



จังหวัดมหาสารคาม

MAHASARAKHAM PROVINCE

แผนรับมือภัยคุกคามทางไซเบอร์ (CYBER INCIDENT RESPONSE PLAN)

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
สำนักงานจังหวัดมหาสารคาม

มกราคม 2568

สารบัญ

	หน้าที่
๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์	๑
๓. รูปแบบภัยคุกคามไซเบอร์	๑
๔. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์	๓
๕. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์	๕
๕.๑ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	๕
๕.๒ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	๕
๕.๓ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)	๖
๖. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของเจ้าหน้าที่จังหวัดมหาสารคาม	๘
๗. การประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์	๙

แผนรับมือภัยคุกคามทางไซเบอร์

จังหวัดมหาสารคาม

๑. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

๑.๑ แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละ ๑ ครั้ง

๑.๒ แผนรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ จังหวัดมหาสารคาม จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่มาในรูปแบบ ไวรัสมัลแวร์ และการโจมตีระบบเครือข่ายคอมพิวเตอร์ของจังหวัดมหาสารคาม โดยการดำเนินงานตามแผน จะมุ่งเน้นในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืน ระบบเครือข่ายคอมพิวเตอร์กลางให้สามารถใช้งานได้

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๒ เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์ของจังหวัดมหาสารคาม ให้สามารถใช้งานได้

๒.๓ เพื่อเตรียมความพร้อมด้านบุคลากรของจังหวัดมหาสารคาม ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

๒.๔ เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทันทั่วทั้งที่ กรณีเกิดสถานการณ์ความไม่แน่นอน

๓. รูปแบบภัยคุกคามทางไซเบอร์

๓.๑ ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือมัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่ทำการงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๓.๒ ไวรัสมัลแวร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่ง ที่สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสมัลแวร์จะแพร่กระจายตัวเองไปสู่ เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหะ เช่น แฟลชไดรฟ์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

๓.๓ หนอนคอมพิวเตอร์ (Computer Worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่าง กับไวรัสตรงที่ ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์ จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอปพลิเคชัน จากนั้น จึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

๓.๔ ม้าโทรจัน (Trojan Horse) เป็นมัลแวร์ชนิดหนึ่ง ที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูล ดังกล่าว ส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็นชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคล อื่น ๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัย พาหะ ซึ่งอาจมาจากแฟลชไดรฟ์ หรือทางอีเมล

๓.๕ สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูลสถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

๓.๖ ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีพฤติกรรมเข้ารหัสไฟล์ต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลย หากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่า จะต้องใช้คีย์ในการปลดล็อกเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

๓.๗ ประตูหลัง (Backdoor) เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบงานคอมพิวเตอร์โดยไม่ต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบงานคอมพิวเตอร์ในภายหลัง

๓.๘ Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้ นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

๓.๙ การโจมตีแบบ DoS/DDOS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตี มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่า ๑ เครื่องและกระทำพร้อม ๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่า การโจมตีแบบ Distributed Denial of Service (DDoS)

๓.๑๐ Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะ เป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เวิร์ดหรืออุปกรณ์ IoT อื่น ๆ เพื่อรองรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุก (Hacker) จะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่น การทำ DDoS เป็นต้น

๓.๑๑ Spam Mail หรืออีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อนรำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการการชักชวน เข้าไปยังเว็บไซต์ต่าง ๆ ซึ่งอาจมีภัยคุกคามชนิด Phishing แฝงเข้ามาด้วย ด้วยเหตุนี้ จึงควรติดตั้งระบบ Anti-Spam หรือหากใช้ฟรีอีเมล ก็จะมีโปรแกรมคัดกรองอีเมลขยะเบื้องต้นอยู่ให้แล้ว

๓.๑๒ Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลข บัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิ่ง เช่น การบอกแก่ผู้รับ ปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบ และใส่ข้อมูลที่ สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

๓.๑๓ Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือจาก เครือข่าย หนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ถูกผู้บุกรุกกระบบนิยมใช้

๓.๑๔ Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่าง ๆ กัน ทั้งนี้โดยทั่วไปแล้วการ Hacking เป็นสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตาม หากได้รับอนุญาตก็ไม่ใช่ว่าผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบเพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

๓.๑๕ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเป็นเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกคาม

๔. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์

จังหวัดมหาสารคาม มีการเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ โดยมีการดำเนินการเตรียมความพร้อมในด้านต่าง ๆ ดังนี้

