คู่มือการให้บริการ

การดำเนินการเกี่ยวกับ ความมั่นคงปลอดภัย ทางไซเบอร์

(Cyber Security)

เสริมสร้างความปลอดภัย ปกป้องข้อมูล มั่นใจในทุกการใช้งาน

ปกป้องข้อมูลสำคัญ
รักษาความลับและความถูกต้องของข้อมูล

เฝ้าระวังและตรวจจับภัยคุกคาม
ติดตาม วิเคราะห์ และแจ้งเตือนเหตุการณ์ผิดปกติ

ควบคุมการเข้าถึงข้อมูล
กำหนดสิทธิ์การใช้งานอย่างเหมาะสมตามนโยบาย

สร้างความตระหนักรู้
ส่งเสริมความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

สำนักงานเขตพื้นที่การศึกษาประกมศึกษาเลย เขต 1
สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
กระทรวงศึกษาธิการ

"ปลอดภัย มั่นใจ ห่างไกลภัยไซเบอร์"

ปลอดภัย มั่นใจ พร้อมดูแล ร่วมสร้างความเชื่อมั่น

คำนำ

คู่มือการให้บริการ **การดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)** จัดทำขึ้นเพื่อเป็นแนวทางในการให้บริการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ สำหรับสำนักงานเขตพื้นที่การศึกษาและสถานศึกษาในสังกัด โดยมีวัตถุประสงค์เพื่อสร้างความเข้าใจเกี่ยวกับขั้นตอน วิธีการ และแนวทางการขอรับบริการ รวมถึงส่งเสริมให้ผู้รับบริการสามารถเข้าถึงบริการด้านความปลอดภัยทางไซเบอร์ได้อย่างถูกต้อง รวดเร็ว และมีประสิทธิภาพ

เนื้อหาภายในคู่มือประกอบด้วยรายละเอียดเกี่ยวกับการให้บริการด้าน Cyber Security การรับแจ้งปัญหา การให้คำปรึกษา การตรวจสอบและวิเคราะห์ปัญหา การดำเนินการแก้ไขหรือให้คำแนะนำ การติดตามผลตลอดจนแนวทางการป้องกันภัยคุกคามทางไซเบอร์ เพื่อช่วยลดความเสี่ยงที่อาจส่งผลกระทบต่อข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่าย และโครงสร้างพื้นฐานด้านสารสนเทศของหน่วยงาน

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาเลย เขต 1 หวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้จะเป็นประโยชน์แก่บุคลากร ผู้รับบริการ และผู้เกี่ยวข้อง ในการใช้เป็นแนวทางการติดต่อขอรับบริการ รวมถึงเป็นเครื่องมือในการส่งเสริมความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ อันจะนำไปสู่การบริหารจัดการระบบเทคโนโลยีสารสนเทศที่มีความมั่นคง ปลอดภัย และมีประสิทธิภาพต่อไป

กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานเขตพื้นที่การศึกษาประถมศึกษาเลย เขต 1

สารบัญ

เรื่อง	หน้า
คำนำ	ก
สารบัญ	ข
คู่มือการให้บริการ การดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)	1
1. ชื่องานและรายละเอียดงานบริการ	1
2. วิธีการ ขั้นตอนการขอรับบริการ	1
2.1 รับคำขอรับบริการ	1
2.2 ตรวจสอบและวิเคราะห์ปัญหา	1
2.3 ดำเนินการแก้ไขหรือให้คำแนะนำ	1
2.4 ติดตามผลการดำเนินงาน	1
2.5 ให้ความรู้และสร้างความตระหนักด้าน Cyber Security	1
3. ระยะเวลาที่ใช้ในการขอรับบริการ	2
4. ช่องทางให้บริการ	2
4.1 ติดต่อด้วยตนเอง	2
4.2 E-Service	2
4.3 One Stop Service	2
4.4 ช่องทางติดต่ออื่น ๆ	2
5. ค่าธรรมเนียม	2
6. รายการเอกสารหลักฐานประกอบการยื่นคำขอรับบริการ	3
6.1 กรณีแจ้งปัญหาหรือขอคำปรึกษา	3
6.2 กรณีแจ้งเหตุด้านความมั่นคงปลอดภัยไซเบอร์	3
6.3 กรณีขอติดตั้งหรือปรับปรุงระบบ	3

