# แผนรับมือ
# ภัยคุกคามทางไซเบอร์
## จังหวัดพังงา


- กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
- สำนักงานจังหวัดพังงา
- www.phangnga.go.th

# สารบัญ

# แผนรับมือภัยคุกคามทางไซเบอร์จังหวัดพังงา

**๑.หลักการและเหตุผล**

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ บัญญัติไว้ดังนี้

มาตรา ๔๑ การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพ และการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมุ่งหมายเพื่อสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวล แนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

๑. แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

๒. แผนรับมือภัยคุกคามทางไซเบอร์ เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสาหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

**๒.วัตถุประสงค์**

๑. เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒. เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๓. เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์ของส่วนราชการ หน่วยงานในจังหวัดพังงาให้สามารถใช้งานได้

๔. เพื่อเตรียมความพร้อมด้านบุคลากรของส่วนราชการ หน่วยงานในจังหวัดพังงา ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

๕. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอน

**๓.รูปแบบภัยคุกคามไซเบอร์**

รูปแบบภัยคุกคามไซเบอร์หมายถึง รูปแบบของการกระทำหรือการดำเนินการใด ๆ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลของบุคคลหรือหน่วยงาน ดังนี้

๓.๑ ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือที่เรียกโดยทั่วไปว่ามัลแวร์ (Malware) เป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๓.๒ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่งที่สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ไวรัส คอมพิวเตอร์สามารถแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหะ เช่น แฟลชไดรว์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

๓.๓ หนอนคอมพิวเตอร์ (Computer worm) เป็นมัลแวร์ชนิดหนึ่งที่สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต หนอน คอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่าย และตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอปพลิเคชัน จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังโดยใช้ช่องโหว่ดังกล่าว

๓.๔ ม้าโทรจัน (Trojan horse) เป็นมัลแวร์ชนิดหนึ่งที่มีจุดประสงค์เพื่อบุกรุก เข้าถึงและควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญหรือทำการคัดลอกข้อมูลดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญ ที่ผู้คุกคามต้องการอาจเป็น ชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่น ๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะซึ่งอาจมาจากแฟลชไดรว์หรือทางอีเมล์

๓.๕ สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดัก ข้อมูลนั้นสามารถรวบรวมข้อมูลสถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

๓.๖ ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่งที่มีพฤติกรรมเข้ารหัสไฟล์ต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถ เปิดไฟล์ใดๆ ได้เลย หากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้ คีย์ในการปลอดล็อคเพื่อกู้ข้อมูลคืนมา โดยผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

๓.๗ Backdoor เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบหรือเครื่องคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลัง เอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบหรือเครื่องคอมพิวเตอร์ในภายหลัง

๓.๘ Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้ นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

๓.๙ การโจมตีแบบ DoS/DDoS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตีมีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมากกว่า ๑ เครื่องและทำการโจมตี พร้อม ๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจก็ตาม จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

๓.๑๐ Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์อื่นๆ เพื่อรอรับสั่งจาก ผู้บุกรุกโดยผู้บุกรุกจะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่นการทำ DDoS เป็นต้น

๓.๑๑ Spam Mail หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับนั้นไม่ต้องการและสร้างความเดือดร้อนรำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการการชักชวนเข้าไปยังเว็บไซต์ต่าง ๆ ซึ่งอาจมีภัยคุกคามชนิด Phishing แฝงเข้ามาด้วย เหตุนี้จึงควรติดตั้งระบบ Anti Spam หรือหากใช้ฟรีอีเมล์ก็ควรมีโปรแกรมคัดกรองอีเมล์ ขยะในชั้นหนึ่งแล้ว

๓.๑๒ Phishing คือการหลอกลวงทางอินเทอร์เน็ตเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมล์หรือเมสเซนเจอร์ ตัวอย่างของการ Phishing เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้นจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