๔.๑ การเตรียมพร้อมด้านอุปกรณ์เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคามสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ โดยได้จัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็น ดังนี้

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

๔.๑.๒ ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคาม

๔.๑.๓ อุปกรณ์ Web App Firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ของจังหวัดมหาสารคาม ที่พัฒนาขึ้นมาให้บริการผ่าน Web Browser ได้แก่ การคุกคามทางไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุก เช่น Cross-site scripting และ SQL injection ได้เป็นอย่างน้อย

๔.๑.๔ ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และการกู้ข้อมูลของระบบเครือข่ายคอมพิวเตอร์ของจังหวัดมหาสารคาม รวมทั้ง ยังสามารถสำรองข้อมูลแบบเข้ารหัสได้

๔.๑.๕ อุปกรณ์จัดเก็บข้อมูลภายนอก (SAN Storage) เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งระบบงานคอมพิวเตอร์ของจังหวัดมหาสารคาม และในการรับมือทางไซเบอร์อุปกรณ์จัดเก็บข้อมูลภายนอกยังสามารถลดผลกระทบที่เกิดจาก Ransomware ได้โดยจังหวัดยโสธรจะใช้อุปกรณ์จัดเก็บข้อมูลภายนอกดังกล่าวจัดทำพื้นที่จัดเก็บข้อมูลส่วนกลาง โดยกำหนดให้แต่ละกลุ่มงานมีพื้นที่จัดเก็บข้อมูล 50 GB และจะมีการสำรองข้อมูลจากพื้นที่จัดเก็บข้อมูลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากส่วนราชการต่าง ๆ นำไฟล์สำคัญมาจัดเก็บเอาไว้ที่พื้นที่จัดเก็บข้อมูลส่วนกลางแล้วแม้ว่าจะเกิดภัยคุกคามไซเบอร์ประเภท Ransomware ก็จะสามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาได้

๔.๑.๖ ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีที่ระบบงานคอมพิวเตอร์ขึ้นมาได้

๔.๑.๗ อุปกรณ์จัดเก็บ Log file ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคาม

๔.๑.๘ อุปกรณ์วิเคราะห์ Log file ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคาม ซึ่งข้อมูลที่ถูวิเคราะห์ดังกล่าวจะช่วยระบุถึงหมายเลข IP Address ของผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคาม และใช้ประกอบการทำรายงานให้แก่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

๔.๑.๙ ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่ายของจังหวัดมหาสารคาม ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer worm, Trojan, Spyware, Ransomware, BOTNET และSpam Mail

๔.๒ แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคาม สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้น ตลอดเวลา จังหวัดมหาสารคามจะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้ อาจสามารถค้นหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนากระบวนการคอมพิวเตอร์ได้

๔.๓ การเตรียมพร้อมด้านบุคลากร

๔.๓.๑ การให้ความรู้ เพื่อให้บุคลากรของจังหวัดมหาสารคาม มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ จังหวัดมหาสารคามจะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรของจังหวัดมหาสารคาม

๔.๓.๒ การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๔๖ กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจังหวัดมหาสารคามจะกำหนดระดับภัยคุกคามทางไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๖๐ และจะแจ้งรายชื่อผู้เจ้าหน้าที่เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับต่าง ๆ

๔.๓.๓ มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคาม

๔.๔ การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง ในกรณีที่ภัยคุกคามทางไซเบอร์ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคามอย่างมาก จนไม่สามารถทำงานได้เป็นเวลานาน จังหวัดมหาสารคามจะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของจังหวัดมหาสารคามสามารถใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้ แนวทางในการกู้คืนข้อมูล และการใช้ระบบคอมพิวเตอร์สำรองจะกำหนดอยู่ในเอกสารแผนสำรองและกู้คืนระบบของจังหวัดมหาสารคาม

๕. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์

ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ทั้งนี้ ทางจังหวัดมหาสารคามได้มีมาตรการสำหรับรับมือกับภัยคุกคามทางไซเบอร์ อยู่ ๓ มาตรการ ดังนี้

๕.๑ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) มีขั้นตอน ดังนี้

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) คือ การที่สร้างกลไกและกระบวนการเพื่อดำเนินการ ดังนี้

- ตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของจังหวัดมหาสารคาม
- การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ
- การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวกับบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย หรือไม่และดำเนินการทบทวนกลไก และกระบวนการอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

๕.๒ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) มี ๓ ขั้นตอน ดังนี้

๕.๒.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ สามารถดำเนินการได้อย่างมีประสิทธิภาพ และประสิทธิผล

