ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่าย

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.)

ตามประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2557 ประกาศใช้เมื่อวันที่ 7 พฤศจิกายน พ.ศ. 2557 และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สป.พม. ส่วนหนึ่งประกอบด้วย แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่าย ซึ่งกำหนดขึ้นเพื่อเป็นมาตรการในการติดตั้งและกำหนดค่าต่างๆ ของระบบเครือข่ายและอุปกรณ์เครือข่าย ได้แก่ ไฟร์วอลล์ (Firewall) ระบบตรวจจับและป้องกันการบุกรุก (IDPS) การป้องกันมัลแวร์และไวรัส (Anti-Malware/Anti-Virus) และระบบเครือข่ายไร้สาย (Wireless LAN) โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ปฏิบัติที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเครือข่ายของ สป.พม.

ผู้ปฏิบัติ

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบ
3. **ผู้ใช้งาน** หมายถึง ผู้ปฏิบัติทั้งภายในและภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเครือข่ายของ สป.พม.

ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่าย ประกอบด้วย

1. ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

1.1 หน้าที่ของ ศทส.

1.1.1 กำหนดให้มีการติดตั้งไฟร์วอลล์ โดย ศทส. มีหน้าที่ในการติดตั้ง กำหนดค่า และบริหารจัดการไฟร์วอลล์ทั้งหมด เพื่อกำหนดค่าต่างๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน และสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายภายในของ สป.พม.

1.1.2 การให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น และจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

1.1.3 ระบบเครื่องคอมพิวเตอร์แม่ข่ายสารสนเทศที่เข้าถึงบริการได้จากทั้งภายในและภายนอกทั้งหมดต้องถูกติดตั้งใน Demilitarized Zone (DMZ) และต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

1.1.4 การให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์บนเครือข่าย จะต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายเป็นลายลักษณ์อักษรก่อน โดยต้องระบุข้อมูล ดังนี้

(1) หมายเลข Port ที่ต้องการขอให้เปิด

(2) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(3) วัตถุประสงค์หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้นๆ

(4) วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

(5) ผู้ดูแล/ผู้รับผิดชอบ/ผู้พัฒนาระบบ

1.1.5 การให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทาง ศทส. อนุญาตให้ใช้งานเท่านั้น ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือจากที่กำหนด จะต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายก่อน

1.1.6 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอก มายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในของ สป.พม. จะต้องดำเนินการผ่าน VPN เท่านั้น และต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายก่อน และต้องบันทึกรายการของการดำเนินการตามที่ขอไว้ด้วย

1.1.7 ระงับการใช้งานระบบเครือข่ายและอินเทอร์เน็ต สป.พม. ของเครื่องคอมพิวเตอร์ลูกข่ายทันที หากพบว่า มีพฤติกรรมการใช้งานที่ขัดต่อประกาศหรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ สป.พม. หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศของ สป.พม. จนกว่าจะได้รับการแก้ไข

1.1.8 ยกเลิกการให้บริการระบบเครือข่ายและอินเทอร์เน็ต สป.พม. ของผู้ใช้งานทันที หากพบว่าผู้ใช้งานมีเจตนาใช้งานที่ขัดต่อประกาศหรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ สป.พม. หรือกฎหมาย หรือการทำงานของโปรแกรมที่อาจทำให้เกิดความเสี่ยงต่อความปลอดภัยหรือทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของ สป.พม.

1.2 หน้าที่ของผู้ดูแลระบบ

1.2.1 เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการอุปกรณ์ไฟร์วอลล์เท่านั้น จึงจะสามารถเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ได้

1.2.2 ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าไฟร์วอลล์ทั้งหมดของอุปกรณ์เครือข่าย สป.พม.