(1) ชื่องาน การให้บริการด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

รายละเอียดงานบริการ

ให้บริการคำปรึกษา สนับสนุน ตรวจสอบ และดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่าย และโครงสร้างพื้นฐานด้านสารสนเทศของสำนักงานเขตพื้นที่การศึกษาและสถานศึกษาในสังกัด

(2) วิธีการ ขั้นตอนการขอรับบริการ

ขั้นตอนการให้บริการ

1. รับคำขอรับบริการ

- ☐ ผู้รับบริการแจ้งปัญหา ขอคำปรึกษา หรือแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
- ☐ ระบุรายละเอียดปัญหา เช่น ระบบขัดข้อง การถูกโจมตี การเข้าถึงข้อมูลผิดปกติ หรือข้อสงสัยด้านความปลอดภัย

2. ตรวจสอบและวิเคราะห์ปัญหา

- ☐ เจ้าหน้าที่กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร ตรวจสอบข้อมูล
- ☐ วิเคราะห์สาเหตุและประเมินความเสี่ยงด้านความปลอดภัย

3. ดำเนินการแก้ไขหรือให้คำแนะนำ

ดำเนินการตามความเหมาะสม เช่น

- ☐ ตรวจสอบระบบเครือข่าย
- ☐ ตรวจสอบการตั้งค่าความปลอดภัย
- ☐ ให้คำแนะนำการป้องกันภัยคุกคาม
- ☐ ดำเนินการเกี่ยวกับระบบ Firewall
- ☐ ระบบ Antivirus/AntiMalware
- ☐ ระบบ Endpoint Security
- ☐ ระบบยืนยันตัวตนและควบคุมสิทธิ
- ☐ ระบบจัดเก็บ Log File ให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

4. ติดตามผลการดำเนินงาน

- ☐ ตรวจสอบผลการแก้ไข
- ☐ ประเมินความเรียบร้อย
- ☐ รายงานผลการดำเนินงานต่อผู้เกี่ยวข้อง

5. ให้ความรู้และสร้างความตระหนัก

- ☐ เผยแพร่แนวทางปฏิบัติด้าน Cyber Security
- ☐ ส่งเสริมความรู้แก่บุคลากรในสำนักงานเขตพื้นที่การศึกษาและสถานศึกษา

(3) ระยะเวลาที่ใช้ในการขอรับบริการ

รายการบริการ	ระยะเวลา
ให้คำปรึกษาและแนะนำด้าน Cyber Security	ภายใน 1 วันทำการ
ตรวจสอบปัญหาระบบทั่วไป	ภายใน 1–3 วันทำการ
ดำเนินการติดตั้ง/ปรับปรุงระบบความปลอดภัย	ตามความซับซ้อนของงาน
กรณีเหตุการณ์ภัยคุกคามทางไซเบอร์	ดำเนินการโดยเร่งด่วนตามระดับความรุนแรง

ระยะเวลาการดำเนินงานอ้างอิงตามขั้นตอนมาตรฐานงาน เช่น การศึกษาแนวทาง 3 วันทำการ การจัดทำแผน 3–5 วันทำการ และการติดตามรายงานผล 3 วันทำการ

(4) ช่องทางให้บริการ

1. ติดต่อด้วยตนเอง

กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาเลย เขต 1

2. E-Service

- ☐ ระบบรับแจ้งปัญหาด้านเทคโนโลยีสารสนเทศ (ถ้ามี)
- ☐ ช่องทางออนไลน์ของสำนักงานเขตพื้นที่การศึกษา