๓.๑๓ Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งหรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งเป็นวิธีการหนึ่งที่ผู้บุกรุกนิยมใช้

๓.๑๔ Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่าง ๆ กัน โดยทั่วไปแล้วการ Hacking เป็นสิ่งผิดกฎหมาย เว้นแต่หากได้รับอนุญาตจากเจ้าของเครื่องคอมพิวเตอร์หรือระบบ โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบ เพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

๓.๑๕ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบหรือเครื่องคอมพิวเตอร์แต่พยายามลักลอกเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ เช่น การโจรกรรมข้อมูล แสวงหา ผลกำไร หรือเพื่อความสนุกส่วนตัว

๓.๑๖ Social Engineering หมายถึง การหลอกลวง ล่อหลอกผู้อื่น ใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล เพื่อให้ได้ผลประโยชน์ตามที่แฮกเกอร์ต้องการ โดยอาศัย จุดอ่อน ความรู้เท่าไม่ถึงการณ์ ความไม่รู้ ความประมาทของผู้ใช้งานระบบคอมพิวเตอร์

๓.๑๗ Password Attack หมายถึง การโจมตีที่ผู้บุกรุกพยายามคาดเดา หรือทำให้ได้มาซึ่ง รหัสผ่านของผู้ใช้คนใดคนหนึ่งสำหรับนำไปโจมตีระบบคอมพิวเตอร์

๓.๑๘ Insider Treats หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากบุคคลภายในองค์กร แบ่งออกเป็น ๓ ประเภท คือ ภัยที่เกิดจากการประมาทโดยไม่ได้ตั้งใจของบุคลากร ภัยที่เกิดจากการขโมยตัวตนหรือข้อมูลบุคลากรที่ทำให้แฮกเกอร์สามารถเจาะเข้าระบบได้และภัยจากตัวบุคลากรเองที่ต้องการจะบ่อนทำลายองค์กรจากภายใน

๓.๑๙ SQL Injection หมายถึง การโจมตีที่ระบบฐานข้อมูลของระบบผ่านช่องโหว่ของ SQL ส่งผลให้ระบบฐานข้อมูลถูกขโมย หรือถูกทำลาย หรือแก้ไขให้เกิดความเสียหายได้

๓.๒๐ Form Jacking หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ไม่ประสงค์ดีสร้างโค้ด แปลกปลอมไว้บนเว็บไซต์ต่าง ๆ เพื่อหลอกลวงเป้าหมาย โดยมีจุดประสงค์ในการเข้าถึงระบบสารสนเทศและข้อมูลเพื่อก่ออาชญากรรม

**๔. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์**

เพื่อให้ส่วนราชการ หน่วยงานในจังหวัดพังงา มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามรูปแบบภัยคุกคามไซเบอร์โดยสามารถดำเนินการเตรียมความพร้อมในด้านต่าง ๆ ดังนี้

๔.๑ การเตรียมพร้อมด้านอุปกรณ์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของหน่วยงานในจังหวัดพังงาสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ ส่วนราชการจึงควรจัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็น ดังนี้

๔.๑.๑ อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DoS/DDoS BOTNET Phishing Sniffing Hacker ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหานอกจากความสามารถในการเป็น Firewall แล้วยังต้องมีความสามารถอื่น ๆ เพิ่มเติม ซึ่งได้แก่ ความสามารถในด้านการตรวจจับการบุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซต์อันตราย (Web filtering) และการควบคุมการใช้งานซอฟต์แวร์ (Application Control) เป็นอย่างน้อย

๔.๑.๒ ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของส่วนราชการ

๔.๑.๓ อุปกรณ์ web app firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ของส่วนราชการที่พัฒนาขึ้นมาให้บริการผ่าน web browser ได้แก่ การคุกคามทางไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุกเช่น Cross-site scripting และ SQL injection ได้เป็นอย่างน้อย

๔.๑.๔ ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูลและการกู้ข้อมูลของระบบเครือข่ายคอมพิวเตอร์ของส่วนราชการ รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้

