กรมโรงงานอุตสาหกรรม

DEPARTMENT OF INDUSTRIAL WORKS

แผนรับมือภัยคุกคามทางไซเบอร์

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

พฤษภาคม 2566

สารบัญ

เรื่อง **หน้า**

แผนรับมือภัยคุกคามทางไซเบอร์

กรมโรงงานและอุตสาหกรรม

1. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

1. แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

2. แผนรับมือภัยคุกคามทางไซเบอร์

เพื่อดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กรมโรงงานอุตสาหกรรม จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ที่มาในรูปแบบไวรัสคอมพิวเตอร์ และการโจมตีระบบเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม โดยการดำเนินงานตามแผนจะมุ่งเน้นในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางให้สามารถใช้งานได้

2. วัตถุประสงค์

1. เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2. เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม ให้สามารถใช้งานได้

3. เพื่อเตรียมความพร้อมด้านบุคลากรของกรมโรงงานอุตสาหกรรม ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

4. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอน

3. รูปแบบภัยคุกคามไซเบอร์

3.1 ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือมัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

3.2 ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่ง ที่สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหะ เช่น แฟลชไดรว์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

3.3 หนอนคอมพิวเตอร์ (Computer Worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอพพลิเคชั่น จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

3.4 ม้าโทรจัน (Trojan Horse) เป็นมัลแวร์ชนิดหนึ่ง ที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็นชื่อผู้ใช้รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคล อื่น ๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะ ซึ่งอาจมาจากแฟลชไดรว์ หรือทางอีเมล

3.5 สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูลสถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

3.6 ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีพฤติกรรมเข้ารหัสไฟล์ต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมาผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ

3.7 ประตูหลัง (Backdoor) เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบงานคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบงานคอมพิวเตอร์ในภายหลัง

3.8 Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้ นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

3.9 การโจมตีแบบ DoS/DDOS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตี มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่า 1 เครื่องและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่า การโจมตีแบบ Distributed Denial of Service (DDoS)

3.10 Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ เพื่อรอรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุก (Hacker) จะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่นการทำ DDoS เป็นต้น

3.11 Spam Mail หรืออีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้า ไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ Anti-Spam หรือหากใช้ฟรีอีเมล ก็จะมีโปรแกรมคัดกรองอีเมลขยะ ในชั้นหนึ่งแล้ว

3.12 Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและ ใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

3.13 Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ผู้บุกรุกระบบนิยมใช้

3.14 Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่าง ๆ กัน ทั้งนี้โดยทั่วไปแล้วการ Hacking เป็นสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตามหากได้รับอนุญาตก็ไม่ใช่สิ่งผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบเพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

3.15 ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่หนัก

4. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์

เพื่อให้กรมโรงงานอุตสาหกรรม มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามที่ระบุในข้อ 3 กรมโรงงานอุตสาหกรรม จะดำเนินการเตรียมความพร้อมในด้านต่าง ๆ ดังนี้

4.1 การเตรียมพร้อมด้านอุปกรณ์

เพื่อให้ ระบบเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ กรมโรงงานอุตสาหกรรม จึงควรจัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็นดังนี้

4.1.1 อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DoS/DDoS BOTNET Phishing Sniffing Hacker ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหานอกจากความสามารถในการเป็น Firewall แล้วยังต้องมีความสามารถอื่น ๆ เพิ่มเติม ซึ่ง ได้แก่ความสามารถในด้านการตรวจจับการบุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซต์อันตราย (Web filtering) และ การควบคุมการใช้งานซอฟต์แวร์ (Application Control) เป็นอย่างน้อย

4.1.2 ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม

4.1.3 อุปกรณ์ web app firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่ เกิดขึ้นกับระบบงานคอมพิวเตอร์ของ กรมโรงงานอุตสาหกรรม ที่พัฒนาขึ้นมาให้บริการผ่าน web browser ได้แก่ การคุกคามทางไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุกเช่น Cross-site scripting และ sql injection ได้เป็นอย่างน้อย

4.1.4 ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และ การกู้ข้อมูล ของระบบเครือข่ายคอมพิวเตอร์ของ กรมโรงงานอุตสาหกรรม รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้