3. One Stop Service

จุดบริการงานเทคโนโลยีสารสนเทศและการสื่อสาร

ให้บริการรับเรื่อง ตรวจสอบ วิเคราะห์ และประสานการแก้ไขปัญหาแบบครบวงจร

4. ช่องทางติดต่อ

- ☐ เว็บไซต์สำนักงานเขตพื้นที่การศึกษาประถมศึกษาเลย เขต 1
- ☐ โทรศัพท์สำนักงาน
- ☐ อีเมลหน่วยงาน

(5) ค่าธรรมเนียม

ไม่มีค่าธรรมเนียมในการขอรับบริการ

การให้บริการด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นภารกิจสนับสนุนด้านเทคโนโลยีสารสนเทศของสำนักงานเขตพื้นที่การศึกษา ไม่มีค่าใช้จ่ายสำหรับผู้รับบริการ

(6) รายการเอกสารหลักฐานประกอบการยื่นคำขอรับบริการ

กรณีแจ้งปัญหาหรือขอคำปรึกษา

1. แบบคำขอรับบริการ (ถ้ามี)
2. รายละเอียดปัญหาหรือเหตุการณ์ที่เกิดขึ้น
3. ข้อมูลผู้ติดต่อ เช่น
    - ชื่อ–นามสกุล
    - หน่วยงาน/สถานศึกษา
    - หมายเลขโทรศัพท์
    - อีเมล

กรณีแจ้งเหตุด้านความมั่นคงปลอดภัยไซเบอร์

1. รายงานเหตุการณ์หรือรายละเอียดภัยคุกคาม
2. วัน เวลา ที่เกิดเหตุ
3. ระบบหรืออุปกรณ์ที่ได้รับผลกระทบ
4. ภาพหน้าจอหรือหลักฐานที่เกี่ยวข้อง (ถ้ามี)
5. รายละเอียดบัญชีผู้ใช้งานหรือระบบที่เกี่ยวข้อง (ตามความจำเป็น)

กรณีขอติดตั้งหรือปรับปรุงระบบ

1. หนังสือขอรับบริการ/ขอความอนุเคราะห์
2. รายละเอียดระบบหรืออุปกรณ์
3. ข้อมูลเครือข่ายหรือโครงสร้างพื้นฐานที่เกี่ยวข้อง
4. แบบรายงานหรือเอกสารประกอบตามที่หน่วยงานกำหนด

๑๓. ดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

๑. ชื่องาน

ดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร (Cyber Security)

๒. วัตถุประสงค

๒.๑ เพื่อให้สำนักงานเขตพื้นที่การศึกษามีกระบวนการบริหารจัดการที่ส งผลให องคกรปราศจากความเสี่ยงและความเสียหายที่มีผลต อความปลอดภัยของข อมูลขาวสาร (Information) ในทุกรูปแบบตามแนวทางความมั่นคงปลอดภัยทางไซเบอร (Cyber Security)

๒.๒ เพื่อให้สำนักงานเขตพื้นที่การศึกษา บริหารจัดการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร (Cyber Security) ของสำนักงานเขตพื้นที่การศึกษาเปนไปตามเกณฑที่กฎหมายกำหนด

๒.๓ เพื่อสงเสริม สนับสนุน กระบวนการการบริหารจัดการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร (Cyber Security) ใหกับสถานศึกษาในสังกัด

๓. ขอบเขตของงาน

ดำเนินการเกี่ยวกับกระบวนการบริหารจัดการที่สงผลให องคกรปราศจากความเสี่ยงและความเสียหายที่มีผลต อความปลอดภัยของข อมูลขาวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป องกันต อการกออาชญากรรมการโจมตี การบอนทำลาย และความผิดพลาดตาง ๆ โดยคำนึงถึงองคประกอบพื้นฐานของความปลอดภัยของข อมูลตามแนวทางความมั่นคงปลอดภัยทางไซเบอร (Cyber Security) รวมถึงการให ความรูความเขาใจกับบุคลากรของสำนักงานเขตพื้นที่การศึกษา และสถานศึกษาในสังกัด