๕.๒.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

- ๑) ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์
- ๒) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตมีขั้นตอนการดำเนินการ ดังนี้
 - จัดตั้งทีมสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต
 - ระบุสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง
 - ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
 - ระบุผู้แทนหน่วยงานหลักและผู้เชี่ยวชาญด้านเทคนิค ที่จะเป็นตัวแทนขององค์กร เมื่อกล่าวแถลงกับสื่อมวลชน
 - ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อสังคมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล
- ๓) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและ สอดคล้องกันในช่วงวิกฤต
- ๔) ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

๕.๒.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๑) จังหวัดมหาสารคาม ในกรณีที่มีส่วนร่วมในการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำ โดยคณะกรรมการการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ จะต้องสามารถดำเนินการได้ ทั้งในระดับชาติ หรือระดับภาคส่วน โดยจังหวัดมหาสารคาม จะต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าวด้วย

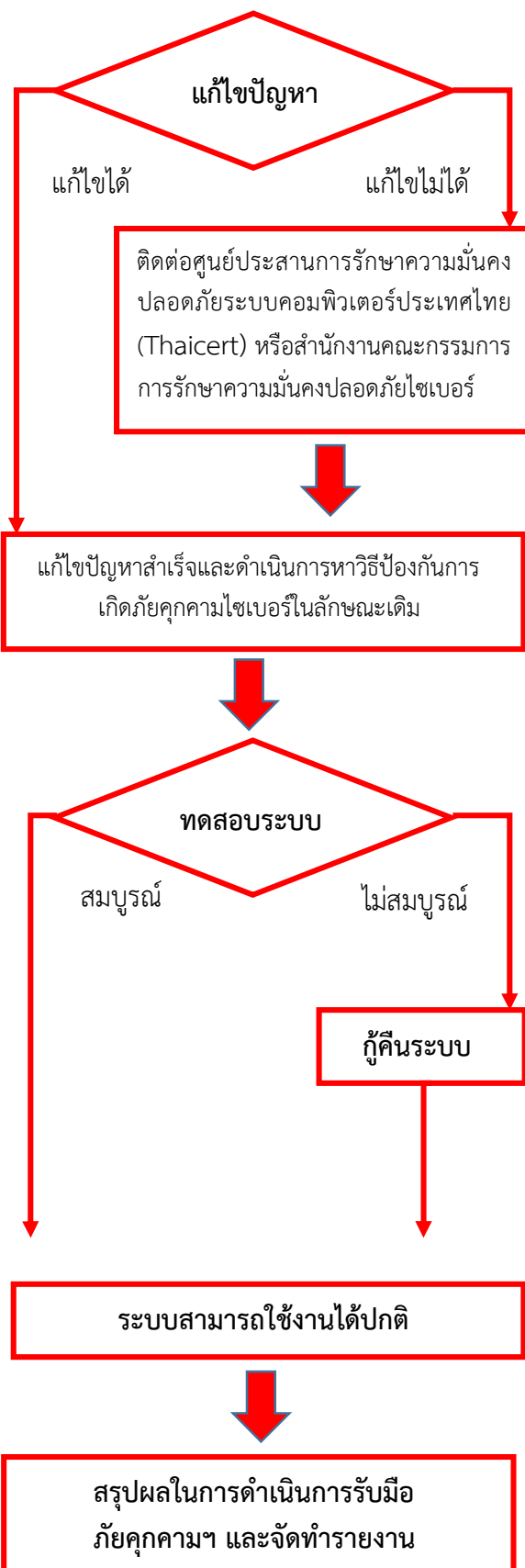
๒) ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของจังหวัดมหาสารคาม เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้ รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์ และแผนการสื่อสารในภาวะวิกฤตและขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย

๕.๓ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

๕.๓.๑ ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึง สอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตค่านิยม และการกำหนดระยะที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time - Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๕.๓.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ จังหวัดมหาสารคามจึงได้จัดทำขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ ซึ่งเป็นการดำเนินการเบื้องต้น ดังนี้

ขั้นตอนการดำเนินงาน	รายละเอียด
ตรวจพบภัยคุกคามทางไซเบอร์ ↓ ตรวจพบภัยคุกคามทางไซเบอร์ ↓ การควบคุมภัยคุกคามทางไซเบอร์ ↓	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอร์ ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่าง ๆ ตามที่กำหนดในข้อ ๔.๑ ซึ่งจะช่วยให้จังหวัดมหาสารคามสามารถตรวจพบการคุกคามทางไซเบอร์อย่างรวดเร็ว ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๒ ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุดและป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วน จังหวัดมหาสารคามจะทำการปิดระบบ หรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว

ขั้นตอนการดำเนินงาน	รายละเอียด
 <pre> graph TD A{แก้ไขปัญหา} -- แก้ไขได้ --> B[แก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม] A -- แก้ไขไม่ได้ --> C[ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์] C --> B B --> D{ทดสอบระบบ} D -- สมบูรณ์ --> E[ระบบสามารถใช้งานได้ตามปกติ] D -- ไม่สมบูรณ์ --> F[กู้คืนระบบ] F --> E E --> G[สรุปผลในการดำเนินการรับมือภัยคุกคามฯ และจัดทำรายงาน] </pre>	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นในทันที ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อขอคำแนะนำหรือขอความช่วยเหลือ
	หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้วจังหวัดมหาสารคาม จะดำเนินการตรวจสอบช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่น ๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม
	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของจังหวัดมหาสารคามว่าสามารถทำงานได้สมบูรณ์หรือไม่ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน
	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ จังหวัดยโสธรจะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์สำรอง และเร่งกู้ระบบงานคอมพิวเตอร์หลัก
	เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของจังหวัดมหาสารคาม สามารถทำงานได้ตามปกติแล้วหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศของจังหวัดมหาสารคาม จะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามทางไซเบอร์
	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการกองผู้บริหารระดับสูงด้านสารสนเทศ

๖. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของผู้เจ้าหน้าที่จังหวัดมหาสารคาม

เมื่อเกิดการคุกคามทางไซเบอร์แล้ว ในบางครั้งผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ของผู้เจ้าหน้าที่จังหวัดมหาสารคามทำงานผิดพลาดหรือล่าช้าลง หรือส่งผลให้ไฟล์ข้อมูลที่ถูกจัดเก็บเอาไว้ในเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้น เจ้าหน้าที่ของจังหวัดมหาสารคาม ควรดำเนินการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ ดังนี้

๖.๑ ดำเนินการตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

๖.๒ ดำเนินการตามนโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และนโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างเคร่งครัด