1.2.3 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

1.2.4 ทุกเส้นทางที่เชื่อมต่ออินเทอร์เน็ต และบริการอินเทอร์เน็ตที่ไม่อนุญาต จะต้องถูกปฏิเสธโดยไฟร์วอลล์

1.2.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

1.2.6 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยเป็นไปตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ.2550

1.2.7 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

1.2.8 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

1.2.9 กำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์บนเครือข่ายของ สป.พม. ตามที่ได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย

1.2.10 การให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทาง ศทส. อนุญาตให้ใช้งานเท่านั้น

1.2.11 การเปิดพอร์ตการเชื่อมต่อนอกเหนือจากที่ทาง ศทส. กำหนด จะต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายก่อน

1.2.12 ดำเนินการเชื่อมต่อในลักษณะของการ Remote Login จากภายนอก มายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในของ สป.พม. ตามที่ได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย และต้องบันทึกรายการของการดำเนินการไว้ด้วย

2. ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบตรวจจับและป้องกันการบุกรุก (IDPS Policy)

2.1 หน้าที่ของ ศทส.

2.1.1 กำหนดให้มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก โดย ศทส. มีหน้าที่ในการติดตั้ง กำหนดค่าและบริหารจัดการระบบตรวจจับและป้องกันการบุกรุกทั้งหมด เพื่อตรวจสอบความปลอดภัยของระบบเครือข่าย และป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูล บนระบบเครือข่ายภายในของ สป.พม. ให้มีความมั่นคงปลอดภัย

2.1.2 IDPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงระบบเครือข่ายของระบบสารสนเทศตามปกติ

2.1.3 IDPS Policy จะต้องครอบคลุมทุกโฮสต์ในระบบเครือข่ายของ สป.พม. และระบบเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ต ทุกเส้นทาง

2.1.4 ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะ จะต้องผ่านการตรวจสอบจาก IDPS

2.1.5 ยกเลิกการเชื่อมต่อระบบเครือข่ายของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

2.2 หน้าที่ของผู้ดูแลระบบ

2.2.1 ตรวจสอบ และ Update Patch/Signature ของ IDPS เป็นประจำ

2.2.2 ตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้ง host-based IDPS เป็นประจำทุกวัน

2.2.3 ตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลที่มีการเข้าใช้งานระบบเครือข่าย เป็นประจำทุกวัน

2.2.4 บันทึกผลการตรวจสอบโฮสต์และระบบเครือข่ายทั้งหมดที่มีการส่งข้อมูลผ่าน IDPS

2.2.5 หากตรวจพบว่า ระบบมีการทำงานที่ผิดปกติ จะต้องรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายทราบ ทันทีที่ตรวจพบ

2.2.6 หากตรวจพบว่า มีพฤติกรรมการใช้งาน หรือกิจกรรม หรือเหตุการณ์ที่น่าสงสัย ซึ่งมีความเสี่ยงต่อการบุกรุกและการโจมตีระบบ หรือการพยายามเข้าระบบทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมายทราบ ทันทีที่ตรวจพบ

2.2.7 การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

2.2.8 ทำการลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ เพื่อลดความเสียหายและป้องกันเหตุการณ์ที่อาจเกิดขึ้นอีกในอนาคต

2.2.9 จัดทำรายงานแสดงผลการตรวจสอบการบุกรุก เป็นประจำทุกเดือน

3. ข้อปฏิบัติในการป้องกันมัลแวร์และไวรัส (Anti-Malware/Anti-Virus Policy)

3.1 หน้าที่ของ ศทส.

3.1.1 กำหนดให้มีการติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย ที่มีคุณสมบัติตรวจจับและป้องกันไวรัส เวิร์ม โทรจัน สปายแวร์ ได้เป็นอย่างน้อย โดย ศทส. มีหน้าที่ในการติดตั้ง กำหนดค่า และบริหารจัดการโปรแกรมป้องกันไวรัสทั้งหมด เพื่อป้องกันไม่ให้เกิดความเสียหายต่อข้อมูลในเครื่องคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตของ สป.พม.

3.1.2 จัดหาโปรแกรมบริหารจัดการระบบป้องกันไวรัสจากส่วนกลาง และโปรแกรมป้องกันไวรัส สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย

3.2 หน้าที่ของผู้ดูแลระบบ

3.2.1 ติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย ทุกเครื่องที่มีการเชื่อมต่อกับระบบเครือข่ายของ สป.พม.