๔. คำจำกัดความ

“ขอมูลขาวสาร” หมายความวา สิ่งที่สื่อความหมายให รูเรื่องราวข อเท็จจริง ขอมูล หรือสิ่งใด ๆ ไมวาการสื่อความหมายนั้นจะทำไดโดยสภาพของสิ่งนั้นเองหรือโดยผานวิธีการใด ๆ และไมวาจะได จัดทำไวในรูปแบบของเอกสารแฟม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถาย ฟลม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอรหรือวิธีอื่นใดที่ทำใหสิ่งที่บันทึกไวปรากฏได

“ความมั่นคงปลอดภัยไซเบอร” (Cyber Security) หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อปองกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอรทั้งจากภายในและภายนอกประเทศอันกระทบต อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร อยภายในประเทศ โดยการนำเครื่องมือทางด านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว เพื่อปองกันและรับมือที่อาจจะถูกโจมตีเขามายังอุปกรณเครือขาย โครงสรางพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเขาถึงจากบุคคลที่สามโดยไมไดรับอนุญาต

“ขอมูลขาวสารของราชการ” หมายความวา ขอมูลขาวสารที่อยู ในความครอบครองหรือควบคุมดูแลของหนวยงานของรัฐ ไมวาจะเปนขอมูลขาวสารเกี่ยวกับการดำเนินงานของรัฐหรือขอมูลขาวสารเกี่ยวกับเอกชน

๕. ขั้นตอนการปฏิบัติงาน

๕.๑ ศึกษากฎหมาย ระเบียบ นโยบาย แนวทางการดำเนินการ

๕.๒ จัดทำแผนการดำเนินการความมั่นคงปลอดภัยทางไซเบอรของสำนักงานเขตพื้นที่การศึกษา

๕.๓ จัดตั้งคณะทำงานเพื่อบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร (Cyber Security)

๕.๔ เสนอผูอำนวยการสำนักงานเขตพื้นที่การศึกษาอนุมัติ

๕.๕ ดำเนินการในสวนที่เกี่ยวข่องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร (Cyber Security) ของสำนักงานเขตพื้นที่การศึกษา

๕.๕.๑ ติดตั้งใชงานอุปกรณ Network Firewall

๕.๕.๒ ติดตั้งใชงานโปรแกรม Antivirus/AntiMalware

๕.๕.๓ ติดตั้งใชงานระบบ Endpoint Security

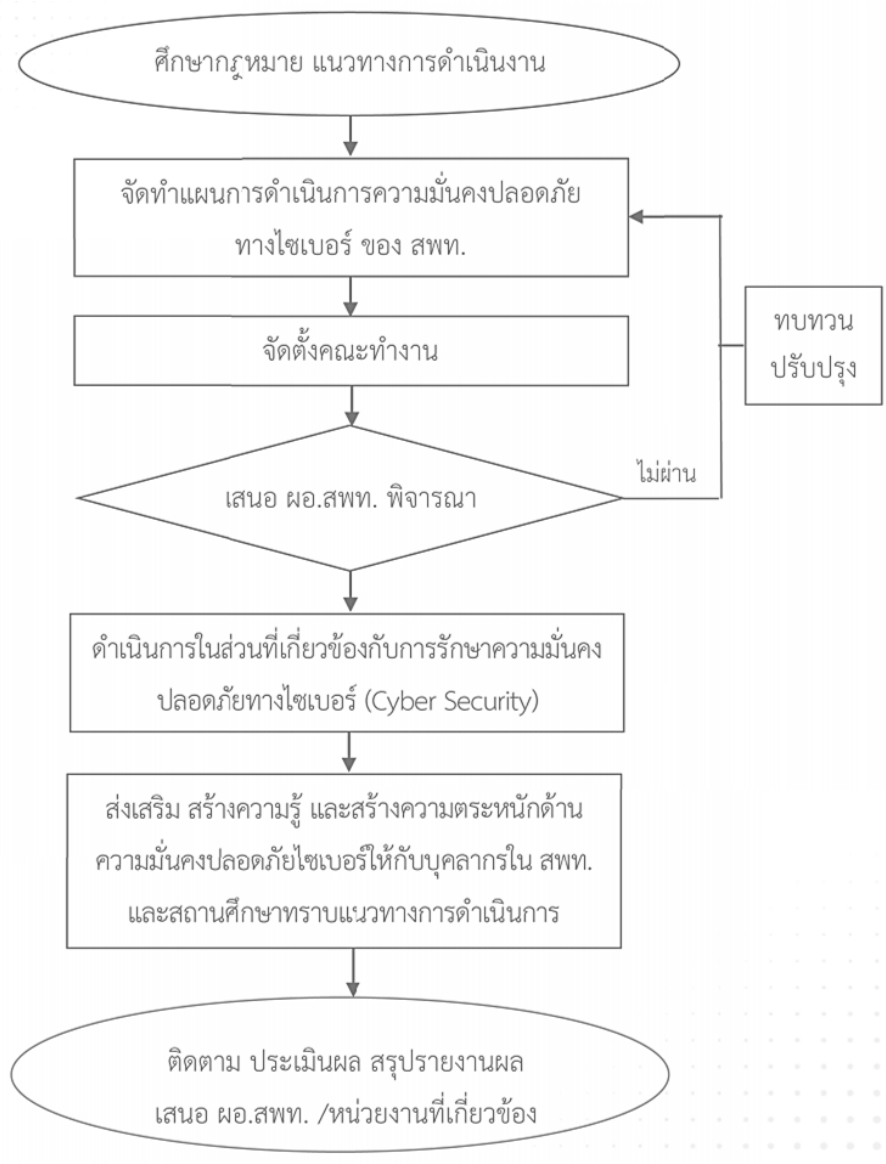
๕.๕.๔ ติดตั้งใชงานระบบยืนยันตัวตน และควบคุมสิทธิ

