1.4.16 หากจำเป็นต้องเชื่อมต่อระบบเครือข่ายไร้สายกับระบบเครือข่ายภายใน LAN จะต้องเลือกใช้ เทคโนโลยี Authentication และมีการกำหนดค่าการเข้ารหัสในการเชื่อมต่อแบบ WPA2 เป็นอย่างน้อย
- 1.4.17 การเข้าถึงระบบเครือข่ายไร้สาย ต้องแบ่งแยกการใช้งานให้แตกต่างกันตามความจำเป็นของผู้ใช้งาน และกำหนดรหัสการเข้าใช้งานตามวัตถุประสงค์ของการใช้งาน
- 1.4.18 อุปกรณ์ที่ใช้ในการเข้าถึงระบบเครือข่ายของ สป.พม. จะต้องรองรับมาตรฐาน IEEE 802.11g/n เป็นอย่างน้อย หากอุปกรณ์ที่ใช้เป็นเครื่องคอมพิวเตอร์ส่วนบุคคล จะต้องมีการติดตั้งโปรแกรม ป้องกันไวรัสที่เครื่องด้วย
- 1.4.19 ตรวจสอบอุปกรณ์ติดตั้ง การกำหนดค่า และจัดการจุดเชื่อมต่อระบบเครือข่ายไร้สายอย่างสม่ำเสมอ
- 1.4.20 Wireless LAN Policy สามารถเปลี่ยนแปลงตามเทคโนโลยีใหม่ๆ และกระบวนการที่สอดคล้อง และเหมาะสมในอนาคตได้

2. ผู้ใช้งานมีหน้าที่ความรับผิดชอบ ดังนี้

- 2.1 ก่อนการใช้งานระบบเครือข่ายและอินเทอร์เน็ตของ สป.พม. ผู้ใช้งานต้องมีการ Authentication ทุกครั้ง ด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User password)
- 2.2 สำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์
- 2.3 ห้ามปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัส ที่ สป.พม. ติดตั้งให้

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การรักษาความมั่นคงปลอดภัยบนเครือข่าย	รหัสเอกสาร : IC-0203

- 2.4 มีส่วนร่วมในการบำรุงรักษาโปรแกรมป้องกันไวรัสที่ใช้ โดยตรวจสอบว่า มีการ Update โปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ ศทส. ทราบ หากไม่สามารถ Update โปรแกรมป้องกันไวรัสให้ทันสมัยได้
- 2.5 แจ้งให้ ศทส. ทราบทันที เมื่อพบว่าคอมพิวเตอร์หรือโปรแกรมที่ใช้มีความผิดปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส
- 2.6 ตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นด้วยโปรแกรมป้องกันไวรัสทุกครั้ง เมื่อมีการนำมาติดตั้งหรือใช้งาน และหากตรวจพบไวรัสจะต้องจัดการทำลายไวรัสโดยเร็วที่สุด
- 2.7 หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมที่นำมาใช้งานได้ ห้ามทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปในเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เด็ดขาด
- 2.8 ห้ามนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access Point, Wireless Router, Wireless USB client หรือ Wireless Card
- 2.9 กรณีที่ผู้ใช้งานพยายามเข้าถึงระบบโดยมิชอบ หรือโจมตีระบบ หรือมีพฤติกรรมการใช้งานที่ขัดต่อประกาศหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ สป.พม. ซึ่งอาจทำให้เกิดความเสี่ยงต่อความปลอดภัยและความเสียหายต่อระบบเทคโนโลยีสารสนเทศของ สป.พม. ผู้ใช้งานจะถูกจับหรือยกเลิกการใช้งานระบบเครือข่ายและอินเทอร์เน็ตของ สป.พม. ทันที
- 2.10 กรณีที่ผู้ใช้งานได้กระทำการใดๆ ที่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของ สป.พม. ผู้ใช้งานจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 4 : การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)	รหัสเอกสาร : IC-0204

การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน จำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน
2. กำหนดเกณฑ์ในการอนุญาตให้เข้าใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้
 - 2.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง
 - (1) อ่านอย่างเดียว
 - (2) สร้างข้อมูล
 - (3) ป้อนข้อมูล
 - (4) แก้ไขข้อมูล
 - (5) อนุมัติ
 - (6) ไม่มีสิทธิ์
 - 2.2 กำหนดเกณฑ์การระงับ/เพิกถอนสิทธิ์ ให้เป็นไปตามแนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งานที่ได้กำหนดไว้
 - 2.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบที่ได้รับมอบหมาย
3. กำหนดเกณฑ์ในการควบคุมการใช้งานสารสนเทศ ดังนี้
 - 3.1 จัดแบ่งประเภทของระบบสารสนเทศ
 - (1) ด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลคำรับรอง ข้อมูลงบประมาณการเงินและบัญชี และข้อมูลระบบบริหารราชการ (Back Office)
 - (2) ด้านการให้บริการ ได้แก่ ข้อมูลผู้รับบริการทางสังคม

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 4 : การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)	รหัสเอกสาร : IC-0204

3.2 จัดแบ่งลำดับความสำคัญของระบบสารสนเทศ

- (1) มากที่สุด
- (2) ปานกลาง
- (3) น้อย

3.3 จัดแบ่งลำดับชั้นความลับของระบบสารสนเทศ

- (1) ลับที่สุด
- (2) ลับมาก
- (3) ลับ

3.4 จัดแบ่งระดับชั้นการเข้าถึงของระบบสารสนเทศ

- (1) เข้าถึงได้เฉพาะผู้ใช้งานที่มีสิทธิ์สูงสุด
- (2) เข้าถึงได้เฉพาะผู้ใช้งานที่ได้รับอนุมัติสิทธิ์เท่านั้น
- (3) เข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง
- (4) เข้าถึงได้ทุกกลุ่มผู้ใช้งาน

3.5 กำหนดเวลาในการเข้าถึงระบบสารสนเทศ

- (1) ในเวลาราชการ (08.30 - 16.30 น.)
- (2) นอกเวลาราชการ (นอกช่วงเวลา 08.30 - 16.30 น.)
- (3) ในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนขัตฤกษ์)
- (4) ในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงเวลาการเข้าถึง)

3.6 กำหนดช่องทางการเข้าถึงระบบสารสนเทศ

- (1) ระบบเครือข่ายบริเวณเฉพาะที่ (LAN) ในลักษณะ Client Server
- (2) ระบบอินทราเน็ต (Intranet) ในลักษณะ Web Base Application
- (3) ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application
- (4) ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 4 : การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)	รหัสเอกสาร : IC-0204

ตารางสรุปการควบคุมการใช้งานสารสนเทศของ สป.พม.

เวลาการเข้าถึง	ประเภทของระบบสารสนเทศ	ลำดับความสำคัญ	ลำดับชั้นความลับ	ระดับชั้นการเข้าถึง	ช่องทางการเข้าถึง
ในเวลาราชการ (08.30-16.30 น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- กลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้งาน	- ระบบเครือข่ายบริเวณเฉพาะที่ (LAN) - ระบบอินทราเน็ต (Intranet) - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN
นอกเวลาราชการ (นอกช่วงเวลา 08.30-16.30 น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- กลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้งาน	- ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN
ในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดชดเชย)	- ด้านการบริหาร - ด้านการให้บริการ	- ปานกลาง - น้อย	-	- กลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้งาน	- ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN
ในช่วงเวลาพิเศษ เป็นรายครั้ง (ระบุช่วงเวลาการเข้าถึง)	- ด้านการบริหาร - ด้านการให้บริการ	มากที่สุด	ลับที่สุด	- ผู้ใช้งานที่มีสิทธิ์สูงสุด - ผู้ใช้งานที่ได้รับอนุมัติสิทธิ์เท่านั้น	- ระบบเครือข่ายบริเวณเฉพาะที่ (LAN) - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN

4. กำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ

4.1 การควบคุมการเข้าถึงสารสนเทศ โดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศ ดังนี้

4.1.1 ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงาน ถูกจำกัดไว้ที่

(1) บุคลากร และกิจกรรมที่ได้รับอนุญาต

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 4 : การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)	รหัสเอกสาร : IC-0204

(2) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

4.1.2 ในส่วนที่เกี่ยวข้องกับภาระหน้าที่การตรวจสอบการเข้าถึงบริการที่สำคัญของหน่วยงาน ต้องกำหนดให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Profile) สำหรับแต่ละโหนดการเข้าถึงบริการที่สำคัญ

4.1.3 ต้องเก็บรักษาบันทึกการเข้าถึงทั้งหมด (Log of All Access) และความพยายามในการเข้าถึงบริการที่สำคัญของหน่วยงาน รวมทั้งตรวจสอบบันทึกเพื่อหากิจกรรมที่ผิดปกติเป็นประจำ และความสอดคล้องกับความถี่หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

4.1.4 ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ เช่น USB, Serial Port และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยหน่วยงาน และดำเนินการภายในสถานที่ (หากเป็นไปได้)

4.2 การปรับปรุงให้สอดคล้อง มีการปรับปรุงแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศ ให้สอดคล้องกับการใช้งานตามภารกิจและด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 5 : การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)	รหัสเอกสาร : IC-0205

การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การใช้งานบริการเครือข่ายของ สป.พม.

- 1.1 ห้ามผู้ใดเข้าใช้งานบริการเครือข่ายของ สป.พม. โดยไม่ได้รับอนุญาต หากบุกรุกหรือพยายามบุกรุก ถือว่าเป็นการพยายามรุกรานล้ำเขตหวงห้ามของทางราชการ
- 1.2 ผู้ที่ประสงค์จะใช้งานบริการเครือข่ายของ สป.พม. จะต้องขออนุญาตจากผู้ดูแลระบบก่อน
- 1.3 ผู้ใช้งานจะได้รับสิทธิ์ให้ใช้งานบริการเครือข่ายของ สป.พม. ได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- 1.4 ผู้ใช้งานที่ได้รับสิทธิ์ให้ใช้งานบริการเครือข่ายของ สป.พม. จะได้รับบัญชีผู้ใช้งาน (Account) เป็นการเฉพาะบุคคลเท่านั้น ซึ่ง Account จะประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) โดยผู้ใช้งานจะโอนหรือแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้
- 1.5 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ทุกครั้งที่เข้าใช้งานบริการเครือข่ายของ สป.พม.
- 1.6 ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ
- 1.7 ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมออนไลน์เพื่อความบันเทิงทุกประเภท ในเวลาราชการ
- 1.8 ห้ามผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 5 : การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)	รหัสเอกสาร : IC-0205

- 1.9 ห้ามผู้ใช้งานละเมิดต่อผู้อื่น เช่น ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มีใช้ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว สป.พม. ไม่มีส่วนร่วมรับผิดชอบต่อความเสียหายดังกล่าว

2. การใช้งานบริการเครือข่ายของ สป.พม. จากภายนอก

- 2.1 ผู้ใช้งานต้องขออนุญาตและได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถเข้าใช้งานบริการเครือข่ายของ สป.พม. จากภายนอกได้ และจะเข้าใช้ได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- 2.2 ผู้ใช้งานที่เข้าใช้งานบริการเครือข่ายของ สป.พม. จากภายนอก หรือ Internet จะต้องเชื่อมต่อด้วยวิธีการ Remote Access ผ่าน VPN
- 2.3 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ของตนเองเพื่อยืนยันตัวตนทุกครั้งที่ใช้บริการเครือข่ายของ สป.พม. จากภายนอก

3. การระบุอุปกรณ์บนเครือข่าย

- 3.1 ระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล หมายเลข MAC Address และหมายเลข IP Address
- 3.2 ใช้ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อกำหนดว่าหมายเลขระบุอุปกรณ์ใดที่สามารถเข้าถึงเครือข่ายส่วนใดของ สป.พม.
- 3.3 อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- 3.4 รักษาความมั่นคงปลอดภัยทางกายภาพต่ออุปกรณ์เครือข่ายหรืออุปกรณ์คอมพิวเตอร์ เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์เหล่านั้น
- 3.5 จัดเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- 3.6 กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่า สามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่
- 3.7 จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวข้องกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย
- 3.8 ทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง

4. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

- 4.1 ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งทางกายภาพ และโดยการล็อกอินเข้ามาใช้งาน
- 4.2 ล็อกอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่า Configuration ด้วยกุญแจ เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์ และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 5 : การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)	รหัสเอกสาร : IC-0205

- 4.3 ยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน
- 4.4 กำหนดการเปิด - ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงและก่อให้เกิดความเสียหายต่อระบบเครือข่าย
- 4.5 ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอหรืออย่างน้อยสัปดาห์ละ 2 ครั้ง
- 4.6 ติดตั้งระบบป้องกันและตรวจสอบการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. อย่างปลอดภัย เช่น ระบบชีวภาพ (Biometric) หรือ สมาร์ทการ์ด (Smartcard) และติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม เป็นต้น
- 4.7 ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. หากมีความจำเป็น ต้องแจ้งให้ผู้ดูแลระบบเป็นผู้รับผิดชอบนำพาเข้าไปเท่านั้น
- 4.8 กำหนดสิทธิบุคคลในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยให้เฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องเท่านั้น

5. การแบ่งแยกเครือข่าย

- 5.1 แยกกลุ่มเครือข่ายเป็น 7 ประเภทใหญ่ๆ คือ
 - 1) เครือข่ายภายนอก (External)
 - 2) ส่วนที่มีการให้บริการสาธารณะ (Demilitarized Zone : DMZ) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก
 - 3) เครือข่ายภายใน (Internal)
 - 4) เครือข่ายสำหรับบริการเชื่อมต่อไร้สาย (Wireless Device)
 - 5) เครือข่ายสำหรับงานบริหารจัดการศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ (DC)
 - 6) เครือข่ายสำหรับติดตั้งระบบงานสารสนเทศต่างๆ ของ สป.พม. (Applications)
 - 7) เครือข่ายสำหรับติดตั้งระบบฐานข้อมูล (Database)
- 5.2 แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่าย โดยไม่ได้รับอนุญาต
- 5.3 แบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบงานต่างๆ ของ สป.พม.
- 5.4 แยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของ สป.พม.
- 5.5 ใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ
- 5.6 ใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอก สป.พม.
- 5.7 กรองและจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อย
- 5.8 ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่ง จะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวงเครือข่ายหนึ่งได้โดยตรง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 5 : การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)	รหัสเอกสาร : IC-0205

5.9 ควบคุมการเข้าถึงทางกายภาพสำหรับเครือข่ายย่อย เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อย และป้องกันการเปลี่ยนแปลงแก้ไขสายสัญญาณ ดักแอบดูข้อมูลบนเครือข่าย หรืออื่นๆ โดยไม่ได้รับอนุญาต

5.10 จัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยมีการปรับปรุงให้เป็นปัจจุบัน อยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง

6. การควบคุมการเชื่อมต่อทางเครือข่าย

6.1 ตรวจสอบและจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่าย ให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง และข้อกำหนดของระบบงาน

6.2 จำกัดสิทธิ์และความสามารถของผู้ใช้งานในการเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่าย สป.พม.

6.3 จำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานต่อระบบงานต่างๆ ของ สป.พม. อาทิ ระบบงานที่ใช้ในการส่งข้อความ (Messaging applications) เช่น ระบบอีเมล ระบบงานสำหรับการโอนย้ายไฟล์ ระบบงานต่างๆ สำหรับใช้งานภายใน สป.พม.

6.4 จำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งาน ตามวันที่ เวลา หรือช่วงเวลาที่ยินยอมให้ใช้งาน

6.5 ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่าย สป.พม. โดยไม่ได้รับอนุญาต

6.6 ระบุอุปกรณ์และเครื่องมือที่ใช้ในการควบคุมการเชื่อมต่อระบบเครือข่าย สป.พม.

6.7 ใช้ไฟร์วอลล์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย ให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง

6.8 ป้องกันเลขที่อยู่ของไอพี (IP Address) ของระบบเครือข่ายภายใน สป.พม. มิให้หน่วยงานภายนอก ที่เชื่อมต่อสามารถมองเห็นได้

6.9 ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของ สป.พม. ในลักษณะที่ผิดปกติ

6.10 การเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก สป.พม. จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก ซึ่งมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware)

6.11 ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายใน สป.พม. เพื่อให้สามารถเข้าถึงเครื่องแม่ข่ายสำหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็น หรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบก่อนดำเนินการ

6.12 กำหนดระยะเวลาที่แน่นอนของการเชื่อมต่อจากระยะไกล เช่น ให้ใช้ในระยะเวลา 7 วัน และหลังจากที่สิ้นสุดการใช้งาน ให้ทำการปิดช่องทางการเชื่อมต่อทันทีโดยทันที

7. การควบคุมการจัดเส้นทางบนเครือข่าย

7.1 ใช้เกตเวย์หรืออุปกรณ์เครือข่ายเพื่อตรวจสอบ IP Address ของทั้งต้นทางและปลายทาง และควบคุมการไหลของข้อมูลผ่านเครือข่ายต่างๆ จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง

7.2 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย IP Address

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 5 : การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)	รหัสเอกสาร : IC-0205

- 7.3 กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายในและภายนอก
- 7.4 จำกัดการใช้เส้นทางบนเครือข่ายจากคอมพิวเตอร์ไปยังเครื่องแม่ข่าย โดยไม่อนุญาตให้ผู้ให้บริการสามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น
- 7.5 กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิ์ในการเข้าใช้บริการระบบเครือข่าย สป.พม.

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 6 : การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	รหัสเอกสาร : IC-0206

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. ขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

- 1.1 ผู้ที่ประสงค์จะเข้าถึงระบบปฏิบัติการของ สป.พม. จะต้องขออนุญาตและได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบอย่างเป็นลายลักษณ์อักษรก่อน
- 1.2 ผู้ใช้งานจะได้รับสิทธิ์ให้เข้าถึงระบบปฏิบัติการของ สป.พม. ได้แต่เพียงระบบที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- 1.3 ผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าถึงระบบปฏิบัติการของ สป.พม. จะได้รับบัญชีผู้ใช้งาน (Account) เป็นการเฉพาะบุคคลเท่านั้น ซึ่ง Account จะประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) โดยผู้ใช้งานจะโอนหรือแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้
- 1.4 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ทุกครั้งที่เข้าถึงระบบปฏิบัติการของ สป.พม.
- 1.5 จำกัดระยะเวลาและจำนวนครั้งในการป้อนรหัสผ่าน เช่น หากผู้ใช้งานป้อนรหัสผ่านผิดเกิน 3 ครั้ง ระบบจะต้องทำการล็อกสิทธิ์ไม่ให้ผู้ใช้งานนั้นเข้าถึงระบบปฏิบัติการได้ จนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อกให้
- 1.6 การใช้งานเครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบ ผู้ใช้งานต้องทำการกำหนดรหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ให้กับเครื่องคอมพิวเตอร์
- 1.7 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของตนในการใช้งานเครื่องคอมพิวเตอร์ร่วมกัน
- 1.8 ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อล็อกหน้าจอคอมพิวเตอร์เมื่อไม่มีการใช้งาน และกำหนดให้ต้องใส่รหัสผ่าน เมื่อต้องการเข้าใช้งานใหม่
- 1.9 ผู้ใช้งานต้องลงบันทึกออก (Logout) ทันที เมื่อเลิกใช้งานเครื่องคอมพิวเตอร์หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 6 : การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	รหัสเอกสาร : IC-0206

- 1.10 ห้ามผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว
- 1.11 ผู้ใช้งานสามารถขอใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ของ สป.พม. ได้ตามหน้าที่ความจำเป็นเท่านั้น
- 1.12 ซอฟต์แวร์ที่ สป.พม. จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น
- 1.13 ห้ามผู้ใช้งานใช้ทรัพยากรทุกประเภทที่เป็นของ สป.พม. เพื่อประโยชน์ทางการค้า
- 1.14 ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ
- 1.15 ในกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม
- 1.16 ห้ามผู้ใช้งานใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. ในการควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาต

2. การระบุและยืนยันตัวตนของผู้ใช้งาน

- 2.1 ผู้ดูแลระบบต้องตั้งชื่อบัญชีผู้ใช้งาน (Account) แต่ละประเภทแตกต่างกัน เช่น บัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบ บัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนาระบบ บัญชีของเจ้าหน้าที่ทางเทคนิคอื่นๆ เป็นต้น
- 2.2 ผู้ใช้งานทุกคนต้องมีบัญชีผู้ใช้งาน (Account) เฉพาะของแต่ละบุคคลแยกจากกัน เพื่อใช้ในการพิสูจน์ตัวตน
- 2.3 สำหรับระบบที่มีความสำคัญสูง ต้องกำหนดให้ผู้ใช้งานพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคงปลอดภัยสูง เช่น ใช้วิธีการเข้ารหัสข้อมูล วิธีการทางชีวภาพ (อาทิ การใช้ลายนิ้วมือ เรตินา ฝ่ามือ เสียง)

3. ระบบบริหารจัดการรหัสผ่าน

- 3.1 ให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับบัญชีผู้ใช้งาน (Account) จากผู้ดูแลระบบ หรือเมื่อเข้าใช้งานระบบเป็นครั้งแรก
- 3.2 ให้ผู้ใช้งานสามารถตั้งหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนการยืนยันรหัสผ่านใหม่ที่ตั้งอีกครั้ง
- 3.3 ให้ผู้ใช้งานสามารถตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่นได้ เช่น ไม่ใช่ชื่อ นามสกุล วันเดือนปีเกิด หมายเลขโทรศัพท์ คำจากพจนานุกรม เป็นต้น
- 3.4 ให้มีการแจ้งเตือนข้อผิดพลาดในการตั้งรหัสผ่านของผู้ใช้งาน เช่น รหัสผ่านมีความยาวของตัวอักษรจะน้อยกว่าที่กำหนด มีรหัสผู้ใช้งานอยู่ในรหัสผ่าน เป็นต้น
- 3.5 ให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุกๆ 3 เดือน
- 3.6 ให้มีการจัดเก็บรหัสผ่านเดิมที่ผู้ใช้งานเคยตั้งไปแล้ว เพื่อตรวจสอบไม่ให้นำกลับมาใช้ใหม่ตามระยะเวลาที่เหมาะสม