3.2.2 ตรวจสอบและบริหารจัดการโปรแกรมป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย

3.2.3 ปรับปรุงระบบฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์เสียหายจากไวรัสคอมพิวเตอร์

3.2.4 หากเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย ตรวจพบหรือมีปัญหาจากไวรัสคอมพิวเตอร์ จะต้องตัดการเชื่อมต่อกับระบบเครือข่ายทันที และดำเนินการตรวจสอบและแก้ไขปัญหาให้แล้วเสร็จ

3.2.5 หากโปรแกรมป้องกันไวรัสมีการปรับเปลี่ยนรุ่น จะต้องดำเนินการปรับเปลี่ยนรุ่นตามโปรแกรมล่าสุดให้กับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายทั้งหมด

3.2.6 จัดทำรายงานแสดงผลการป้องกันไวรัสของระบบคอมพิวเตอร์ สป.พม. เป็นประจำทุกเดือน

4. ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless LAN Policy)

4.1 หน้าที่ของ ศทส.

4.1.1 กำหนดให้มีการติดตั้งระบบเครือข่ายไร้สาย โดย ศทส. มีหน้าที่ในการติดตั้ง กำหนดค่า และบริหารจัดการระบบเครือข่ายไร้สายทั้งหมด เพื่อควบคุมการเข้าถึงและสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สายของ สป.พม.

4.1.2 การติดตั้งอุปกรณ์เครือข่ายไร้สายทั้งหมดต้องผ่านความเห็นชอบจาก ศทส.

4.1.3 การติดตั้งระบบเครือข่ายไร้สายสำหรับให้บริการระบบอินเทอร์เน็ต จะต้องติดตั้งโดยการแยกระบบเครือข่ายไร้สายออกจากระบบเครือข่ายภายใน LAN เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก

4.1.4 กรณีที่มีความจำเป็นต้องเชื่อมต่อระบบเครือข่ายไร้สายกับระบบเครือข่ายภายใน LAN จะต้องเลือกใช้เทคโนโลยี Authentication และมีการกำหนดค่าการเข้ารหัสในการเชื่อมต่อแบบ WPA2 เป็นอย่างน้อย

4.1.5 กำหนดให้การเข้าถึงระบบเครือข่ายไร้สาย ต้องแบ่งแยกการใช้งานให้แตกต่างกันตามความจำเป็นของผู้ใช้งาน และกำหนดรหัสการเข้าใช้งานตามวัตถุประสงค์ของการใช้งาน

4.1.6 กำหนดให้อุปกรณ์ที่ใช้ในการเข้าถึงระบบเครือข่ายของ สป.พม. จะต้องรองรับมาตรฐาน IEEE 802.11g/n เป็นอย่างน้อย หากอุปกรณ์ที่ใช้เป็นเครื่องคอมพิวเตอร์ส่วนบุคคล จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องด้วย

4.1.7 Wireless LAN Policy สามารถเปลี่ยนแปลงตามเทคโนโลยีใหม่ๆ และกระบวนการที่สอดคล้องและเหมาะสมในอนาคตได้

4.2 หน้าที่ของผู้ดูแลระบบ

4.2.1 เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น ที่สามารถเข้าถึงฟังก์ชันที่ใช้ในการตั้งค่าของจุดเชื่อมต่อระบบเครือข่ายไร้สายได้

4.2.2 บริหารจัดการ ติดตั้ง และกำหนดค่าการให้บริการ และการเชื่อมต่อระบบเครือข่ายไร้สายทั้งหมด

4.2.3 ตรวจสอบอุปกรณ์ติดตั้ง กำหนดค่า และจัดการจุดเชื่อมต่อระบบเครือข่ายไร้สายในพื้นที่ สป.พม.

4.2.4 ที่จุดเชื่อมต่อระบบเครือข่ายไร้สาย จะต้องมีการกำหนดค่า Gateway ที่เป็นค่าที่กำหนดไว้ของระบบเครือข่ายส่วนนั้นเท่านั้น

4.2.5 ทุกจุดเชื่อมต่อระบบเครือข่ายไร้สายและอุปกรณ์ที่เกี่ยวข้อง เช่น Access Point จุดเชื่อมต่อสายสัญญาณ Switch จะต้องมีความปลอดภัย และมีรูปแบบในการจัดเก็บและเข้าถึงอุปกรณ์

