



นโยบายด้านความมั่นคงปลอดภัย และการบริหารความเสี่ยง ของระบบเทคโนโลยีสารสนเทศ จังหวัดพังงา

จัดทำโดย

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด

สำนักงานจังหวัดพังงา

สารบัญ

นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศจังหวัดพังงา	1
1. นโยบายการใช้งานอย่างถูกต้อง (Acceptable Use Policy Solution)	1
1.1 คำนิยาม	1
1.2 การใช้งานระบบเทคโนโลยีสารสนเทศ.....	2
1.3 การรักษาความปลอดภัยของข้อมูล.....	3
1.4 การดูแล บำรุงรักษา และการปฏิบัติของเจ้าหน้าที่	4
1.5 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ.....	5
2. นโยบายด้านการเชื่อมโยงเครือข่ายแบบไร้สาย (Wireless Policy)	5
3. นโยบายด้านการรักษาความปลอดภัยเครือข่าย (Network Security Policy).....	6
4. นโยบายด้านการใช้จดหมายอิเล็กทรอนิกส์ (E-mail Policy).....	7
5. นโยบายด้านการใช้อินเทอร์เน็ต (Internet Security Policy)	8
6. มาตรการและวิธีปฏิบัติการรักษาความปลอดภัยเว็บไซต์.....	9
การบริหารความเสี่ยงของระบบสารสนเทศ.....	13
นิยาม ความเสี่ยงของระบบสารสนเทศ	14
การประเมินความเสี่ยง	14
องค์ประกอบการคุกคามหลัก	14
โดยพิจารณาองค์ประกอบการคุกคามหลัก จะใช้การวัดระดับความเสี่ยง ตามตารางนี้.....	14
โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง	15
การพิจารณาองค์ประกอบการคุกคามหลัก.....	15
แผนจัดการความเสี่ยง (Risk management action plan)	17
แผนแก้ไขปัญหากจากภัยพิบัติ (Contingency Plan)	21

นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศจังหวัดพังงา

นโยบายเกี่ยวกับระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูลและสารสนเทศของจังหวัดพังงา มีดังนี้

1. นโยบายการใช้งานอย่างถูกต้อง (Acceptable Use Policy Solution)

จังหวัดพังงา ได้จัดทำข้อปฏิบัติในการใช้งานระบบเทคโนโลยีสารสนเทศของจังหวัดพังงา สร้างมาตรฐานการรักษาความปลอดภัยระบบสารสนเทศในระดับของผู้ใช้งานให้ตระหนักถึงความสำคัญและความจำเป็นของการรักษาความปลอดภัยและการใช้ประโยชน์ร่วมกันในระบบสารสนเทศของจังหวัดพังงา และนำไปสู่การพัฒนาและจัดทำเป็นแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของจังหวัดพังงาตามที่กฎหมายกำหนดต่อไป รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง เพื่อให้หน่วยงานของรัฐในพื้นที่จังหวัดพังงาใช้เป็นแนวทางในการปฏิบัติงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ จึงกำหนดข้อปฏิบัติการใช้งานระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 คำนิยาม

1.1.1 “หน่วยงานของรัฐ” หมายความว่า สำนักงานจังหวัด ราชการส่วนภูมิภาคอื่นที่ตั้งอยู่ในพื้นที่จังหวัดพังงา

1.1.2 “ระบบเทคโนโลยีสารสนเทศ” หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบสารสนเทศ ชุดคำสั่งงานคอมพิวเตอร์สำหรับการบันทึกประมวลผลเรียกดู พิมพ์ออกรายงานในระบบของสำนักงาน และโปรแกรมการใช้งานที่เจ้าหน้าที่ทำการติดตั้งประจำเครื่องคอมพิวเตอร์

1.1.3 “ข้อมูล” หมายความว่า สิ่งที่สามารถทำให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใด ๆ ไม่ว่าการสื่อสารความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยการผ่านวิธีการใด ๆ และได้จัดทำไว้ในรูปแบบเอกสาร แฟ้ม รายงาน หนังสือ แผ่นผิง แผนที่ ภาพวาด ภาพถ่าย फिल्म ภาพเคลื่อนไหว เสียงการบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่ทำการบันทึกไว้ปรากฏได้

1.1.4 “เครื่องคอมพิวเตอร์” หมายความว่า เครื่องคอมพิวเตอร์แม่ข่าย (Server) และรวมถึงเครื่องคอมพิวเตอร์ลูกข่าย (Client) ชนิดตั้งโต๊ะ (Personal Computer) และชนิดพกพา (Notebook, Palm, PDA)

1.1.5 “เครือข่ายคอมพิวเตอร์” หมายความว่า เครือข่ายคอมพิวเตอร์และการสื่อสารของจังหวัดพังงา

1.1.6 “เจ้าหน้าที่” หมายความว่า ผู้ซึ่งได้รับมอบหมายให้ดูแลการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัด ราชการส่วนภูมิภาคอื่นที่ตั้งอยู่ในพื้นที่จังหวัดพังงา

1.1.7 “ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงาน และลูกจ้างของสำนักงานจังหวัด ราชการส่วนภูมิภาคอื่นที่ตั้งอยู่ในพื้นที่จังหวัดพังงา

/1.2 การใช้งาน...

1.2 การใช้งานระบบเทคโนโลยีสารสนเทศ

1.2.1 ผู้ใช้งานมีสิทธิ์ใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐได้ภายใต้ข้อปฏิบัติการใช้งานนี้รวมทั้งต้องปฏิบัติตามแนวทางหรือหลักเกณฑ์อื่นใดจะออกต่อไป

1.2.2 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของหน่วยงานของรัฐให้ปฏิบัติดังนี้