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 6 : การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	รหัสเอกสาร : IC-0206

- 3.7 ไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอ ในขณะที่ผู้ใช้งานกำลังใส่ข้อมูลเพื่อใช้งานระบบ เช่น ให้แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอ เป็นต้น
- 3.8 ให้มีการป้องกันไฟล์ข้อมูลรหัสผ่านที่ได้มีการจัดเก็บไว้หรือที่จำเป็นต้องส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น ป้องกันโดยการเข้ารหัสข้อมูล (Encryption) พร้อมการคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้
- 3.9 การจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานจะต้องแยกต่างหากจากข้อมูลของระบบงาน

4. การใช้งานโปรแกรมมัลแวร์หรือโปรแกรมประเภทยูทิลิตี้

- 4.1 การจัดเก็บโปรแกรมมัลแวร์หรือโปรแกรมประเภทยูทิลิตี้ ต้องแยกจัดเก็บไว้ต่างหาก เช่น แยกไว้ในไดเรกทอรีที่ต่างจากไดเรกทอรีของซอฟต์แวร์ระบบงาน
- 4.2 จัดทำบัญชีรายชื่อโปรแกรมมัลแวร์หรือโปรแกรมประเภทยูทิลิตี้ ที่อนุญาตให้ใช้งานได้
- 4.3 ห้ามผู้ใช้งานทั่วไปใช้งานโปรแกรมมัลแวร์หรือโปรแกรมประเภทยูทิลิตี้ โดยจำกัดสิทธิ์ให้เฉพาะผู้ดูแลระบบหรือผู้ใช้งานที่ได้รับอนุญาตเท่านั้น
- 4.4 ผู้ใช้งานที่ต้องการใช้งานโปรแกรมมัลแวร์หรือโปรแกรมประเภทยูทิลิตี้ ต้องขออนุญาตจากผู้ดูแลระบบก่อน โดยระบุเหตุผลความจำเป็นหรือความต้องการใช้งาน และต้องให้ผู้บังคับบัญชาของผู้ใช้งานลงนามให้ความเห็นชอบเป็นลายลักษณ์อักษร
- 4.5 ผู้ใช้งานต้องขออนุญาตใช้งานโปรแกรมมัลแวร์หรือโปรแกรมประเภทยูทิลิตี้เป็นรายครั้ง และสามารถใช้งานได้ตามระดับสิทธิ์ที่ สป.พม. กำหนดเท่านั้น
- 4.6 มีการบันทึกข้อมูลล็อก (Log) เพื่อแสดงการใช้งานโปรแกรมมัลแวร์หรือโปรแกรมประเภทยูทิลิตี้
- 4.7 ยกเลิกหรือลบทิ้งโปรแกรมมัลแวร์หรือโปรแกรมประเภทยูทิลิตี้ ที่ไม่มีความจำเป็นต้องใช้งานแล้ว

5. การหมดเวลาใช้งานระบบสารสนเทศ

- 5.1 ให้มีการเคลียร์หน้าจอคอมพิวเตอร์เพื่อป้องกันไม่ให้ผู้อื่นเห็นข้อมูล หลังจากไม่มีกิจกรรมการใช้งานระบบสารสนเทศเป็นระยะเวลาเกิน 10 นาที
- 5.2 เมื่อไม่มีกิจกรรมการใช้งานระบบสารสนเทศในระยะเวลาหนึ่ง ต้องกำหนดให้มีการตัดและหมดเวลาการใช้งานระบบสารสนเทศ เช่น ตัดการใช้งานระบบทันทีหลังจากไม่มีการใช้งานเป็นระยะเวลาเกิน 10 นาที
- 5.3 สำหรับระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูง ต้องจำกัดระยะเวลาการเชื่อมต่อของระบบสารสนเทศนั้น เช่น ตัดการเชื่อมต่อของระบบทันทีหลังจากใช้งานเป็นระยะเวลาเกิน 30 นาที ต่อการพิสูจน์ตัวตน (Authentication) ใช้งาน
- 5.4 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) เพื่อใช้งานระบบสารสนเทศอีกครั้ง หลังจากที่ได้หมดเวลาการใช้งานไปแล้ว

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 7 : การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)	รหัสเอกสาร : IC-0207

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การจำกัดการเข้าถึงสารสนเทศ

1.1 กำหนดการควบคุมการเข้าถึงกับระบบงาน

- 1.1.1 แสดงข้อความเตือน เพื่อห้ามผู้ไม่มีสิทธิ์เข้าถึงระบบ
- 1.1.2 จำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลผิดในการล็อกอินได้
- 1.1.3 จำกัดช่วงระยะเวลาที่นานที่สุด ที่ผู้ใช้งานต้องล็อกอินเข้าใช้งานให้สำเร็จ
- 1.1.4 ส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่าผู้ใช้งานพยายามล็อกอินแต่ผิดพลาดหลายครั้ง
- 1.1.5 กำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบได้ ภายหลังจากที่ใส่ข้อมูลการล็อกอินผิดเกินกว่าจำนวนครั้งที่กำหนด
- 1.1.6 ตรวจสอบข้อมูลการล็อกอิน หลังจากผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว
- 1.1.7 บันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ
- 1.1.8 แสดงวันเวลาของการล็อกอินครั้งที่แล้วทั้งที่สำเร็จและไม่สำเร็จ
- 1.1.9 แสดงรายละเอียดของระบบเท่าที่จำเป็น หลังจากที่ได้ล็อกอินแล้ว
- 1.1.10 แสดงข้อมูลพื้นฐานเท่าที่จำเป็น เพื่อให้ผู้ใช้งานได้รับทราบข้อมูล
- 1.1.11 ใช้เมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบ
- 1.1.12 จำกัดสิทธิ์การเข้าถึงจากอีกระบบหนึ่ง โดยให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันที่จำเป็นต้องใช้งานเท่านั้น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 7 : การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)	รหัสเอกสาร : IC-0207

1.1.13 จำกัดการนำข้อมูลออกจากระบบ เพื่อให้เข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้องและจำเป็นในการนำไปใช้งานเท่านั้น

1.1.14 ไม่แสดงความช่วยเหลือใดๆ ในกรณีเกิดเหตุการณ์ไม่พึงประสงค์ขึ้นกับระบบ

1.1.15 จำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อทันทีเมื่อพ้นช่วงเวลาที่กำหนด

1.1.16 เปลี่ยนรหัสผ่านของระบบตามระยะเวลาที่กำหนด

1.2 กำหนดขั้นตอนและแบบฟอร์มในการเข้าถึงและใช้งานระบบ เพื่อกำหนดสิทธิผู้ใช้งานในการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบ และใช้ในการตรวจสอบและยืนยันตัวตนของผู้ใช้งาน เช่น สิทธิในการอ่าน เขียน ลบ หรือสั่งให้โปรแกรมทำงาน โดยแบบฟอร์มต้องระบุข้อมูลอย่างน้อย ดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน เหตุผล และระยะเวลาที่ขอเข้าถึงและใช้งานระบบ

1.3 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ตามมาตรฐานสากล

2. ระบบที่ไวต่อการรบกวน

2.1 กำหนดคุณลักษณะของระบบ โดยมีรายละเอียดอย่างน้อย ดังนี้ ประเภทของระบบ ลำดับความสำคัญ ลำดับชั้นความลับ ระดับชั้นการเข้าถึง เวลาในการเข้าถึง และช่องทางการเข้าถึง

2.2 ระบบที่ไวต่อการรบกวนและมีผลกระทบสูงต่อ สป.พม. โดยเป็นระบบที่มีลำดับชั้นความลับและมีลำดับความสำคัญมากที่สุด

2.3 ประเมินความเสี่ยงในการใช้ทรัพยากรร่วมกัน ระหว่างระบบที่ไวต่อการรบกวนกับระบบอื่นๆ เช่น ความเสี่ยงในการใช้เครื่องคอมพิวเตอร์เดียวกันในการให้บริการ

2.4 ติดตั้งระบบที่ไวต่อการรบกวนแยกไว้ในเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งต่างหาก

2.5 ควบคุมสภาพแวดล้อม อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอก สป.พม. ที่เกี่ยวข้องกับระบบที่ไวต่อการรบกวนโดยเฉพาะ

2.6 ควบคุมการเข้าใช้งานระบบที่ไวต่อการรบกวนจากเครือข่ายภายในและเครือข่ายภายนอก ตามที่ตั้งค่าไวไฟร์วอลล์

3. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

3.1 ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์หรือไม่

3.2 ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

3.3 เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รับนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

3.4 เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนให้อยู่ในสภาพพร้อมใช้งาน

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 7 : การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)	รหัสเอกสาร : IC-0207

3.5 หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบ
ต่อความเสียหายที่เกิดขึ้น

4. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

- 4.1 จัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสาร ไว้ให้กับ
ผู้ใช้งานจากระยะไกล
- 4.2 ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ของ สป.พม. จากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามแนวปฏิบัติในการรักษา
ความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 4.3 ตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ของ สป.พม. จากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนดหรือไม่
- 4.4 ผู้ใช้งานจากระยะไกลทุกคน ต้องทำการพิสูจน์ตัวตน (Authentication) ก่อนใช้งานระบบเทคโนโลยี
สารสนเทศและการสื่อสารของ สป.พม.
- 4.5 กำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของหน่วยงาน
ที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล
- 4.6 กำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน
และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล
- 4.7 สำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกลอย่างสม่ำเสมอ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 8 : การควบคุมการเข้าถึงของหน่วยงานภายนอก (outsource control)	รหัสเอกสาร : IC-0208

การควบคุมการเข้าถึงของหน่วยงานภายนอก (outsource control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงของหน่วยงานภายนอก (outsource control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.

- 1.1 ผู้ใช้งานต้องขออนุญาตล่วงหน้าก่อนวันที่จะเข้าออกพื้นที่ โดยต้องกรอกข้อมูลความต้องการและรายละเอียดตามแบบกำหนดสิทธิการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ที่ทาง ศทส. กำหนด
- 1.2 ผู้ใช้งานต้องได้รับอนุมัติสิทธิในการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. จากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน จึงจะเข้าออกพื้นที่ได้
- 1.3 ผู้ใช้งานจะถูกบันทึกรายละเอียดข้อมูลลงในทะเบียนผู้มีสิทธิเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.
- 1.4 ผู้ใช้งานต้องแลกบัตรที่ใช้ระบุตัวตนของแต่ละบุคคล เช่น บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ หรือบัตรอนุญาตเข้าออกภายในอาคารที่ได้แลกมาก่อนหน้า เป็นต้น เพื่อรับบัตรผู้มาติดต่อ (Visitor) และบันทึกข้อมูลลงในแบบบันทึกการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้งที่มีการเข้าออก
- 1.5 ผู้ใช้งานต้องติดบัตรผู้มาติดต่อ (Visitor) ตรงจุดที่สามารถมองเห็นได้ชัดเจน ตลอดเวลาที่อยู่ภายในพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.
- 1.6 กรณีที่ต้องการนำอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้ามาภายในบริเวณพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. จะต้องบันทึกรายการอุปกรณ์ที่นำเข้ามา ลงในแบบบันทึกการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ให้ถูกต้อง และจะต้องได้รับอนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร
- 1.7 ผู้ใช้งานต้องคืนบัตรผู้มาติดต่อ (Visitor) กับผู้ดูแลระบบ โดยผู้ดูแลระบบจะตรวจสอบแต่ละบุคคลและอุปกรณ์ พร้อมลงบันทึกเวลาออกและรายการอุปกรณ์ ในแบบบันทึกการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้งที่มีการเข้าออก

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 8 : การควบคุมการเข้าถึงของหน่วยงานภายนอก (outsourcing control)	รหัสเอกสาร : IC-0208

1.8 กรณีที่จะเข้ามาปฏิบัติงานในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ในวันหยุดหรือนอกเวลาราชการ จะต้องขออนุญาตจากผู้ดูแลระบบล่วงหน้าก่อนทุกครั้ง และการดำเนินงานจะต้องอยู่ในการกำกับดูแลของผู้ดูแลระบบเท่านั้น

2. การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

- 2.1 ผู้ใช้งานต้องขออนุญาตไว้ล่วงหน้าเป็นลายลักษณ์อักษรก่อนเข้าถึงระบบทุกครั้ง พร้อมทั้งแจ้งให้ผู้ดูแลระบบทราบ โดยต้องระบุข้อมูลอย่างน้อย ดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน เหตุผล โครงการที่รับจ้าง และระยะเวลาที่ขอเข้าถึงและใช้งานระบบ
- 2.2 ผู้ใช้งานต้องได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่าย บริหารจัดการผ่านระบบเครือข่าย และการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. ได้ และจะดำเนินการได้เฉพาะรายการที่ได้รับอนุญาตเท่านั้น
- 2.3 ผู้ใช้งานต้องทำการสำรองค่า Config ของอุปกรณ์ทุกชนิดภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โปรแกรม/โมดูลของระบบงานสารสนเทศ และโครงสร้างฐานข้อมูล ทุกครั้งก่อนแก้ไขหรือเปลี่ยนแปลงค่า รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไข หากการแก้ไขมีปัญหาเกิดขึ้นทำให้ไม่สามารถใช้งานระบบได้ ผู้ใช้งานจะต้องเรียกคืนข้อมูลที่ได้สำรองไว้กลับมา เพื่อให้ระบบสามารถใช้งานได้ตามสภาพเดิม
- 2.4 การเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายคอมพิวเตอร์ของ สป.พม. จะต้องดำเนินการ ดังนี้
 - 2.4.1 ขออนุญาตและได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถเชื่อมต่อจากภายนอกได้ โดยจะต้องระบุ บริการที่ขออนุญาต วัน เวลา และระยะเวลาในการเชื่อมต่อให้ชัดเจน
 - 2.4.2 จะต้องเชื่อมต่อด้วยวิธีการ Remote Access VPN
 - 2.4.3 จะต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ของตนเอง เพื่อยืนยันตัวตน ทุกครั้งที่เชื่อมต่อจากภายนอก
- 2.5 กรณีจำเป็นต้องสำเนาฐานข้อมูลทุกประเภทออกจาก สป.พม. จะต้องทำหนังสือขอความเห็นชอบจาก สป.พม. ล่วงหน้าก่อนทุกครั้ง โดยจะต้องระบุเหตุผลในการนำไปใช้งานอย่างชัดเจน และต้องรับผิดชอบต่อความเสียหายที่อาจจะเกิดขึ้นด้วย
- 2.6 กรณีที่ผู้ใช้งานประมาท ทำให้อุปกรณ์ และระบบสารสนเทศของ สป.พม. ได้รับความเสียหายหรือสูญหาย ผู้ใช้งานจะต้องรับผิดชอบในการซ่อมแซมแก้ไขหรือเปลี่ยนใหม่ให้อยู่ในสภาพที่สามารถใช้งานได้ดังเดิม
- 2.7 หากมีการเปลี่ยนแปลงรายชื่อผู้ใช้งาน จะต้องแจ้งให้ผู้ดูแลระบบทราบล่วงหน้าเป็นลายลักษณ์อักษรก่อนมีการเปลี่ยนแปลงทุกครั้ง
- 2.8 ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ที่กำหนดไว้โดยไม่มีข้อยกเว้น หากมีการฝ่าฝืน สป.พม. จะทำหนังสือแจ้งไปยังหน่วยงานของผู้ใช้งาน และจะไม่อนุญาตให้ดำเนินการใดๆ ภายใน สป.พม.

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 9 : การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	รหัสเอกสาร : IC-0209

การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

วัตถุประสงค์

เพื่อป้องกันระบบจากการถูกโจมตีทั้งจากภายในและภายนอก เช่น การเจาะระบบ การโจมตีด้วยมัลแวร์ และการโจมตีทางไซเบอร์อื่นๆ ลดความเสี่ยงจากช่องโหว่ ป้องกันข้อมูลสำคัญ รักษาความต่อเนื่องของการดำเนินงานได้อย่างปลอดภัยและมีประสิทธิภาพ และสร้างความมั่นคงปลอดภัยในระบบสารสนเทศของ สป.พม.

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. ต้องสร้างมาตรฐานกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของหน่วยงาน
2. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้
 - 2.1 Operating System Hardening ให้มีการกำหนดการตั้งค่าความปลอดภัยของระบบปฏิบัติการ เช่น Windows, Linux การปิดบริการหรือฟีเจอร์ที่ไม่จำเป็น เช่น Remote Desktop, FTP การอัปเดตแพตช์ และการแก้ไขช่องโหว่ความปลอดภัยของระบบปฏิบัติการอย่างสม่ำเสมอ
 - 2.2 Account and Access Control ให้มีการกำหนดนโยบายรหัสผ่านที่เข้มงวด (เช่น ความยาว ความซับซ้อน และการหมุนอายุของรหัสผ่าน) การจำกัดสิทธิ์ของผู้ใช้ (Least Privilege) โดยให้สิทธิ์เฉพาะที่จำเป็นต่อการทำงาน และการตั้งค่าการล็อกบัญชีหากมีการพยายามเข้าสู่ระบบล้มเหลวหลายครั้ง
 - 2.3 Network Security Configuration ให้มีการตั้งค่าการควบคุมการเข้าถึงเครือข่าย (Network Access Control) การตั้งค่าไฟร์วอลล์ และการกำหนดกฎการเข้าถึง (Access Control Lists, ACLs) การตั้งค่า VPN และการเข้ารหัสข้อมูลในการสื่อสารระหว่างระบบ
 - 2.4 Application Security ให้มีการกำหนดนโยบายการอัปเดตและแพตช์สำหรับซอฟต์แวร์แอปพลิเคชันต่างๆ การจำกัดการเข้าถึงและควบคุมสิทธิ์การใช้งานแอปพลิเคชัน และการตั้งค่าความปลอดภัยพื้นฐาน เช่น การใช้ SSL/TLS สำหรับเว็บเซิร์ฟเวอร์หรือแอปพลิเคชันที่ทำงานบนอินเทอร์เน็ต

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 9 : การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	รหัสเอกสาร : IC-0209

- 2.5 Audit and Logging ให้มีการตั้งค่าการบันทึกเหตุการณ์ (Event Logging) เพื่อให้สามารถตรวจสอบกิจกรรมในระบบได้ การเก็บบันทึกการเข้าถึงระบบและการใช้งานระบบเพื่อวิเคราะห์เหตุการณ์ผิดปกติหรือการโจมตี และการกำหนดนโยบายการจัดเก็บและการเข้าถึง Log เพื่อให้สอดคล้องกับกฎหมายหรือข้อบังคับที่เกี่ยวข้อง
- 2.6 Malware and Intrusion Protection ให้มีการติดตั้งและตั้งค่าซอฟต์แวร์ป้องกันไวรัส (Anti-Virus) และ Anti-Malware การติดตั้งระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection and Prevention System - IDS/IPS) และการอัปเดตและสแกนระบบเป็นประจำเพื่อหาไวรัสหรือภัยคุกคามอื่น ๆ
- 2.7 Data Protection and Encryption ให้มีการเข้ารหัสข้อมูลที่สำคัญทั้งในขณะพัก (Data at Rest) และขณะส่งผ่านเครือข่าย (Data in Transit) การใช้ระบบสำรองข้อมูล (Backup) และการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ การจำกัดการเข้าถึงข้อมูลที่สำคัญตามความจำเป็น
- 2.8 Patch Management ให้มีการอัปเดตและจัดการแพตช์ความปลอดภัยสำหรับระบบปฏิบัติการซอฟต์แวร์และเฟิร์มแวร์ต่างๆ การวางแผนการทดสอบและการอัปเดตแพตช์เพื่อไม่ให้เกิดปัญหาในการทำงานของระบบ
- 2.9 Physical Security Configuration ให้มีการกำหนดมาตรการความปลอดภัยทางกายภาพ เช่น การจำกัดการเข้าถึงเซิร์ฟเวอร์หรืออุปกรณ์เครือข่าย การใช้ระบบตรวจสอบการเข้าถึง (Access Control Systems) และกล้องวงจรปิด (CCTV) เพื่อป้องกันการบุกรุก
- 2.10 Backup and Recovery Procedures ให้มีการกำหนดนโยบายการสำรองข้อมูลที่สำคัญ การจัดเก็บข้อมูลสำรองในสถานที่ที่ปลอดภัย วางแผนและทดสอบกระบวนการกู้คืนข้อมูลหลังจากเกิดเหตุผิดปกติหรือการโจมตี
- 2.11 Mobile Device Security ให้มีการตั้งค่าความปลอดภัยบนอุปกรณ์พกพา เช่น การเข้ารหัสข้อมูล การตั้งรหัสผ่าน การจัดการอุปกรณ์ระยะไกล การใช้ Mobile Device Management (MDM) เพื่อควบคุมและจัดการความปลอดภัยของอุปกรณ์เคลื่อนที่ในหน่วยงาน
3. ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใดๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน
4. ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงาน อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรฐานมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์
5. ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 10 : การเชื่อมต่อระยะไกล (Remote Connection)	รหัสเอกสาร : IC-0210

การเชื่อมต่อระยะไกล (Remote Connection)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบภายในของ สป.พม. จากระยะไกลได้อย่างมั่นคงปลอดภัยและมีประสิทธิภาพ ลดความเสี่ยงจากการที่ผู้ไม่ประสงค์ดีหรือบุคคลภายนอกที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลหรือระบบที่สำคัญของ สป.พม.