4.2.6 SSID (Service Set Identifier) ที่กำหนด จะต้องถูกต้องตามรูปแบบที่ ศทส. กำหนดไว้ และจะต้องไม่มีการบ่งบอกหรือแสดงตำแหน่งของสาย ที่จุดเชื่อม LAN หรือชื่ออื่นๆ

4.2.7 เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

4.2.8 SSID ที่ Broadcast จะให้บริการเฉพาะระบบเครือข่ายภายนอก ยกเว้นจุดที่ ศทส. อนุญาตให้ใช้ระบบเครือข่ายภายใน สป.พม. จะต้องยกเลิกค่าการ Broadcast SSID

4.2.9 อุปกรณ์ที่ ศทส. อนุญาตให้ใช้ระบบเครือข่ายภายใน สป.พม. จะต้องระบุ SSID ที่ถูกต้อง จึงจะสามารถเข้าใช้งานได้

4.2.10 SNMP จะต้องถูกยกเลิกหากไม่จำเป็นสำหรับการบริหารจัดการระบบเครือข่าย หรือหากมีความจำเป็นต้องใช้จะต้องมีการเปลี่ยนแปลงค่าเริ่มต้น (Default) ของ Community String

4.2.11 กำหนดให้มีการ Authentication ทุกครั้งก่อนการใช้งาน ด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

4.2.12 กำหนดรายการ MAC Address ให้สามารถเข้าใช้ Access Point ได้ เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามรหัสผู้ใช้ (User account) และรหัสผ่าน (User password) ที่กำหนดไว้เท่านั้น

4.2.13 ยกเลิกการเชื่อมต่อระบบเครือข่ายไร้สายของอุปกรณ์ทุกชนิด ที่ไม่เป็นไปตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ สป.พม. หรือมีความเสี่ยงต่อระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

4.2.14 ห้ามไม่ให้ผู้ดูแลระบบ บอกค่าติดตั้งของระบบเครือข่ายไร้สายกับผู้ใช้งานหรือบุคคลภายนอก

5. ข้อปฏิบัติของผู้ใช้งาน

ผู้ใช้งานทั้งภายในและภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเครือข่ายของ สป.พม. มีข้อปฏิบัติดังนี้

5.1 ผู้ใช้งานระบบเครือข่ายและอินเทอร์เน็ตของ สป.พม. จะต้องมีการ Authentication ทุกครั้งก่อนการใช้งาน ด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

5.2 ผู้ใช้งานต้องสำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

5.3 ห้ามผู้ใช้งานปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัส ที่ สป.พม. ติดตั้งให้

5.4 ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาโปรแกรมป้องกันไวรัสที่ใช้ โดยตรวจสอบว่า มีการ Update โปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ ศทส. ทราบ หากไม่สามารถ Update โปรแกรมป้องกันไวรัสให้ทันสมัยได้

5.5 ผู้ใช้งานต้องแจ้งให้ ศทส. ทราบทันที เมื่อพบว่าคอมพิวเตอร์หรือโปรแกรมที่ใช้มีความผิดปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส

5.6 ผู้ใช้งานต้องตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นด้วยโปรแกรมป้องกันไวรัสทุกครั้ง เมื่อมีการนำมาติดตั้งหรือใช้งาน และหากตรวจพบไวรัสจะต้องจัดการทำลายไวรัสโดยเร็วที่สุด

5.7 หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมที่นำมาใช้งานได้ ห้ามผู้ใช้งานทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปบนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เด็ดขาด

5.8 ห้ามผู้ใช้งานนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access Point, Wireless Router, Wireless USB client หรือ Wireless Card

5.9 กรณีที่ผู้ใช้งานพยายามเข้าถึงระบบโดยมิชอบ หรือโจมตีระบบ หรือมีพฤติกรรมการใช้งานที่ขัดต่อประกาศหรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ สป.พม. ซึ่งอาจทำให้เกิดความเสี่ยงต่อความปลอดภัยและความเสียหายต่อระบบเทคโนโลยีสารสนเทศของ สป.พม. ผู้ใช้งานจะถูกระงับหรือยกเลิกการใช้งานระบบเครือข่ายและอินเทอร์เน็ตของ สป.พม. ทันที

5.10 กรณีที่ผู้ใช้งานได้กระทำการใดๆ ที่มีความผิด ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของ สป.พม. ผู้ใช้งานจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย