

# มาตรการและวิธีปฏิบัติการรักษาความปลอดภัยเว็บไซต์ กองเทคโนโลยีสารสนเทศ

## โรงเรียนนายร้อยพระจุลจอมเกล้า

### 1. มาตรการและวิธีปฏิบัติการรักษาความปลอดภัยเว็บไซต์

1.1 การป้องกันและรักษาความปลอดภัยของข้อมูลและเว็บไซต์ของ รร.จปร. ให้ผู้ดูแลเว็บไซต์ กำหนดสิทธิการใช้งานเครื่องแม่ข่าย (Server) ระบบงาน Application Server และเครื่องแม่ข่าย (Server) ฐานข้อมูล Database Server ที่ติดตั้ง ณ กทท.รร.จปร. ดังนี้

1.1.1 การใช้งานเว็บไซต์ต้องกำหนดให้มีผู้รับผิดชอบดูแลระบบ (Administrator)

1.1.2 ให้บริหารจัดการ ติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

1.1.3 การกำหนดค่าเริ่มต้นพื้นฐานของการใช้งานเว็บจะต้องเป็นการปฏิเสธทั้งหมด เปิดให้ใช้เฉพาะที่จำเป็นใช้งาน

1.1.4 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาต จะต้อง ถูกบล็อก (Block) โดยระบบรักษาความปลอดภัยเครือข่ายของหน่วยงาน

1.1.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์เช่น ค่าพารามิเตอร์การกำหนดค่าใช้ บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

1.1.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึง ได้เฉพาะผู้ที่ได้รับ มอบหมายให้ดูแลจัดการเท่านั้น

1.1.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไป จัดเก็บที่ อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

1.1.8 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลด (Download) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องตรวจสอบความถูกต้องปลอดภัย ก่อนนำไปใช้งาน

1.1.9 การกำหนดค่าการให้บริการของเครื่องแม่ข่าย (Server) ที่ใช้งานเว็บไซต์ จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อกำหนดนโยบายจะต้องถูกระบุให้กับเครื่องแม่ข่าย (Server) เป็นรายชื่อเครื่องที่ให้บริการจริง

1.1.10 จะต้องมีการสำรองข้อมูลและกำหนดค่าต่าง ๆ ของเครื่องแม่ข่าย (Server) คอมพิวเตอร์เป็นประจำทุกเดือน หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

1.1.11 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย (Server) หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องแม่ข่าย (Server) และอุปกรณ์เครือข่ายและจะต้องได้รับความเห็นชอบจากรร.จปร.

1.1.12 คู่มือ บำรุงรักษา เครื่องแม่ข่าย (Server) คอมพิวเตอร์ให้ใช้งานอย่างมีประสิทธิภาพ

1.1.13 ต้องทำการตรวจสอบการเข้าใช้งานเครื่องแม่ข่าย (Server) จากภายนอกว่ามี การใช้งานที่ผิดปกติหรือไม่เป็นประจำ

1.1.14 จัดเจ้าหน้าที่ตรวจสอบและเฝ้าระวังเว็บไซต์ของ รร.จปร. หากตรวจพบการบุกรุกหรือโจมตีให้ทำการระงับยับยั้งหรือปิดระบบในทันทีและทำการแก้ไขโดยด่วน

1.1.15 ให้มีการเปลี่ยนรหัสผ่านในการเข้าถึงระบบคอมพิวเตอร์โดยตั้งรหัสผ่านให้ยากเช่น อักษรตัวใหญ่ผสมกับอักษรตัวเล็กและตัวเลขสลับกันไปโดยให้มีการเปลี่ยนอย่างน้อยทุกๆ 2 เดือนหรือเร็วกว่านั้น

1.1.16 ให้เลือกใช้โปรแกรมในการพัฒนาเว็บไซต์ที่มีระบบป้องกันการบุกรุก/โจมตีและมี การปรับปรุง (Update) ให้เป็นปัจจุบันอย่างต่อเนื่อง

1.1.17 ให้จัดทำระบบสำรองข้อมูลเมื่อเกิดเหตุสุควิสัยสามารถเปิดใช้งานได้ภายใน 3 - 5 ชั่วโมง

1.2 การเข้าถึงข้อมูลและการดูแลเครื่องแม่ข่าย (Server)

1.2.1 นขต.รร.จปร. ที่ได้รับการติดตั้งระบบรักษาความปลอดภัยเครือข่ายสารสนเทศและการสื่อสารของ กทท.รร.จปร. แล้วให้ดำเนินการนำเครื่องแม่ข่าย (Server) ไปติดตั้งภายใน โซนรักษาความปลอดภัย (DMZ)

1.2.2 รร.จปร. จะต้องกำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องแม่ข่าย (Server)

1.2.3 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจาก กทท.รร.จปร. และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

1.2.4 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อ โดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อ กทท.รร.จปร. และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้บริการอื่น ๆ

1.2.5 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

1.2.6 มีการควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการเครื่องแม่ข่าย (Server) ได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งาน เฉพาะเครื่องแม่ข่าย (Server) ข่ายที่ได้รับอนุญาตเท่านั้น

(2) ต้องจำกัดเส้นทางการเข้าถึงเครื่องแม่ข่าย (Server) ที่มีการใช้งานร่วมกัน

(3) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่อง คอมพิวเตอร์ไปยังเครื่องแม่ข่าย (Server) เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

(4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อ ไปยังระบบเครือข่าย อื่น ๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรม ประสงค์ร้าย (Malware) ด้วย

(5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ หน่วยงานในลักษณะที่ผิดปกติ

(6) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบ ความถูกต้องของผู้ใช้บริการ

(7) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(8) กำหนดให้มีผู้รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆของซอฟต์แวร์ระบบ (Systems Software)

1.3 รร.จปร. จะต้องกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องแม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

1.3.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและ เครื่องแม่ข่าย (Server) ของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจาก กทท.รร.จปร.