4.1.5 อุปกรณ์จัดเก็บข้อมูลภายนอก (SAN Storage) เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งระบบงานคอมพิวเตอร์ของ กรมโรงงานอุตสาหกรรม และในการรับมือทางไซเบอร์อุปกรณ์จัดเก็บข้อมูลภายนอกยังสามารถลดผลกระทบที่เกิดจาก Ransomware ได้โดย กรมโรงงานอุตสาหกรรม จะใช้อุปกรณ์จัดเก็บข้อมูลภายนอกดังกล่าวจัดทำพื้นที่ จัดเก็บข้อมูลส่วนกลาง โดยกำหนดให้แต่ละกองมีพื้นที่จัดเก็บข้อมูล ๕-0 GB และจะมีการสำรองข้อมูลจากพื้นที่จัดเก็บข้อมูลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากกองต่าง ๆ นำไฟล์สำคัญมาจัดเก็บเอาไว้ที่พื้นที่จัดเก็บข้อมูลส่วนกลางแล้วแม้ว่าจะเกิดภัยคุกคามไซเบอร์ประเภท Ransomware ก็จะสามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาได้

4.1.6 ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีที่ไม่สามารถกู้ระบบงานคอมพิวเตอร์ขึ้นมาได้

4.1.7 อุปกรณ์จัดเก็บ Log file ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม

4.1.8 อุปกรณ์วิเคราะห์ Log file ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม ซึ่งข้อมูลที่ถูกวิเคราะห์ดังกล่าวจะช่วยระบุถึงหมายเลข IP Address ของผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางของกรมโรงงานอุตสาหกรรม และใช้ประกอบการทำรายงานให้แก่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

4.1.9 ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่ายของ กรมโรงงานอุตสาหกรรม ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer worm, Trojan, Spyware, Ransomware, BOTNET, Spam Mail

4.2 แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา กรมโรงงานอุตสาหกรรม จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ 1 ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้ อาจสามารถดันหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได้

4.3 การเตรียมพร้อมด้านบุคลากร

4.3.1 การให้ความรู้

เพื่อให้บุคลากรของ กรมโรงงานอุตสาหกรรม มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ กรมโรงงานอุตสาหกรรม จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรของ กรมโรงงานอุตสาหกรรม

4.3.2 การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตาม พ.ร.บ.. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตราที่ 46 กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดย กรมโรงงานอุตสาหกรรม จะกำหนดระดับภัยคุกคามทางไซเบอร์ตาม พ.ร.บ.. กรรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตราที่ 60 และจะแจ้งรายชื่อ ผู้เจ้าหน้าที่เพื่อประสานงานด้านการรักษาความปลอดภัยไซเบอร์ในระดับต่าง ๆ

4.3.3 มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และ ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม

4.4 การเตรียมพร้อมต้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง

ในกรณีที่ภัยคุกคามทางไซเบอร์ ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางของกรมโรงงานอุตสาหกรรม อย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน กรมโรงงานอุตสาหกรรม จะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของ กรมโรงงานอุตสาหกรรม สามารถใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้แนวทางในการกู้คืนข้อมูล และ การใช้ระบบคอมพิวเตอร์สำรองจะกำหนดอยู่ในแอกสารแผนสำรองและกู้คืนระบบ ของกรมโรงงานอุตสาหกรรม

5. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์

ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ทั้งนี้ ทางกรมโรงงานอุตสาหกรรม ได้มีมาตรการสำหรับรับมือกับภัยคุกคามทางไซเบอร์ 3 มาตรการดังนี้

5.1 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) มีขั้นตอนดังนี้

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) คือการที่ต้องสร้างกลไกและกระบวนการเพื่อ

- ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของกรมโรงงานอุตสาหกรรม

- การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

- การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย หรือไม่

และดำเนินการทบทวนกลไก และกระบวนการอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่างๆ ยังคงมีประสิทธิภาพ

5.2 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) มี 3 ขั้นตอน ดังนี้

5.2.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

5.2.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

1) ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์

2) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีการดำเนินการต่อไปนี้

- จัดตั้งทีมสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต

- ระบุสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

- ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

- ระบุผู้แทนหน่วยงานหลักและผู้เชี่ยวชาญด้านเทคนิคที่ จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

- ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

3) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

4) ต้องตำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

5.2.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

1) กรมโรงงานอุตสาหกรรม ต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำ โดยคณะกรรมการการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติ หรือระดับภาคส่วน กรมโรงงานอุตสาหกรรม ต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้อง ที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วม ในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

2) ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการ เพื่อให้ข้อมูลที่ เกี่ยวข้องกับบริการที่สำคัญกรมโรงงานอุตสาหกรรม เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย

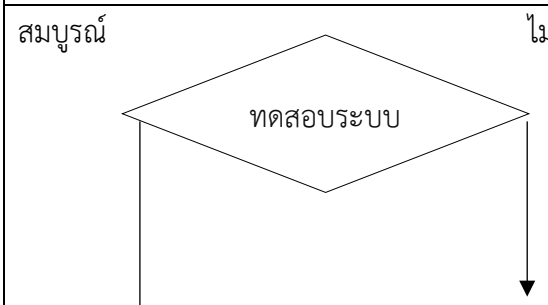
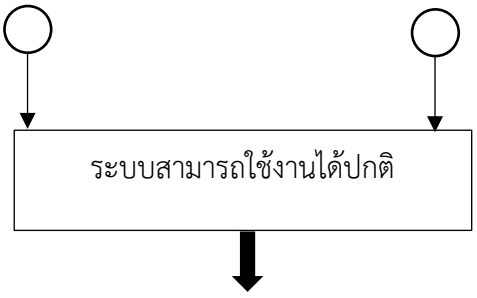
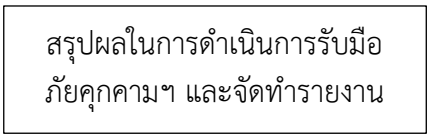
5.3 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

5.3.1 ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย สามารถให้บริการที่ จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

5.3.2 ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BPC อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

กรมโรงงานอุตสาหกรรม ได้จัดทำขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ซึ่งเป็นการดำเนินการเบื้องตัน ดังนี้

ขั้นตอน	รายละเอียด
ตรวจพบภัยคุกคามทางไซเบอร์	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทาง ไซเบอร์ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่าง ๆ ตามที่กำหนดในข้อ 3.1 ซึ่งจะช่วยให้กรมโรงงานอุตสาหกรรม สามารถตรวจพบการคุกคามทางไซเบอร์อย่างรวดเร็ว
ตรวจสอบภัยคุกคามทางไซเบอร์	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 62
การควบคุมภัยคุกคามทางไซเบอร์	ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุดและป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วนกรมโรงงานอุตสาหกรรม จะทำการ ปิดระบบ หรือ ตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว
แก้ได้ แก้ไขปัญหา แก้ไม่ได้	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นในทันที
ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ
แก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม	หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว กรมโรงงานอุตสาหกรรม จะดำเนินการตรวจหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่น ๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคาม ไซเบอร์ในลักษณะเดิม

ขั้นตอน	รายละเอียด
	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของกรมโรงงานอุตสาหกรรม ว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน
	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ กรมโรงงานอุตสาหกรรมจะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์สำรอง และ เร่งกู้ระบบงานคอมพิวเตอร์หลัก
	เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของ กรมโรงงานอุตสาหกรรม สามารถทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศของ กรมโรงงานอุตสาหกรรม จะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์
	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการกอง ผู้บริหารระดับสูงด้านสารสนเทศ

6. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของเจ้าหน้าที่กรมโรงงานอุตสาหกรรม

เมื่อเกิดการคุกคามทางไซเบอร์แล้ว ในบางครั้งผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ กรมโรงงานอุตสาหกรรม ทำงานผิดพลาดหรือล่าช้าลง หรือส่งผลให้ไฟล์ข้อมูลที่ถูกจัดเก็บเอาไว้ในเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้นเจ้าหน้าที่ของ สดช. ควรดำเนินการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ดังนี้

6.1 ดำเนินการตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

6.2 ดำเนินการตามนโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และ นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างเคร่งครัด

7. การประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
1. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)							
1) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	1. ระบบคอมพิวเตอร์และระบบเครือข่ายถูกทำลาย 2. ระบบสารสนเทศและระบบฐานข้อมูลถูกทำลาย	1	5	5	1. ตรวจสอบระบบดับเพลิงแบบอัตโนมัติตามมาตรฐานทุก 3 เดือน 2. ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก 3 เดือน	การควบคุม (Treat)	กลุ่มบริการระบบสารสนเทศ 2 ศส.
2) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	1. ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้ 2. ไม่สามารถระบบสารสนเทศและระบบฐานข้อมูลได้ 3. ระบบปฏิบัติการ และระบบฐานข้อมูลเกิดความเสียหายจากเครื่องไม่ได้ถูกทำการปิดอย่างเหมาะสม	1	4	4	1. ตรวจสอบระบบสำรองไฟฟ้า (UPS) ในศูนย์คอมพิวเตอร์แม่ข่ายกลาง ทุก 3 เดือน	การถ่ายโอน (Transfer)	กลุ่มบริการระบบสารสนเทศ 2 ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
3) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)	เกิดความเสียหายต่อเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย	1	4	4	ตรวจสอบเครื่องปรับอากาศที่ควบคุมอุณหภูมิ และความชื้น ทุก 3 เดือน	การถ่ายโอน (Transfer)	กลุ่มบริการระบบสารสนเทศ 2 ศส.
4) ความเสี่ยงจากแมลง สัตว์กัดแทะอุปกรณ์เครือข่ายและระบบไฟฟ้า	1. ไม่สามารถใช้งานระบบเครือข่ายได้ 2. ไม่สามารถให้บริการระบบเครือข่ายได้อย่างต่อเนื่อง	1	3	3	ตรวจสอบอุปกรณ์เครือข่ายและระบบไฟฟ้า ทุก 3 เดือน	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.
5) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง	1. อุปกรณ์ และข้อมูลที่มีความสำคัญสูญหาย 2. เสียภาพลักษณ์ของหน่วยงาน	1	3	3	1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า - ออกห้องคอมพิวเตอร์แม่ข่าย 2. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ๆ มี เครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้ง 3. ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก 3 เดือน	การยอมรับ (Take)	1. กลุ่มบริการระบบสารสนเทศ 2 2. กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
2. ความเสี่ยงด้านบุคลากร (Human Risk)							
6) ความเสี่ยงจากผู้ดูแลระบบ	ข้อมูลที่อยู่ในชั้นความลับ รั่วไหล ทำให้เสียหายต่อความน่าเชื่อถือของหน่วยงาน	1	3	3	1. การทำ Authentication การเข้าใช้ระบบสารสนเทศ รวมถึงการยกเลิกทะเบียน (เกษียณอายุ/ลาออก ฯลฯ) 2. การจัดระดับการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล	การยอมรับ (Take)	1. กลุ่มบริการระบบสารสนเทศกลาง ศส.
7) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย	1. สูญเสีย Bandwidth ในระบบเครือข่ายทำให้ต้องเพิ่ม Bandwidth ให้มากขึ้น เนื่องจากการใช้งานนอกเหนือจากงานราชการ 2. เครื่องคอมพิวเตอร์ เสียหายและเสื่อมอายุการใช้งานเร็วกว่าปกติ	2	3	6	1. กำหนด Policy ของ Firewall ให้เหมาะสมต่อการใช้งาน 2. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์หรือ Resources ไปใช้นอกเหนือจากงานราชการ และรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา 3. ตรวจสอบและแนะนำผู้ใช้งานให้ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอย่างเหมาะสม	การควบคุม (Treat)	1. กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
3. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)							
8) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1. เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล 2. ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	3	4	12	1. ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหลัก ทุกวัน 2. สำรองระบบและข้อมูล (Backup) ทุกวัน 3. ทดสอบการกู้คืนระบบแม่ข่ายหลัก เดือนละ 1 ครั้ง	การควบคุม (Treat)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.
9) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	1. โปรแกรมหรือข้อมูลถูกทำลาย 2. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3. การถูกขโมยข้อมูลที่สำคัญ	3	2	6	1. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ) 2. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งคัด	การควบคุม (Treat)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
10) ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	1.ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้ 2. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย 3. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของหน่วยงาน 4. ถูกโจรกรรมข้อมูลที่เป็นความลับ 5. ไม่สามารถเข้าใช้ระบบสารสนเทศได้	4	4	16	1. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ 2. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวังเครือข่าย ทุกวัน	การควบคุม (Treat)	1. กลุ่มบริการอุปกรณ์และระบบเครือข่าย 2. กลุ่มบริการระบบสารสนเทศกลาง ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
11) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน	1. ระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตไม่สามารถใช้งานได้ 2. ไม่สามารถเข้าใช้งานระบบสารสนเทศ ผ่านเครือข่ายอินทราเน็ต และอินเทอร์เน็ตได้	2	3	6	1. ตรวจสอบระบบเครือข่ายสื่อสารหลักทุกวัน 2. ควบคุมการเข้าใช้เครือข่ายอินทราเน็ต และอินเทอร์เน็ต โดยใช้ระบบยืนยันตน (Authentication)	การยอมรับ (Take)	1. กลุ่มบริการอุปกรณ์และระบบเครือข่าย 2. กลุ่มบริการระบบสารสนเทศกลาง ศส.
12) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)	1. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ 2. ลดความน่าเชื่อถือของหน่วยงาน	1	3	3	1. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ 2. ปรับปรุง Policy Firewall 3. Monitoring ระบบเครือข่าย เป็นประจำทุกวัน	การยอมรับ (Take)	1.กลุ่มบริการอุปกรณ์และระบบเครือข่าย 2.กลุ่มบริการระบบสารสนเทศกลาง ศส.
13) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ขัดข้อง ทำให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องไม่สามารถเข้าร่วมประชุมได้	1	3	3	ตรวจสอบการเชื่อมต่ออุปกรณ์ การทำงานของระบบชุดประชุมทางไกลผ่านเครือข่าย (VDO Conference) ก่อนใช้งาน	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
14) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)	1. ระบบโทรศัพท์ (IP Phone) ขัดข้อง ทำให้เจ้าหน้าที่ในหน่วยงานไม่สามารถใช้งานระบบโทรศัพท์ติดต่อประสานงานทั้งภายใน/ภายนอก ได้อย่างต่อเนื่อง	1	3	3	ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone) อย่างสม่ำเสมอ	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.
4. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)							
15) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	1. การถูกฟ้องร้อง และเสื่อมเสียชื่อเสียง และ ความน่าเชื่อถือของหน่วยงาน 2. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ 3. หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	1	3	3	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งาน Open Source	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.
16) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1. สร้างความเสียหายต่อระบบคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศและระบบฐานข้อมูล 2. ลดความน่าเชื่อถือต่อหน่วยงาน	1	3	3	1. อัพเดทเครื่องมือและโปรแกรมที่ใช้พัฒนาอย่างสม่ำเสมอ 2. ตรวจสอบช่องโหว่และดำเนินการแก้ไขทุก 3 เดือน	การยอมรับ (Take)	ศส. หรือ กลุ่ม/กองที่มีการพัฒนาโปรแกรม