- (1) ให้ใช้งานเพื่อภารกิจของหน่วยงานของรัฐเท่านั้น
- (2) หน่วยงานของรัฐต้องจัดให้มีเจ้าหน้าที่ผู้ดูแลรับผิดชอบเป็นผู้ประสานการปฏิบัติด้านระบบเทคโนโลยีสารสนเทศ การจัดทำระเบียบครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงการติดตามปรับปรุงและแก้ไขทะเบียนครุภัณฑ์อย่างต่อเนื่อง
- (3) ห้ามนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงของหน่วยงานของรัฐไปใช้งานนอกสถานที่เว้นแต่จะนำไปใช้งานภารกิจของหน่วยงานของรัฐ โดยจะต้องได้รับอนุญาตเป็นหนังสือจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงานที่ผู้ใช้งานสังกัดหรือผู้ที่ได้รับมอบหมาย
- (4) ห้ามผู้ใช้งานและบุคคลภายนอกนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงจากภายนอกหน่วยงานของรัฐเข้ามาเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานของรัฐ เว้นแต่จะได้รับความเห็นชอบจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมาย
- (5) ห้ามผู้ใช้งานทำการตัดต่อเพิ่ม ลบ แก้ไข หรือเปลี่ยนแปลงโปรแกรมใด ๆ บนเครื่องคอมพิวเตอร์ของหน่วยงานของรัฐนอกเหนือจากที่เจ้าหน้าที่ได้ทำการติดตั้งและใช้งานไว้แล้ว
- (6) ต้องจัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ไว้ในสถานที่ที่ปลอดภัย ห้ามเปิดฝาคอยล์ เพิ่ม หรือเปลี่ยนชิ้นส่วน เครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง เว้นแต่เป็นการดำเนินการเพื่อซ่อมแซมบำรุงรักษาโดยเจ้าหน้าที่
- (7) ห้ามผู้ใช้งานแก้ไข เปลี่ยนแปลง หรือปรับค่าต่าง ๆ ที่กำหนดไว้ในเครื่องคอมพิวเตอร์เพื่อให้ทำงานได้ในระบบเครือข่าย (Network Configuration/IP Address) เว้นแต่เป็นการดำเนินการโดยเจ้าหน้าที่
- (8) กรณีมีการย้ายจุดติดตั้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง ผู้ใช้งานต้องได้รับความเห็นชอบจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงานทราบเป็นหนังสือหรือผู้ที่ได้รับมอบหมาย
- (9) ห้ามผู้ใช้งานติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อใช้งานในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานของรัฐ หรือเปิดการใช้แฟ้มข้อมูลร่วมกัน (Share File/Directory) ให้ผู้อื่นสามารถเข้าถึง (Access) ข้อมูลที่ไม่ใช่เพื่อประโยชน์ หรือภารกิจในการปฏิบัติงาน
- (10) ให้ปิดเครื่องคอมพิวเตอร์และอุปกรณ์ทุกครั้งที่เลิกใช้งาน หรือเมื่อไม่ได้ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 1 ชั่วโมง

1.2.3 ผู้ใช้งานพึงใช้ทรัพยากรเครือข่ายคอมพิวเตอร์ให้เกิดประสิทธิภาพและประโยชน์ในการปฏิบัติงานส่วนรวม โดยให้ปฏิบัติ ดังนี้

/ (1) ไม่ใช่เครือข่าย...

(1) ไม่ใช่เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ต่อไปนี้

- 1.1) กระทำผิดกฎหมายหรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
 - 1.2) กระทำขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
 - 1.3) เพื่อการพาณิชย์
 - 1.4) เปิดเผยข้อมูลที่เป็นความลับซึ่งได้จากการปฏิบัติงาน
 - 1.5) เป็นการละเมิดทรัพย์สินทางปัญญา
 - 1.6) รับหรือส่งข้อมูลซึ่งก่อให้เกิดความเสียหายแก่หน่วยงานของรัฐ เช่น การรับหรือส่งจดหมายที่มีลักษณะเป็นจดหมายลูกโซ่
 - 1.7) ขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของผู้ใช้งานอื่น หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของหน่วยงานของรัฐไม่สามารถใช้งานได้ตามปกติ
 - 1.8) รับรู้ รับทราบข้อมูล ส่งต่อ ประกาศ หรือแสดงความคิดเห็นในเรื่องที่ไม่เกี่ยวข้องกับการดำเนินงานของศาลและหน่วยงานของรัฐ ในลักษณะที่จะก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
- (2) ไม่ถ่ายโอนข้อมูลที่มีขนาดใหญ่ที่ไม่เกี่ยวข้องกับการปฏิบัติงานโดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงาน
- (3) ไม่นำเครื่องคอมพิวเตอร์ของหน่วยงานของรัฐ ไปติดตั้งหรือเชื่อมโยงกับเครือข่ายคอมพิวเตอร์ภายนอกโดยผ่านทางช่องทางโทรศัพท์หรือช่องทางอื่นที่หน่วยงานของรัฐไม่ได้กำหนดไว้
- (4) ไม่ควรติดตั้งและใช้งานโปรแกรมการสนทนาผ่านเครือข่ายคอมพิวเตอร์ เช่น โปรแกรม IRC, ICQ, MSN เป็นต้น

1.3 การรักษาความปลอดภัยของข้อมูล

เพื่อความปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐให้ผู้ใช้ปฏิบัติงานดังนี้

- 1.3.1 สำรองแฟ้มข้อมูลต่าง ๆ ที่ได้บันทึกไว้ในแผ่นบันทึกข้อมูลเครื่องคอมพิวเตอร์ (Hard Disk) อย่างสม่ำเสมอและลบแฟ้มข้อมูลหรือข้อมูลที่ไม่จำเป็นออกไปเพื่อให้มีเนื้อที่ในการบันทึกข้อมูลอื่น ๆ เพิ่มมากขึ้น และเป็นการเพิ่มสมรรถนะในการประมวลผลข้อมูลของเครื่องคอมพิวเตอร์ให้เร็วยิ่งขึ้นได้
- 1.3.2 ข้อมูลที่เป็นความลับ หรือข้อมูลที่ไม่พึงเปิดเผย ให้บันทึกข้อมูลลงในแผ่นบันทึกข้อมูลที่สามารถแยกเก็บไว้ต่างหากในที่ปลอดภัย กรณีมีข้อมูลที่มีความสำคัญให้สำรองข้อมูล (Back Up) และจัดเก็บแยกต่างหากในที่ที่ปลอดภัย
- 1.3.3 กรณีมีความจำเป็นต้องนำข้อมูลจากแหล่งจัดเก็บข้อมูลภายนอกมาใช้งานกับเครื่องคอมพิวเตอร์ของหน่วยงานของรัฐ ให้ตรวจไวรัสคอมพิวเตอร์ก่อนทุกครั้งโดยใช้โปรแกรมตรวจสอบไวรัสคอมพิวเตอร์ที่เจ้าหน้าที่ได้ติดตั้งไว้กับเครื่องคอมพิวเตอร์นั้น และหากตรวจพบไวรัสคอมพิวเตอร์ฝังอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด

1.3.4 ลงทะเบียนการใช้งานระบบงานสารสนเทศของหน่วยงานของรัฐโดยผู้บังคับบัญชาระดับหัวหน้าหน่วยงานในสังกัดที่ผู้ใช้งานสังกัดอยู่เป็นผู้พิจารณา

1.3.5 กรณีผู้ใช้งานโอนย้าย เปลี่ยนแปลงหน้าที่ หรือไม่มีความจำเป็นในการใช้งานระบบงานสารสนเทศใด แจ้งให้เจ้าหน้าที่ทราบ เพื่อปรับปรุงเปลี่ยนแปลงสิทธิ์ หรือยกเลิกชื่อหรือรหัสของผู้ใช้งานนั้นต่อไป

1.3.6 ในการใช้งานระบบสารสนเทศของหน่วยงานของรัฐ ผู้ใช้จะต้องใส่ชื่อผู้ใช้งาน (Log in Name) และกำหนดรหัสผ่าน (Password) เพื่อเชื่อมต่อเข้าสู่ระบบงานสารสนเทศ และเมื่อเสร็จสิ้นการใช้งานให้ปิดระบบ (Exit) ทันที

1.3.7 ดูแล และใช้รหัสผ่านที่ได้รับ ความระมัดระวังและรักษาเป็นความลับ มิให้แจ้งรหัสผ่านของตนเองให้กับบุคคลภายนอกหรือบุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานเพื่อป้องกันมิให้ผู้อื่นนำชื่อรหัสผ่าน ไปใช้งานในระบบงานสารสนเทศของหน่วยงานของรัฐ ซึ่งอาจก่อให้เกิดความเสียหายขึ้นได้