๔.๑.๕ อุปกรณ์จัดเก็บข้อมูลภายนอก (SAN Storage) เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งระบบงานคอมพิวเตอร์ของส่วนราชการและในการรับมือทางไซเบอร์อุปกรณ์จัดเก็บข้อมูลภายนอกยังสามารถลดผลกระทบที่เกิดจาก Ransomware ได้โดยสำนักงานจังหวัดพังงาจะใช้อุปกรณ์จัดเก็บข้อมูลภายนอกดังกล่าวจัดทำพื้นที่จัดเก็บข้อมูลส่วนกลาง โดยกำหนดให้แต่ละกลุ่มงานมีพื้นที่จัดเก็บข้อมูล ๕๐ GB และมีการสำรองข้อมูลจากพื้นที่จัดเก็บข้อมูลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากส่วนราชการต่าง ๆ นำไฟล์สำคัญมาจัดเก็บเอาไว้ที่พื้นที่จัดเก็บข้อมูลส่วนกลางแล้วแม้ว่าจะเกิดภัยคุกคามไซเบอร์ประเภท Ransomware ก็จะสามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาได้

๔.๑.๖ ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีที่ไม่สามารถกู้ระบบงานคอมพิวเตอร์ขึ้นมาได้

๔.๑.๗ อุปกรณ์จัดเก็บ Log file ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของส่วนราชการ

๔.๑.๘ อุปกรณ์วิเคราะห์ Log file ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของส่วนราชการ ซึ่งข้อมูลที่ถูกวิเคราะห์ดังกล่าวจะช่วยระบุถึงหมายเลข IP Address ของผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางของส่วนราชการและใช้ประกอบการทำรายงานให้แก่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

๔.๑.๙ ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอรปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่ายของส่วนราชการ ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer worm, Trojan, Spyware, Ransomware, BOTNET และ Spam Mail

๔.๒ แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของส่วนราชการสามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา ส่วนราชการจะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้ อาจสามารถหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได้

๔.๓ การเตรียมพร้อมด้านบุคลากร

๔.๓.๑ การให้ความรู้เพื่อให้บุคลากรของส่วนราชการมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

๔.๓.๒ การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ตามมาตราที่ ๔๖ กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยส่วนราชการจะกำหนดระดับภัยคุกคามทางไซเบอร์พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๐ และจะแจ้งรายชื่อผู้เจ้าหน้าที่เพื่อประสานงานด้านการรักษาความปลอดภัยไซเบอร์ในระดับต่าง ๆ

๔.๓.๓ มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของส่วนราชการ

๔.๔ การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรองในกรณีที่ภัยคุกคามทางไซเบอร์ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางของส่วนราชการอย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน ส่วนราชการจะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหายหรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของส่วนราชการสามารถใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้ แนวทางในการกู้คืนข้อมูล และการใช้ระบบคอมพิวเตอร์สำรองจะกำหนดอยู่ในแอกสารแผนสำรองและกู้คืนระบบของส่วนราชการ

**๕. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์**

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ทั้งนี้ ส่วนราชการได้มีมาตรการสำหรับรับมือกับภัยคุกคามทางไซเบอร์ ๓ มาตรการ ดังนี้

๕.๑ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) มีขั้นตอนดังนี้ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) คือการที่ต้องสร้างกลไกและกระบวนการเพื่อ

– ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของส่วนราชการ

- การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

- การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับบริการที่สำคัญของส่วนราชการหรือไม่ และดำเนินการทบทวนกลไกกระบวนการอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่างๆ ยังคงมีประสิทธิภาพ

๕.๒ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) มี ๓ ขั้นตอน ดังนี้

๕.๒.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๕.๒.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๑) ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์

๒) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีการดำเนินการต่อไปนี้

- จัดตั้งทีมสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต

- ระบุสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

- ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

- ระบุผู้แทนหน่วยงานหลักและผู้เชี่ยวชาญด้านเทคนิคที่ จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

- ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม เช่น สื่อดั้งเดิมและโซเชียลมีเดีย สำหรับการเผยแพร่ข้อมูล

๓) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔) ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤต อันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕.๒.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๑) ส่วนราชการต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์หาก ได้รับคำสั่งเป็นลายลักษณอักษรให้ทำโดยคณะกรรมการการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติ หรือระดับภาคส่วน สำนักงานจังหวัดพังงาต้องตรวจสอบให้แน่ใจว่า บุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคง ปลอดภัยไซเบอร์ดังกล่าว

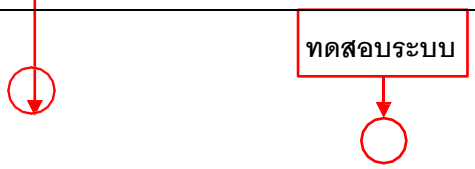
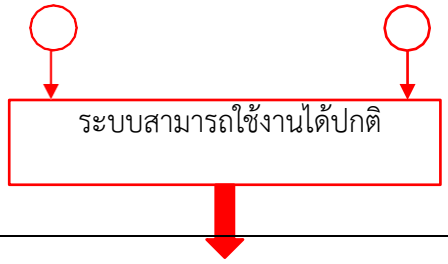
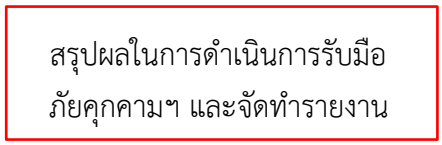
๒) ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการ ที่สำคัญของส่วนราชการเพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัย คุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้ รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์ และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการ ปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการ ที่สำคัญของส่วนราชการ

๕.๓ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

๕.๓.๑ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจ ว่าบริการที่สำคัญของสำนักงานจังหวัดพังงา สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริงรวมถึงสอบทาน แผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐและหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการ กำหนดระยะที่ สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๕.๓.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BPC อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมิน ประสิทธิภาพ ของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ส่วน ราชการได้จัดทำขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ซึ่งเป็นการดำเนินการเบื้องตัน ดังนี้

| ขั้นตอน | รายละเอียด |
|---|---|
| ตรวจพบภัยคุกคามทางไซเบอร์ | มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอร์ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือ เครื่องมือต่าง ๆ ตามที่กำหนดในข้อ ๓.๑ ซึ่งจะช่วยให้ส่วนราชการสามารถตรวจพบการคุกคามทางไซเบอร์อย่างรวดเร็ว |
| ตรวจสอบภัยคุกคามทางไซเบอร์ | ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์และประเมิน ระดับภัยคุกคามตามที่กำหนดในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๒ |
| ควบคุมภัยคุกคามทางไซเบอร์ | ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ให้ส่งผลกระทบน้อยที่สุดและป้องกันไม่ให้เกิดการแพร่กระจาย ไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วนส่วนราชการจะทำการปิดระบบหรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว |
| แก้ไขปัญหา<br>แก้ได้ / แก้ไม่ได้ | ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นในทันที |
| ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ | ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ |
| แก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม | หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว ส่วนราชการจะดำเนินการตรวจหาช่องโหว่โดยอุปกรณ์ตรวจสอบ ช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่น ๆ และหาวิธี เพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม |

| ขั้นตอน | รายละเอียด |
|---|---|
|  | ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของส่วนราชการว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่การทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะเข้าสู่กระบวนการกู้คืนระบบงาน |
|  | ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ส่วนราชการจะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์ สำรอง และเร่งกู้ระบบงานคอมพิวเตอร์หลัก |
|  | เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของส่วนราชการสามารถทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศของส่วนราชการจะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์ |
|  | สรุปผลในการรับมือภัยคุกคามทางไซเบอร์และแจ้งผล การดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการกอง ผู้บริหารระดับสูงด้านสารสนเทศ |