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **เจ้าหน้าที่/ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. **ผู้ใช้งาน** หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. ต้องตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาตในการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของหน่วยงาน
2. การเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงาน ต้องได้รับอนุญาตอย่างเป็นทางการเป็นลายลักษณ์อักษรจากเจ้าหน้าที่ และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงให้เปิดใช้งานการเชื่อมต่อไปยังไซต์ระยะไกล เมื่อจำเป็นเท่านั้น โดยใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
3. การใช้ VPN (Virtual Private Network) กำหนดให้ใช้ VPN ในการเชื่อมต่อระยะไกลในการเข้าถึงเครือข่ายหรือระบบขององค์กรจากภายนอก ต้องทำการเชื่อมต่อที่เข้ารหัสผ่าน VPN เท่านั้น เพื่อเพิ่มความปลอดภัยในการสื่อสารและป้องกันการดักฟังข้อมูล
4. การจัดการบัญชีผู้ใช้และการเข้าถึง (User Access Management) หลักการสิทธิ์น้อยที่สุด (Least Privilege) ผู้ใช้งานควรได้รับสิทธิ์ในการเข้าถึงเฉพาะระบบหรือข้อมูลที่จำเป็นต่อการปฏิบัติงานเท่านั้น เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่จำเป็นและลดความเสี่ยงในการรั่วไหลของข้อมูล และการตั้งค่านโยบายที่ปลอดภัยโดยกำหนดให้ใช้รหัสผ่านที่มีความซับซ้อน เช่น ต้องมีความยาวขั้นต่ำและมีตัวอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ รวมถึงบังคับให้เปลี่ยนรหัสผ่านเป็นระยะๆ
5. การเข้ารหัสข้อมูล (Data Encryption) เข้ารหัสข้อมูลที่ส่งผ่านการเชื่อมต่อระยะไกลทุกการเชื่อมต่อและการรับ - ส่งข้อมูลระหว่างผู้ใช้และระบบต้องใช้ในการเข้ารหัส (Encryption) เพื่อป้องกันการดักฟังและการโจมตีจากผู้ไม่ประสงค์ดี และใช้โปรโตคอลการสื่อสารที่ปลอดภัย เช่น SSL/TLS สำหรับเว็บแอปพลิเคชัน และ SSH สำหรับการเชื่อมต่อไปยังเซิร์ฟเวอร์

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 10 : การเชื่อมต่อระยะไกล (Remote Connection)	รหัสเอกสาร : IC-0210

6. การตรวจสอบและติดตาม (Monitoring and Logging) บันทึกข้อมูลการเข้าถึง (Access Logging) ทุกครั้งที่มีการเชื่อมต่อระยะไกลเข้าสู่ระบบ รวมถึงการบันทึกเวลา, ชื่อผู้ใช้, IP Address ที่ใช้ และกิจกรรมที่ทำบนระบบ เพื่อใช้ในการตรวจสอบเหตุการณ์ผิดปกติ และให้ระบบมีการแจ้งเตือนเหตุการณ์ผิดปกติ หากพบว่าการพยายามเข้าถึงระบบที่ผิดปกติ เช่น มีความพยายามเข้าสู่ระบบหลายครั้งโดยไม่สำเร็จ หรือมีการเชื่อมต่อจากตำแหน่งที่ไม่คุ้นเคย ควรมีระบบแจ้งเตือนหรือระบบป้องกันการบุกรุก (Intrusion Detection System - IDS)
7. การรักษาความปลอดภัยของอุปกรณ์ที่ใช้เชื่อมต่อใช้ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่ได้รับการอัปเดตอย่างสม่ำเสมอ และต้องอัปเดตแพตช์ความปลอดภัย (Patch Management) ที่ได้รับการอัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้ทันสมัยเพื่อปิดช่องโหว่ของระบบ
8. ผู้ใช้งานเชื่อมต่อระยะไกลห้ามเชื่อมต่อกับระบบขององค์กรผ่านเครือข่าย Wi-Fi สาธารณะที่ไม่มีการเข้ารหัส หรือมีมาตรการความปลอดภัยต่ำ เนื่องจากเสี่ยงต่อการถูกโจมตีหรือดักฟังข้อมูล ซึ่งหากจำเป็นต้องใช้เครือข่ายสาธารณะ ควรใช้ VPN เพื่อรักษาความปลอดภัยในการเชื่อมต่อ
9. ต้องมีการกำหนดสิทธิ์ใช้งาน เวลาที่อนุญาตให้เชื่อมต่อ และรูปแบบการใช้งานที่ปลอดภัย รวมถึงกำหนดขอบเขตการเชื่อมต่อ โดยตั้งค่าการเข้าถึงเฉพาะบางส่วนของระบบที่จำเป็นต้องใช้สำหรับการทำงานระยะไกลเท่านั้น เพื่อลดความเสี่ยงในการโจมตีทั้งระบบ สำหรับบุคคลภายนอก อาจกำหนดสิทธิ์การเข้าถึงระบบแบบชั่วคราวหรือจำกัดเวลาในการใช้งานเพื่อลดความเสี่ยงในการใช้งานที่ผิดปกติ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 11 : การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Bring Your Own Device)	รหัสเอกสาร : IC-0211

การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Bring Your Own Device)

วัตถุประสงค์

เพื่อกำหนดแนวทางการใช้งานอุปกรณ์คอมพิวเตอร์พกพา และการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงานให้เป็นไปอย่างมั่นคงปลอดภัย และเพื่อเป็นการป้องกันมิให้เกิดการรั่วไหลหรือสูญหายของข้อมูลจากการใช้อุปกรณ์คอมพิวเตอร์พกพา และการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

คำจำกัดความ

อุปกรณ์คอมพิวเตอร์พกพา ที่กำหนดในนโยบายนี้ หมายถึง อุปกรณ์คอมพิวเตอร์พกพาใดๆ ที่ใช้ในการเชื่อมต่อเข้าสู่ระบบเครือข่าย และ/หรือ ที่ใช้ในการเก็บรักษาข้อมูล ดังต่อไปนี้

- สมาร์ทโฟน โทศัพท์เคลื่อนที่ และอุปกรณ์มือถือ
- แท็บเล็ต
- Thumb-Drive
- External Hard disk

แนวปฏิบัติ

1 การใช้อุปกรณ์คอมพิวเตอร์พกพา

- 1.1 ผู้ใช้งานต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. อย่างเคร่งครัด เมื่อมีการใช้งานเครื่องคอมพิวเตอร์พกพา หรืออุปกรณ์คอมพิวเตอร์พกพาอื่นๆ
- 1.2 อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการตรวจสอบ เพื่อให้มั่นใจว่าปราศจากซอฟต์แวร์ที่ไม่ได้รับอนุญาต ไวรัสคอมพิวเตอร์ หรือโปรแกรมมัลแวร์ต่างๆ ก่อนที่จะได้รับอนุญาตให้เชื่อมต่อเข้าสู่ระบบเครือข่ายของ สป.พม.
- 1.3 ผู้ใช้งานอุปกรณ์คอมพิวเตอร์พกพาต้องทำการปกป้องอุปกรณ์ และข้อมูลที่อยู่ในอุปกรณ์เหล่านั้นอย่างเหมาะสม
- 1.4 ผู้ใช้งานคอมพิวเตอร์พกพาต้องมีการปกป้องทางกายภาพของอุปกรณ์คอมพิวเตอร์พกพาเหล่านั้นอย่างเหมาะสม
- 1.5 การติดตั้งซอฟต์แวร์ในอุปกรณ์คอมพิวเตอร์พกพาต้องเป็นไปตามที่ ศทส. กำหนดเท่านั้น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 11 : การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Bring Your Own Device)	รหัสเอกสาร : IC-0211

- 1.6 อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการปรับปรุงเวอร์ชันและติดตั้ง Patch ของอุปกรณ์คอมพิวเตอร์พกพาเหล่านั้นให้ทันสมัยอยู่เสมอ
- 1.7 ศทส. ไม่อนุญาตให้ทำการ Jailbreak (สำหรับ iOS) หรือ Rooted (สำหรับ Android) ในอุปกรณ์สมาร์ทโฟน
- 1.8 อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส และต้องได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ
- 1.9 ข้อมูลที่เป็นความลับหรือมีความอ่อนไหวสูงที่อยู่บนอุปกรณ์คอมพิวเตอร์พกพา ต้องได้รับการเข้ารหัสข้อมูลตาม Encryption Standard ของ ศทส. เพื่อป้องกันไม่ให้ข้อมูลรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลเหล่านั้นได้
- 1.10 อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์พกพาเหล่านั้นโดยการกำหนดรหัสผ่านที่มั่นคงปลอดภัย
- 1.11 อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการสำรองข้อมูลที่มีความสำคัญที่ถูกจัดเก็บไว้บนอุปกรณ์เหล่านั้นอย่างสม่ำเสมอ

2. การใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน

- 2.1 ศทส. มีสิทธิ์ในการปฏิเสธการเข้าใช้งานจากอุปกรณ์คอมพิวเตอร์ส่วนตัวของผู้ใช้งานในการเข้าถึงข้อมูลและระบบสารสนเทศของ สป.พม. หาก ศทส. พบว่าอุปกรณ์ดังกล่าวอาจก่อให้เกิดความเสี่ยงต่อข้อมูลและระบบสารสนเทศของ สป.พม.
- 2.2 ศทส. มีสิทธิ์ในการติดตั้งโปรแกรมทำลายข้อมูล (Self-Destruct) บนอุปกรณ์คอมพิวเตอร์ส่วนตัวของผู้ใช้งานที่นำมาใช้ปฏิบัติงาน โดย ศทส. อาจจะมีการส่งลบข้อมูลบนอุปกรณ์คอมพิวเตอร์ส่วนตัวของผู้ใช้งานในกรณีที่เกิดเหตุการณ์การรั่วไหลหรือความไม่ปลอดภัยของข้อมูล
- 2.3 ศทส. มีสิทธิ์ที่จะตรวจสอบอุปกรณ์คอมพิวเตอร์ส่วนตัวที่มีการใช้งานกับ Infrastructure ของ สป.พม. และหากผู้ใช้งานปฏิเสธการตรวจสอบ ศทส. สามารถยกเลิกสิทธิ์ในการเข้าถึง รวมทั้ง User ID และ Password ของผู้ใช้งานได้
- 2.4 ก่อนที่ผู้ใช้งานจะนำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาใช้งานภายใน สป.พม. ผู้ใช้งานจะต้องได้รับการอนุมัติและลงทะเบียนอุปกรณ์คอมพิวเตอร์ส่วนตัวนั้นกับ ศทส. ก่อน โดยที่ผู้ใช้งานจะต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. อย่างเคร่งครัด เพื่อความมั่นคงปลอดภัยด้านสารสนเทศของ สป.พม.
- 2.5 ผู้ใช้งานที่ต้องการเข้าถึงข้อมูลภายในของ สป.พม. จากเครือข่ายที่ไม่ใช่เครือข่ายของ สป.พม. จะต้องทำการติดตั้งและเปิดการใช้งาน Personal Firewall และ Antivirus รวมถึงซอฟต์แวร์อื่นๆ ที่จำเป็นที่ถูกกำหนดโดย ศทส.

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 11 : การใช้งานคอมพิวเตอร์แบบพกพา (Bring Your Own Device)	รหัสเอกสาร : IC-0211

- 2.6 อุปกรณ์คอมพิวเตอร์ส่วนตัวทั้งหมดที่เข้าถึงเครือข่ายของ สป.พม. จะสามารถถูกตรวจสอบได้ว่าได้รับอนุญาตจาก ศทส. แล้วหรือไม่ หากพบว่าเป็นอุปกรณ์คอมพิวเตอร์ส่วนตัวที่ไม่ได้รับอนุญาตและพยายามที่จะเข้าถึงเครือข่ายของ สป.พม. จะถูกปฏิเสธการเข้าถึงทันที
- 2.7 อุปกรณ์คอมพิวเตอร์ส่วนตัวจะสามารถเข้าถึงเครือข่ายและข้อมูลของ สป.พม. โดยการใช้งานผ่าน SSL/TLS VPN โดยข้อมูลการเข้าถึง SSL/TLS VPN Portal ของ สป.พม. จะถูกส่งให้ผู้ใช้งานเมื่อได้รับอนุญาตจาก ศทส.
- 2.8 ผู้ใช้งานที่ใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. อย่างเคร่งครัด
- 2.9 อุปกรณ์คอมพิวเตอร์ส่วนตัวต้องได้รับการป้องกันการเข้าถึงโดยใช้รหัสผ่าน และข้อมูลที่อยู่ในอุปกรณ์คอมพิวเตอร์ส่วนตัวต้องมีการเข้ารหัสข้อมูล โดยผู้ใช้งานสามารถมาตรฐานการเข้ารหัสข้อมูลได้จาก Encryption Standard
- 2.10 ผู้ใช้งานที่ใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวต้องเก็บรักษารหัสผ่านโดยไม่ให้บุคคลอื่นทราบ โดยเฉพาะบุคคลภายในครอบครัว หากมีการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวทำงานที่บ้าน
- 2.11 ผู้ใช้งานที่มีการใช้งานอุปกรณ์คอมพิวเตอร์ส่วนตัวต้องมีการป้องกันทางด้านกายภาพของเครื่องทั้งในขณะที่ใช้งานและในขณะที่มีการเคลื่อนย้ายอุปกรณ์ โดยการป้องกันเหล่านี้รวมถึงการป้องกันด้วยรหัสผ่าน การเข้ารหัสข้อมูล และการป้องกันทางด้านกายภาพของอุปกรณ์คอมพิวเตอร์ส่วนตัวที่มีข้อมูลของ สป.พม. โดยหากอุปกรณ์คอมพิวเตอร์ส่วนตัวมีการ Synchronize กับอุปกรณ์อื่นๆ อุปกรณ์นั้นๆ จะต้องได้รับการติดตั้งและเปิดการใช้งาน Antivirus และ Anti-malware และซอฟต์แวร์อื่นๆ ที่ถูกกำหนดให้มีการติดตั้งโดย ศทส.
- 2.12 Antivirus signature บนอุปกรณ์คอมพิวเตอร์ส่วนตัวต้องได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ
- 2.13 รหัสผ่านและข้อมูลความลับอื่นๆ ที่ถูกกำหนดโดย ศทส. ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ต้องได้รับการเข้ารหัสบนอุปกรณ์คอมพิวเตอร์ส่วนตัว

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 12 : การเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)	รหัสเอกสาร : IC-0212

การเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)

วัตถุประสงค์

เพื่อกำหนดและควบคุมสิทธิ์การเข้าถึงและการใช้งานการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ เพื่อลดความเสี่ยงป้องกันความเสี่ยงด้านความปลอดภัยของข้อมูลและระบบภายในองค์กร โดยกำหนดมาตรการเพื่อควบคุมการใช้งาน การป้องกันการรั่วไหลของข้อมูล และการป้องกันมัลแวร์หรือไวรัส จากอุปกรณ์ภายนอกที่นำเข้ามาใช้กับระบบเครือข่ายและบริการสำคัญของ สป.พม.

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. ควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ กับเครือข่ายคอมพิวเตอร์ และบริการที่สำคัญของ สป.พม. อย่างเข้มงวด โดยมีมาตรการในการปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้และเปิดใช้งานเมื่อจำเป็นเท่านั้น
2. ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของข้อมูลบริการที่สำคัญของ สป.พม. บนสื่อบันทึกข้อมูลแบบถอดได้
3. การอนุญาตใช้งานอนุญาตให้ใช้เฉพาะสื่อบันทึกข้อมูลแบบถอดได้ที่ผ่านการตรวจสอบและได้รับอนุญาตจากเจ้าหน้าที่แล้วเท่านั้นที่สามารถเชื่อมต่อกับระบบของ สป.พม. ได้
4. ก่อนใช้งานสื่อบันทึกข้อมูลแบบถอดได้ทุกครั้ง ต้องทำการสแกนหาไวรัสและมัลแวร์ด้วยโปรแกรมป้องกันที่เป็นมาตรฐาน เพื่อป้องกันการนำมัลแวร์เข้าสู่ระบบเครือข่าย และต้องมีการบล็อกอุปกรณ์สื่อบันทึกข้อมูลที่ไม่ผ่านการรับรองหรือตรวจสอบ เพื่อป้องกันการเชื่อมต่ออุปกรณ์ที่ไม่ปลอดภัย
5. ข้อมูลที่ถูกเก็บหรือถ่ายโอนผ่านสื่อบันทึกข้อมูลแบบถอดได้ควรได้รับการเข้ารหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตในกรณีที่อุปกรณ์สูญหายหรือถูกขโมย และควรเลือกใช้ซอฟต์แวร์หรือเทคโนโลยีการเข้ารหัสที่เป็นมาตรฐานสากล
6. การถ่ายโอนข้อมูลระหว่างระบบและสื่อบันทึกข้อมูลแบบถอดได้ควรถูกจำกัดเฉพาะข้อมูลที่ต้องใช้งานจริงเท่านั้น เพื่อลดความเสี่ยงในการรั่วไหลของข้อมูลสำคัญ และข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับขององค์กร ควรมีมาตรการเข้มงวดในการควบคุมการถ่ายโอนผ่านสื่อบันทึกข้อมูลแบบถอดได้ หรือห้ามถ่ายโอนโดยเด็ดขาด

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 12 : การเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)	รหัสเอกสาร : IC-0212

7. การใช้งานสื่อบันทึกข้อมูลแบบถอดได้ต้องมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูล เช่น สิทธิ์ในการอ่านหรือเขียนข้อมูลบนอุปกรณ์ เพื่อให้มั่นใจว่าผู้ใช้งานมีสิทธิ์เพียงพอในการใช้งาน กรณีบุคคลภายนอก ควรมีมาตรการควบคุมการใช้งานสื่อบันทึกข้อมูลอย่างเข้มงวด เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูลแบบชั่วคราว หรือการอนุญาตเป็นรายกรณี
8. ระบบควรมีการบันทึกข้อมูลการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ทุกครั้ง เช่น เวลาที่เชื่อมต่อ, ผู้ใช้, ไฟล์ที่ถูกถ่ายโอน และข้อมูลอุปกรณ์ เพื่อใช้ในการตรวจสอบในกรณีที่มีเหตุการณ์ผิดปกติ และควรมีการแจ้งเตือนเมื่อพบการใช้งานที่น่าสงสัย หรือเมื่อมีการเชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาต
9. เมื่อสิ้นสุดการใช้งานหรือเมื่อต้องการลบข้อมูลจากสื่อบันทึกข้อมูลแบบถอดได้ ควรใช้เทคนิคการลบข้อมูลที่ปลอดภัย (Secure Erase) เพื่อให้แน่ใจว่าข้อมูลไม่สามารถกู้คืนได้ กรณีอุปกรณ์สื่อบันทึกข้อมูลแบบถอดได้ที่ไม่ใช่แล้วหรือเสื่อมสภาพ ควรถูกทำลายอย่างปลอดภัย เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 13 : การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์	รหัสเอกสาร : IC-0213

การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์

วัตถุประสงค์

เพื่อใช้เป็นแนวทางในการดำเนินการรับมือ ป้องกัน ภัยคุกคามทางไซเบอร์ของมัลแวร์ ในการดูแลระบบสารสนเทศที่สำคัญ และให้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ส่งผลต่อบริการภาครัฐ และจากเหตุภัยคุกคามที่เกิดขึ้นในปัจจุบัน เพื่อให้หน่วยงานสามารถรับมือและป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์และภัยคุกคามต่างๆ ได้อย่างทันสถานการณ์

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. มาตรการเตรียมความพร้อมในการรับมือ

- 1.1 จัดทำหรือทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงาน ให้ครอบคลุมการสำรองข้อมูล การควบคุมการเข้าถึงเครือข่ายและระบบสารสนเทศ และการประเมินความเสี่ยง

1.2 สำรองข้อมูลที่สำคัญ

- 1.2.1 การสำรองข้อมูล ควรจัดทำอย่างน้อย 2 เวอร์ชัน ไว้ในอุปกรณ์จัดเก็บข้อมูลที่ไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ ยกเว้นเวลาสำรองข้อมูล และในการสำรองข้อมูลแต่ละเวอร์ชันให้มีการจัดเก็บลงในอุปกรณ์ที่แตกต่างกัน

- 1.2.2 ทดสอบการกู้คืนข้อมูลที่สำรองเพื่อให้แน่ใจว่าสามารถนำมาใช้งานได้เมื่อต้องการ

1.3 ควบคุมการเข้าถึงเครือข่าย และระบบสารสนเทศ

- 1.3.1 แยกส่วนเครือข่าย (Network segregation) ของระบบสารสนเทศตามรูปแบบการให้บริการ เพื่อลดผลกระทบจากการแพร่กระจายมัลแวร์ผ่านเครือข่าย

- 1.3.2 ทบทวนการกำหนดสิทธิการเข้าถึงเครือข่ายและระบบสารสนเทศตามความจำเป็น การแบ่งแยกหน้าที่ (need to know, least privilege, separation of duties) รวมถึงควรตั้งค่าควบคุมในลักษณะการอนุญาตให้ใช้งานตามรายการสิทธิที่กำหนดไว้เท่านั้น (whitelisting)

- 1.3.3 กำหนดให้มีการยืนยันตัวตน (authentication) ตามสิทธิในการเข้าถึงเครือข่าย และระบบสารสนเทศ โดยไม่อนุญาตให้แชร์บัญชีผู้ใช้งาน

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 13 : การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์	รหัสเอกสาร : IC-0213