1.3.8 ไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลที่สำคัญไว้ในที่ที่สามารถพบเห็นได้ง่าย โดยให้มีการจัดเก็บไว้ในที่ปลอดภัย

1.3.9 ต้องป้องกันข้อมูลและอุปกรณ์ที่อยู่ในเครื่องคอมพิวเตอร์ ชนิดพกพาเมื่อปฏิบัติงานนอกสถานที่ เช่นการใส่รหัสผ่านป้องกันการเข้าถึงหน้าจอ หรือการเข้ารหัสแฟ้มข้อมูลที่สำคัญ

1.3.10 กรณีที่ตรวจสอบหรือพบเห็นเหตุการณ์หรือการกระทำอื่นใดที่เป็นผลเสียต่อการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐรวมถึงการตรวจพบจุดอ่อนหรือภัยที่พบในระบบงานสารสนเทศที่ใช้งานอยู่ ให้รายงานให้หน่วยงานต้นสังกัดเพื่อป้องกันแก้ไขต่อไปโดยเร็ว

1.3.11 กรณีพบปัญหา หรือข้อบกพร่องของระบบงานสารสนเทศของหน่วยงานของรัฐ ผู้ใช้งานรายงานปัญหาหรือข้อบกพร่องที่พบให้เจ้าหน้าที่ทราบ เพื่อแก้ปัญหาโดยเร็วที่สุด

1.4 การดูแล บำรุงรักษา และการปฏิบัติของเจ้าหน้าที่

เจ้าหน้าที่ต้องดูแล บำรุงรักษา ระบบเทคโนโลยีสารสนเทศ ให้สามารถใช้งานได้ดีอยู่เสมอ และจะต้องตรวจสอบดูแลการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปตามข้อปฏิบัติ ดังนี้

1.4.1 เจ้าหน้าที่ต้องดำเนินการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ตามที่กฎหมายกำหนดไว้

1.4.2 เจ้าหน้าที่ต้องไม่ใช้สิทธิ์หรืออำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่ได้รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิ์ในการเข้าถึงข้อมูลนั้น เว้นแต่กรณีที่ได้รับมอบหมายให้ดำเนินการเพื่อแก้ไขปัญหาที่เกี่ยวข้อง และจะต้องไม่เปิดเผยหรือเผยแพร่ข้อมูลที่ได้รับจากการปฏิบัติหน้าที่

1.4.3 เจ้าหน้าที่ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของผู้ใช้งาน เช่น ข้อมูลในระบบไปรษณีย์อิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล

1.4.4 เจ้าหน้าที่ต้องบันทึกเหตุการณ์ที่มีการละเมิดความมั่นคงปลอดภัย จุดอ่อน ภัยคุกคาม หรือการทำการบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขปัญหาที่เกิดขึ้น

/1.4.5 เจ้าหน้าที่...

1.4.5 เจ้าหน้าที่ต้องติดตั้งซอฟต์แวร์หรืออุปกรณ์ป้องกันไวรัสคอมพิวเตอร์ และตรวจสอบไวรัสคอมพิวเตอร์ที่อาจบุกรุกเข้ามาทางเครือข่ายคอมพิวเตอร์อย่างสม่ำเสมอ หากตรวจพบต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์นั้นโดยเร็วที่สุด

1.4.6 เจ้าหน้าที่ต้องสำรองข้อมูลในระบบสารสนเทศ โดยต้องมีข้อมูลการสำรองข้อมูลและจัดทำบันทึกรายละเอียดการสำรองข้อมูล รวมถึงการรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นและวิธีการแก้ไขปัญหาที่เกิดขึ้น

1.4.7 เจ้าหน้าที่ต้องจัดการให้มีระบบการบริหารจัดการเกี่ยวกับการกำหนดสิทธิ์การใช้งานระบบงานสารสนเทศและทำการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบงานสารสนเทศแต่ละระบบ

1.4.8 เจ้าหน้าที่ต้องจัดให้มีการควบคุมการใช้งานของชุดคำสั่งงานคอมพิวเตอร์ (Program source library) ไม่เก็บซอร์สโค้ด (source code) ไว้ในเครื่องที่ใช้ปฏิบัติงานระบบงานสารสนเทศ ไม่เก็บซอร์สโค้ดที่อยู่ระหว่างทำการทดสอบรวมไว้กับไลบรารีที่ใช้งานได้จริงแล้ว และต้องเก็บซอร์สโค้ดไว้ในที่ที่ปลอดภัย เจ้าหน้าที่หรือผู้ใช้งานฝ่าฝืนหรือไม่ปฏิบัติตามข้อปฏิบัตินี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่หน่วยงานของรัฐหรือบุคคลหนึ่งบุคคลใด หน่วยงานของรัฐจะต้องพิจารณาระงับสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

1.5 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

หน่วยงานของรัฐ จัดให้ผู้ใช้งาน เข้ารับการอบรมให้ตระหนักถึงความปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง เพื่อรับทราบถึงนโยบายความปลอดภัยเพิ่มเติมของหน่วยงาน ส่วนเจ้าหน้าที่ควรได้รับการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศหรือด้านเทคโนโลยีสารสนเทศอื่นๆ จากหน่วยงานภายนอกอย่างน้อย ปีละ 1 ครั้ง

2. นโยบายด้านการเชื่อมโยงเครือข่ายแบบไร้สาย (Wireless Policy)

หน่วยงานของรัฐที่มีการให้บริการเชื่อมโยงเครือข่ายแบบไร้สายในบางจุดที่การให้บริการเชื่อมโยงแบบใช้สาย (LAN) ไม่เหมาะสม โดยมีข้อกำหนดในการให้บริการแบบไร้สาย (Wireless LAN) ดังนี้

2.1 มีการควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

2.2 มีการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

2.3 มีการกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

- 2.4 มีการใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ให้บริการที่มีสิทธิ์ในการใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น ให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง
- 2.5 มีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน
- 2.6 มีการใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย
- 2.7 การควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

3. นโยบายด้านการรักษาความปลอดภัยเครือข่าย (Network Security Policy)

ในการป้องกันและรักษาความปลอดภัยของข้อมูล จังหวัดพังงา มีนโยบายในการกำหนดสิทธิ์การใช้งานเครื่องแม่ข่ายระบบงาน Application Server และเครื่องแม่ข่ายฐานข้อมูล Database Server ของหน่วยงานของรัฐ ดังนี้

- 3.1 การบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด
- 3.2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
- 3.3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยระบบรักษาความปลอดภัยเครือข่ายของหน่วยงานของรัฐ
- 3.4 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
- 3.5 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
- 3.6 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน
- 3.7 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกเดือน หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า
- 3.8 เจ้าหน้าที่ที่มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมใช้งานที่ผิดนโยบาย หรือเกิดจากการทำการของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข
- 3.9 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงานก่อน

3.10 ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานในระบบการสืบค้นข้อมูลสารสนเทศทันที

3.11 จัดให้มีระบบรักษาความปลอดภัยเครือข่ายที่เหมาะสมกับเครือข่ายและไม่ทำให้เกิดความล่าช้าในการใช้งานเครือข่าย