**๖. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของเจ้าหน้าที่สำนักงาน**

เมื่อเกิดการคุกคามทางไซเบอร์แล้ว ในบางครั้งผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ของเจ้าหน้าที่สำนักงานทำงานผิดพลาดหรือล่าช้าลงหรือส่งผลให้ไฟล์ข้อมูลที่ถูกจัดเก็บเอาไว้ ในเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้นเจ้าหน้าที่ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติควรดำเนินการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ ดังนี้

๖.๑ ดำเนินการตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

๖.๒ ดำเนินการตามนโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และนโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างเคร่งครัด

๗. การประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| **๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)** | | | | | | | |
| ๑) ความเสี่ยงจากการเกิดไฟไหม้ ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center) | ๑. ระบบคอมพิวเตอร์และระบบ เครือข่ายถูกทำลาย<br>๒. ระบบสารสนเทศและระบบฐานข้อมูลถูกทำลาย | ๑ | ๕ | ๕ | ๑. ตรวจสอบระบบดับเพลิงแบบอัตโนมัติตามมาตรฐาน ทุก ๓ เดือน<br>๒. ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก ๓ เดือน | การควบคุม (Treat) | งานสื่อสารในสำนักงาน |
| ๒) ความเสี่ยงจากระบบกระแสไฟฟ้า ขัดข้องของห้องศูนย์คอมพิวเตอร์ แม่ข่ายกลาง (Data Center) | ๑. ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้ ๒. ไม่สามารถระบบสารสนเทศและระบบฐานข้อมูลได้<br>๓. ระบบปฏิบัติการ และระบบฐานข้อมูลเกิดความเสียหายจาก เครื่องไม่ได้ถูกทำการปิดอย่าง เหมาะสม | ๑ | ๔ | ๔ | ๑. ตรวจสอบระบบสำรองไฟฟ้า (UPS) ในศูนย์คอมพิวเตอร์แม่ข่ายกลาง ทุก ๓ เดือน | การถ่ายโอน (Transfer) | งานสื่อสารในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| ๓) ความเสี่ยงจากอุณหภูมิและ ความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center) | เกิดความเสียหายต่อเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย | ๑ | ๔ | ๔ | ตรวจสอบเครื่องปรับอากาศ ที่ควบคุมอุณหภูมิ และที่ ควบคุมอุณหภูมิ | การถ่ายโอน (Transfer) | งานสื่อสารในสำนักงาน |
| ๔) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า | ๑. ไม่สามารถใช้งานระบบเครือข่ายได้<br>๒. ไม่สามารถให้บริการระบบเครือข่ายได้อย่างต่อเนื่อง | ๑ | ๓ | ๓ | ตรวจสอบอุปกรณ์เครือข่ายและระบบไฟฟ้า ทุก ๓ เดือน | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |
| ๕) ความเสี่ยงจากการโจรกรรม อุปกรณ์คอมพิวเตอร์ เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพวง | ๑. อุปกรณ์ และข้อมูลที่มีความสำคัญสูญหาย<br>๒. เสียภาพลักษณของหน่วยงาน | ๑ | ๓ | ๓ | ๑. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า - ออกห้องคอมพิวเตอร์แม่ข่าย<br>๒. ติดตั้งกลองวงจรปิดให้ครอบคลุมทุกที่ ๆ มี เครื่องคอมพิวเตอร์และอุปกรณ์ ติดตั้ง<br>๓. ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก ๓ เดือน | | งานสื่อสารในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| **๒. ความเสี่ยงด้านบุคลากร (Human Risk)** | | | | | | | |
| ๖) ความเสี่ยงจากผู้ดูแลระบบ | ข้อมูลที่อยู่ในชั้นความลับรั่วไหล ทำให้เสียหายต่อความน่าเชื่อถือ ของหน่วยงาน | ๑ | ๓ | ๓ | ๑. มีการ Authentication เข้าใช้ระบบสารสนเทศ รวมถึงการยกเลิกทะเบียน (เกษียณอายุ/ลาออก ฯลฯ)<br>๒. การจัดระดับการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล | การยอมรับ (Take) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |
| ๗) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย | ๑. สูญเสีย Bandwidth ในระบบ เครือข่ายทำให้ต้องเพิ่ม Bandwidth ให้มากขึ้น เนื่องจากการใช้งานนอกเหนือจากงานราชการ<br>๒. เครื่องคอมพิวเตอร์ เสียหายและเสื่อมอายุการใช้งานเร็วกว่าปกติ | ๒ | ๓ | ๖ | ๑. กำหนด Policy ของ Firewall ให้เหมาะสมต่อ การใช้งาน<br>๒. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำเครื่องคอมพิวเตอร์ หรือ resources ไปใช้นอกเหนือ จากงานราชการ และ รายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา<br>๓. ตรวจสอบและแนะนำ ผู้ใช้งานให้ใช้อุปกรณ์ คอมพิวเตอร์อย่างเหมาะสม | | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| **๓. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)** | | | | | | | |