1.3.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

1.3.3 วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับ การอนุญาตจาก กทท.รร.จปร.

1.3.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความ จำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

1.3.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของ กทท.รร.จปร. ก่อน

1.3.6 ห้องเครื่องแม่ข่าย(Server) จะมีระบบรักษาความปลอดภัย คือ มีระบบตรวจสอบ การเข้าออกห้อง ต้องมีการตรวจสอบก่อนว่ามีสิทธิ์ในการเข้าห้องหรือไม่โดยมีประกาศเงื่อนไขการใช้ห้อง ติด ไว้ที่หน้าห้องเครื่องแม่ข่ายให้ทุกคนทราบ

2. กทท.รร.จปร. ติดตามประเมินผลการดูแลรักษาและเฝ้าระวังเว็บไซต์และ เครื่องแม่ข่าย (Server) โดยจัดทำแบบสำรวจ แบบสอบถาม ถึงวิธีการดูแลและเฝ้าระวัง

3. กทท.ร.ร.จปร. ประเมินความเสี่ยงของเว็บไซต์ ร.ร.จปร. ที่มีความเสี่ยงต่อการโจมตีหรือปรับเปลี่ยนข้อมูลในเว็บไซต์พร้อมทั้งดำเนินการระงับยับยั้งเว็บไซต์ที่มีความเสี่ยงเพื่อทำการแก้ไขให้ปลอดภัยต่อไป

#### 4. วิธีดำเนินการของเจ้าหน้าที่ผู้ดูแลเว็บไซต์

4.1 ตรวจสอบเว็บไซต์ของหน่วยงานทุกวัน อย่างน้อยวันละ 3 ครั้ง โดยเฉพาะในช่วงวันหยุดราชการให้มีเจ้าหน้าที่ตรวจสอบเฝ้าระวัง หากตรวจพบการบุกรุกโจมตีให้ทำการแก้ไขในทันที

4.2 ตรวจสอบ ป้องกัน และแก้ไขจุดอ่อนของโปรแกรมที่พัฒนาขึ้น หรือนำมาใช้งาน (Application Software Security) หากตรวจพบให้ดำเนินการแก้ไขทันที

4.3 ป้องกันอุปกรณ์และโปรแกรมต่าง ๆ จากโปรแกรมไม่ประสงค์ดี (Malware Defenses)

4.4 มีการกำหนดสิทธิ์การเข้าถึงระบบคอมพิวเตอร์ควบคุมผู้ใช้งานที่ได้สิทธิ์สูง เช่น สิทธิ์เป็น ผู้ดูแลระบบ (Controlled Use of Administrative Privileges)

4.5 ทำการสำรองข้อมูลที่สำคัญ ๆ และมีการซ้อมการกู้คืนระบบอย่างสม่ำเสมอ (Data Recovery Capability) โดยต้องสามารถกู้คืนได้ทันทีที่ระบบถูกโจมตี

4.6 ตรวจสอบ วิเคราะห์และแก้ไขช่องโหว่ต่างๆ ของระบบอย่างต่อเนื่อง (Continuous Vulnerability Assessment and Remediation)

4.7 ปรับแต่งอุปกรณ์เครือข่ายให้มีการใช้งานตามที่ได้กำหนดไว้เช่น กฎของไฟร์วอลล์การ ตั้งค่าเส้นทางอุปกรณ์ค้นหาเส้นทาง (Secure Configurations for Network Devices such as Firewalls, Routers, and Switches)

4.8 ควบคุม และตรวจสอบข้อมูลที่ผ่านเข้าออกระบบ (Data Loss Prevention)

4.9 จำกัดและควบคุมการใช้งาน การเข้าถึงเครื่องแม่ข่าย (Server) และบริการต่างๆอย่างเหมาะสม

4.10 ควบคุม และตรวจสอบการเข้าถึงข้อมูลที่มีความลับในลำดับชั้นต่างๆ ตามที่ได้รับอนุญาต(Controlled Access Based on the Need to Know)

4.11 เปลี่ยนรหัสผ่านของผู้ดูแลระบบทุก ๆ 2 เดือนหรือเร็วกว่านั้น โดยการตั้ง รหัสผ่านให้มี ความยาว อักขระพิเศษ ตัวอักษร และตัวเลข ผสมกัน

4.12 ให้เจ้าหน้าที่ติดตามและแจ้งเหตุภัยคุกคามการแจ้งเตือนภัยจากช่องโหว่ต่าง ๆ การ ตรวจสอบช่องโหว่และข้อเสนอแนะในการป้องกันและแก้ไขจากเว็บไซต์ของศูนย์ประสานการรักษา ความมั่นคง ปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมทาง อิเล็กทรอนิกส์ (องค์การมหาชน)