4. นโยบายด้านการใช้จดหมายอิเล็กทรอนิกส์ (E-mail Policy)

จังหวัดพังงาจึงกำหนดแนวทางการปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ดังนี้

4.1 ผู้ใช้มีหน้าที่และความรับผิดชอบพึงระวังไม่ให้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบ ผู้ใช้ต้องรักษารหัสผ่านเป็นความลับเฉพาะ และไม่อนุญาตให้อื่นเข้าใช้จดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี ดังนั้นหน่วยงานของรัฐจะไม่รับผิดชอบผลเสียหายต่าง ๆ อันจะเกิดขึ้นจากการยินยอมให้อื่นใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) นั้น ยกเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น ผู้ใช้เป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์และการอนุญาตให้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ในนามของตนเอง

4.2 การใช้จดหมายอิเล็กทรอนิกส์ที่หน่วยงานของรัฐจัดทำให้ ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

(1) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อก่อให้เกิดความเสียหายแก่หน่วยงานของรัฐและบุคคลอื่นหรือละเมิดสิทธิหรือสร้างความรำคาญต่อผู้อื่น เช่น การจงใจส่งข้อมูลที่มีไวรัสให้กับผู้อื่น การส่งจดหมายลูกโซ่ การส่ง Spam Mail เป็นต้น

(2) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อใช้ประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว

(3) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การส่งภาพ วีดีโอ ที่มีลักษณะหยาบคายหรือลามกอนาจารให้กับผู้อื่น เป็นต้น

(4) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อการเปิดเผยข้อมูลที่เป็นความลับ หรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจากองค์กรหรือผู้ที่มีสิทธิให้ข้อมูลดังกล่าว

(5) การส่งจดหมายอิเล็กทรอนิกส์เผยแพร่โปรแกรมหรืองาน หรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรมหรืองาน ในลักษณะละเมิดลิขสิทธิ์

(6) การส่งจดหมายอิเล็กทรอนิกส์ โฆษณาสินค้า ผลิตภัณฑ์ หรือส่งข้อความลักษณะของสแปมเมล(Spam Mail) ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

(7) การส่งจดหมายอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบต่อระบบจดหมายอิเล็กทรอนิกส์หรือเครือข่ายลดทอนประสิทธิภาพลง

(8) การส่งจดหมายอิเล็กทรอนิกส์ กระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

(9) ผู้ใช้งานไม่ควรเปิด-ส่งต่อจดหมายอิเล็กทรอนิกส์ที่ไม่ทราบแหล่งที่มา หรือไม่น่าเชื่อถือ เช่น E-Mail โฆษณา ขยายสินค้า E-Mail ให้สินค้า E-Mail เสนอให้รางวัล E-Mail ทาคุ เป็นต้น

(10) ผู้ใช้งานต้องตรวจสอบไวรัสกับไฟล์ที่แนบมาพร้อม E-Mail ทุกครั้ง ถึงแม้ว่าจะมาจากผู้ส่งจดหมายอิเล็กทรอนิกส์ที่รู้จักก็ตาม

4.3 นโยบายความมั่นคงปลอดภัยของอีเมล (E-Mail Policy)

4.3.1 ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

4.3.2 ควรเปลี่ยนรหัสผ่าน (Password) ทุก 3 – 6 เดือน

4.3.3 ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตน

4.3.4 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

4.3.5 การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวจดหมายอิเล็กทรอนิกส์ (E-Mail)

5. นโยบายด้านการใช้อินเทอร์เน็ต (Internet Security Policy)

จังหวัดพังงามีนโยบายในการให้บริการอินเทอร์เน็ตในองค์กร คือ

5.1 ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่สามารถก่อให้เกิดความเสียหายให้กับหน่วยงาน

5.2 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

5.3 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลด (Download) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

5.4 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

5.5 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

5.6 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

5.7 เมื่อผู้ใช้งานรายใดไม่ได้เป็นข้าราชการ ลูกจ้าง พนักงานราชการ เจ้าหน้าที่บริษัทตามสัญญาต่าง ๆ ที่เข้ามาปฏิบัติการในเครือข่ายของหน่วยงานของรัฐ หรือเป็นนักศึกษาฝึกงานที่หมดช่วงระยะเวลาฝึกงานกับหน่วยงานของรัฐจะหมดสิทธิ์ในการให้บริการอินเทอร์เน็ตทันที

5.8 ไม่อนุญาตให้เปิดเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์เกี่ยวกับลามกอนาจาร การพนัน และจำกัดเวลาการใช้งานเว็บที่ทำให้ระบบการสืบค้นข้อมูลสารสนเทศแออัดล่าช้า เช่น การใช้งาน MSN เป็นต้น

5.9 ไม่อนุญาตให้เปิดเว็บที่มีการส่งผ่านข้อมูลปริมาณมาก ๆ เช่น การดาวน์โหลด (Download) ภาพยนตร์ วิดีโอต่าง ๆ

6. มาตรการและวิธีปฏิบัติการรักษาความปลอดภัยเว็บไซต์

มาตรการและวิธีปฏิบัติการรักษาความปลอดภัยเว็บไซต์ ดังนี้

6.1 มาตรการที่หน่วยงานของรัฐจะต้องดำเนินการในการดูแลเว็บไซต์

6.1.1 การป้องกันและรักษาความปลอดภัยของข้อมูลและเว็บไซต์ของหน่วยงานของรัฐ ให้ผู้ดูแลเว็บไซต์กำหนดสิทธิ์การใช้งานเครื่องแม่ข่าย(Server) ระบบงาน Application Server และเครื่องแม่ข่าย (Server) ฐานข้อมูล Database Server ดังนี้

6.1.1.1 การใช้งานเว็บไซต์ ต้องกำหนดให้มีผู้รับผิดชอบดูแลระบบ (ADMIN)

6.1.1.2 ให้บริหารจัดการ ติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

6.1.1.3 การกำหนดค่าเริ่มต้นพื้นฐานของการใช้งานเว็บไซต์จะต้องเป็นการปฏิเสธทั้งหมดเปิดให้ใช้เฉพาะที่จำเป็นใช้งาน

6.1.1.4 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาต จะต้องถูกบล็อก (Block) โดยระบบรักษาความปลอดภัยเครือข่ายของหน่วยงาน

6.1.1.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

6.1.1.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

6.1.1.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

6.1.1.8 รั้วมัตระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลด (Download) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องตรวจสอบความถูกต้องปลอดภัยก่อนนำไปใช้งาน

6.1.1.9 จะต้องมีการสำรองข้อมูลและกำหนดค่าต่าง ๆ ของเครื่องแม่ข่าย (Server) คอมพิวเตอร์เป็นประจำทุกเดือน หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

6.1.1.10 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย(Server) หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องแม่ข่าย (Server) และอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมาย

/6.1.1.11 ดูแล...