| ๘) ความเสี่ยงด้านระบบคอมพิวเตอร์ และระบบเครือข่าย (Computer and Network Risk) | ๑. เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล<br>๒. ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน | ๓ | ๔ | ๑๒ | ๑. โปรแกรมหรือข้อมูลถูกทำลาย<br>๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ ตามปกติ<br>๓. การถูกขโมยข้อมูลที่สำคัญ | การควบคุม (Treat) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |
| ๙) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์ | ๑. โปรแกรมหรือข้อมูลถูกทำลาย<br>๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ<br>๓. การถูกขโมยข้อมูลที่สำคัญ | ๓ | ๕ | ๖ | ๑. อัพเดตโปรแกรมป้องกัน ไวรัสให้สามารถป้องกันไวรัส ได้ทุกรูปแบบ (อัตโนมัติ)<br>๒. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งครัด | การควบคุม (Treat) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| ๑๐) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่าย จากภายในและภายนอกองค์กร | ๑.ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้<br>๒. ทำให้ระบบเครื่องแม่ข่าย หรือ ลูกข่ายติดไวรัส และแพร่กระจาย สู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย<br>๓. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของหน่วยงาน<br>๔. ถูกโจรกรรมข้อมูลที่เป็นความลับ<br>๕. ไม่สามารถเข้าใช้ระบบสารสนเทศได้ | ๔ | ๔ | ๑๖ | ๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ<br>๒. ตรวจสอบ Policy และการทำงานของระบบ ป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวัง เครือข่าย ทุกวัน | การควบคุม (Treat) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |
| ๑๑) ความเสี่ยงจากการเชื่อมต่อ ระบบเครือข่ายอินทราเน็ต และ อินเทอร์เน็ต ภายในและภายนอก สถานที่ทำงาน | ๑. โปรแกรมหรือข้อมูลถูกทำลาย<br>๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ<br>๓. การถูกขโมยข้อมูลที่สำคัญ | ๓ | ๕ | ๖ | ๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ)<br>๒. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งครัด | การควบคุม (Treat) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| ๑๐) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่าย จากภายในและภายนอกองค์กร | ๑.ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้<br>๒. ทำให้ระบบเครื่องแม่ข่าย หรือ ลูกข่ายติดไวรัส และแพร่กระจาย สู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย<br>๓. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของหน่วยงาน<br>๔. ถูกโจรกรรมข้อมูลที่เป็นความลับ<br>๕. ไม่สามารถเข้าใช้ระบบสารสนเทศได้ | ๔ | ๔ | ๑๖ | ๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ<br>๒. ตรวจสอบ Policy และการทำงานของระบบ ป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวังเครือข่ายทุกวัน | การควบคุม (Treat) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |
| ๑๑) ความเสี่ยงจากการเชื่อมต่อ ระบบเครือข่ายอินทราเน็ต และ อินเทอร์เน็ต ภายในและภายนอก สถานที่ทำงาน | ๑. โปรแกรมหรือข้อมูลถูกทำลาย<br>๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ<br>๓. การถูกขโมยข้อมูลที่สำคัญ | ๓ | ๕ | ๖ | ๑. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ)<br>๒. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและ ให้มีผลบังคับใช้อย่างเคร่งครัด | การควบคุม (Treat) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| ๑๒) ความเสี่ยงจากการถูกบล็อกจาก ผู้ให้บริการเครือข่าย (Black List) | ๑. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไป ไม่ สามารถเข้าใช้งาน Web Server ได้<br>๒. ลดความน่าเชื่อถือของหน่วยงาน | ๑ | ๓ | ๓ | ๑.อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ<br>๒.ปรับปรุง Policy Firewall<br>๓. Monitoring ระบบเครือข่ายเป็นประจำทุกวัน | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |
| ๑๓) ความเสี่ยงจากการใช้งานระบบ ประชุมทางไกลผ่านเครือข่าย (VDO Conference) | ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ขัดข้อง ทำให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องไม่สามารถเข้าร่วมประชุมได้ | ๑ | ๓ | ๓ | ตรวจสอบการเชื่อมต่อ อุปกรณ์การทำงานของ ระบบชุดประชุมทางไกล ผ่านเครือข่าย (VDO Conference) ก่อนใช้งาน | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |
| ๑๔) ความเสี่ยงจากการใช้งานระบบ โทรศัพท์ (IP Phone) | ระบบโทรศัพท์ (IP Phone) ขัดข้องทำให้เจ้าหน้าที่ในหน่วยงานไม่สามารถใช้งานระบบโทรศัพท์ติดต่อ ประสานงานทั้งภายใน/ภายนอก ได้อย่างต่อเนื่อง | ๑ | ๓ | ๓ | ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone) อย่างสม่ำเสมอ | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| ๑๒) ความเสี่ยงจากการถูกบล็อกจาก ผู้ให้บริการเครือข่าย (Black List) | ๑. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไป ไม่ สามารถเข้าใช้งาน Web Server ได้<br>๒. ลดความน่าเชื่อถือของหน่วยงาน | ๑ | ๓ | ๓ | ๑.อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ<br>๒.ปรับปรุง Policy Firewall<br>๓. Monitoring ระบบ เครือข่ายเป็นประจำทุกวัน | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |
| ๑๓) ความเสี่ยงจากการใช้งานระบบ ประชุมทางไกลผ่านเครือข่าย (VDO Conference) | ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ขัดข้อง ทำให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องไม่สามารถเข้าร่วมประชุมได้ | ๑ | ๓ | ๓ | ตรวจสอบการเชื่อมต่ออุปกรณ์การทำงานของ ระบบชุดประชุมทางไกล ผ่านเครือข่าย (VDO Conference) ก่อนใช้งาน | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |
| ๑๔) ความเสี่ยงจากการใช้งานระบบ โทรศัพท์ (IP Phone) | ระบบโทรศัพท์ (IP Phone) ขัดข้องทำให้เจ้าหน้าที่ในหน่วยงานไม่สามารถใช้งานระบบโทรศัพท์ติดต่อ ประสานงานทั้งภายใน/ภายนอก ได้อย่างต่อเนื่อง | ๑ | ๓ | ๓ | ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone) อย่างสม่ำเสมอ | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| **๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)** | | | | | | | |
| ๑๕) การใช้ซอฟแวร์ผิดลิขสิทธิ์ | ๑.การถูกฟ้องร้อง เสื่อมเสียชื่อเสียง และความน่าเชื่อถือของหน่วยงาน<br>๒. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ<br>๓.หน่วยงานอาจ ถูกฟ้องร้องเรียกค่าเสียหายจาก ผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ | ๑ | ๓ | ๓ | ๑. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น<br>๒.การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานโปรแกรมแบบ Open Source | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |
| ๑๖) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร | ๑.สร้างความเสียหายต่อระบบคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ และระบบฐานข้อมูล<br>๒. ลดความน่าเชื่อถือต่อหน่วยงาน | ๑ | ๓ | ๓ | ๑. อัพเดทเครื่องมือและโปรแกรมที่ใช้พัฒนาอย่าง<br>๒. ตรวจสอบช่องโหว่และดำเนินการแก้ไข ทุก ๓ เดือน | การยอมรับ (Take) | งานสื่อสารในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| ๑๗) ความเสี่ยงจากการจัดจ้างพัฒนา โปรแกรมหรือดูแลระบบโดยผู้รับจ้าง ภายนอก (Outsource) | ๑. ไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่ และแก้ไขการทำงานที่ผิดพลาดได้อย่างทันท่วงที<br>๒. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว เนื่องจากโปรแกรมหมดลิขสิทธิ์และขาดการปรับปรุง (Update) โปรแกรม | ๑ | ๒ | ๒ | ๑.กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการวิเคราะห์ออกแบบการพัฒนาระบบ และชุดคำสั่ง (Source Code) ฉบับสมสมบูรณ์ทั้ง ในกรณีพัฒนาเสร็จสิ้นและเมื่อมีการปรับปรุงแก้ไข<br>๒. ส่งมอบชุดคำสั่ง (Source Code) ชุดสมบูรณ์<br>๓. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่<br>๔. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลให้มีความทันสมัยและใช้งานได้อย่างต่อเนื่อง | การควบคุม (Treat) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |

| ความเสี่ยง | การประเมินความเสี่ยง | | | | วิธีการบริหารความเสี่ยง | | |
|---|---|---|---|---|---|---|---|
| | ผลกระทบ | โอกาส | ผลกระทบ | ระดับความเสี่ยง | แนวทางการควบคุม | วิธีจัดการความเสี่ยง | ผู้รับผิดชอบ |
| **๕. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)** | | | | | | | |
| ๑๘) ความเสี่ยงจากระบบฐานข้อมูล ไม่ถูกต้อง ไม่เป็นปัจจุบัน และ ไม่ครบถ้วน | ๑. ระบบฐานข้อมูลไม่สามารถนำไปใช้สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ<br>๒. ลดความน่าเชื่อถือของหน่วยงาน | ๑ | ๓ | ๓ | ๑. จัดทำรายการข้อมูล และ ความถี่ในการปรับปรุง<br>๒. กำหนดมาตรการแนวทางการปรับปรุง และช่องทางการเข้าถึงข้อมูลเพื่อให้ผู้ดูแลข้อมูลถือปฏิบัติ | การยอมรับ (Take) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |
| ๑๙) ความเสี่ยงจากการไม่สำรองข้อมูลและไม่สามารถกู้คืนระบบฐานข้อมูล | ๑. เกิดการสูญหายของข้อมูล และ กระทบต่อการทำงานตามปกติ<br>๒.ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้ สนับสนุนการปฏิบัติงานได้ | ๑ | ๓ | ๓ | ๑. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน<br>๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) ทุกสัปดาห์ | การยอมรับ (Take) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |
| ๒๐) ความเสี่ยงจากการโจมตีระบบฐานข้อมูล | ๑. ข้อมูลที่สำคัญรั่วไหลสู่ภายนอก หรือสาธารณะ<br>๒. ข้อมูลที่สำคัญสูญหายและถูกทำลาย | ๑ | ๔ | ๔ | ๑. ตรวจสอบระบบป้องกันการบุกรุกและระบบ ตรวจสอบและเฝ้าระวัง เครือข่าย เป็นประจำทุกวัน<br>๒. ตรวจสอบ Policy และ Log ของระบบป้องกันการ บุกรุกและระบบเฝ้าระวัง เครือข่าย เป็นประจำทุกวัน | การยอมรับ (Take) | เจ้าหน้าที่ทางด้าน IT ในสำนักงาน |