๕.๕.๕ ติดตั้งใหงานระบบจัดเก็บ Log File ใหสอดคลองกับกฎหมายและพระราชบัญญัติวาดวยการกระทำความผิดเกี่ยวกับคอมพิวเตอร พ.ศ. ๒๕๖๐ และที่แกไขเพิ่มเติม

๕.๖ สงเสริม สรางความรู และสรางความตระหนักดานความมั่นคงปลอดภัยไซเบอรใหกับบุคลากรผูปฏิบัติงานภายในสำนักงานเขตพื้นที่การศึกษา และขาราชการครูและบุคลากรทางการศึกษาของสถานศึกษารับทราบแนวทางการดำเนินการ

๕.๗ ติดตาม ผลการดำเนินการ รายงานผูอำนวยการสำนักงานเขตพื้นที่การศึกษาและหนวยงานที่เกี่ยวของ

๖. Flow Chart การปฏิบัติงาน



๗. แบบฟอรมที่ใช

๗.๑ รายงานสถิติการใชงานระบบคอมพิวเตอรและเครือขาย

๗.๒ แบบรายงานการดำเนินการความมั่นคงปลอดภัยทางไซเบอร (Cyber Security) ตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด กรณีมีการจัดเก็บขอมูลรายงาน

๘. เอกสาร/หลักฐานอางอิง :

๘.๑ พระราชบัญญัติขอมูลขาวสารของราชการ พ.ศ. ๒๕๔๐ และที่แกไขเพิ่มเติมจนถึงฉบับปจจุบัน

๘.๒ พระราชบัญญัติวาดวยการกระทำความผิดเกี่ยวกับคอมพิวเตอร พ.ศ.๒๕๕๐ และที่แกไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๘.๓ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร พ.ศ. ๒๕๖๒

๘.๔ แผนพัฒนาคุณภาพดานเทคโนโลยีดิจิทัลเพื่อการศึกษาของสำนักงานเขตพื้นที่การศึกษา

๙. รายละเอียด โครงสรางสวนประกอบมาตรฐานงาน

ชื่องาน : ดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)	**สพท. :** กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร	**รหัสเอกสาร :**

ตัวชี้วัดที่สำคัญของกระบวนงาน : สำนักงานเขตพื้นที่การศึกษามีระบบแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)เป็นไปตามที่กฎหมายกำหนด