6.1.1.11 ดูแล บำรุงรักษา เครื่องแม่ข่าย (Server) คอมพิวเตอร์ให้ใช้งานอย่างมีประสิทธิภาพ

6.1.1.12 ต้องทำการตรวจสอบการเข้าใช้งานเครื่องแม่ข่าย (Server) จากภายนอกว่ามีการใช้งานที่ผิดปกติหรือไม่เป็นประจำ

6.1.1.13 จัดเจ้าหน้าที่ตรวจสอบและเฝ้าเว็บไซต์ของหน่วยงานของรัฐหากตรวจพบการบุกรุกหรือโจมตีให้ทำการระงับยับยั้งหรือปิดระบบในทันทีและทำการแก้ไขโดยด่วน

6.1.1.14 ให้มีการเปลี่ยนรหัสผ่านในการเข้าถึงระบบคอมพิวเตอร์โดยตั้งรหัสผ่านให้ยาก เช่น อักษรตัวใหญ่ผสมกับอักษรตัวเล็กและตัวเลขสลับกันไปโดยให้มีการเปลี่ยนอย่างน้อยทุก ๆ 3 เดือนหรือเร็วกว่านั้น

6.1.1.15 ให้เลือกใช้โปรแกรมในการพัฒนาเว็บไซต์ที่มีระบบป้องกันการบุกรุก/โจมตีและมีการปรับปรุง (Update) ให้เป็นปัจจุบันอย่างต่อเนื่อง

6.1.1.16 ให้จัดทำระบบสำรองข้อมูลเมื่อเกิดเหตุสุดวิสัยสามารถเปิดใช้งานได้ภายใน 3 - 5 ชั่วโมง

6.1.2 การเข้าถึงข้อมูลและการดูแลเครื่องแม่ข่าย (Server)

6.1.2.1 หน่วยงานของรัฐต้องติดตั้งระบบรักษาความปลอดภัยเครือข่ายสารสนเทศและการสื่อสาร แล้วให้ดำเนินการนำเครื่องแม่ข่าย (Server) ไปติดตั้งภายในโซนรักษาความปลอดภัย (DMZ)

6.1.2.2 หน่วยงานของรัฐจะต้องกำหนดมาตรการควบคุมการเข้า - ออกห้องควบคุมเครื่องแม่ข่าย (Server)

6.1.2.3 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงานที่ผู้ใช้งานสังกัดและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

6.1.2.4 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

6.1.2.6 มีการควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการเครื่องแม่ข่าย (Server) ได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ให้บริการให้สามารถใช้งานเฉพาะเครื่องแม่ข่าย (Server) ข่ายที่ได้รับอนุญาตเท่านั้น

(2) ต้องจำกัดเส้นทางการเข้าถึงเครื่องแม่ข่าย (Server) ที่มีการใช้งานร่วมกัน

(3) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย (Server) เพื่อไม่ให้ผู้ให้บริการสามารถใช้เส้นทางอื่น ๆ ได้

/ (4) ระบบเครือข่าย...

(4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรม ประสงค์ร้าย (Malware) ด้วย

(5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(6) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

(7) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(8) กำหนดให้ผู้รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

6.1.3 หน่วยงานของรัฐจะต้องกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องแม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

6.1.3.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องแม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงาน

6.1.3.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

6.1.3.3 วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงาน

6.1.3.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

6.1.3.5 การเข้าใช้งานระบบต้องผ่านระบบการพิสูจน์ตัวตนของหน่วยงานก่อน

6.1.3.6 ห้องเครื่องแม่ข่าย (Server) จะมีระบบรักษาความปลอดภัย คือ มีระบบตรวจสอบการเข้าออกห้อง ต้องมีการตรวจสอบก่อนว่ามีสิทธิในการเข้าห้องหรือไม่โดยมีประกาศแจ้งไขการเข้าใช้ห้องติดไว้ที่หน้าห้องเครื่องแม่ข่ายให้ทุกคนทราบ

6.2 จังหวัดพังงาจะดำเนินการติดตามประเมินผลการดูแลรักษาและเฝ้าระวังเว็บไซต์และเครื่องแม่ข่าย (Server) โดยแบบสำรวจสอบถาม ถึงวิธีการดูแลและเฝ้าระวัง

6.3 จังหวัดพังงาจะดำเนินการประเมินความเสี่ยงของระบบเว็บไซต์ของหน่วยงานของรัฐในพื้นที่จังหวัด พร้อมทั้งดำเนินการระงับยับยั้งเว็บไซต์ที่มีความเสี่ยงเพื่อดำเนินการแก้ไขให้ปลอดภัยต่อไป

/6.4 วิธีดำเนินการ...

6.4 วิธีดำเนินการของเจ้าหน้าที่ผู้ดูแลเว็บไซต์หรือระบบงานอื่นๆ

6.4.1 ตรวจสอบเว็บไซต์ระบบงานอื่นๆ ของหน่วยงานทุกวัน อย่างน้อยวันละ 2 ครั้ง โดยเฉพาะในช่วงวันหยุดราชการให้มีเจ้าหน้าที่ตรวจสอบเผื่อระวัง หากตรวจพบการบุกรุกโจมตีให้ทำการแก้ไขในทันที

6.4.2 ตรวจสอบ ป้องกัน และแก้ไขจุดอ่อนของโปรแกรมที่พัฒนาขึ้น หรือนำมาใช้งาน (Application Software Security) หากตรวจพบให้ดำเนินการแก้ไขทันที

6.4.3 ป้องกันอุปกรณ์ และโปรแกรมต่างๆ จากโปรแกรมไม่ประสงค์ดี (Malware Defenses)

6.4.4 มีการกำหนดสิทธิ์การเข้าถึงระบบคอมพิวเตอร์ ควบคุมผู้ใช้งานที่ได้สิทธิ์สูง เช่น สิทธิ์เป็นผู้ดูแลระบบ (Controlled Use of Administrative Privileges)

6.4.5 ทำการสำรองข้อมูลที่สำคัญๆ และมีการซ้อมการกู้คืนระบบอย่างสม่ำเสมอ (Data Recovery Capability) โดยต้องสามารถกู้คืนได้ทันทีที่ระบบถูกโจมตี

6.4.6 ตรวจสอบ วิเคราะห์ และแก้ไขช่องโหว่ต่าง ๆ ของระบบอย่างต่อเนื่อง (Continuous Vulnerability Assessment and Remediation)

6.4.7 ปรับแต่งอุปกรณ์เครือข่ายให้มีการใช้งานตามที่ได้กำหนดไว้ เช่น กฎของไฟร์วอลล์ การตั้งค่าเส้นทางอุปกรณ์ ค้นหาเส้นทาง (Secure Configurations for Network Devices such as Firewalls, Routers, and Switches)

6.4.8 ควบคุม และตรวจสอบข้อมูลที่ผ่านเข้าออกระบบ (Data Loss Prevention)

6.4.9 จำกัด และควบคุมการใช้งานเครื่องแม่ข่าย (Server) และบริการต่าง ๆ อย่างเหมาะสม

6.4.10 ควบคุม และตรวจสอบการเข้าถึงข้อมูลที่มีความลับในลำดับขั้นต่างๆ ตามที่ได้รับอนุญาต (Controlled Access Based on the Need to Know)

6.4.11 ให้ทำการเปลี่ยนรหัสผ่านของผู้ดูแลระบบทุก ๆ 2 เดือนหรือเร็วกว่านั้น โดยการตั้งรหัสผ่านให้มีความยาว อักขระพิเศษ ตัวอักษร และตัวเลข ผสมกัน