1.4 ประเมินความเสี่ยงด้านระบบสารสนเทศและภัยไซเบอร์

- 1.4.1 จัดทำหรือทบทวนทะเบียนสินทรัพย์ (inventory of asset) รวมถึงข้อมูลที่สำคัญในการให้บริการ
- 1.4.2 จัดทำหรือทบทวนแผนผังการเชื่อมต่อเครือข่าย และระบบสารสนเทศที่ให้บริการ
- 1.4.3 จัดทำข้อมูลการติดต่อสำหรับผู้ดูแลหรือผู้ให้บริการสินทรัพย์ และเครือข่ายเพื่อเตรียมความพร้อมในกรณีที่ต้องการประสานการแก้ไขปัญหา หรือรับมือสถานการณ์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น
- 1.4.4 ระบุความเสี่ยงที่อาจเกิดขึ้นสำหรับการให้บริการ เพื่อพิจารณาช่องทางสำรองสำหรับให้บริการกรณีที่ช่องทางหลักได้รับผลกระทบ
- 1.4.5 จัดเตรียมเครื่องมือ อุปกรณ์ และทรัพยากรที่จำเป็นสำหรับการให้บริการช่องทางสำรอง

1.5 จัดเก็บบันทึกกิจกรรม (log) ไปยังพื้นที่จัดเก็บในส่วนกลางที่มีการควบคุมการเข้าถึงอย่างรัดกุม เพื่อให้แน่ใจว่าข้อมูลดังกล่าวจะไม่ถูกทำลายหรือเปลี่ยนแปลง โดยบันทึกกิจกรรมควรครอบคลุม ดังนี้

- 1.5.1 ข้อมูลการใช้งานระบบสารสนเทศ เช่น application log
- 1.5.2 ข้อมูลการเชื่อมต่อทางเครือข่ายหรือระบบป้องกันการโจมตีทางเครือข่าย เช่น firewall log, intrusion prevention system (IPS) log
- 1.5.3 ข้อมูลบันทึกกิจกรรมของระบบปฏิบัติการ เช่น event log, system log, security log, audit log
- 1.5.4 การจัดเก็บข้อมูล log ควรมีระยะเวลาในการจัดเก็บที่เหมาะสมเพื่อประโยชน์ในการนำมาใช้งานภายหลัง ทั้งนี้ อาจพิจารณากำหนดระยะเวลาในการจัดเก็บตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการโดยอนุโลม

1.6 ทบทวน และยกเลิกบริการที่ไม่จำเป็นบนเครื่องให้บริการ

1.7 กำหนดเจ้าหน้าที่ประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับบริหารกับระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

1.8 ให้ความรู้กับผู้ใช้งานในหน่วยงานเกี่ยวกับการป้องกันตนเองจากโปรแกรมประสงค์ร้ายหรือมัลแวร์

2. มาตรการการดูแลสารสนเทศที่สำคัญ

2.1 การสำรองข้อมูลในอุปกรณ์จัดเก็บข้อมูล ควรมีการเข้ารหัสลับเพื่อป้องกันความเสี่ยงจากการเข้าถึงข้อมูลในอุปกรณ์กรณีที่อุปกรณ์นั้นสูญหาย รวมถึงควรพิจารณานำอุปกรณ์จัดเก็บข้อมูลที่สำรองข้อมูลแล้วไปเก็บยังนอกพื้นที่หน่วยงาน

2.2 ป้องกันการติดมัลแวร์

- 2.2.1 ติดตั้งโปรแกรมตรวจจับมัลแวร์บนเครื่องให้บริการ และเครื่องผู้ใช้งาน
- 2.2.2 อัปเดตซอฟต์แวร์ที่ใช้ให้บริการเป็นเวอร์ชันล่าสุด
- 2.2.3 ใช้ระบบป้องกันการโจมตีทางเครือข่าย เช่น intrusion prevention system (IPS)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 13 : การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์	รหัสเอกสาร : IC-0213

2.2.4 ตรวจสอบพฤติกรรมของมัลแวร์ด้วยระบบหรือกลไกที่เหมาะสม เช่น การตรวจสอบการเชื่อมต่อทางเครือข่ายของเครื่องคอมพิวเตอร์ไปยังไอพีแอดเดรสหรือโดเมนของเครื่องควบคุมมัลแวร์ (command and control server) การตรวจสอบค่าแฮชของไฟล์มัลแวร์

2.2.5 ตรวจสอบความผิดปกติของรายการบัญชีผู้ใช้งาน และข้อมูลบันทึกกิจกรรม (log) อย่างสม่ำเสมอ

2.2.6 ตรวจสอบช่องโหว่ (vulnerability assessment) ของระบบสารสนเทศ หรือซอฟต์แวร์ที่ให้บริการอย่างสม่ำเสมอ และให้รีบแก้ไขช่องโหว่ทันทีหากพบว่าเป็นความเสี่ยงที่รุนแรง

2.2.7 ลงทะเบียนเพื่อขอรับการสนับสนุนเกี่ยวกับข้อมูลแจ้งเตือนภัยคุกคามทางไซเบอร์ และการดำเนินการตามมาตรการป้องกันและตรวจจับภัยคุกคามดังกล่าว

3. การดำเนินการกรณีพบความเสียหายที่เกิดขึ้นจากมัลแวร์

3.1 ตัดการเชื่อมต่อทางเครือข่าย

3.1.1 เครื่องคอมพิวเตอร์ที่ติดมัลแวร์ เพื่อป้องกันการกระจายของมัลแวร์ไปยังระบบสารสนเทศอื่น

3.1.2 ระบบสำรองข้อมูล รวมถึงการเชื่อมต่ออุปกรณ์จัดเก็บข้อมูลภายนอก เพื่อป้องกันข้อมูลสำรองถูกเข้ารหัสลับ

3.1.3 ระบบสารสนเทศที่อยู่ในเครือข่ายเดียวกัน เพื่อป้องกันการกระจายของมัลแวร์ไประบบดังกล่าว

3.2 สำรองข้อมูลที่ยังใช้งานได้อยู่จากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ ไปยังอุปกรณ์บันทึกข้อมูลภายนอก ซึ่งไม่ควรเป็นอุปกรณ์เดียวกับที่ใช้สำรองข้อมูลตามปกติ

4. การดำเนินการเพิ่มเติม ดังนี้

4.1 แจ้งเหตุไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และไทยเซิร์ต

4.2 เปลี่ยนรหัสผ่านที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงรหัสผ่านที่ใช้งานผ่านระบบควบคุมบัญชีผู้ใช้งานทั้งหมด

4.3 ตรวจสอบสายพันธุ์ของมัลแวร์ โดยอาศัยข้อมูลที่ปรากฏในเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ เช่น นามสกุลของไฟล์ที่เปลี่ยนไป ข้อความที่ปรากฏบนหน้าจอในการเรียกค่าไถ่ เพื่อประเมินวิธีการแก้ไขปัญหาการกู้คืนข้อมูล

4.4 หากมีความประสงค์ในการใช้เครื่องมือถอดรหัสลับข้อมูล ควรทำในสภาพแวดล้อมที่ไม่มีการเชื่อมต่อทางเครือข่าย เพื่อลดความเสี่ยงที่อาจเกิดจากการใช้เครื่องมือดังกล่าว

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 14 : การใช้งานระบบเครือข่ายไร้สาย	รหัสเอกสาร : IC-0214

การใช้งานระบบเครือข่ายไร้สาย

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ สป.พม. โดยการกำหนดสิทธิ์ของผู้ใช้งานตามความเหมาะสม ผู้ใช้งานต้องผ่านการพิสูจน์ตัวตนจริงและได้รับการอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การลงทะเบียนผู้ใช้งาน

- 1.1 ผู้ขอใช้งานเครือข่ายไร้สายของ สป.พม. จะต้องลงทะเบียนเพื่อขอใช้งานจากผู้ดูแลระบบก่อน โดยการกรอกข้อมูลส่วนบุคคลในแบบฟอร์มลงทะเบียนที่ สป.พม. กำหนดไว้
- 1.2 ผู้ใช้งานต้องยอมรับและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. อย่างเคร่งครัด
- 1.3 ผู้ใช้งานที่ได้รับสิทธิ์ จะได้รับบัญชีผู้ใช้งาน (Account) ซึ่งประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

2. การใช้งานบัญชีผู้ใช้งานเครือข่ายไร้สาย (Account)

- 2.1 ระบบเครือข่ายไร้สาย หมายถึง บริการสัญญาณอินเทอร์เน็ตไร้สาย MSO-WIFI ที่มีไว้ให้บริการภายในบริเวณพื้นที่ของ สป.พม. เท่านั้น
- 2.2 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งานเครือข่ายไร้สาย (Account) ที่ได้รับจากการลงทะเบียนผู้ใช้งาน
- 2.3 ผู้ใช้งานต้องใช้ Account ของตนเองเท่านั้น ในการเข้าใช้งานเครือข่ายไร้สายของ สป.พม. โดย Account จะมีอายุการใช้งาน 24 ชั่วโมง
- 2.4 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้ Account ในนามของตนเองไม่ว่ากรณีใดๆ
- 2.5 ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดจากการใช้งาน Account ในนามของตนเอง
- 2.6 ผู้ใช้งานต้องทำการ Logout ออกจากคอมพิวเตอร์ หรือคอมพิวเตอร์แบบพกพา ทันทีเมื่อเลิกใช้งานเครือข่ายไร้สาย หรือเมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์ หรือคอมพิวเตอร์แบบพกพา นานเกิน 15 นาที

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 14 : การใช้งานระบบเครือข่ายไร้สาย	รหัสเอกสาร : IC-0214

- 2.7 ผู้ใช้งานสามารถใช้งานเครือข่ายไร้สายได้ภายในบริเวณพื้นที่ที่อยู่ในความรับผิดชอบของ สป.พม.
- 2.8 ผู้ใช้งานต้องไม่ใช้เครือข่ายไร้สายโดยก่อให้เกิดความเสียหายต่อ สป.พม. และบุคคลอื่น หรือละเมิดสิทธิ์ หรือสร้างความรำคาญต่อผู้อื่น เช่น การแสดงความเห็นดูหมิ่นผู้อื่นบนเว็บไซต์
- 2.9 ผู้ใช้งานต้องตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานอันเกิดจากการใช้งานเครือข่ายสังคมออนไลน์
- 2.10 ผู้ใช้งานต้องรับผิดชอบทั้งด้านสังคมและกฎหมาย เนื่องจากการโพสต์ข้อความหรือแสดงความคิดเห็น เพื่อให้เผยแพร่บนเครือข่ายสังคมออนไลน์ เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ

3. การระงับ/เพิกถอน บัญชีผู้ใช้งานเครือข่ายไร้สาย (Account)

ผู้ดูแลระบบมีสิทธิ์ระงับ Account ของผู้ใช้งานได้ทันที หากได้รับแจ้งหรือตรวจพบการกระทำใดที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย หรือการกระทำที่ละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 15 : การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.	รหัสเอกสาร : IC-0215

การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.

วัตถุประสงค์

เพื่อเป็นมาตรการควบคุมการใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม. ให้มีความมั่นคงปลอดภัยและลดความเสี่ยงหรือผลกระทบที่อาจเกิดจากการใช้งานอินเทอร์เน็ตของผู้ใช้งาน ตลอดจนป้องกันมิให้ผู้ใช้งานละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.

แนวปฏิบัติ

1. การลงทะเบียนผู้ใช้งาน

- 1.1 ผู้ใช้งานอินเทอร์เน็ต สป.พม. จะต้องลงทะเบียนเพื่อขอใช้งานจากผู้ดูแลระบบก่อน โดยการกรอกข้อมูลส่วนบุคคลในแบบฟอร์มลงทะเบียนผู้ใช้งานที่ สป.พม. จัดเตรียมไว้
- 1.2 ผู้ใช้งานต้องยอมรับและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. อย่างเคร่งครัด
- 1.3 ผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าใช้งานอินเทอร์เน็ต สป.พม. จะได้รับบัญชีผู้ใช้งานอินเทอร์เน็ต (Account) ซึ่งประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่านชั่วคราว (Password)

2. การใช้งานบัญชีผู้ใช้งานอินเทอร์เน็ต (Account)

- 2.1 ผู้ใช้งานต้องเปลี่ยน Password โดยทันทีหลังจากที่ได้รับ Account จากผู้ดูแลระบบ
- 2.2 ผู้ใช้งานควรตั้ง Password โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ และควรมีความยาวอย่างน้อย 12 ตัวอักษร
- 2.3 ผู้ใช้งานควรเปลี่ยน Password ทุกๆ 3 เดือน หรือตามที่ผู้ดูแลระบบกำหนด
- 2.4 ผู้ใช้งานควรเปลี่ยน Password ใหม่ทันที หากถูกเปิดเผยหรือสงสัยว่าถูกผู้อื่นนำ Password ไปใช้
- 2.5 ผู้ใช้งานต้องใช้ Account ของตนเองเท่านั้น ในการเข้าใช้งานอินเทอร์เน็ต สป.พม.
- 2.6 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้ Account ในนามของตนเองไม่ว่ากรณีใดๆ
- 2.7 ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดจากการใช้งาน Account ในนามของตนเอง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 15 : การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.	รหัสเอกสาร : IC-0215

2.8 ผู้ใช้งานต้องทำการ Logout ออกจากคอมพิวเตอร์ทันทีเมื่อเลิกใช้งานอินเทอร์เน็ต หรือเมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน 15 นาที

3. การใช้งานอินเทอร์เน็ต สป.พม.

3.1 ผู้ใช้งานสามารถเข้าใช้งานได้ภายในบริเวณพื้นที่ที่อยู่ในความรับผิดชอบของ สป.พม.

3.2 ผู้ใช้งานสามารถเข้าใช้งานได้ 2 ช่องทาง ดังนี้

3.2.1 เชื่อมต่อกับระบบเครือข่ายแบบ LAN

3.2.2 เชื่อมต่อกับระบบเครือข่ายแบบไร้สาย หรือ Wireless LAN

3.3 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งานอินเทอร์เน็ต (Account) ที่ได้รับจากการลงทะเบียนผู้ใช้งาน

4. การใช้งานอินเทอร์เน็ต สป.พม. อย่างปลอดภัย

4.1 การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อใช้งานอินเทอร์เน็ต ควรเชื่อมต่อผ่านระบบรักษาความมั่นคงปลอดภัย ที่ สป.พม. จัดสรรไว้เท่านั้น

4.2 ผู้ใช้งานต้องไม่ใช้อินเทอร์เน็ต สป.พม. ในการเผยแพร่หรือใช้งานโดยมีวัตถุประสงค์ ดังนี้

4.2.1 ก่อให้เกิดความเสียหายต่อ สป.พม. และบุคคลอื่น หรือละเมิดสิทธิ หรือสร้างความรำคาญต่อผู้อื่น เช่น การตัดต่อภาพของผู้อื่นแล้วนำมาเผยแพร่ทำให้เกิดความอับอาย ลักลอบแก้ไขข้อมูลส่วนบุคคลของผู้อื่น การแสดงความเห็นดูหมิ่นผู้อื่นบนเว็บไซต์ เป็นต้น

4.2.2 หาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์ เช่น การจำลอง Mail Server เพื่อส่ง mail จำนวนมาก และการจำลอง Web Server เพื่อจัดทำเว็บไซต์สำหรับค้าขาย เป็นต้น

4.2.3 การกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การเข้าสู่เว็บไซต์ที่ไม่เหมาะสม การใช้ข้อความที่สร้างความตื่นตระหนกกับสังคมโดยรวม เป็นต้น

4.2.4 เปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจาก สป.พม. หรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

4.3 ผู้ใช้งานไม่ควรดาวน์โหลดหรือใช้งานข้อมูลมัลติมีเดีย ที่มีลักษณะยึดครองช่องสัญญาณการสื่อสารข้อมูลตลอดเวลา (Consume Bandwidth) ผ่านอินเทอร์เน็ต สป.พม. ในเวลาราชการ เช่น เล่นเกม/ดูหนัง/ฟังเพลงออนไลน์ ดูคลิปวิดีโอผ่านเว็บไซต์ ดาวน์โหลดซอฟต์แวร์ที่มีขนาดใหญ่ผ่านเว็บไซต์ เป็นต้น

4.4 ผู้ใช้งานไม่ควรดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือหรือไม่มั่นใจว่าปลอดภัย เช่น Freeware โปรแกรมรักษาจอภาพ เกมส์ และโปรแกรมที่ลงท้ายด้วย exe หรือ com หากมีความจำเป็นต้องดาวน์โหลด ต้องมีการตรวจสอบด้วยโปรแกรมป้องกันไวรัส ก่อนการนำไปใช้ทุกครั้ง

4.5 หากผู้ใช้งานมีความจำเป็นต้องส่งข้อมูลที่มีขนาดใหญ่ ให้ติดต่อผู้ดูแลระบบดำเนินการเท่านั้น

4.6 ผู้ใช้งานที่มีความจำเป็นต้องนำคอมพิวเตอร์โน้ตบุ๊กไปเชื่อมต่อเข้ากับอินเทอร์เน็ตอื่นที่มีใช้ สป.พม. จะต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่คอมพิวเตอร์โน้ตบุ๊กดังกล่าว และต้อง Update ไวรัสให้เป็นปัจจุบันอยู่เสมอ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 15 : การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.	รหัสเอกสาร : IC-0215

4.7 ผู้ใช้งานควรแจ้งข้อเท็จจริงต่อผู้ดูแลระบบ หากพบเห็นการใช้งานอินเทอร์เน็ต สป.พม. ไปในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิของ สป.พม.

5. การใช้งานเครือข่ายสังคมออนไลน์

- 5.1 ผู้ใช้งานต้องตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานอันเกิดจากการใช้งานเครือข่ายสังคมออนไลน์
- 5.2 ผู้ใช้งานต้องรับผิดชอบต่อทั้งด้านสังคมและกฎหมาย เนื่องจากการโพสต์ข้อความหรือแสดงความคิดเห็น เพื่อให้เผยแพร่บนเครือข่ายสังคมออนไลน์เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ
- 5.3 ผู้ใช้งานไม่ควรเปิดเผยข้อมูลส่วนตัวมากเกินไป รวมถึงข้อมูลทางการเงิน
- 5.4 ผู้ใช้งานไม่ควรโพสต์ข้อความที่บอกลักษณะความเคลื่อนไหวของตนเอง เพราะจะทำให้ผู้ไม่หวังดีวางแผนมาทำร้ายหรือขโมยทรัพย์สินได้
- 5.5 ผู้ใช้งานต้องระมัดระวังอย่างยิ่งในการโพสต์หรือเผยแพร่ ส่งต่อข้อความ รูปภาพ วิดีโอ ที่อาจทำให้ผู้อื่นเสียหาย เช่น ภาพหลุด คลิปหลุด หรือโพสต์รูปภาพที่สื่อถึงอบายมุขต่างๆ และไม่ควรใช้ถ้อยคำหยาบคาย ถ้อยคำลามก อนาจาร ดูหมิ่น ส่อเสียด เสียดสี ให้ร้ายผู้อื่นในทางเสียหาย หรือสร้างความแตกแยกในสังคม
- 5.6 ผู้ใช้งานต้องระมัดระวังอย่างยิ่งที่จะไว้วางใจหรือเชื่อใจคนที่รู้จักผ่านอินเทอร์เน็ต ในการแลกเปลี่ยนข้อมูลส่วนตัว เช่น ชื่อ อีเมล หมายเลขโทรศัพท์ ที่อยู่ เพราะอาจถูกหลอกลวงหรือล่อลวงไปทำอันตรายได้
- 5.7 ผู้ใช้งานต้องระมัดระวังการเช็คอิน (Check-in) โดยใช้กล้องโทรศัพท์ถ่ายภาพ ระบุพิกัด และเวลา เพราะภาพทุกภาพ การโพสต์ทุกอย่างจะอยู่บนอินเทอร์เน็ตอย่างถาวร ไม่สามารถถูกลบได้อย่างแท้จริง

6. การใช้งานเครื่องคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของ สป.พม.

