|  |
| --- |
|  |
| **ภาคผนวก ค** |
| **แผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน กรมปศุสัตว์ กรณีไวรัสคอมพิวเตอร์ / การบุกรุกระบบคอมพิวเตอร์** |
|  |
|  |
|  |

|  |
| --- |
|  |

**แผนรองรับสถานการณ์ฉุกเฉิน จากไวรัสคอมพิวเตอร์/**

**การบุกรุกระบบคอมพิวเตอร์**

**1. วัตถุประสงค์ของแผนฯ**

1.1 เพื่อสร้างความเข้าใจแก่บุคลากรในการเตรียมความพร้อมจากสถานการณ์ฉุกเฉินจากไวรัสคอมพิวเตอร์ / การ

บุกรุกระบบคอมพิวเตอร์

1.2 เพื่อลดความเสียหายที่จะเกิดขึ้นแก่ระบบเครือข่าย ฮาร์ดแวร์ ซอฟท์แวร์ และฐานข้อมูล

1.3 เพื่อให้การดำเนินการของกรมปศุสัตว์ที่เป็นระบบอิเล็กทรอนิกส์ที่สำคัญ สามารถให้บริการได้อย่างรวดเร็ว

**2. ขอบเขตการดำเนินงานของแผนฯ**

แผนนี้ใช้ควบคุมระบบเครื่องคอมพิวเตอร์ที่ติดตั้ง ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมปศุสัตว์ พญาไทเท่านั้น

**3. ขั้นตอนแนวปฏิบัติ**

**3.1 ก่อนเกิดเหตุ จากไวรัสคอมพิวเตอร์/การบุกรุกระบบคอมพิวเตอร์** ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องดำเนินการ ดังนี้

1) จัดให้มีเจ้าหน้าที่ทำการตรวจสอบ

- การใช้งานข้อมูลระบบงานที่สำคัญ

- เครื่องคอมพิวเตอร์แม่ข่าย

- ระบบเครือข่ายคอมพิวเตอร์และระบบสายสัญญาณสื่อสาร

- System Software

- ระบบ Firewall

- Virus, Worm, Spy ware

- Transaction log files

- Proxy server

- ระบบฐานข้อมูล

- การเปลี่ยนแปลงของไฟล์ต่างๆ /ความถูกต้องของไฟล์ข้อมูล

- ค่า Configuration ของระบบ

- ระบบสัญญาณจากผู้ให้บริการอินเตอร์เน็ตและอินทราเน็ต

2) จัดเตรียมระบบแจ้งเตือนภัยข้อมูลเตือนภัยไวรัสคอมพิวเตอร์เครือข่ายอย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสคอมพิวเตอร์

3) กำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมปศุสัตว์ รวมทั้งประชาสัมพันธ์แจ้งเวียนนโยบายดังกล่าวให้ทุกหน่วยงานทราบและถือปฏิบัติ

4) ควรจัดจ้างบริษัทที่มีบุคลากรซึ่งมีความรู้ความชำนาญทำหน้าที่ดูแลให้คำปรึกษา ตรวจสอบ และบำรุงรักษาระบบเครือข่ายทั้งทางด้าน Hardware และ Software

5) กำหนดสิทธิ์ในการเข้าถึงการเข้าใช้ระบบเครือข่าย ระบบฐานข้อมูล ให้เป็นปัจจุบันและควรมีการทบทวนสิทธิ์เป็นประจำทุกปี

6) Update ฐานข้อมูลไวรัส (Definition) อยู่เสมอ

7) Update patch ของระบบปฏิบัติการและโปรแกรมให้เป็นปัจจุบันเพื่อปิดช่องโหว่ของระบบ

8) จัดให้มีการสำรองข้อมูลระบบงานที่สำคัญ ลงบนสื่อจัดเก็บที่มีความเหมาะสม เช่น DVD, CD,   
External Hard disk, Handy drive แยกเก็บไว้คนละสถานที่กับห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Data center)

9) จัดให้มีการซ้อมรับสถานการณ์ฉุกเฉินจากภัยพิบัติจากไวรัสคอมพิวเตอร์ / การบุกรุกระบบคอมพิวเตอร์ อย่างน้อยปีละ 1 ครั้ง

**3.2 ขณะเกิดเหตุ จากไวรัสคอมพิวเตอร์/การบุกรุกระบบคอมพิวเตอร์**

1) กรณีพบความผิดปกติ หรือเครื่องคอมพิวเตอร์แม่ข่าย ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ เนื่องจากถูกไวรัสคอมพิวเตอร์หรือถูกเจาะระบบในเครื่องคอมพิวเตอร์ ให้ผู้ดูแลระบบทำการปลดสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายและป้องกันข้อมูลรั่วไหลหรือขอความช่วยเหลือศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (thaicert) ทางหมายเลขโทรศัพท์ 0–2142-2483

2) ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน / หน่วยงานภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ปลดสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด ผู้ดูแลระบบดำเนินการตรวจสอบ ค้นหาสาเหตุ ประเมินสถานการณ์ เร่งแก้ไขปัญหาและทดสอบระบบให้ทำงานได้ตามปกติ หากพบว่าเกิดความเสียหายต่อระบบหรือข้อมูล ให้ทำการกู้คืนข้อมูลโดยอาจขอความร่วมมือจากบริษัทผู้รับจ้างซ่อมแซม แก้ไข ดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้ มาร่วมดำเนินการให้แล้วเสร็จโดยเร็วที่สุด

3) เรียกประชุมทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติ (Crisis Operation Team) ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่าย ระบบเครื่องคอมพิวเตอร์แม่ข่าย ระบบป้องกันไวรัส ระบบฐานข้อมูลและระบบปฏิบัติการ ทำการกู้ระบบกลับมาโดยเร็ว

เจ้าหน้าที่ผู้ดูแลระบบคอมพิวเตอร์

เจ้าหน้าที่ผู้แลระบบคอมพิวเตอร์

จำกัดการเชื่อมต่อเข้าระบบเครือข่าย เช่น ปลดสาย (LAN) ออก

วิเคราะห์หาสาเหตุและผลกระทบที่เกิดขึ้น

ป้องกันระบบเครือข่ายและดำเนินการหยุดยั้ง การระบาดของไวรัส

ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

**ผังแสดงขั้นตอนการรับมือภัยพิบัติและสถานการณ์ฉุกเฉินจากไวรัสคอมพิวเตอร์ / การบุกรุกระบบคอมพิวเตอร์**

**3.3 การปฏิบัติภายหลังเกิดเหตุ จากไวรัสคอมพิวเตอร์ / การบุกรุกระบบคอมพิวเตอร์**

1) ทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติ (Crisis Operation Team) เข้าควบคุม แก้ไข และตรวจสอบความเสียหายของระบบสารสนเทศในภาพรวม โดยทำการ

- ตรวจสอบ Log ของระบบสารสนเทศเพื่อค้นหาสาเหตุและความผิดปกติใดๆ ที่เกิดขึ้น

- ปิด service ของโปรแกรม Remote ทั้งหมดที่ติดตั้งในเครื่องที่ถูกเจาะระบบ

- ตรวจสอบและอัพเดท patch ของระบบปฏิบัติการและโปรแกรมให้เป็นปัจจุบัน เพื่อปิดช่องโหว่ที่พบ

- ตรวจสอบการทำงานของโปรแกรม Anti-virus ทำการอัพเดท Virus Definition ให้เป็นปัจจุบัน

2) ให้ทำการกู้ระบบสารสนเทศนั้นๆ

3) ทำการทดสอบระบบต่างๆและเมื่อผ่านการทดสอบแล้วแจ้งให้ผู้ใช้งานทราบ ทำการเปิดใช้ระบบงาน

**4. การติดตามและประเมินผล**

เมื่อภัยพิบัติและสถานการณ์ฉุกเฉินยุติแล้ว ให้หัวหน้าหน่วยงานที่รับผิดชอบ ดำเนินการติดตามและประเมินผลการป้องกันและแก้ไขปัญหาสถานการณ์ที่เกิดขึ้น ทั้งด้านสถานการณ์ภัยพิบัติ ด้านการปฏิบัติในการระงับและบรรเทาภัย และรายงานต่ออธิบดีกรมปศุสัตว์ เพื่อให้ทราบข้อบกพร่องที่ต้องปรับปรุงแก้ไข และเป็นแนวทางในการบริหารจัดการภัยพิบัติและสถานการณ์ฉุกเฉินในอนาคต และควรปรับปรุงแผนฯ ทุกๆ 1 ปี