6.4.12 ให้ติดตามและแจ้งเหตุภัยคุกคามการแจ้งเตือนภัยจากช่องโหว่ต่างๆ การตรวจสอบช่องโหว่และข้อเสนอแนะในการป้องกันและแก้ไขจากเว็บไซต์ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) หน่วยงานของรัฐพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

การบริหารความเสี่ยงของระบบสารสนเทศ

จังหวัดพังงา

นิยาม ความเสี่ยง (Risk)

คือ การวัดความสามารถ ที่จะดำเนินการให้วัตถุประสงค์ของงานประสบความสำเร็จ ภายใต้การตัดสินใจ งบประมาณ กำหนดเวลา และข้อจำกัดด้านเทคนิคที่เผชิญอยู่ อย่างเช่น การจัดทำโครงการเป็นชุดของกิจกรรม ที่จะดำเนินการเรื่องใดเรื่องหนึ่งในอนาคต โดยใช้ทรัพยากรที่มีอยู่อย่างจำกัด มาดำเนินการให้ประสบความสำเร็จ ภายใต้กรอบเวลาอันจำกัด ซึ่งเป็นกำหนดการปฏิบัติการในอนาคต ความเสี่ยงจึงอาจเกิดขึ้นได้ตลอดเวลา อันเนื่องมาจากความไม่แน่นอน และความจำกัดของทรัพยากรโครงการ ผู้บริหารโครงการจึงต้องจัดการความเสี่ยงของโครงการ เพื่อให้ปัญหาของโครงการลดน้อยลง และสามารถดำเนินการให้ประสบความสำเร็จตามเป้าหมายที่ตั้งไว้อย่างมีประสิทธิภาพ

นิยาม ระบบสารสนเทศ (Information System หรือ IS)

คือ ระบบพื้นฐานของการทำงานต่าง ๆ ในรูปแบบของการเก็บ (input) การประมวลผล (processing) เผยแพร่ (output) และมีส่วนจัดเก็บข้อมูล (storage) โดยองค์ประกอบของระบบสารสนเทศได้แก่ ฮาร์ดแวร์, ซอฟต์แวร์, มนุษย์, กระบวนการ, ข้อมูล, เครือข่าย ซึ่งระบบสารสนเทศจะประกอบด้วย

1. ข้อมูล (Data) หมายถึง ค่าของความจริงที่ปรากฏขึ้น โดยค่าความจริงที่ได้จะนำมาจัดการปรับแต่ง หรือประมวลผลเพื่อให้ได้สารสนเทศที่ต้องการ
2. สารสนเทศ (Information) คือ กลุ่มของข้อมูลที่ถูกตามกฎเกณฑ์ตามหลักความสัมพันธ์ เพื่อให้ข้อมูลเหล่านั้นมีประโยชน์และมีความหมายมากขึ้น
3. การจัดการ (Management) คือ การบริหารอย่างเป็นระบบ เป็นการกำหนดเป้าหมาย และทิศทางการจัดการขององค์กรนั้น ซึ่งต้องมีการวางแผน กำหนดการ และจัดการทรัพยากรภายในองค์กร เพื่อให้บรรลุถึงวัตถุประสงค์ขององค์กรนั้น ๆ

องค์ประกอบของระบบคอมพิวเตอร์

1. Hardware หมายถึง อุปกรณ์ต่างๆ ที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์ และไม่ใช่คอมพิวเตอร์
2. Software หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน
3. บุคลากร หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้ นำ จัดการข้อมูล และนำ ผลลัพธ์ออกจากระบบคอมพิวเตอร์
4. ข้อมูลและแฟ้มข้อมูล หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง
5. หน้าที่การปฏิบัติงาน หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

/องค์ประกอบ...

องค์ประกอบของระบบสารสนเทศ

องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่างๆ ขององค์กร

บุคลากร บุคลากรที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

นิยาม ความเสี่ยงของระบบสารสนเทศ

คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหายหรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จ ต่อการบริหารงานของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการบริหาร

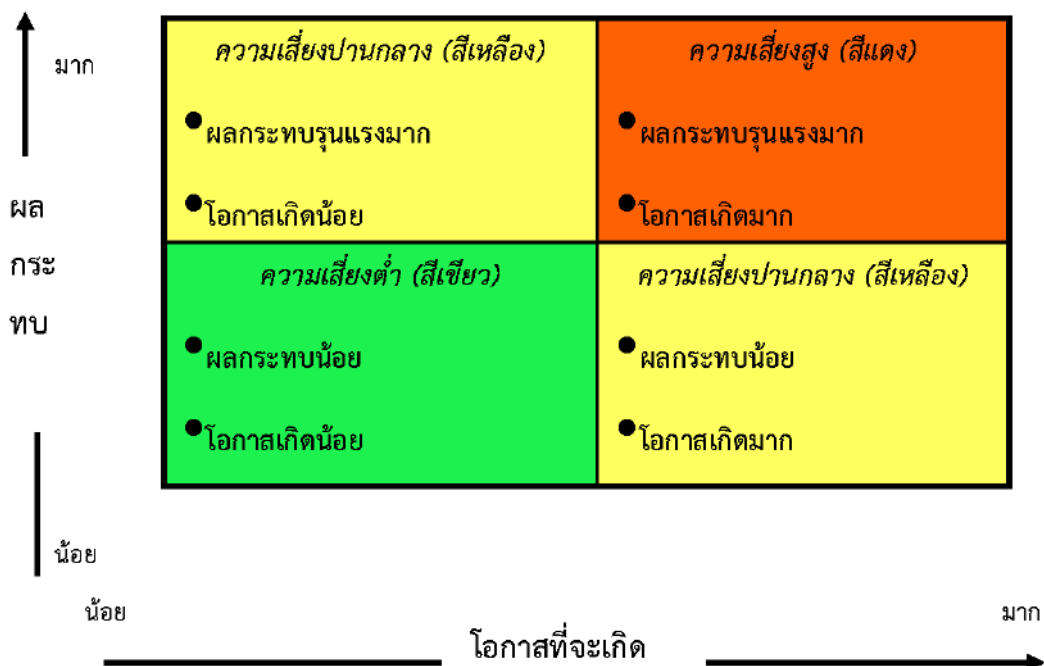
การประเมินความเสี่ยง

องค์ประกอบการคุกคามหลัก

1. บุคลากร
2. เครื่องแม่ข่ายและอุปกรณ์ (Hardware & accessory)
3. โปรแกรม (Software)
4. องค์ประกอบการคุกคามหลัก : องค์ประกอบอื่นๆ (Other Unexpected condition)

โดยพิจารณาองค์ประกอบการคุกคามหลัก จะใช้การวัดระดับความเสี่ยง ตามตารางนี้

การวัดระดับความเสี่ยง



/โอกาสที่จะเกิดเหตุการณ์...

โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง

โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้น (เฉลี่ย)	ระดับคะแนน
สูงมาก	มากกว่า 1 ครั้งต่อเดือน	5
สูง	ระหว่าง 1-6 เดือนต่อครั้ง	4
ปานกลาง	ระหว่าง 6-12 เดือนต่อครั้ง	3
น้อย	มากกว่า 1 ปีต่อครั้ง	2
น้อยมาก	มากกว่า 5 ปีต่อครั้ง	1

ผลกระทบต่อองค์กร

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	มากกว่า 10 ล้านบาท	5
สูง	5 แสนบาท - 10 ล้านบาท	4
ปานกลาง	1 - 5 แสนบาท	3
น้อย	1 หมื่นบาท - 1 แสนบาท	2
น้อยมาก	น้อยกว่า 1 หมื่นบาท	1

การพิจารณาองค์ประกอบการคุกคามหลัก

1. องค์ประกอบการคุกคามหลัก : บุคลากร

ความถี่ : 0 = ไม่เกิด, 1 = ทุกสัปดาห์, 2 = ทุกปี, 3 = ทุกเดือน, 4 = ทุกสัปดาห์, 5 = ทุกวัน

ผลกระทบ : 0 = ไม่มี, 1 = น้อยมาก, 2 = น้อย, 3 = ปานกลาง, 4 = มาก, 5 = มากที่สุด

องค์ประกอบ ความเสี่ยง	สถานการณ์	โอกาส/ ความถี่	ผลกระทบ	ผลลัพธ์
บุคลากรด้านเทคโนโลยีสารสนเทศ				
ไม่ปฏิบัติหน้าที่	ป่วย/ขาดงานโดยไม่ได้แจ้ง	2	2	เฉี่ยว
	อุบัติเหตุ	1	2	เฉี่ยว
	ติดภารกิจด่วนมาก	4	2	เหลื่อม
ปฏิบัติหน้าที่ผิดพลาด	ประมาทเลินเล่อในการรักษาความปลอดภัย	1	5	เหลื่อม
	มอบสิทธิ์ให้ผู้ที่ไม่เกี่ยวข้องโดยพลการ	1	5	เหลื่อม
	ไม่ดูแล Server อย่างสม่ำเสมอ	1	4	เหลื่อม

/องค์ประกอบ...

องค์ประกอบ ความเสี่ยง	สถานการณ์	โอกาส/ ความถี่	ผลกระทบ	ผลลัพธ์
บุคลากรอื่นๆ และบุคคลากรภายนอก				
	การแพร่กระจาย Virus	1	4	เหลือง
	ทำลายอุปกรณ์ Hardware	1	4	เหลือง
	ขโมยอุปกรณ์ Hardware	1	3	เขียว

2. องค์ประกอบการคุกคามหลัก : เครื่องแม่ข่ายและอุปกรณ์ (Hardware & Accessory)

องค์ประกอบ ความเสี่ยง	สถานการณ์	โอกาส/ ความถี่	ผลกระทบ	ผลลัพธ์
Server	Server ไม่ทำงาน/ Start up	1	4	เหลือง
	Server หยุดทำงานโดยไม่ทราบสาเหตุ	1	4	เหลือง
	ไฟฟ้าดับ	3	1	เขียว
	Server ตั้งอยู่ในที่ที่อุณหภูมิสูง	1	2	เขียว

3. องค์ประกอบการคุกคามหลัก : โปรแกรม (Software)

องค์ประกอบ ความเสี่ยง	สถานการณ์	โอกาส/ ความถี่	ผลกระทบ	ผลลัพธ์
OS server	มี File โดนลบ/ทำลาย	0	4	เหลือง
	โดน Virus โจมตี	0	4	เหลือง
	Server หยุดทำงานโดยไม่ทราบสาเหตุ	1	4	เหลือง
OS Client	มี File โดนลบ/ทำลาย	1	2	เขียว
	โดน Virus โจมตี	1	2	เขียว
	OS ไม่ทำงาน	1	2	เขียว

/4.องค์ประกอบ...

4.องค์ประกอบการคุกคามหลัก : องค์ประกอบอื่นๆ(Other Unexpected condition)

ความถี่ : 0 = ไม่เกิด, 1 = ทุกสัปดาห์, 2 = ทุกปี, 3 = ทุกเดือน, 4 = ทุกสัปดาห์, 5 = ทุกวัน

ผลกระทบ : 0 = ไม่มี, 1 = น้อยมาก, 2 = น้อย, 3 = ปานกลาง, 4 = มาก, 5 = มากที่สุด

องค์ประกอบ ความเสี่ยง	สถานการณ์	โอกาส/ ความถี่	ผลกระทบ	ผลลัพธ์
ภัยธรรมชาติ	น้ำท่วม	0	3	เฉียว
	ไฟไหม้	0	4	เหลื่อง
	พายุ	3	2	เฉียว
	แผ่นดินไหว	1	2	เฉียว

แผนจัดการความเสี่ยง (Risk management action plan)

หัวข้อ (Process Title) : การรักษาความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย

วัตถุประสงค์ : จัดการความเสี่ยงกรณีเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถให้บริการได้

วิธีกำหนดแนวทางจัดการความเสี่ยง ประกอบด้วย 4 รูปแบบ

1. Risk Acceptance การยอมรับความเสี่ยง เหตุผล คือ ค่าใช้จ่าย จะสูงกว่า ผลที่ได้รับ แต่จะมีมาตรการหรือแผน ในการกำกับดูแล
2. Risk Reduction / Control การลด/ควบคุม ความเสี่ยง ด้วยมาตรการต่างๆ
3. Risk Avoidance การหลีกเลี่ยง ความเสี่ยง โดยการ ปรับ/เปลี่ยนแปลง รูปแบบการทำงาน
4. Risk Sharing การกระจายความเสี่ยง ด้วยการโอนความเสี่ยงไปให้หน่วยงานอื่นรับผิดชอบ เช่น จ้างผู้อื่นมาดูแล

ลำดับความเร่งด่วนในการจัดการความเสี่ยง(กลั่นกรอง)

โดยให้ความสำคัญและจัดการโดยเร่งด่วน กับ กลุ่มความเสี่ยง มาก (สีแดง, R) ส่วนกลุ่มความเสี่ยงต่ำ จะใช้วิธีออกมาตรการ กำกับ ดูแล ให้อยู่ในระดับที่ยอมรับได้

ผลกระทบต่อวัตถุประสงค์ของการควบคุม มี 3 ด้าน คือ

1. ด้านการดำเนินงาน (O)
2. ด้านการเงิน (F)
3. ด้านการปฏิบัติ ด้านกฎหมาย กฎ ระเบียบ (C)

/องค์ประกอบ...