- 6.1 ห้ามนำข้อมูลส่วนตัวที่ไม่เกี่ยวข้องกับงานของหน่วยงานมาเก็บไว้ในเครื่องคอมพิวเตอร์ของหน่วยงาน
- 6.2 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของ สป.พม. เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขายหรือเผยแพร่สิ่งผิดกฎหมาย การตั้งกระทู้หรือตอบกระทู้บนกระดานถาม - ตอบ หรือบนเว็บไซต์ประเภท social network หรือบริการบล็อก (Blog) เพื่อเผยแพร่สิ่งผิดกฎหมาย และขัดต่อศีลธรรม เป็นต้น
- 6.3 ห้ามเข้าใช้เครือข่ายคอมพิวเตอร์ของ สป.พม. ด้วยบัญชีของผู้อื่น ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี
- 6.4 ห้ามเข้าถึงระบบคอมพิวเตอร์และข้อมูลที่มีมาตรการป้องกันการเข้าถึงของผู้อื่น เพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม เช่น มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นเข้ามาใช้เครื่องคอมพิวเตอร์หรือเข้าดูข้อมูล เป็นต้น
- 6.5 ห้ามเผยแพร่ข้อมูลของผู้ใช้งานหรือหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้ที่เป็นเจ้าของหรือเป็นผู้จัดทำข้อมูลนั้นๆ
- 6.6 ห้ามก่อวินาศกรรม ขัดขวาง ชะลอหรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของ สป.พม. และระบบเครือข่ายอื่นเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ เพื่อให้เกิดผลชะลอการทำงาน

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 15 : การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.	รหัสเอกสาร : IC-0215

การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) หรือทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายทำงานได้ช้าลง เป็นต้น

- 6.7 ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมประเภทที่ละเมิดลิขสิทธิ์และชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ หรือเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดบนเครือข่ายคอมพิวเตอร์ของ สป.พม.
- 6.8 ห้ามลักลอบดักจับข้อมูลบนเครือข่ายคอมพิวเตอร์ของ สป.พม. และของผู้อื่น ที่อยู่ระหว่างการรับและส่งบนเครือข่ายคอมพิวเตอร์ของ สป.พม.
- 6.9 ห้ามส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-Mail) ในรูปแบบภาพนิ่ง ภาพเคลื่อนไหว ภาพที่เกิดจากการสร้างขึ้น ตัดต่อ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ และข้อความที่เกี่ยวกับการลามกอนาจาร การละเมิดทรัพย์สินทางปัญญา การหมิ่นพระบรมเดชานุภาพ การสร้างปัญหาความมั่นคงของประเทศ หรือการทำให้บุคคลเสียชื่อเสียงหรือได้รับความอับอาย การปลอมแปลงหรือแอบอ้างชื่อเป็นบุคคลอื่นเพื่อสร้างความเข้าใจผิด การส่งอีเมลมากจนล้นระบบเครือข่ายคอมพิวเตอร์ของบุคคลอื่น จนทำให้เกิดความยุ่งยากในการใช้งานระบบเครือข่ายคอมพิวเตอร์
- 6.10 ห้ามเผยแพร่หรือเข้าถึงสื่อที่เกี่ยวข้องกับเรื่องลามกอนาจาร การละเมิดทรัพย์สินทางปัญญา การหมิ่นพระบรมเดชานุภาพ การสร้างปัญหาความมั่นคงของประเทศ หรือการทำให้บุคคลเสียชื่อเสียงหรือได้รับความอับอาย
- 6.11 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจการค้า หรือเปิดให้บริการใดๆ นอกจากจะได้รับอนุญาตจากหน่วยงานหรือผู้รับผิดชอบทรัพยากรและเครือข่ายคอมพิวเตอร์
- 6.12 ห้ามกระทำการเคลื่อนย้าย หรือทำการใดๆ ต่อทรัพยากรและเครือข่ายคอมพิวเตอร์ของ สป.พม. โดยพลการ นอกจากได้รับอนุญาตจากหน่วยงานหรือผู้รับผิดชอบทรัพยากรและเครือข่ายคอมพิวเตอร์
- 6.13 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบาย ระเบียบ ข้อบังคับ และประกาศของหน่วยงาน

7. การใช้งานแบนด์วิดท์เครือข่ายที่เหมาะสม

- 7.1 รมณรงคให้ผูัใช้งานเครือข่ายใช้งานระบบอีเมลที่หน่วยงานจัดให้ เนื่องจากการที่ผู้ใช้งานเครือข่ายใช้ระบบอีเมลจากภายนอก เช่น Hotmail Gmail เป็นต้น ทำให้ผู้ใช้งานนั้นต้องเชื่อมต่อเครื่องลูกข่ายของตนไปยังเครื่องแม่ข่ายภายนอก ส่งผลให้มีการใช้งานแบนด์วิดท์ของเครือข่ายหน่วยงานเป็นจำนวนมาก ทำให้เหลือแบนด์วิดท์เพื่อการใช้งานแอปพลิเคชันอื่นน้อยลง
- 7.2 หลีกเลียงการสำรองข้อมูลขึ้นระบบ Cloud Computing หรือการดาวน์โหลดไฟล์ขนาดใหญ่ในช่วงเวลาปฏิบัติงาน กรณีตั้งค่าการสำรองข้อมูลขึ้นระบบ Cloud อัตโนมัติ ควรตั้งเวลาที่เหมาะสม เช่น ระหว่างเวลา 23.00 – 03.00 น. เป็นต้น
- 7.3 ควรใช้พร็อกซี (Proxy) ในการใช้งานเว็บไซต์ เนื่องจากเครื่องลูกข่ายไม่ต้องเชื่อมโยงเข้ากับเครื่องแม่ข่ายที่อยู่ระยะไกลทุกครั้งที่มีการเรียกใช้เว็บไซต์ ทำให้ลดการใช้งานแบนด์วิดท์ของเครือข่ายลงได้

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 15 : การใช้งานอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ของ สป.พม.	รหัสเอกสาร : IC-0215

- 7.4 หน่วยงานขอสงวนสิทธิ์ในการตรวจจับแบนด์วิดท์ของแพ็กเกจ ทั้งการจราจรขาเข้า (Inbound Traffic) และการจราจรขาออก (Outbound Traffic) ของบัญชีผู้ใช้งานโดยไม่ต้องแจ้งให้ทราบล่วงหน้า
- 7.5 กรณีที่หน่วยงานตรวจสอบแล้วพบว่าบัญชีผู้ใช้งานใดมีพฤติกรรมเสี่ยง เช่น โหลดบิต เป็นต้น หน่วยงานขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเทอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้นั้น
- 7.6 รมรงค์ให้ผู้ใช้งานเครือข่ายลดการเข้าถึงเว็บไซต์ประเภทสื่อสังคมออนไลน์ ที่ใช้เผยแพร่ข้อมูล และแสดงความคิดเห็นบนโลกออนไลน์ เช่น Facebook Twitter เป็นต้น ในช่วงเวลาปฏิบัติงาน และ/หรือในช่วงเวลาที่มีการใช้งานแบนด์วิดท์เครือข่ายปริมาณสูง และ/หรือส่งผลกระทบการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย เนื่องจากเว็บไซต์ดังกล่าวมีแอปพลิเคชันที่จองช่องทางจราจรอินเทอร์เน็ตอยู่ตลอดเวลา ส่งผลให้แบนด์วิดท์เต็มหรือเหลือน้อยได้
- 7.7 หน่วยงานขอสงวนสิทธิ์ในการจัดสรรแบนด์วิดท์ (Bandwidth Quota) ของผู้ใช้งานแต่ละคนเพื่อการจัดการทรัพยากรแบนด์วิดท์ที่เหมาะสม

8. การระงับ/เพิกถอน บัญชีผู้ใช้งานอินเทอร์เน็ต (Account)

- 8.1 ผู้ดูแลระบบมีสิทธิ์ระงับ Account ของผู้ใช้งานได้ทันที หากได้รับแจ้งหรือตรวจพบการกระทำใดที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย หรือการกระทำที่ละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง
- 8.2 ผู้ดูแลระบบมีสิทธิ์เพิกถอน Account ของผู้ใช้งานออกจากระบบได้ทันที หากไม่มีการติดต่อกลับภายในระยะเวลา 90 วัน นับจากวันที่ถูกระงับ Account หรือไม่มีการร้องขอขยายสิทธิ์การใช้งาน
- 8.3 ผู้ดูแลระบบมีสิทธิ์เพิกถอน Account ของผู้ใช้งานออกจากระบบได้ ดังนี้
- 8.3.1 กรณีเป็นเจ้าหน้าที่ของ สป.พม. ให้เพิกถอนเมื่อผู้ใช้นั้นลาออกหรือพ้นสภาพจากการเป็นเจ้าหน้าที่ของ สป.พม. หรือเมื่อไม่มีการเข้าใช้งานอินเทอร์เน็ต สป.พม. เป็นระยะเวลาติดต่อกันเกิน 90 วัน
- 8.3.2 กรณีเป็นบุคคลจากหน่วยงานภายนอก ให้เพิกถอนตามวันที่ระบุในแบบฟอร์มลงทะเบียนผู้ใช้งาน หรือเมื่อไม่มีการเข้าใช้งานอินเทอร์เน็ต สป.พม. เป็นระยะเวลาติดต่อกันเกิน 30 วัน
- 8.4 ผู้ใช้งานสามารถร้องขอขยายสิทธิ์การใช้งาน Account ได้ เพื่อคงสิทธิ์เดิมไว้เมื่อต้องพ้นสภาพจากการเป็นเจ้าหน้าที่ของ สป.พม. โดยยื่นคำร้องส่งถึงศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ทั้งนี้ การอนุญาตและระยะเวลาการขยายสิทธิ์ ให้เป็นอำนาจของผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.พม.

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 16 : การใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)	รหัสเอกสาร : IC-0216

การใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)

วัตถุประสงค์

ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) ภายใต้ชื่อโดเมน @m-society.go.th ให้บริการเพื่อสนับสนุนการดำเนินงานของเจ้าหน้าที่ในสังกัดสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) และสำนักงานรัฐมนตรี (สร.) สำหรับใช้ติดต่อสื่อสารงานราชการ ให้มีความปลอดภัยและเชื่อถือได้ รวมถึงมีแนวปฏิบัติที่สอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่หรือหน่วยงานในสังกัด สป.พม. และ สร.

แนวปฏิบัติ

1. การลงทะเบียนผู้ใช้งาน

- 1.1 ผู้ใช้งานจะต้องลงทะเบียนเพื่อขอใช้งาน e-Mail จากผู้ดูแลระบบก่อน โดยการกรอกข้อมูลในแบบฟอร์มลงทะเบียนผู้ใช้งานที่ สป.พม. จัดเตรียมไว้
- 1.2 ผู้ใช้งานต้องยอมรับและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์อย่างเคร่งครัด
- 1.3 ผู้ใช้งานที่ได้รับสิทธิ์ให้ใช้งาน e-Mail ได้ จะได้รับบัญชีผู้ใช้งาน (Account) ภายใต้ชื่อโดเมน @m-society.go.th ซึ่งประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่านชั่วคราว (Password)
- 1.4 ผู้ใช้งาน e-Mail จะได้รับพื้นที่ใช้งาน จำนวน 10 GB และแนบไฟล์ได้ 25 MB

2. การเข้าใช้งาน e-Mail

- 2.1 ผู้ใช้งานสามารถเข้าใช้งาน e-Mail ได้ที่เว็บไซต์ <https://www.workd.go.th/login>
- 2.2 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีที่เข้าใช้งานครั้งแรก (เนื่องจากรหัสผ่านที่ได้รับจากผู้ดูแลระบบเป็นรหัสผ่านชั่วคราวเท่านั้น)

3. การใช้งานบัญชีผู้ใช้งาน e-Mail

- 3.1 ผู้ใช้งานต้องเปลี่ยน Password โดยทันทีหลังจากที่ได้รับ Account จากผู้ดูแลระบบ
- 3.2 ผู้ใช้งานควรตั้ง Password ให้มีความยาวอย่างน้อย 12 ตัวอักษร และต้องประกอบด้วย ตัวอักษรภาษาอังกฤษ พิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษ
- 3.3 ผู้ใช้งานควรเปลี่ยน Password ทุกๆ 3 เดือน หรือตามที่คุณผู้ดูแลระบบกำหนด

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 16 : การใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)	รหัสเอกสาร : IC-0216

- 3.4 ผู้ใช้งานควรเปลี่ยน Password ใหม่ทันที หากถูกเปิดเผยหรือสงสัยว่าถูกผู้อื่นนำ Password ไปใช้
- 3.5 ผู้ใช้งานต้องใช้ Account ของตนเองหรือที่ได้รับมอบหมายเท่านั้น ในการใช้งาน e-Mail
- 3.6 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้ Account ในนามของตนเองไม่ว่ากรณีใดๆ
- 3.7 ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดจากการใช้งาน Account ในนามของตนเอง
- 3.8 ผู้ใช้งานต้องทำการ Logout ออกจากการใช้งาน e-Mail ทันทีเมื่อเลิกใช้งาน หรือเมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน 15 นาที

4. การรับ - การส่ง e-Mail

- 4.1 ผู้ใช้งาน e-Mail ต้องตรวจสอบไวรัสกับไฟล์ที่แนบมาพร้อม e-Mail ทุกครั้ง ถึงแม้ว่าจะมาจากผู้ส่งที่รู้จัก
- 4.2 หากผู้ใช้งาน e-Mail ต้องการส่ง e-Mail ถึงผู้ใช้งานทุกคนหรือส่งแบบกลุ่ม ควรแจ้งให้ผู้ดูแลระบบทราบ เนื่องจากผู้ดูแลระบบได้สร้างบัญชีผู้ใช้งานแบบกลุ่มไว้แล้ว เพื่ออำนวยความสะดวก และป้องกันการส่ง e-Mail ในลักษณะ Spam mail
- 4.3 ห้ามผู้ใช้งาน ใช้ e-Mail ในลักษณะดังต่อไปนี้
 - 4.3.1 ไม่ควรเปิดหรือส่งต่อ e-Mail ที่ไม่ทราบแหล่งที่มาหรือไม่น่าเชื่อถือ
 - 4.3.2 การใช้ e-Mail เพื่อลงทะเบียนสมัครงานบนเว็บไซต์สมัครงาน
 - 4.3.3 การใช้ e-Mail เพื่อแสดงความคิดเห็นบนเว็บไซต์ขายสินค้า
 - 4.3.4 การใช้ e-Mail เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น
 - 4.3.5 การปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่า e-Mail นั้นๆ ส่งมาจากบุคคลอื่น
 - 4.3.6 การปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันเวลาการส่ง
 - 4.3.7 การปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง
 - 4.3.8 การส่ง e-Mail เพื่อเผยแพร่จดหมายลูกโซ่
 - 4.3.9 การส่ง e-Mail เพื่อเผยแพร่ข้อมูลชั้นความลับของหน่วยงาน
 - 4.3.10 การส่ง e-Mail เพื่อเผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล
 - 4.3.11 การส่ง e-Mail เพื่อเผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่ดูหมิ่น เหยียดหยาม หรือแบ่งแยกทางศาสนา เชื้อชาติ หรือเพศ
 - 4.3.12 การส่ง e-Mail เพื่อเผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่มีลักษณะหยาบคายหรือลามกอนาจาร
 - 4.3.13 การส่ง e-Mail เพื่อเผยแพร่โปรแกรมหรือรหัสสำหรับการเข้าถึงโปรแกรมในลักษณะที่ละเมิดลิขสิทธิ์
 - 4.3.14 การส่ง e-Mail เพื่อกระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร
 - 4.3.15 การส่ง e-Mail เพื่อโฆษณาสินค้า ผลิตภัณฑ์ หรือส่งข้อความในลักษณะ Spam Mail ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร
 - 4.3.16 การส่ง e-Mail ซึ่งส่งผลกระทบทำให้ระบบ e-Mail หรือระบบเครือข่ายลดทอนประสิทธิภาพลง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 16 : การใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)	รหัสเอกสาร : IC-0216

4.3.17 การส่ง e-Mail เพื่อกระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบ

4.3.18 การส่ง e-Mail ต้องไม่เข้าข่ายการกระทำความผิดหรือขัดต่อกฎหมายอื่นๆ ที่เกี่ยวข้อง

5. การส่ง e-Mail ผ่านบัญชีผู้ใช้งานแบบกลุ่ม

5.1 ผู้ดูแลระบบจัดให้มีระบบบัญชีผู้ใช้งาน e-Mail แบบกลุ่มตามคำร้องขอของหน่วยงาน ทั้งนี้ ผู้ดูแลระบบขอสงวนสิทธิ์ในการอนุมัติการขอจดทะเบียนชื่อกลุ่ม ตลอดจนการตั้งชื่อกลุ่ม โดยจะต้องตั้งชื่อกลุ่มตามหลักการที่ได้กำหนดไว้ หรือตามความเหมาะสมเป็นกรณีๆ ไป

5.2 ผู้ดูแลระบบใช้เพื่อแจ้งเตือนหรือแจ้งข่าวที่เกี่ยวข้องกับความมั่นคงปลอดภัย หรือการรักษาประสิทธิภาพของระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

5.3 ผู้ใช้งานใช้เพื่อส่งข้อมูลหรือเผยแพร่ข่าวสารประชาสัมพันธ์ เพื่อการดำเนินงานตามภารกิจ หรือสิทธิประโยชน์ต่างๆ ที่ควรทราบ

6. การระงับ/เพิกถอน บัญชีผู้ใช้งาน e-Mail

6.1 ผู้ดูแลระบบสามารถระงับบัญชีผู้ใช้งาน e-Mail นั้นได้ หากผู้ใช้งานพ้นสภาพจากการสังกัด สป.พม. หรือ สร.

6.2 ผู้ใช้งานสามารถร้องขอการขยายสิทธิ์การใช้งานบัญชีผู้ใช้ได้ เพื่อคงสิทธิ์เดิมไว้เมื่อต้องพ้นสภาพจากการสังกัด สป.พม. หรือ สร. โดยยื่นคำร้องส่งถึงศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ทั้งนี้ การอนุญาตและระยะเวลาการขยายสิทธิ์ ให้เป็นอำนาจของผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.พม.

6.3 ผู้ดูแลระบบสามารถเพิกถอนบัญชีผู้ใช้งาน e-Mail ออกจากระบบได้ โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า หากตรวจพบว่าบัญชี e-Mail ของผู้ใช้งานนั้น ไม่มีการใช้งานหรือความเคลื่อนไหวใดๆ เป็นระยะเวลาเกิน 1 ปี

6.4 ผู้ดูแลระบบสามารถระงับบัญชีผู้ใช้งาน e-Mail นั้นได้ หากได้รับแจ้งหรือตรวจพบการกระทำใดที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย หรือการกระทำที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่นๆ ที่เกี่ยวข้อง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 17 : การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	รหัสเอกสาร : IC-0217

การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของ สป.พม. ตลอดจนการแสดงความคิดเห็นของบุคลากรในหน่วยงาน ผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้องเหมาะสม เพื่อรักษาภาพลักษณ์ของบุคลากรและการดำเนินงานของหน่วยงาน ให้มีความเป็นระเบียบเรียบร้อย และเกิดประโยชน์สูงสุด ตลอดจนป้องกันมิให้เกิดการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

- หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) รับผิดชอบในการให้บริการอินเทอร์เน็ตของ สป.พม.
- เจ้าหน้าที่/ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบอินเทอร์เน็ตของ สป.พม.
- ผู้ใช้งาน** หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานอินเทอร์เน็ตของ สป.พม.

แนวปฏิบัติ

1. การใช้สื่อสังคมออนไลน์ทั่วไป

1.1 หลักการและแนวปฏิบัติทั่วไป

- 1.1.1 สป.พม. อนุญาตให้ใช้ระบบเครือข่ายสำหรับเข้าถึงสื่อสังคมออนไลน์ประเภทเว็บไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมาย ศีลธรรม และหลักจรรยาบรรณของหน่วยงาน
- 1.1.2 หน่วยงานภายใน สป.พม. บุคลากร สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์ เพื่อประโยชน์ในการเผยแพร่ ประชาสัมพันธ์ที่เกี่ยวข้องกับ สป.พม. ในการติดต่อสื่อสารระหว่างกันได้ แต่ต้องแยกให้ชัดเจนว่าข้อความใดเป็น “ข่าวประชาสัมพันธ์” “ความคิดเห็น” “ความคิดเห็นส่วนบุคคล” “การแลกเปลี่ยนข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่นๆ และความคิดเห็นดังกล่าวควรคำนึงถึงประโยชน์สาธารณะด้วย
- 1.1.3 การเผยแพร่ประชาสัมพันธ์ในนามของหน่วยงาน ผู้เผยแพร่ต้องแสดงตำแหน่งหน้าที่ สังกัดให้ชัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ที่ติดตามสามารถใช้ดุลพินิจในการติดตามได้
- 1.1.4 พึงระมัดระวังการใช้ถ้อยคำและภาษา ที่อาจเป็นการดูหมิ่น หรือหมิ่นประมาทบุคคลอื่น และควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์
- 1.1.5 พึงงดเว้นการโต้ตอบด้วยความรุนแรง ในกรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง การละเว้นไม่โต้ตอบจะสร้างความขัดแย้งไม่บานปลายจนหาที่สิ้นสุดไม่ได้

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 17 : การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	รหัสเอกสาร : IC-0217

- 1.1.6 พึงงดเว้นการใช้สื่อสังคมออนไลน์วิพากษ์ วิจารณ์ ตลอดจนแสดงความคิดเห็นในเรื่องที่เป็นข้อมูลภายในหน่วยงาน หรืออาจส่งผลกระทบต่อหน่วยงานได้
- 1.1.7 พึงใช้รูปแสดงตัวตนที่แท้จริง และพึงงดเว้นการนำรูปบุคคลอื่น รูปบุคคลสาธารณะ มาแสดงว่าเป็นรูปของตนเอง
- 1.1.8 หน่วยงานที่สังกัด อาจใช้รูปสัญลักษณ์ เครื่องหมายแสดงสังกัดได้ แต่ต้องคำนึงถึงความเหมาะสมในการใช้งาน
- 1.1.9 พึงระมัดระวังข้อความที่ส่งผลกระทบต่อเด็ก สตรี หรือละเมิดสิทธิมนุษยชน
- 1.1.10 การใช้สื่อสังคมออนไลน์ที่แสดงสังกัดภายในหน่วยงาน ควรแจ้งให้ผู้บังคับบัญชาทราบก่อนทุกครั้ง

1.2 หลักการส่งต่อข้อมูล

- 1.2.1 ควรส่งข้อมูลข่าวสารเฉพาะบุคคลที่รู้จัก แสดงตัวตน ตำแหน่ง หน้าที่การงาน สถานที่ชัดเจนเท่านั้น
- 1.2.2 ละเว้นการส่งข้อมูลที่เป็นข่าวดู ข่าวไม่ปรากฏที่มา หรือเป็นเพียงการคาดเดา
- 1.2.3 งดเว้นการส่งต่อข้อความที่เกี่ยวข้องกับหน่วยงานทุกกรณี ยกเว้นข้อความนั้นๆ เป็นที่เผยแพร่ต่อสาธารณะแล้ว
- 1.2.4 พึงระลึกเสมอว่า การส่งต่อข้อความที่เป็นเท็จหรือข้อความที่เจ้าของประสงคจะกระจายข่าว เพื่อสร้างความสับสนวุ่นวายในบ้านเมือง เท่ากับตกเป็นเครื่องมือของบุคคลเหล่านั้น
- 1.2.5 ควรงดเว้นการส่งต่อข้อความเรื่องบุคคลเสียชีวิต เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้ว
- 1.2.6 การส่งต่อข้อความเชิญชวนไปร่วมชุมนุมหรือกระทำการกิจกรรมทางสังคมใดๆ ต้องตรวจสอบข้อเท็จจริงให้แน่ชัดเสียก่อน

1.3 หลักการรับผิดชอบ

- 1.3.1 ควรแสดงความรับผิดชอบด้วยการขอโทษ แสดงความเสียใจทันทีเมื่อรู้ว่าการเผยแพร่ข้อมูลที่ผิดพลาดหรือกระทบต่อบุคคลอื่น
- 1.3.2 กรณีการส่งต่อข้อความข่าวดูหรือข่าวเท็จ ต้องแก้ไขข้อความนั้นโดยทันที หากสามารถตรวจสอบข้อเท็จจริงได้ พึงแสดงข้อเท็จจริงให้เป็นที่ประจักษ์
- 1.3.3 หากพบข้อมูลที่ไม่ถูกต้อง ควรดำเนินการแก้ไขอย่างรวดเร็ว และแสดงให้เห็นอย่างชัดเจนว่าเป็นผู้ดำเนินการดังกล่าว
- 1.3.4 หากพบข้อมูลใดๆ ที่ไม่เหมาะสม (เช่น สิ่งที่เป็นลิขสิทธิ์ของผู้อื่น หรือการแสดงความคิดเห็นที่เป็นการหมิ่นประมาท) ควรดำเนินการอย่างรวดเร็ว โดยลบข้อความดังกล่าวออกทันที เพื่อลดโอกาสที่จะเกิดข้อขัดแย้งทางกฎหมาย และผลกระทบด้านลบต่อหน่วยงาน

1.4 การพบข้อร้องเรียนและประเด็นขัดแย้ง

หากพบเห็นข้อร้องเรียนหรือการบิดเบือนข้อเท็จจริงเกี่ยวกับบริการอิเล็กทรอนิกส์ของหน่วยงาน หรือพบเห็นข้อร้องเรียนอื่นๆ ที่เกี่ยวข้องกับหน่วยงาน ควรหลีกเลี่ยงการถกเถียงหรือโต้ตอบ ซึ่งนำไปสู่การกระตุ้นให้เกิดอารมณ์รุนแรง และพาดพิงไปยังผู้อื่น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 17 : การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	รหัสเอกสาร : IC-0217

1.5 การไม่เปิดเผยข้อมูลที่เป็นความลับ

การพูดคุยแลกเปลี่ยนกับชุมชนออนไลน์ รวมถึงการโพสต์ข้อความที่เกี่ยวข้องกับงานประจำ เป็นสิ่งที่คุณจะสามารถทำได้ ถ้าไม่ขัดต่อหลักจรรยาบรรณของหน่วยงาน เว้นแต่ข้อมูลนั้นเป็นข้อมูลที่มีความสำคัญหรือเป็นความลับของหน่วยงาน ซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการลงทุน ข้อมูลสำคัญทางการเงิน งานวิจัย เป็นต้น

1.6 ความน่าเชื่อถือของข้อมูล

ไม่โพสต์ข้อความที่เป็นเท็จหรือก่อให้เกิดความเข้าใจผิด และระบุที่มาของข้อมูลนั้นอย่างชัดเจน การโพสต์ข้อความใดๆ ควรพิจารณาเนื้อหาอย่างรอบคอบและระมัดระวัง โดยเฉพาะการเปิดเผยข้อมูลส่วนบุคคล

1.7 ไม่ละเมิดกฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญา

ไม่ละเมิดกฎหมายลิขสิทธิ์การใช้งานใดๆ ที่เป็นลิขสิทธิ์ของผู้อื่น รวมทั้งของหน่วยงานเอง ทั้งนี้ การอ้างอิงคำพูดหรือข้อมูลของผู้อื่น ควรใช้ข้อความที่คัดลอกมาสั้นๆ เท่านั้น และควรระบุถึงที่มาของแหล่งข้อมูลหรือเจ้าของผลงานเสมอ การเชื่อมโยงไปยังงานของเจ้าของข้อมูล ถือเป็นการปฏิบัติที่เหมาะสมกว่าการคัดลอกข้อมูลมาใช้งาน

1.8 คำนึงถึงผู้เข้าชมและผู้เกี่ยวข้อง

บุคลากรของหน่วยงานไม่ควรโพสต์ข้อมูลใดๆ ที่ขัดแย้งกับข้อกำหนดของหน่วยงาน รวมถึงละเว้นการแสดงออกถึงความคิดเห็นที่ก้าวร้าว หมิ่นประมาท ดูถูกเป็นการส่วนตัว ลามกอนาจาร และอื่นๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วหรือขัดต่อจริยธรรม เช่น การเมือง ศาสนา ชนชาติ เป็นต้น การแสดงความคิดเห็นต่างๆ ที่โพสต์โดยบุคลากรของหน่วยงาน โดยที่ไม่ได้รับมอบหมายอย่างเป็นทางการ ถือเป็นการแสดงความคิดเห็นส่วนบุคคลเท่านั้น ไม่ได้เป็นความคิดเห็นอย่างเป็นทางการของหน่วยงาน

1.9 การปกป้องผู้มีส่วนได้ส่วนเสีย หน่วยงานพันธมิตร และผู้มีส่วนเกี่ยวข้อง

ไม่ควรอ้างอิงหรือเปิดเผยถึงข้อมูลผู้มีส่วนได้ส่วนเสีย และหน่วยงานพันธมิตร ตลอดจนผู้มีส่วนเกี่ยวข้องอย่างเปิดเผยก่อนได้รับอนุญาต และไม่พาดพิงถึงรายละเอียดที่เป็นความลับเกี่ยวกับข้อมูลผูกพันกับผู้มีส่วนได้ส่วนเสีย ทั้งนี้ ควรพึงระวังการใช้งานเครือข่ายสังคมออนไลน์เป็นเครื่องมือในการทำธุรกรรมทางการค้ากับผู้มีส่วนได้ส่วนเสีย หน่วยงานพันธมิตร รวมถึงผู้มีส่วนเกี่ยวข้องกับหน่วยงาน

1.10 การคำนึงถึงผลกระทบจากการใช้งาน

คำนึงถึงผลกระทบของการโพสต์ข้อความในเว็บบล็อกส่วนตัว โดยเฉพาะข้อความที่อาจก่อให้เกิดความขัดแย้งกับหน่วยงาน ดังนั้น จึงควรระมัดระวังในการถกเถียงข้อความในเว็บบล็อกส่วนตัวมาเป็นข้อมูลอ้างอิง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 17 : การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	รหัสเอกสาร : IC-0217

1.11 การคำนึงถึงผลกระทบต่อการปฏิบัติงาน

การใช้สื่อเครือข่ายสังคมออนไลน์จะต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

1.12 การฝ่าฝืนและบทลงโทษ

1.12.1 หน่วยงานไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งาน และ/หรือบัญชีผู้ใช้งานที่ฝ่าฝืนต่อนโยบายนี้

1.12.2 หากหน่วยงานตรวจสอบแล้วพบว่าบัญชีผู้ใช้งานใดละเมิดต่อนโยบายนี้ หน่วยงานขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเทอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้น

1.12.3 หากการกระทำอันฝ่าฝืนต่อนโยบายนี้เป็นความผิดตามกฎหมาย ให้หน่วยงานดำเนินคดีตามกฎหมายโดยลำดับต่อไป

2. การใช้สื่อสังคมออนไลน์ในระดับบุคคล

การนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรในหน่วยงานมีข้อปฏิบัติ ดังนี้

- 2.1 กรณีใช้ชื่อบัญชีผู้ใช้งาน (user account) ที่ระบุถึงต้นสังกัด ผู้ใช้งานพึงใช้ความระมัดระวังในการปฏิบัติตามข้อบังคับ จริยธรรม หลักเกณฑ์ และแนวปฏิบัติของหน่วยงานตามที่ได้ระบุไว้ โดยเฉพาะความถูกต้องและการใช้ภาษาที่เหมาะสม
- 2.2 กรณีใช้ชื่อบัญชีผู้ใช้งานที่ระบุถึงตัวตนอันอาจทำให้ผู้ติดตาม (followers) หรือเพื่อนในเครือข่าย (friends) เข้าใจได้ว่าเป็นบุคลากรในหน่วยงาน ผู้ใช้งานพึงระมัดระวังการนำเสนอข้อมูลข่าวสารและการแสดงความคิดเห็นที่อาจนำไปสู่การละเมิดจริยธรรมของผู้อื่น
- 2.3 ในการรวบรวมข้อมูลข่าวสาร การนำเสนอ และการแสดงความคิดเห็น ผู้ใช้งานพึงระวังการละเมิดสิทธิส่วนบุคคล ศักดิ์ศรีความเป็นมนุษย์ สิทธิเด็กและสตรี ภาพอูจาด ลามก อนาจาร
- 2.4 หากการนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรในหน่วยงานเกิดความผิดพลาด จนก่อให้เกิดความเสียหายต่อบุคคลหรือหน่วยงานอื่น ผู้ใช้งานต้องดำเนินการแก้ไขข้อความที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคำขอโทษต่อบุคคลหรือหน่วยงานที่ได้รับความเสียหาย ทั้งนี้ ต้องให้ผู้ได้รับความเสียหายได้มีโอกาสชี้แจงข้อมูลข่าวสารในส่วนของตนด้วย

3. การใช้สื่อสังคมออนไลน์ในระดับหน่วยงาน

3.1 การจัดทำสื่อสังคมออนไลน์ในระดับหน่วยงาน ควรที่จะคำนึงถึงหลักการพื้นฐานดังต่อไปนี้

3.1.1 วัตถุประสงค์ของการจัดทำ

3.1.2 แนวทางการใช้งานสื่อสังคมออนไลน์เพื่อช่วยพัฒนาและดำเนินงานของหน่วยงาน

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 17 : การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	รหัสเอกสาร : IC-0217

3.2 การตั้งค่าบนสื่อสังคมออนไลน์ของหน่วยงาน

การใช้ชื่อหรือตราสัญลักษณ์ของหน่วยงาน เพื่อเปิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ โดยมีวัตถุประสงค์เพื่อการประชาสัมพันธ์ เผยแพร่ข้อมูลข่าวสาร หรือการสื่อสารภายในหน่วยงาน จะต้องผ่านการรับทราบและเห็นชอบจาก DCIO ของหน่วยงานก่อน รวมทั้งจะต้องมีการตระหนักถึงหลักการพื้นฐานดังที่กล่าวมาข้างต้น

3.3 การนำเสนอข่าวโดยการใช้สื่อสังคมออนไลน์ของหน่วยงาน ควรมีหลักในการอ้างอิงถึงหน่วยงานดังต่อไปนี้

- 3.3.1 ชื่อหน่วยงานที่เผยแพร่ข้อมูลข่าวสาร
- 3.3.2 รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงหน่วยงาน
- 3.3.3 มาตรการทางเทคนิคที่ยืนยันถึงสถานะและความมีตัวตนของหน่วยงาน (ถ้ามี)
- 3.3.4 ชื่อตัวแทนหน่วยงานที่นำเสนอข่าวสาร (ถ้ามี)

3.4 การปกป้องข้อมูลที่เป็นความลับของหน่วยงาน

ในกรณีที่มีบัญชีผู้ใช้งานของหน่วยงาน ควรมีการตั้งค่าความเป็นส่วนตัว (Privacy) เพื่อป้องกันไม่ให้บุคคลอื่นโพสต์ข้อความหรือเข้าถึงข้อมูลที่มีความสำคัญหรือเป็นความลับของหน่วยงาน ซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการลงทุน ข้อมูลสำคัญทางการเงิน งานวิจัย เป็นต้น โดยมีการกำหนดให้อยู่ในวงจำกัดเท่านั้น และควรให้ความระมัดระวังในการโพสต์ข้อความเฉพาะกลุ่มหรือส่วนบุคคล ที่ไม่ต้องการเผยแพร่ให้สาธารณะชนรับรู้

3.5 การนำเสนอข้อมูลข่าวสารของหน่วยงานผ่านสื่อสังคมออนไลน์

ควรเป็นไปตามข้อบังคับจริยธรรม หลักเกณฑ์ และข้อปฏิบัติของหน่วยงานตามที่ได้ระบุไว้ และต้องไม่เป็นการสร้างความเกลียดชังระหว่างคนในชาติ จนอาจนำไปสู่ความขัดแย้งและเสียหายรุนแรงขึ้นในสังคม

3.6 หน่วยงานต้องให้ความเคารพและยอมรับข้อมูลข่าวสารหรือภาพข่าวที่ผลิตโดยบุคคลอื่นผ่านสื่อสังคมออนไลน์

การคัดลอกข้อความใดๆ จากสื่อสังคมออนไลน์ พึงได้รับการอนุญาตจากเจ้าของข้อความนั้นๆ ตามแต่กรณีจำเป็น เพื่อประโยชน์ในการเผยแพร่ข้อมูลข่าวสาร ต้องอ้างอิงถึงแหล่งที่มาของข้อความและข่าวสารนั้นโดยรับรู้ถึงสิทธิ หรือลิขสิทธิ์ของหน่วยงานหรือบุคคลผู้เป็นเจ้าของข้อมูลดังกล่าว

3.7 หลีกเลี่ยงการสื่อสาร

ควรหลีกเลี่ยงการสื่อสารข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง และข้อมูลใดๆ ของหน่วยงานหรือที่เกี่ยวข้องกับหน่วยงานที่ก่อให้เกิดความขัดแย้ง หรือโต้แย้งในสังคม ขัดต่อหลักกฎหมายทั้งในประเทศและในระดับสากล หรือการเสนอเรื่องราวตลกไร้สาระ เพื่อผื่น ไร้ศีลธรรม เกินความจริง ไม่ให้เกียรติ ถูกเหยียดหยาม และลอกเลียนแบบผู้อื่น

3.8 ไม่เผยแพร่ข้อมูลที่เป็นความลับของหน่วยงาน

ไม่นำข้อมูลที่เป็นความลับทุกระดับชั้นของหน่วยงาน มาเผยแพร่ผ่านสื่อสังคมออนไลน์ทุกประเภท

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 18 : การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)	รหัสเอกสาร : IC-0218

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) ให้มีการเรียนรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในการทำงาน รวมถึงวิธีการป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ และสามารถบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. สป.พม. ต้องให้ความสำคัญกับแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) สำหรับเจ้าหน้าที่ ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลที่สาม ที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ โดยต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้
 - 1.1 กิจกรรมให้ความรู้แก่ผู้ใช้งานทุกประเภท ได้แก่
 - (1) พนักงานใหม่ (New employees)
 - (2) ผู้ใช้งานและระดับบริหาร (User and Management)
 - (3) เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT
 - (4) ผู้ขาย ผู้รับจ้าง และผู้ให้บริการ (Vendor, Contractor and Service Provider)
 - 1.2 การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับ สำหรับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของบริการสำคัญของหน่วยงาน
 - 1.3 การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
 - 1.4 การสื่อสารอย่างสม่ำเสมอและทันทั่วถึง ครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ
2. ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบัน และมีรายละเอียดที่เกี่ยวข้องเหมาะสม

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 19 : การแบ่งปันข้อมูล (Information Sharing)	รหัสเอกสาร : IC-0219

การแบ่งปันข้อมูล (Information Sharing)

วัตถุประสงค์

เพื่อกำหนดขั้นตอนการแบ่งปันข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกันผลกระทบใดๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามที่เกิดขึ้นกับบุคคลที่ได้รับผลกระทบ การรักษาความปลอดภัยของข้อมูล การปฏิบัติตามกฎหมาย การควบคุมการเข้าถึง และการใช้งานข้อมูลอย่างถูกต้อง รวมถึงการสร้างความร่วมมือในการทำงานเพื่อให้เกิดประสิทธิภาพสูงสุดในการแบ่งปันข้อมูลภายใน สป.พม. อย่างปลอดภัยและมีความรับผิดชอบ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

- หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
- เจ้าหน้าที่** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
- ผู้ใช้งาน** หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

- การแบ่งปันข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย
 - 1.1 การตรวจสอบเหตุการณ์โดยระบุและตรวจสอบเหตุการณ์ที่เกิดขึ้น เช่น การบุกรุกข้อมูล หรือการโจมตีจากมัลแวร์
 - 1.2 การวิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อเข้าใจลักษณะของเหตุการณ์และผลกระทบที่อาจเกิดขึ้น
 - 1.3 การจัดหมวดหมู่ข้อมูลตามระดับความรุนแรง เช่น ข้อมูลที่เป็นความลับ ข้อมูลที่สามารถเผยแพร่ได้ หรือข้อมูลที่มีความเสี่ยง
 - 1.4 การสรุปข้อมูลที่เกี่ยวข้องให้ชัดเจนและเข้าใจง่าย พร้อมกับระบุแหล่งที่มาของข้อมูล และส่งข้อมูลไปยังหน่วยงานที่เกี่ยวข้อง
 - 1.5 การติดตามผลกระทบจากการแบ่งปันข้อมูล เพื่อปรับปรุงการดำเนินการในอนาคต
- ให้เจ้าหน้าที่ดำเนินการแบ่งปันข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ผ่านระบบ MISP (Malware Information Sharing Platform) ทุกครั้งหลังจากมีการแก้ไขสถานการณ์ความมั่นคงปลอดภัยไซเบอร์เรียบร้อยแล้ว ซึ่ง ระบบ MISP เป็นเครื่องมือในการแบ่งปันข้อมูลเกี่ยวกับภัยคุกคาม ทำให้ผู้ใช้สามารถตอบสนองต่อเหตุการณ์ได้รวดเร็วและมีประสิทธิภาพมากขึ้น โดยมีขั้นตอนการใช้งาน ดังนี้
 - 2.1 ติดตั้ง MISP บนเซิร์ฟเวอร์และตั้งค่าพื้นฐาน รวมถึงการกำหนดผู้ใช้และสิทธิการเข้าถึง
 - 2.2 สร้างบัญชีผู้ใช้สำหรับสมาชิกในองค์กรและพันธมิตรที่ต้องการเข้าถึงข้อมูล
 - 2.3 สร้างเหตุการณ์ (Event) ใหม่ใน MISP โดยกรอกข้อมูลที่เกี่ยวข้อง เช่น วันที่ เวลา ประเภทภัยคุกคาม และรายละเอียดอื่นๆ
 - 2.4 เพิ่มข้อมูลเฉพาะเกี่ยวกับภัยคุกคาม เช่น IP address, URL, hash ของไฟล์ และข้อมูลที่เกี่ยวข้องอื่นๆ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 19 : การแบ่งปันข้อมูล (Information Sharing)	รหัสเอกสาร : IC-0219

- 2.5 จัดกลุ่มข้อมูลตามลักษณะ เช่น ประเภทของภัยคุกคาม (malware, phishing, etc.) และระดับความรุนแรง
- 2.6 กำหนดระดับการเข้าถึงข้อมูล (Public, Private, Community) เพื่อให้สมาชิกสามารถเข้าถึงข้อมูลที่เหมาะสม
- 2.7 ส่งข้อมูลไปยังเครือข่ายอื่นโดยใช้ฟีดเจอร์การเชื่อมต่อกับระบบอื่นๆ เช่น STIX/TAXII เพื่อแบ่งปันข้อมูลกับหน่วยงานภายนอก
- 2.8 ตรวจสอบการเข้าถึงและการเปลี่ยนแปลงข้อมูลในระบบ เพื่อเพิ่มความปลอดภัยและความโปร่งใส
- 2.9 ใช้ประโยชน์จากข้อมูลที่แบ่งปันเพื่อวิเคราะห์และปรับปรุงการตอบสนองต่อภัยคุกคามในอนาคต

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 20 : การบริหารจัดการข้อมูลองค์กร และป้องกันข้อมูลส่วนบุคคล หรือข้อมูลที่มีความสำคัญรั่วไหล	รหัสเอกสาร : IC-0220

การบริหารจัดการข้อมูลองค์กร และป้องกันข้อมูลส่วนบุคคล หรือข้อมูลที่มีความสำคัญรั่วไหล

วัตถุประสงค์

เพื่อให้ สป.พม. สามารถบริหารจัดการข้อมูลหน่วยงาน และป้องกันข้อมูลส่วนบุคคล หรือข้อมูลที่มีความสำคัญรั่วไหล รักษาความลับและความปลอดภัยของข้อมูลที่สำคัญต่อหน่วยงาน ให้เป็นไปตามกฎระเบียบและกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยไซเบอร์ รวมถึงสร้างความมั่นใจให้แก่บุคลากร และผู้รับบริการของ สป.พม.