ลำดับที่	ผังขั้นตอนการดำเนินงาน	รายละเอียดงาน	เวลาดำเนินการ	มาตรฐานคุณภาพงาน	ผู้รับผิดชอบ
1		ศึกษากฎหมาย ระเบียบ นโยบาย แนวทางการดำเนินการ	3 วันทำการ	ผู้รับผิดชอบเข้าใจแนวทางการดำเนินการได้อย่างถูกต้อง	กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร
2		จัดทำแผนการดำเนินการความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานเขตพื้นที่การศึกษา	3 - 5 วันทำการ	แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เป็นไปตามที่กฎหมายกำหนด	
3		จัดตั้งคณะทำงานเพื่อบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)	3 - 5 วันทำการ	คณะทำงาน มีความรู้ ความสามารถและปฏิบัติหน้าที่ตามคำสั่งได้อย่างมีประสิทธิภาพ	
4		เสนอ ผอ.สพท. พิจารณา	3 วันทำการ		
5		ดำเนินการในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)		สพท. ดำเนินการติดตั้งระบบต่าง ๆ ที่เกี่ยวข้องตามแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ได้อย่างครบถ้วน สมบูรณ์	
6		ติดตั้งใช้งานอุปกรณ์ Network Firewall	1 วัน		
7		ติดตั้งใช้งานโปรแกรม Antivirus/AntiMalware	3 ชั่วโมง		
8		ติดตั้งใช้งานระบบ Endpoint Security	1 วัน		
9		ติดตั้งใช้งานระบบยืนยันตัวตน และควบคุมสิทธิ	3 ชั่วโมง		
10		ติดตั้งให้งานระบบจัดเก็บ Log File ให้สอดคล้องกับกฎหมายฯ	3 วัน		

๙. รายละเอียด โครงสรางสวนประกอบมาตรฐานงาน (ต่อ)

ชื่องาน : ดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)	**สพท. :** กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร	**รหัสเอกสาร :**

ตัวชี้วัดที่สำคัญของกระบวนงาน : สำนักงานเขตพื้นที่การศึกษามีระบบแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)เป็นไปตามที่กฎหมายกำหนด

ลำดับที่	ผังขั้นตอนการดำเนินงาน	รายละเอียดงาน	เวลาดำเนินการ	มาตรฐานคุณภาพงาน	ผู้รับผิดชอบ
11		ส่งเสริม สร้างความรู้ และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรผู้ปฏิบัติงานภายในสำนักงานเขตพื้นที่การศึกษาและข้าราชการครูและบุคลากรทางการศึกษาของสถานศึกษารับทราบแนวทางการดำเนินการ	ตลอดระยะเวลา	ข้าราชการครูและบุคลากรทางการศึกษาของสถานศึกษาในสังกัด และบุคลากรผู้ปฏิบัติงานใน สพท. มีความรู้ความเข้าใจ และตระหนักความมั่นคงปลอดภัยไซเบอร์และสามารถปฏิบัติได้ตามแนวทางที่กฎหมายกำหนด	กลุ่มส่งเสริมการศึกษาทางไกลเทคโนโลยีสารสนเทศและการสื่อสาร
12		ติดตาม ผลการดำเนินการ รายงาน ผอ.สพท. และหน่วยงานที่เกี่ยวข้อง	3 วันทำการ	ผลการดำเนินการเป็นไปตามเป้าหมาย ข้อมูลการรายงานมีความถูกต้อง ครบถ้วน สมบูรณ์ สามารถรายงาน/เผยแพร่ได้อย่างมีประสิทธิภาพ	

อธิบายสัญลักษณ์ผังขั้นตอน

จุดเริ่มต้นหรือสิ้นสุดกระบวนงาน | กิจกรรมงานหรือการปฏิบัติ | การตัดสินใจ | ทิศทางหรือการเคลื่อนไหวของงาน | จุดเชื่อมต่อระหว่างหน้า (ถ้าไม่จบภายใน 1 หน้า)