องค์ประกอบ ความเสี่ยง	เหตุการณ์	กระทบ วัตถุประสงค์ของ การควบคุมด้าน	ระดับ	วิธี	มาตรการ	ระดับการ ยอมรับได้
บุคลากร	ติดภารกิจด่วนมาก	C	เหลือ	2	มีมาตรการการมอบหมายผู้รับผิดชอบ อย่างชัดเจน	
	ประมาทเลินเล่อในการรักษาความปลอดภัย	O,C	เหลือ	2	มีมาตรการการมอบหมายผู้รับผิดชอบ อย่างชัดเจน	
	มอบสิทธิ์ให้ผู้ที่ไม่เกี่ยวข้องโดยพลการ	O,C	เหลือ	2	มีการมอบหมายผู้รับผิดชอบดูแลเข้า ห้องเครื่องแม่ข่ายมีการลงชื่อเข้าใช้ห้อง	
	ไม่ดูแล Server อย่างสม่ำเสมอ	O,C	เหลือ	2	มีมาตรการการบำรุงรักษาอุปกรณ์ เครือข่ายอย่างชัดเจน	
	การแพร่กระจาย Virus	O,C	เหลือ	2,4	มีการติดตั้งโปรแกรมป้องกันไวรัส และมีการสำรองโปรแกรม เป็นประจำ เมื่อโปรแกรมมีปัญหา สามารถนำโปรแกรมที่สำเนาไว้ มาติดตั้งใหม่และมีการ Update ตลอดเวลา	ยอมรับได้
	ทำลายอุปกรณ์ Hardware	O,F,C	เหลือ	2	มีการมอบหมายผู้รับผิดชอบดูแลเข้า ห้องเครื่องแม่ข่ายมีการลงชื่อเข้าใช้ห้อง	

/องค์ประกอบ...

องค์ประกอบ ความเสี่ยง	เหตุการณ์	กระทบ วัตถุประสงค์ของ การควบคุมด้าน	ระดับ	วิธี	มาตรการ	ระดับการยอมรับได้
Server	Server ไม่ทำงาน/ Start up	O,C	เหลือง	2,4	มีมาตรการการบำรุงรักษาอุปกรณ์ เครือข่ายอย่างชัดเจน	ข้อมูลไม่สูญหายและ สามารถกู้คืนได้
	Server หยุดทำงานโดยไม่ทราบสาเหตุ	O,C	เหลือง	2,4	มีมาตรการการบำรุงรักษาอุปกรณ์ เครือข่ายอย่างชัดเจน	ข้อมูลไม่สูญหายและ สามารถกู้คืนได้
OS server	มี File โดนลบ/ทำลาย	O,F,C	เหลือง	2,4	มีมาตรการการบำรุงรักษาอุปกรณ์ เครือข่ายอย่างชัดเจน	สามารถกู้คืนได้
	โดน Virus โจมตี	O,C	เหลือง	2,4	1.มีมาตรการการบำรุงรักษาอุปกรณ์ เครือข่ายอย่างชัดเจน 2. มีการติดตั้งโปรแกรมป้องกันไวรัส และมีการทำสำรองโปรแกรม เป็นประจำ เมื่อโปรแกรมมีปัญหา สามารถนำโปรแกรมที่ สำเนาไว้ มาติดตั้งใหม่และมีการ Update ตลอดเวลา	ข้อมูลไม่สูญหายและ สามารถกู้คืนได้
	Server หยุดทำงานโดยไม่ทราบ สาเหตุ	O,C	เหลือง	2,4	มีมาตรการการบำรุงรักษาอุปกรณ์ เครือข่ายอย่างชัดเจน	ข้อมูลไม่สูญหายและ สามารถกู้คืนได้

/องค์ประกอบ...

องค์ประกอบ ความเสี่ยง	เหตุการณ์	กระทบ วัตถุประสงค์ของ การควบคุมด้าน	ระดับ	วิธี	มาตรการ	ระดับการยอมรับได้
ภัยธรรมชาติ	ไฟไหม้	O,C,F	เหลือง	2,4	1. ติดตั้งอุปกรณ์จับควัน ซึ่งจะส่งสัญญาณเตือน เมื่อเกิดควันขึ้นภายในห้อง 2 ตรวจสอบสภาพอุปกรณ์ไฟฟ้าอย่างสม่ำเสมอ 3. ติดตั้งระบบตัดวงจรไฟฟ้ากรณีไฟฟ้าลัดวงจร (Circuit Breaker) 4. มีการติดตั้งอุปกรณ์ดับเพลิงชนิดไพโรเจน (Pyrogen) ในห้องเครื่องแม่ข่ายและห้องเครือข่าย	อุปกรณ์จับควันต้องตรวจจับได้

/แผนแก้ไขปัญหา...

แผนแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan)

กรณีเครื่องแม่ข่าย ไม่สามารถให้บริการได้เนื่องจากเกิดภัยพิบัติจากสาเหตุต่อไปนี้

1. เครื่องแม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี
2. เกิดไฟไหม้ตัวเครื่องแม่ข่าย หรือภายในห้องเครื่องแม่ข่าย
3. ข้อมูลสูญหาย

ภัยพิบัติ	แผนการดำเนินงาน		
	แผนการควบคุม	แผนการแก้ไข	ผู้รับผิดชอบ
1. เครื่องแม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี	ป้องกันไม่ให้ไวรัสคอมพิวเตอร์โจมตีเครื่องแม่ข่ายได้ ดังนี้ 1.มีการติดตั้งโปรแกรมป้องกันไวรัส 2. มีการกำหนด กฎ (Rule) ของ Firewall ให้เครื่องลูกข่ายที่เข้ามาใช้บริการมีสิทธิ์ใช้ได้เฉพาะ เว็บเพจ เท่านั้น 3.มีการตรวจสอบการเข้าโจมตีเครื่องแม่ข่าย 4.มีการสำรองข้อมูลอยู่เสมอ	1. กำจัดไวรัสคอมพิวเตอร์ โดย ค้นหา โปรแกรม กำจัดไวรัสจากอินเทอร์เน็ต 2. กรณีที่ไวรัสคอมพิวเตอร์ ทำลายระบบจนไม่สามารถให้บริการต่อไปได้จะทำการ format เครื่องแม่ข่ายแล้วติดตั้งระบบใหม่และนำข้อมูลที่สำเนาไว้มาติดตั้ง	เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย
2.เกิดไฟไหม้ตัวเครื่องแม่ข่าย หรือภายในห้องเครื่องแม่ข่าย	1. มีการติดตั้งแผงวงจรตัดไฟฟ้ากรณีไฟฟ้าลัดวงจร 2. ติดตั้งอุปกรณ์ตรวจจับควันทั้งอาคาร ส่งสัญญาณแจ้งเตือน, ติดตั้งอุปกรณ์ดับเพลิง 3. ป้องกันไม่ให้มีผู้ที่ไม่เกี่ยวข้องเข้าไปในห้องเครื่องแม่ข่าย 4. มีการติดตั้งอุปกรณ์ดับเพลิงชนิดโฟโรเจน (Pyrogen) ในห้องเครื่องแม่ข่าย และห้องเครื่องข่าย	-	เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

/ภัยพิบัติ...

ภัยพิบัติ	แผนการดำเนินงาน		
	แผนการควบคุม	แผนการแก้ไข	แผนการควบคุม
2. ข้อมูลสูญหาย	1. มีการสำรองข้อมูลอยู่เป็นประจำอย่างน้อย 1 ครั้ง/เดือน 2. ใช้ระบบสำรองข้อมูล Cloud ที่มีประสิทธิภาพ	2. ข้อมูลสูญหาย	1. มีการสำรองข้อมูลอยู่เป็นประจำอย่างน้อย 1 ครั้ง/เดือน 2. ใช้ระบบสำรองข้อมูล Cloud ที่มีประสิทธิภาพ