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การป้องกันด้านการบริหารจัดการ (Administrative Safeguard)

- 1.1 มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บ และประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น กำหนดให้มีบันทึกการเข้าออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้าออก มีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง โดยให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้น หากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมีขอบ
- 1.2 มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (User Responsibilities) แบ่งเป็น รูปแบบต่างๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผย และเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

2. การป้องกันด้านเทคนิค (Technical Safeguard)

- 2.1 จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- 2.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 20 : การบริหารจัดการข้อมูลองค์กร และป้องกันข้อมูลส่วนบุคคล หรือข้อมูลที่มีความสำคัญรั่วไหล	รหัสเอกสาร : IC-0220

2.3 จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่างๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

3. การป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control)

3.1 มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้าออกพื้นที่ มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง และล็อกประตูทุกครั้ง มีระบบบัตร/รหัสผ่าน เฉพาะผู้มีสิทธิเข้าออก

3.2 กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

4. การส่งมอบข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล

4.1 การประเมินก่อนส่งมอบข้อมูล

4.1.1 ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล

4.1.2 ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด และจำเป็นต้องทราบข้อมูลที่ชี้เฉพาะบุคคลหรือไม่ หากแปลงข้อมูลที่ชี้เฉพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงพอต่อการนำไปใช้ประโยชน์หรือไม่

4.2 เมื่อส่งมอบข้อมูล

4.2.1 จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน

4.2.2 ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

4.2.3 แจ้งให้บุคคลหรือนิติบุคคลนั้นทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกันตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

4.3 หลังส่งมอบข้อมูล

4.3.1 ติดตามการใช้งานเป็นครั้งคราว เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็น ต้องใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคลหรือนิติบุคคลนั้น ลบทำลายข้อมูล

4.3.2 กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากัน โดยอัตโนมัติตลอดเวลา

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 20 : การบริหารจัดการข้อมูลองค์กร และป้องกันข้อมูลส่วนบุคคล หรือข้อมูลที่มีความสำคัญรั่วไหล	รหัสเอกสาร : IC-0220

5. การลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ

- 5.1 ตรวจสอบข้อมูลส่วนบุคคลที่อยู่ในความดูแลของ สป.พม. (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ ตามที่ประกาศความเป็นส่วนตัว (Privacy Notice) หรือตามที่ขอความยินยอมไว้ เพื่อดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี
- 5.2 กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) และผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคลเช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี
- 5.3 การลบ ทำลายข้อมูล หรือการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น การจัดทำเอกสารประวัติศาสตร์ การศึกษาวิจัยหรือสถิติ การสร้างประโยชน์สาธารณะ การประเมินความสามารถในการทำงาน การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ การป้องกันโรคติดต่อ หรือการให้บริการด้านสังคมสงเคราะห์

6. แจ้งเหตุการณั้ละเมิดข้อมูลส่วนบุคคล

- 6.1 กำหนดผู้รับผิดชอบและวิธีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ในกรณีที่เป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน โดยต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน 72 ชั่วโมง (นับแต่ทราบเหตุ)
- 6.2 การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 21 : การบริหารจัดการการเข้ารหัสลับ (Encryption)	รหัสเอกสาร : IC-0221

การบริหารจัดการการเข้ารหัสลับ (Encryption)

วัตถุประสงค์

เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและรักษาไว้ซึ่งความลับของข้อมูล รวมถึงป้องกันการปลอมแปลงหรือแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต และการพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศของ สป.พม.

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การควบคุมการเข้ารหัสเพื่อป้องกันข้อมูลสารสนเทศ

มีการพิจารณาถึงการควบคุมการเข้ารหัสและผลของการประเมินความเสี่ยง เพื่อระบุระดับการป้องกัน ดังนี้

- 1.1 การรับส่งข้อมูลผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL หรือการใช้ VPN เป็นต้น
- 1.2 การรับส่งข้อมูลสำคัญผ่านเครือข่ายภายใน สป.พม. หากไม่มีข้อจำกัดอื่นใด ต้องได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL หรือการใช้ VPN เป็นต้น
- 1.3 ให้ ศทส. กำหนดวิธีการเข้ารหัสข้อมูล (Encryption) รวมทั้งติดตั้งระบบเข้ารหัสข้อมูล (Encryption) ในฮาร์ดแวร์ของ สป.พม. หรือที่ใช้ในกิจการของ สป.พม. เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล สื่อบันทึกข้อมูลประเภท Flash Drive หรือ External Hard Disk เพื่อให้ผู้ใช้งานสามารถเข้ารหัสข้อมูล (Encryption) สำหรับข้อมูลสารสนเทศที่บันทึกไว้ในสื่อบันทึกข้อมูลของฮาร์ดแวร์นั้นได้
- 1.4 การพัฒนาระบบงานที่ต้องมีการเก็บข้อมูลประเภทรหัสผ่านลงในฐานข้อมูล จะต้องเข้ารหัสผ่านก่อนที่จะเก็บลงในระบบฐานข้อมูล

2. การบริหารจัดการกุญแจ

การบริหารจัดการการเข้ารหัส (key management) และมาตรฐานอื่นๆ ที่มีประสิทธิภาพ การใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ ต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ ดังนี้

- 2.1 กุญแจหรือ certificate ที่ได้รับจากหน่วยงานภายนอกหรือที่ สป.พม. เป็นผู้สร้าง ต้องจัดเก็บไว้ในระบบที่สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์เท่านั้น
- 2.2 การสร้างกุญแจหรือ certificate ที่ สป.พม. เป็นผู้สร้าง ต้องใช้วิธีการสร้างที่เป็นมาตรฐานสากล เช่น 3DES หรือ AES เป็นต้น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 21 : การบริหารจัดการการเข้ารหัสลับ (Encryption)	รหัสเอกสาร : IC-0221

2.3 การสร้างกุญแจหรือ certificate หากผู้ร้องขอไม่ระบุเป็นอย่างอื่น ให้กำหนดอายุไว้ 1 ปี นับจากวันที่สร้าง

2.4 หากพบว่ากุญแจหรือ certificate ใดที่หมดอายุไปแล้ว หรือยังไม่หมดอายุ แต่ไม่ได้ใช้งานแล้ว ให้ revoke กุญแจหรือ certificate นั้นทันที

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 22 : การกำหนดการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร	รหัสเอกสาร : IC-0222

การกำหนดการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์

เพื่อบำรุงรักษาอุปกรณ์และระบบเทคโนโลยีต่างๆ ให้สามารถใช้งานได้อย่างต่อเนื่อง เพราะหากระบบเทคโนโลยีสารสนเทศไม่ได้รับการพัฒนาและบำรุงรักษาที่ดี อาจส่งผลให้ระบบไม่สามารถทำงานได้อย่างมีประสิทธิภาพ (ฮาร์ดแวร์ และระบบเครือข่าย) ไม่มีความน่าเชื่อถือ (ข้อมูลสารสนเทศ) และไม่สอดคล้องกับความต้องการของผู้ใช้งาน (Software) ซึ่งจะมีผลทำให้องค์กรไม่สามารถดำเนินงานได้อย่างมีประสิทธิภาพ รวมทั้งผู้บริหารไม่สามารถกำหนดนโยบายและการตัดสินใจได้อย่างถูกต้อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การจัดหา การพัฒนา และการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ศทส. และหน่วยงานเจ้าของระบบสารสนเทศ มีหน้าที่ดำเนินการเพื่อการจัดหาและการพัฒนาระบบสารสนเทศในการใช้งานตามภารกิจภายใน สป.พม. ดังนี้

- 1.1 กำหนดให้มีขั้นตอนในการปฏิบัติงานการควบคุมการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่เป็นลายลักษณ์อักษร ทั้งในกรณีการพัฒนาขึ้นใหม่ หรือเปลี่ยนแปลงแก้ไขระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงการตรวจสอบภายหลังการเปลี่ยนแปลงแก้ไข เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารสามารถทำงานได้อย่างเป็นปกติ
- 1.2 ให้มีการทดสอบระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งประเภทที่พัฒนาขึ้นใหม่ การเปลี่ยนแปลงแก้ไข หรือระหว่างการพัฒนา ระบบ ซึ่งให้มีข้อกำหนดการทดสอบในการตรวจรับ โดยพิจารณา ดังนี้
 - (1) ทดสอบระบบ (System Test)
 - (2) ทดสอบเฉพาะส่วน (Unit Test)
 - (3) ทดสอบการทำงานร่วมกัน (Integration Test)
 - (4) ทดสอบประสิทธิภาพ (Performance/Stress Test)
 - (5) ทดสอบการใช้งานโดยผู้ใช้งาน (User Acceptance Test)
 - (6) ทดสอบด้านความมั่นคงปลอดภัย (Security Test)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 22 : การกำหนดการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร	รหัสเอกสาร : IC-0222

1.3 การพัฒนาระบบต้องเป็นไปตามข้อกำหนดตามหลักการด้านความมั่นคงปลอดภัย ดังต่อไปนี้

- (1) การรักษาความลับของข้อมูลสารสนเทศ (Confidentiality)
- (2) การรักษาความถูกต้องสมบูรณ์ของข้อมูลสารสนเทศ (Integrity)
- (3) ความพร้อมใช้ของข้อมูลสารสนเทศ (Availability)
- (4) การระบุตัวตนผู้ใช้งาน (Identification)
- (5) การพิสูจน์ตัวตนผู้ใช้งาน (Authentication)
- (6) การกำหนดสิทธิ (Authorization)
- (7) การเก็บบันทึกเหตุการณ์ของการพัฒนาระบบ (Audit Logging) ที่เกี่ยวข้องกับการเปลี่ยนแปลงเพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ
- (8) มาตรฐานรักษาความมั่นคงปลอดภัยที่ต้องปฏิบัติตาม เช่น OWASP, SANS Top 20 เป็นต้น
- (9) ความต่อเนื่องของการให้บริการระบบสารสนเทศ (Continuity)

2. การจ้างบุคคลภายนอกพัฒนาและบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- 2.1 ผู้รับจ้างจะต้องจัดเก็บรักษาข้อมูลต่างๆ ที่เกี่ยวกับการดำเนินงานตามสัญญา ซึ่งรวมถึงข้อมูลต่างๆ ที่ผู้ว่าจ้างได้จัดทำขึ้นเนื่องจากการดำเนินงานนี้อย่างเป็นความลับ และผู้รับจ้างต้องหามาตรการในการจัดเก็บข้อมูลที่เป็นความลับให้มิดชิด ทั้งนี้ ผู้รับจ้างจะต้องลงนามใน "สัญญาไม่เปิดเผยข้อมูลที่เป็นความลับ" พร้อมสัญญาจ้าง
- 2.2 ข้อมูลและเอกสารใดๆ ที่ผู้รับจ้างได้รับทราบหรือได้รับจาก สป.พม. หรือผู้รับบริการของ สป.พม. รวมทั้งผลงานที่ส่งมอบ ผู้รับจ้างจะต้องถือเป็นความลับ ไม่นำไปเผยแพร่ให้บุคคลใดทราบเป็นอันขาด เว้นแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง
- 2.3 ผู้รับจ้างจะต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และกฎหมายอื่นที่เกี่ยวข้อง รวมถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม. ประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ สป.พม. และนโยบาย คำสั่ง และข้อปฏิบัติอื่นๆ ที่เกี่ยวข้อง
- 2.4 ผู้รับจ้างจะต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้อง รวมถึงนโยบาย คำสั่ง และข้อปฏิบัติอื่นๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของ สป.พม.
- 2.5 ผู้รับจ้างจะต้องพัฒนาระบบสารสนเทศให้มีการปกป้องข้อมูลสารสนเทศและการใช้งานระบบสารสนเทศผ่านเครือข่ายสาธารณะ (Public networks) อย่างปลอดภัย ดังนี้
 - (1) ไม่พัฒนาระบบสารสนเทศที่จะทำลายกลไกรักษาความปลอดภัยของระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแaggerรหัสผ่านของบุคคลอื่น
 - (2) ไม่พัฒนาระบบสารสนเทศซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญ (Priority) ในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 2 : การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 22 : การกำหนดการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร	รหัสเอกสาร : IC-0222

(3) ไม่พัฒนาระบบสารสนเทศที่จะทำให้ซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือมัลแวร์

(4) ไม่พัฒนาระบบสารสนเทศที่จะทำให้ลายสิทธิการใช้งานซอฟต์แวร์

(5) ไม่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพ ที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย ไม่ว่าจากช่องทางการสื่อสารใดๆ ก็ตาม

2.6 ผู้รับจ้างจะต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้

(1) การให้สิทธิต่ำที่สุด (Least Privileges)

(2) การให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (Need to know)

(3) การออกแบบระบบให้สามารถป้องกันได้หลายๆ ชั้น (Defense in-Depth)

(4) การออกแบบในลักษณะเปิด (Open Design)

(5) พัฒนาระบบสารสนเทศตามหลักการด้านความมั่นคงปลอดภัย (Security Engineering Principles)

2.7 กำหนดให้มีการทดสอบระบบสารสนเทศที่มีการพัฒนา การปรับปรุง หรือจัดหาใหม่ และลงชื่อยอมรับผลการทดสอบโดยผู้ใช้งานระบบ และ/หรือเจ้าของระบบ และ/หรือผู้ดูแลระบบที่เกี่ยวข้องแล้วแต่กรณี ก่อนการดำเนินการติดตั้งเพื่อใช้งานจริง (Production)

2.8 ให้มีการจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูปเฉพาะที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกควบคุมอย่างเข้มงวด ดังนี้

(1) จัดทำรายการ Standard Software List ที่อนุญาตให้ติดตั้งบนระบบปฏิบัติการ (Operating System)

(2) จัดให้มีเครื่องมือ (Tools) หรือการสุ่มตรวจสอบ Software ที่เครื่องคอมพิวเตอร์ของบุคลากรว่าตรงตาม Standard Software List ที่กำหนดไว้

2.9 ผู้ดูแลระบบการให้บริการมีหน้าที่ควบคุมการติดตั้งซอฟต์แวร์โปรแกรมของระบบสารสนเทศสำหรับการใช้งานจริง โดยมีการควบคุมอย่างน้อย ดังนี้

(1) มีการอนุมัติตามขั้นตอน

(2) มีการควบคุมเวอร์ชันหรือการเปลี่ยนแปลงรุ่นของซอฟต์แวร์หรือโปรแกรมที่ใช้งานจริง (Version Change Control)

(3) มีการจัดเก็บรักษาและควบคุมการเข้าถึงชุดคำสั่งต้นฉบับของซอฟต์แวร์โปรแกรม (Source Code)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์
สำนักงานปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์

ส่วนที่ 3

การกำหนดมาตรการตรวจสอบ
และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 3 : การกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	รหัสเอกสาร : IC-0301

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

วัตถุประสงค์

เพื่อเป็นการป้องกันความเสี่ยงที่อาจเกิดจากการโจมตีทางไซเบอร์ โดยการจัดตั้งระบบเฝ้าระวังที่ทำให้สามารถตอบสนองต่อเหตุการณ์ที่น่าสงสัยหรือเป็นภัยคุกคามได้อย่างทันท่วงที

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **เจ้าหน้าที่/ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. **ผู้ใช้งาน** หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. กลไกและขอบเขตของการตรวจสอบและเฝ้าระวัง

- 1.1 ให้จัดทำแผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ และมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายในหรือภายนอกหน่วยงาน โดยมีขอบเขตของการตรวจสอบ ดังนี้
 - 1.1.1 ตรวจสอบการปฏิบัติของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย คำสั่ง แนวปฏิบัติ ข้อปฏิบัติ ที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง
 - 1.1.2 ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของ หน่วยงาน ตามหลักการบริหารความเสี่ยง
 - 1.1.3 ตรวจสอบบริการที่สำคัญของหน่วยงาน ทั้งกรณีที่หน่วยงานเป็นเจ้าของ และใช้บริการจากผู้ให้บริการภายนอก
- 1.2 สร้างกลไกและกระบวนการเพื่อตรวจสอบเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน และทบทวนกลไกและกระบวนการอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่างๆ ยังคงมีประสิทธิภาพ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 3 : การกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	รหัสเอกสาร : IC-0301

2. ระบบตรวจจับภัยคุกคาม (Threat Detection Systems)

ให้มีการจัดหาระบบป้องกันการบุกรุก (Intrusion Prevention Systems - IPS) ในการรักษาความปลอดภัยของเครือข่ายและระบบข้อมูล โดย IPS ทำหน้าที่ตรวจจับและตอบสนองต่อการบุกรุกหรือการกระทำที่ไม่พึงประสงค์ ดังนี้

- 2.1 การตรวจจับการบุกรุก โดยวิเคราะห์ข้อมูลที่ไหลผ่านเครือข่ายและใช้เทคนิคต่างๆ เช่น การตรวจจับตามลายเซ็น (signature-based detection) และการตรวจจับแบบพฤติกรรม (anomaly-based detection) เพื่อตรวจสอบพฤติกรรมที่น่าสงสัย
- 2.2 การตอบสนอง เมื่อ IPS ตรวจพบการกระทำที่เป็นภัยคุกคาม สามารถทำการตอบสนองโดยอัตโนมัติ เช่น การบล็อก IP ของผู้โจมตี, ปิดกั้นการเชื่อมต่อ, หรือแจ้งเตือนผู้ดูแลระบบ เป็นต้น
- 2.3 การบันทึกและรายงาน ซึ่ง IPS บันทึกข้อมูลที่เกี่ยวข้องกับเหตุการณ์การโจมตีและสามารถสร้างรายงานที่ช่วยในการวิเคราะห์และตอบสนองต่อภัยคุกคามในอนาคต

3. การใช้เครื่องมือเฝ้าระวังและตรวจสอบ (Monitoring Tools)

- 3.1 การใช้ Security Information and Event Management (SIEM) โดยระบบ SIEM รวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่ง เช่น เครือข่าย, อุปกรณ์, แอปพลิเคชัน เพื่อตรวจหาภัยคุกคามหรือพฤติกรรมที่ผิดปกติ รวมถึงการแจ้งเตือนในกรณีที่เกิดเหตุการณ์ที่น่าสงสัย
- 3.2 การติดตามกิจกรรมเครือข่าย (Network Monitoring) ใช้ซอฟต์แวร์ตรวจสอบทราฟฟิกในเครือข่ายอย่างละเอียดเพื่อค้นหาการโจมตี เช่น การสแกนพอร์ตที่น่าสงสัยหรือทราฟฟิกที่ผิดปกติ
- 3.3 การวิเคราะห์ Log (Log Analysis) เป็นการวิเคราะห์ Log ที่ถูกบันทึกจากเซิร์ฟเวอร์, อุปกรณ์เครือข่าย และระบบต่างๆ อย่างต่อเนื่อง เพื่อค้นหาสัญญาณที่บ่งบอกถึงการโจมตี

4. การป้องกันภัยคุกคามจากภายนอก (External Threat Protection)

- 4.1 ตรวจสอบข้อมูลที่เกี่ยวข้องกับองค์กรซึ่งอาจรั่วไหลหรือถูกขายใน Dark Web เพื่อป้องกันการโจมตีหรือการใช้ข้อมูลที่ไม่ถูกต้อง
- 4.2 การใช้ Threat Intelligence Feeds : ระบบที่รวบรวมข้อมูลเกี่ยวกับภัยคุกคามใหม่ๆ ทั่วโลก ทำให้สามารถป้องกันการโจมตีที่เกิดขึ้นใหม่ได้ทันเวลา

5. การตรวจสอบและป้องกันภัยจากภายใน (Insider Threat Monitoring)

ให้สิทธิ์การเข้าถึงข้อมูลเฉพาะกับผู้ที่มีความจำเป็น เพื่อลดโอกาสการรั่วไหลหรือการโจมตีจากภายในหน่วยงาน และต้องมีการวิเคราะห์ตรวจสอบพฤติกรรมผู้ใช้งาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์
สำนักงานปลัดกระทรวงการพัฒนากำลังคนและความมั่นคงของมนุษย์

ส่วนที่ 4

การกำหนดมาตรการเผชิญเหตุ
เมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 4 : การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response)	รหัสเอกสาร : IC-0401

การรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response)

วัตถุประสงค์

เพื่อให้ สป.พม. มีการจัดการ และรับมือกับภัยคุกคามทางไซเบอร์ ปกป้องข้อมูล ระบบสารสนเทศ และทรัพย์สินของ สป.พม. จากการโจมตีหรือการละเมิดที่เกิดขึ้น และลดผลกระทบที่อาจเกิดขึ้น

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การเตรียมความพร้อม (Preparation)

- 1.1 ต้องมีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response Plan) โดยมีรายละเอียดอย่างน้อย ดังนี้
 - 1.1.1 สร้างแผนการรับมือเมื่อเกิดเหตุการณ์ภัยคุกคามที่เป็นจริง โดยกำหนดหน้าที่ของบุคลากร และวิธีการสื่อสารในกรณีฉุกเฉิน
 - 1.1.2 ตั้งทีมสำหรับการตอบสนองต่อเหตุการณ์ที่สามารถวิเคราะห์และแก้ไขปัญหาเมื่อเกิดเหตุการณ์การโจมตี รวมถึงทำการกู้คืนข้อมูลหรือระบบให้กลับสู่สภาวะปกติ
 - 1.1.3 นำผลการวิเคราะห์และสรุปบทเรียนจากการโจมตี เพื่อนำไปปรับปรุงมาตรการเฝ้าระวังในอนาคต ทั้งนี้ เพื่อให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ จะต้องมีการทบทวนแผนฯ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อม การปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของหน่วยงาน หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- 1.2 ต้องมีการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ ให้เจ้าหน้าที่และบุคลากรในหน่วยงานรับทราบ
- 1.3 ต้องมีการฝึกซ้อม และจัดฝึกอบรมทีมงานเกี่ยวกับวิธีการรับมือกับเหตุการณ์และการใช้เครื่องมือต่างๆ รวมถึงสร้างความตระหนักในหน่วยงานเกี่ยวกับภัยคุกคามทางไซเบอร์
- 1.4 จัดเตรียมเครื่องมือที่จำเป็นสำหรับการตรวจจับและตอบสนองต่อเหตุการณ์ เช่น ระบบตรวจจับภัยคุกคาม (IDS/IPS) ระบบจัดเก็บ Log และซอฟต์แวร์รักษาความปลอดภัย

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 4 : การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response)	รหัสเอกสาร : IC-0401

2. การตรวจจับและการวิเคราะห์ (Identification & Detection)

2.1 ใช้เครื่องมือและเทคนิคต่างๆ เช่น ระบบตรวจจับการบุกรุก หรือการตรวจสอบบันทึกกิจกรรม (Log Monitoring) เพื่อตรวจจับเหตุการณ์ที่อาจเป็นภัยคุกคาม

2.2 เมื่อถูกตรวจพบเหตุการณ์ความไม่มั่นคงปลอดภัย จะต้องทำการวิเคราะห์ว่าปัญหาคืออะไร มาจากที่ใด และมีผลกระทบอย่างไร

3. การควบคุมสถานการณ์ (Containment)

3.1 การควบคุมระยะสั้น ต้องดำเนินการเพื่อยุติการแพร่กระจายของภัยคุกคามอย่างรวดเร็ว เช่น การตัดการเชื่อมต่อระบบที่ได้รับผลกระทบ