๗. การประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	ผู้รับผิดชอบ
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)							
๑) ความเสี่ยงจากการเกิดไฟไหม้ ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๑. ระบบคอมพิวเตอร์และระบบ เครือข่ายถูกทำลาย ๒. ระบบสารสนเทศและระบบ ฐานข้อมูลถูกทำลาย	๑	๕	๕	๑. ตรวจสอบระบบดับเพลิง แบบอัตโนมัติตามมาตรฐาน ทุก ๓ เดือน ๒. ตรวจสอบการทำงานของ ศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก ๓ เดือน	การควบคุม (Treat)	งานสื่อสาร กลุ่มงาน อำนวยการ สนจ.มค.
๒) ความเสี่ยงจากระบบกระแสไฟฟ้า ขัดข้องของห้องศูนย์คอมพิวเตอร์ แม่ข่ายกลาง (Data Center)	๑. ไม่สามารถใช้งานระบบ คอมพิวเตอร์และระบบ เครือข่ายได้ ๒. ไม่สามารถระบบสารสนเทศ และระบบฐานข้อมูลได้ ๓. ระบบปฏิบัติการ และระบบ ฐานข้อมูลเกิดความเสียหาย จากเครื่องไม่ได้ถูกทำการ ปิดอย่างเหมาะสม	๑	๔	๔	ตรวจสอบระบบสำรอง ไฟฟ้า (UPS) ในศูนย์ คอมพิวเตอร์แม่ข่ายกลาง ทุก ๓ เดือน	การถ่ายโอน (Transfer)	งานสื่อสาร กลุ่มงาน อำนวยการ สนจ.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๓) ความเสี่ยงจากอุณหภูมิและความชื้นของศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center) ผิดปกติ	เกิดความเสียหายต่อเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย	๑	๔	๔	ตรวจสอบเครื่องปรับอากาศที่ควบคุมอุณหภูมิ	การถ่ายโอน (Transfer)	งานสื่อสาร กลุ่มงาน อำนวยการ สนจ.มค.
๔) ความเสี่ยงจากแมลงสัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า	๑. ไม่สามารถใช้งานระบบเครือข่ายได้ ๒. ไม่สามารถให้บริการระบบเครือข่ายได้อย่างต่อเนื่อง	๑	๓	๓	ตรวจสอบอุปกรณ์เครือข่าย และระบบไฟฟ้า ทุก ๓ เดือน	การยอมรับ (Take)	งานสื่อสาร กลุ่มงาน อำนวยการ สนจ.มค.
๕) ความเสี่ยงจากการโจรกรรม อุปกรณ์คอมพิวเตอร์ เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง	๑. อุปกรณ์ และข้อมูลที่มีความสำคัญสูญหาย ๒. เสียภาพลักษณ์ของหน่วยงาน	๑	๓	๓	๑. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า – ออก ห้องคอมพิวเตอร์แม่ข่าย ๒. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกพื้นที่ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้ง ๓. ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก ๓ เดือน		งานสื่อสาร กลุ่มงาน อำนวยการ สนจ.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๒. ความเสี่ยงด้านบุคลากร (Human Risk)							
๖) ความเสี่ยงจากผู้ดูแลระบบ	ข้อมูลที่อยู่ในชั้นความลับ รั่วไหล ทำให้เสียหายต่อความน่าเชื่อถือของหน่วยงาน	๑	๓	๓	๑. การทำ Authentication การเข้าใช้ระบบสารสนเทศ รวมถึงการยกเลิกทะเบียน (เกษียณอายุ/ลาออก ฯลฯ) ๒. การจัดระดับการเข้าถึง ข้อมูลอย่างเป็นระบบ และ สิทธิในการกระทำกับข้อมูล	การยอมรับ (Take)	กลุ่มงาน ยุทธศาสตร์ และข้อมูล เพื่อการพัฒนาจังหวัด สนจ.มค.
๗) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย	๑. สูญเสีย Bandwidth ในระบบ เครือข่ายทำให้ต้องเพิ่ม Bandwidth ให้มากขึ้น เนื่องจาก การใช้งานนอกเหนือจากงานราชการ ๒. เครื่องคอมพิวเตอร์ เสียหาย และเสื่อมอายุการใช้งาน เร็วกว่าปกติ	๒	๖	๖	๑. กำหนด Policy ของ Firewall ให้เหมาะสมต่อการใช้งาน ๒. การมีข้อตกลงที่ผู้ใช้งาน ต้องเป็นผู้รับผิดชอบในการ นำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ resources ไปใช้นอกเหนือจากงานราชการ และ รายงานการใช้งานของ ผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา ๓. ตรวจสอบและแนะนำ ผู้ใช้งานให้ใช้อุปกรณ์ คอมพิวเตอร์อย่างเหมาะสม	การควบคุม (Treat)	กลุ่มงาน ยุทธศาสตร์ และข้อมูล เพื่อการพัฒนาจังหวัด สนจ.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๓. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)							
๘. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)	๑. เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล ๒. ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	๓	๔	๑๒	๑. โปรแกรมหรือข้อมูลถูกทำลาย ๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ ๓. การถูกขโมยข้อมูลที่สำคัญ	การควบคุม (Treat)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สنج.มค.
๙) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	๑. โปรแกรมหรือข้อมูลถูกทำลาย ๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ ๓. การถูกขโมยข้อมูลที่สำคัญ	๓	๕	๖	๑. อัปเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ) ๒. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งครัด	การควบคุม (Treat)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สنج.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๐) ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	๑. ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้ ๒. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย ๓. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูลหรือรูปภาพบน Web Site ของหน่วยงาน ๔. ถูกโจรกรรมข้อมูลที่เป็นความลับ ๕. ไม่สามารถเข้าใช้ระบบสารสนเทศได้	๔	๔	๑๖	๑. อัปเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันได้ทุกรูปแบบ ๒. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวังเครือข่าย ทุกวัน	การควบคุม (Treat)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สนจ.มค.
๑๑) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน	๑. ระบบเครือข่ายอินเทอร์เน็ตและอินเทอร์เน็ตไม่สามารถใช้งานได้ ๒. ไม่สามารถเข้าใช้งานระบบสารสนเทศ ผ่านเครือข่ายอินเทอร์เน็ตและอินเทอร์เน็ตได้	๒	๓	๖	๑. ตรวจสอบระบบเครือข่ายสื่อสารหลักทุกวัน ๒. ควบคุมการเข้าใช้เครือข่ายอินเทอร์เน็ตและอินเทอร์เน็ต โดยใช้ระบบยืนยันตน (Authentication)	การยอมรับ (Take)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สนจ.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๒) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)	๑. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ ๒. ลดความน่าเชื่อถือของหน่วยงาน	๑	๓	๓	๑. อัปเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันได้ทุกรูปแบบ ๒. ปรับปรุง Policy Firewall ๓. Monitoring ระบบเครือข่ายเป็นประจำทุกวัน	การยอมรับ (Take)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สنج.มค.
๑๓) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ชัดข้อง ทำให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องไม่สามารถเข้าร่วมประชุมได้	๑	๓	๓	ตรวจสอบการเชื่อมต่ออุปกรณ์ การทำงานของระบบชุดประชุมทางไกลผ่านเครือข่าย (VDO Conference) ก่อนใช้งาน	การยอมรับ (Take)	งานสื่อสารกลุ่มงานอำนวยการ สنج.มค.
๑๔) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)	ระบบโทรศัพท์ (IP Phone) ชัดข้องทำให้เจ้าหน้าที่ในหน่วยงานไม่สามารถใช้ งานระบบโทรศัพท์ติดต่อ ประสานงานได้ทั้งภายใน/ภายนอกได้อย่างต่อเนื่อง	๑	๓	๓	ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone) อย่างสม่ำเสมอ	การยอมรับ (Take)	งานสื่อสารกลุ่มงานอำนวยการ สنج.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)							
๑๕) ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone) อย่างสม่ำเสมอ	๑. การถูกฟิชจิ้ง และเสื่อมเสียชื่อเสียง และความน่าเชื่อถือของหน่วยงาน ๒. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้น ๆ ๓. หน่วยงานอาจถูกฟิชจิ้งเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้น ๆ	๑	๓	๓	๑. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๒. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งาน Open Source	การยอมรับ (Take)	งานสื่อสารกลุ่มงานอำนวยการสนจ.มค.
๑๖) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑. สร้างความเสียหายต่อระบบคอมพิวเตอร์แม่ข่ายระบบสารสนเทศและระบบฐานข้อมูล ๒. ลดความน่าเชื่อถือต่อหน่วยงาน	๑	๓	๓	๑. อัปเดตเครื่องมือและโปรแกรมที่ใช้พัฒนา ๒. ตรวจสอบช่องโหว่และดำเนินการแก้ไขทุก ๓ เดือน	การยอมรับ (Take)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัดสนจ.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๗) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	๑. ไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่ และแก้ไขการทำงานที่ผิดพลาดได้อย่างทันท่วงที ๒. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาวเนื่องจากโปรแกรมหมดลิขสิทธิ์และขาดการปรับปรุง (Update) โปรแกรม	๑	๓	๓	๑. กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการวิเคราะห์ออกแบบการพัฒนาระบบและชุดคำสั่ง (Source Code) ฉบับสมบูรณ์ทั้ง ในกรณีพัฒนาเสร็จสิ้นและเมื่อมีการปรับปรุงแก้ไข ๒. ส่งมอบชุดคำสั่ง (Source Code) ชุดสมบูรณ์ ๓. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ ๔. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลให้มีความทันสมัยและใช้งานได้อย่างต่อเนื่อง	การควบคุม (Treat)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สนจ.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๕. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)							
๑๘) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	๑. ระบบฐานข้อมูลไม่สามารถนำไปใช้สนับสนุนการปฏิบัติงาน ได้อย่างมีประสิทธิภาพ ๒. ลดความน่าเชื่อถือของหน่วยงาน	๑	๓	๓	๑. จัดทำรายการข้อมูลและความถี่ในการปรับปรุง ๒. กำหนดมาตรการแนวทางการปรับปรุง และช่องทางการเข้าถึงข้อมูล เพื่อให้ผู้ดูแลข้อมูลถือปฏิบัติ	การยอมรับ (Take)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สنج.มค.
๑๙) ความเสี่ยงจากการไม่สำรองข้อมูลและไม่สามารถกู้คืนระบบฐานข้อมูล	๑. เกิดการสูญหายของข้อมูลและกระทบต่อการทำงานตามปกติ ๒. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้สนับสนุนการปฏิบัติงานได้	๑	๓	๓	๑. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน ๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) ทุกสัปดาห์	การยอมรับ (Take)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สنج.มค.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๒๐) ความเสี่ยงจากการโจมตีระบบฐานข้อมูล	๑. ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ ๒. ข้อมูลที่สำคัญสูญหายและถูกทำลาย	๑	๔	๔	๑. ตรวจสอบระบบป้องกันการบุกรุกและระบบตรวจสอบและเฝ้าระวังเครือข่ายเป็นประจำทุกวัน ๒. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกและระบบเฝ้าระวังเครือข่ายเป็นประจำทุกวัน	การยอมรับ (Take)	กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัดสนจ.มค.



**กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
สำนักงานจังหวัดมหาสารคาม**