3.2 การควบคุมระยะยาว วางแผนเพื่อให้สามารถดำเนินการแก้ไขได้อย่างถาวรและลดความเสี่ยงที่เหตุการณ์จะเกิดซ้ำ เช่น การปรับปรุงการตั้งค่าความปลอดภัย

4. การกำจัด (Eradication)

เมื่อสามารถควบคุมสถานการณ์ได้แล้ว ให้ดำเนินการกำจัดสาเหตุของภัยคุกคาม เช่น การลบมัลแวร์ การกำจัดบัญชีผู้ใช้ที่เป็นอันตราย หรือการแก้ไขช่องโหว่ในระบบ

5. การกู้คืน (Recovery)

หลังจากกำจัดภัยคุกคามแล้ว จำเป็นต้องกู้คืนระบบให้กลับมาใช้งานได้ตามปกติ โดยต้องตรวจสอบว่าระบบปลอดภัยเพียงพอและไม่มีภัยคุกคามหลงเหลืออยู่ เช่น การนำระบบกลับมาออนไลน์ การทดสอบการทำงานของระบบ และการสำรองข้อมูล

6. การเรียนรู้และการปรับปรุง (Lessons Learned)

หลังจากเหตุการณ์สิ้นสุด ควรมีการวิเคราะห์เหตุการณ์เพื่อเรียนรู้จากข้อผิดพลาดหรือปัญหาที่เกิดขึ้น บันทึกและรายงานเหตุการณ์ เพื่อให้หน่วยงานสามารถปรับปรุงกระบวนการตอบสนองในอนาคตได้ดียิ่งขึ้น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 4 : การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การสื่อสารในภาวะวิกฤต (Crisis Communication)	รหัสเอกสาร : IC-0402

การสื่อสารในภาวะวิกฤต (Crisis Communication)

วัตถุประสงค์

เพื่อให้ สป.พม. มีแนวทางที่ชัดเจนในการสื่อสารในภาวะวิกฤต สร้างความเชื่อมั่น ลดความตื่นตระหนก และสามารถรับมือและบริหารจัดการกับสถานการณ์ฉุกเฉินทางด้านความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ได้อย่างมีประสิทธิภาพ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **เจ้าหน้าที่/ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. **ผู้ใช้งาน** หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การเตรียมความพร้อมก่อนภาวะวิกฤต

- 1.1 จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ โดยมีรายละเอียด ดังนี้
 - 1.1.1 จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต
 - 1.1.2 ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง
 - 1.1.3 ระบุกลุ่มเป้าหมาย และผู้ที่มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
 - 1.1.4 ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนของหน่วยงานเมื่อกล่าวแถลงกับสื่อมวลชน
 - 1.1.5 ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม สำหรับการเผยแพร่ข้อมูล
 - 1.1.6 การประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบมีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต
- 1.2 ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันทั่วถึง และมีประสิทธิภาพในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
- 1.3 จัดเตรียมเอกสารข้อมูลพื้นฐานเกี่ยวกับองค์กร การป้องกัน และการดำเนินงาน เพื่อใช้ในการสื่อสารเมื่อเกิดวิกฤต

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 4 : การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การสื่อสารในภาวะวิกฤต (Crisis Communication)	รหัสเอกสาร : IC-0402

2. การตอบสนองต่อการเกิดสถานการณ์วิกฤต

- 2.1 ต้องตอบสนองอย่างรวดเร็วภายในช่วงเวลาแรกที่เกิดวิกฤต เพื่อแสดงความรับผิดชอบและสร้างความเชื่อมั่นให้กับสาธารณะ
- 2.2 การสื่อสารควรเน้นความถูกต้อง โปร่งใส และไม่ปกปิดข้อมูลที่สำคัญ แม้ว่ายังไม่มีข้อมูลที่ครบถ้วน ก็ควรสื่อสารสิ่งที่รู้ ณ ขณะนั้น
- 2.3 ควรมีโฆษกหรือผู้บริหารระดับสูงเป็นตัวแทนในการสื่อสารเพื่อเพิ่มความน่าเชื่อถือ และมั่นใจได้ว่าข้อความที่สื่อออกมาเป็นไปในแนวทางเดียวกัน

3. การฟื้นฟูหลังจากเกิดสถานการณ์วิกฤต

- 3.1 หลังจากสถานการณ์วิกฤตสิ้นสุดลง ควรมีการทบทวนและวิเคราะห์ถึงการสื่อสารและการจัดการสถานการณ์วิกฤตว่าได้ผลอย่างไร เพื่อปรับปรุงแผนการสื่อสารในอนาคต
- 3.2 ควรฟื้นฟูภาพลักษณ์และความน่าเชื่อถือของหน่วยงานต่อสาธารณะ
- 3.3 หากมีการเปลี่ยนแปลงใดๆ ควรสื่อสารให้สาธารณะทราบอย่างชัดเจน เพื่อสร้างความเชื่อมั่นว่าสถานการณ์วิกฤตได้รับการแก้ไขแล้ว

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 4 : การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Exercise)	รหัสเอกสาร : IC-0403

การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Exercise)

วัตถุประสงค์

เพื่อทดสอบและพัฒนาขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่นๆ ที่เกี่ยวข้อง ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ทั้งในด้านกระบวนการบริหารจัดการขีดความสามารถขององค์กร และแผนที่เกี่ยวข้อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. กำหนดวัตถุประสงค์และเป้าหมายของการฝึกซ้อม

- 1.1 ระบุสิ่งที่ต้องการทดสอบ เช่น การตอบสนองต่อเหตุการณ์ (incident response) การป้องกันระบบ หรือการตรวจสอบการละเมิดข้อมูล
- 1.2 วัตถุประสงค์อาจรวมถึงการตรวจสอบกระบวนการภายใน การทดสอบความสามารถของทีมรักษาความปลอดภัย หรือการสร้างความตระหนักในความเสี่ยงไซเบอร์ให้กับเจ้าหน้าที่

2. ประเภทของการฝึกซ้อม

- 2.1 Tabletop Exercise (TTX) : การจำลองสถานการณ์เป็นการประชุมหรือสนทนาระหว่างผู้ที่มีบทบาทสำคัญในการจัดการกับเหตุการณ์ โดยไม่มีการใช้งานระบบจริง
- 2.2 Red Team vs Blue Team : ฝ่ายแดง (Red Team) ทำหน้าที่โจมตีเพื่อหาช่องโหว่ ขณะที่ฝ่ายน้ำเงิน (Blue Team) ป้องกันและรับมือกับการโจมตี
- 2.3 Full-scale Simulation : การจำลองสถานการณ์อย่างเต็มรูปแบบที่ใช้ระบบจริงและทดสอบการทำงานของทุกฝ่ายที่เกี่ยวข้อง

3. ออกแบบสถานการณ์การฝึกซ้อม

- 3.1 การกำหนดภัยคุกคาม : กำหนดภัยคุกคามตามความเป็นจริง เช่น การโจมตีแบบ Phishing, Ransomware, DDoS, หรือการโจมตีผ่านทาง Insider Threat
- 3.2 การกำหนดผลกระทบ : ระบุว่าภัยคุกคามนั้นจะส่งผลกระทบต่อหน่วยงานอย่างไร เช่น การสูญเสียข้อมูล การหยุดชะงักของบริการ หรือการสูญเสียความเชื่อมั่นจากผู้ใช้งาน
- 3.3 ระยะเวลาของการฝึกซ้อม : ระบุเวลาที่จะใช้ในการฝึกซ้อม รวมถึงการตอบสนองในสถานการณ์วิกฤต

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 4 : การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 3 : การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Exercise)	รหัสเอกสาร : IC-0403

4. กำหนดทีมที่เข้าร่วม

- 4.1 ผู้บริหาร : ผู้บริหารระดับสูงที่มีหน้าที่ตัดสินใจในกรณีเกิดเหตุฉุกเฉิน
- 4.2 ทีม IT และ Cyber Security : ทีมที่รับผิดชอบในการรักษาความปลอดภัยของระบบ
- 4.3 ทีมกฎหมายและประชาสัมพันธ์ : มีหน้าที่ติดต่อสื่อสารกับสาธารณะและดูแลเรื่องการปฏิบัติตามกฎหมาย
- 4.4 ทีมจากฝ่ายอื่นๆ : การฝึกซ้อมควรรวมถึงตัวแทนจากทุกส่วนงานที่อาจได้รับผลกระทบจากการโจมตี

5. การวัดผลและประเมินผล

- 5.1 การติดตามการตอบสนอง : ประเมินการตอบสนองของทีมว่าทำงานได้รวดเร็วและมีประสิทธิภาพหรือไม่
- 5.2 การบันทึกและรายงาน : บันทึกเหตุการณ์ที่เกิดขึ้นจริงและผลกระทบที่ได้รับในสถานการณ์จำลองเพื่อใช้เป็นบทเรียน
- 5.3 การสรุปผล : หลังการฝึกซ้อม ควรมีการสรุปผล วิเคราะห์ความสำเร็จและข้อบกพร่อง รวมถึงการปรับปรุงแผนการรักษาความปลอดภัยไซเบอร์ในอนาคต

6. การปรับปรุงแผนการรักษาความปลอดภัยไซเบอร์

เมื่อสิ้นสุดการฝึกซ้อม ควรนำข้อมูลที่ได้จากการประเมินมาปรับปรุงแผนการรักษาความปลอดภัยและเตรียมพร้อมสำหรับการฝึกซ้อมในครั้งต่อไป

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ส่วนที่ 5

การกำหนดมาตรการรักษาและฟื้นฟูความเสียหาย
ที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การสำรองและทดสอบกู้คืนข้อมูล	รหัสเอกสาร : IC-0501

การสำรองและทดสอบกู้คืนข้อมูล

วัตถุประสงค์

เพื่อให้หน่วยงานมีระบบสำรองข้อมูลและสารสนเทศที่เหมาะสม และมีการเตรียมความพร้อมกรณีฉุกเฉิน หากไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้หน่วยงานสามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **คณะทำงาน** หมายถึง คณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
3. **เจ้าหน้าที่** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย

แนวปฏิบัติ

1. การดำเนินงาน

- 1.1 แต่งตั้งคณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนาระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นประธาน
- 1.2 ประชุมคณะทำงานฯ เพื่อจัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉินของ สป.พม.
- 1.3 นำเสนอร่างแผนฯ ต่อปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ เพื่อขอความเห็นชอบ
- 1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน
- 1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผนฯ
- 1.6 ทบทวน/ปรับปรุงแผนฯ ปีละ 1 ครั้ง

2. การสำรองและทดสอบกู้คืนข้อมูล

- 2.1 จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของ สป.พม.
- 2.2 พิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นตามลำดับความสำคัญ เพื่อจัดทำระบบสำรอง
- 2.3 กำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง
- 2.4 กำหนดสื่อที่ใช้ในการเก็บข้อมูล และรูปแบบของการสำรองข้อมูล ซึ่งมี 2 ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การสำรองและทดสอบกู้คืนข้อมูล	รหัสเอกสาร : IC-0501

2.5 รายการที่ต้องสำรองข้อมูลและความถี่อย่างน้อย ดังนี้

- เว็บไซต์หน่วยงาน : สำรองข้อมูลที่เผยแพร่บนเว็บไซต์ 1 ครั้ง/สัปดาห์
- Web Application Servers : สำรองข้อมูลที่เผยแพร่บนเว็บไซต์ 1 ครั้ง/เดือน
- Database Servers : สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ ทุกวัน
- Firewall Server : สำรองข้อมูล Rule ของ Firewall 1 ครั้ง/สัปดาห์
- Server อื่นๆ : สำรองข้อมูลบนเซิร์ฟเวอร์อื่นๆ เช่น ระบบงานต่างๆ 1 ครั้ง/เดือน

2.6 มีการสำรองข้อมูลเครื่องแม่ข่ายทั้งระบบ (Full System Backup) อย่างน้อยปีละ 1 ครั้ง

2.7 กำหนดขั้นตอนปฏิบัติและโปรแกรมในการสำรองข้อมูลและทดสอบกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้อง

2.8 กำหนดการเข้ารหัสข้อมูลในการสำรองข้อมูลที่สำคัญ โดยใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

2.9 จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูลที่เหมาะสมกับสำคัญของแต่ละระบบสารสนเทศ

2.10 รายละเอียดที่ปรากฏในแผนการสำรองและทดสอบกู้คืนข้อมูล ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้

- รายการที่ต้องสำรองข้อมูล
- การสำรองข้อมูล
- การทดสอบกู้คืนข้อมูล
- ปฏิทินการสำรองและทดสอบกู้คืนข้อมูล
- ผู้รับผิดชอบ
- การติดตามประเมินผล

2.11 มอบหมายเจ้าหน้าที่หลักเพื่อดำเนินงานตามแผนการสำรองและทดสอบกู้คืนข้อมูล และเจ้าหน้าที่สำรองเพื่อทำหน้าที่สำรองข้อมูลในกรณีที่เจ้าหน้าที่หลักไม่สามารถปฏิบัติงานได้ โดยเจ้าหน้าที่มีหน้าที่ ดังนี้

2.11.1 จัดทำคู่มือการสำรองและทดสอบกู้คืนข้อมูล

2.11.2 ดำเนินการตามปฏิทินการสำรองและทดสอบกู้คืนข้อมูล

2.11.3 บันทึกการสำรองข้อมูล (Operator Logs) และจัดทำรายงานผลการสำรองข้อมูลประจำเดือน โดยมีรายละเอียดอย่างน้อย ดังนี้ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

2.11.4 กรณีพบปัญหาในการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหา และรายงานให้ผู้บังคับบัญชาทราบ

2.11.5 ตรวจสอบผลการสำรองข้อมูลว่าถูกต้องและสมบูรณ์ พร้อมทั้งบันทึกผลการตรวจสอบ

2.11.6 จัดเก็บสื่อบันทึกข้อมูลไว้ในที่ที่ปลอดภัย

2.11.7 มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล

2.11.8 มีการทดสอบกู้คืนข้อมูลจากข้อมูลที่สำรองเก็บไว้ อย่างน้อยปีละ 1 ครั้ง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การสำรองและทดสอบกู้คืนข้อมูล	รหัสเอกสาร : IC-0501

2.11.9 กรณีพบปัญหาที่สร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนทำให้ต้องกู้คืนระบบ เจ้าหน้าที่จะต้องดำเนินการแก้ไขปัญหา พร้อมทั้งสรุปรายงานการปฏิบัติงาน และการแก้ไขปัญหาให้ผู้บังคับบัญชาทราบ

2.11.10 การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

2.11.11 หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้ระบบทราบทันที พร้อมทั้งรายงานความก้าวหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

2.11.12 สรุปรผลการดำเนินงานรายปีให้ผู้บังคับบัญชารับทราบ โดยการวิเคราะห์ผลการปฏิบัติงาน และรายงานตามประเด็นสำคัญอย่างน้อย ดังนี้ สรุปรผลการดำเนินงาน ปัญหาอุปสรรค วิธีการแก้ไข และข้อเสนอแนะ

2.12 ติดตามประเมินผล และทบทวน/ปรับปรุงแผนการสำรองและทดสอบกู้คืนข้อมูล ปีละ 1 ครั้ง

3. การเตรียมความพร้อมกรณีฉุกเฉิน

3.1 จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของ สป.พม.

3.2 พิจารณาคัดเลือกสถานการณ์ฉุกเฉินหรือภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของ สป.พม. โดยมีสถานการณ์อย่างน้อย ดังนี้ อัคคีภัย ระบบไฟฟ้าขัดข้อง และระบบปรับอากาศผิดปกติ

3.3 รายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉิน ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้

- ประเภทของสถานการณ์ฉุกเฉินหรือภัยพิบัติ
- การเตรียมความพร้อม
- การแก้ปัญหา
- ขั้นตอนการปฏิบัติ
- ผู้รับผิดชอบ
- การติดตามประเมินผล

3.4 พิจารณาคัดเลือกสถานการณ์ฉุกเฉินหรือภัยพิบัติ เพื่อซักซ้อมแผนรับสถานการณ์ อย่างน้อยปีละ 1 กรณี

3.5 มอบหมายเจ้าหน้าที่ผู้รับผิดชอบเพื่อดำเนินงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน โดยเจ้าหน้าที่มีหน้าที่ ดังนี้

3.5.1 จัดเตรียมอุปกรณ์ที่จำเป็น เพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่อาจเกิดขึ้น

3.5.2 ตรวจสอบและบันทึกผลการตรวจสอบความพร้อมของระบบและอุปกรณ์ตามระยะเวลา พร้อมทั้งจัดทำรายงานผลการดำเนินงาน โดยมีรายละเอียดอย่างน้อย ดังนี้ วันที่ทำการตรวจสอบ เอกสารหลักฐาน/ซอฟต์แวร์ที่ควรจัดเตรียม เป็นต้น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การสำรองและทดสอบกู้คืนข้อมูล	รหัสเอกสาร : IC-0501

3.5.3 กรณีชักซ้อมแผน/เกิดปัญหา เจ้าหน้าที่จะต้องรายงานข้อเท็จจริงและการแก้ไขปัญหา พร้อมทั้งสรุปผลการปฏิบัติงานและการแก้ไขปัญหาให้ผู้บังคับบัญชาทราบ

3.5.4 บันทึกเหตุการณ์/สถานการณ์ฉุกเฉินที่เกิดขึ้น โดยพิจารณาถึง ประเภท ปริมาณ และหลักฐานสำหรับอ้างอิง เพื่อใช้ในการกรณีที่เหตุการณ์มีความเกี่ยวข้องกับทางกฎหมาย

3.5.5 สรุปผลการดำเนินงานรายปีให้ผู้บังคับบัญชารับทราบ โดยการวิเคราะห์ผลการปฏิบัติงานและรายงานตามประเด็นสำคัญอย่างน้อย ดังนี้ สรุปผลการดำเนินงาน ปัญหาอุปสรรค วิธีการแก้ไข และข้อเสนอแนะ

3.6 ติดตามประเมินผล และทบทวน/ปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ปีละ 1 ครั้ง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	รหัสเอกสาร : IC-0502

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

วัตถุประสงค์

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) เป็นกระบวนการสำคัญในการทำให้องค์กรกลับมาดำเนินงานได้อย่างปกติ โดยมีวัตถุประสงค์หลักเพื่อเร่งรัดการฟื้นฟูระบบและข้อมูลที่เสียหาย ให้สามารถกลับมาใช้งานได้อย่างรวดเร็วและปลอดภัย รวมถึงการปรับปรุงระบบความปลอดภัยเพื่อป้องกันภัยคุกคามในอนาคต การฟื้นฟูยังต้องอาศัยการประสานงานกับผู้เชี่ยวชาญทั้งภายในและภายนอกองค์กรเพื่อให้การแก้ไขปัญหาเป็นไปอย่างมีประสิทธิภาพ นอกจากนี้ การบันทึกเหตุการณ์และเรียนรู้จากการโจมตีจะช่วยให้องค์กรพัฒนากลยุทธ์การป้องกันและฟื้นฟูในระยะยาว อีกทั้งยังสามารถสื่อสารกับลูกค้าและผู้ใช้งานได้อย่างโปร่งใส เพื่อสร้างความมั่นใจว่าข้อมูลและระบบได้รับการปกป้องอย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การวางแผนฟื้นฟูระบบ

องค์กรควรมีแผนฟื้นฟูระบบ (Disaster Recovery Plan) ที่ครอบคลุมทั้งการกู้คืนข้อมูล การฟื้นฟูระบบงาน และการจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีการทบทวนและปรับปรุงแผนอย่างต่อเนื่อง จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงาน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบถามแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน ความสอดคล้องกับขอบเขต คำนิยาม และการกำหนดระยะเวลาที่สำคัญ เช่น Maximum Tolerance Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น และต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์ และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 2 : การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	รหัสเอกสาร : IC-0502

2. การสำรองข้อมูล

ควรมีนโยบายในการสำรองข้อมูล (Backup Policy) ที่ชัดเจนและครอบคลุมข้อมูลสำคัญทั้งหมด การสำรองข้อมูลควรทำอย่างสม่ำเสมอ และเก็บข้อมูลสำรองไว้ในที่ปลอดภัยหรือสถานที่นอกกระบวนหลัก (Offsite)

3. การฝึกอบรมและการจำลองสถานการณ์

จัดการฝึกอบรมบุคลากรให้มีความรู้ความเข้าใจในการรับมือกับภัยคุกคามทางไซเบอร์ และจัดทำ การจำลองสถานการณ์ (Incident Response Drills) เพื่อทดสอบกระบวนการฟื้นฟูและการกู้คืนระบบ

4. การประสานงานกับหน่วยงานที่เกี่ยวข้อง

ควรมีการกำหนดบทบาทและความรับผิดชอบของแต่ละฝ่ายในการฟื้นฟูระบบ รวมถึงการประสานงานกับหน่วยงานภายนอก เช่น บริษัทผู้ให้บริการด้านความปลอดภัยทางไซเบอร์ หรือหน่วยงานภาครัฐที่เกี่ยวข้อง

5. การวิเคราะห์และปรับปรุงระบบหลังการโจมตี

หลังจากการฟื้นฟู องค์กรควรทำการวิเคราะห์สาเหตุของการโจมตี รวมถึงช่องโหว่ที่ถูกโจมตี เพื่อปรับปรุงระบบความปลอดภัยและป้องกันไม่ให้เกิดปัญหาซ้ำ

6. การสื่อสารในภาวะวิกฤต

ควรมีแนวทางในการสื่อสารกับบุคลากร ผู้ใช้งาน และผู้รับบริการอย่างโปร่งใสและรวดเร็ว เมื่อเกิด การโจมตี เพื่อสร้างความมั่นใจว่ามีการฟื้นฟูและป้องกันความเสียหายอย่างเต็มที่



ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ICTC.M-SOCIETY.GO.TH