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
17) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	1. ไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่ และแก้ไขการทำงานที่ผิดพลาดได้อย่างทันท่วงที 2. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว เนื่องจากโปรแกรมหมดลิขสิทธิ์ และขาดการปรับปรุง (Update) โปรแกรม	1	3	3	1. กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการวิเคราะห์ออกแบบการพัฒนาระบบและชุดคำสั่ง (Source Code) ฉบับสมสมบูรณ์ ทั้งในกรณีพัฒนาเสร็จสิ้น และเมื่อมีการปรับปรุงแก้ไข 2. ส่งมอบชุดคำสั่ง (Source Code) ชุดสมบูรณ์ 3. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ 4. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลให้มีความทันสมัยและใช้งานได้อย่างต่อเนื่อง	การควบคุม (Treat)	ศส. หรือกลุ่ม/กองที่มีการจัดจ้างผู้รับจ้างภายนอก

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับ ความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
5. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)							
18) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	1. ระบบฐานข้อมูลไม่สามารถนำไปใช้สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ 2. ลดความน่าเชื่อถือของหน่วยงาน	1	3	3	1. จัดทำรายการข้อมูลและความถี่ในการปรับปรุง 2. กำหนดมาตรการแนวทางการปรับปรุง และช่องทางการเข้าถึงข้อมูลเพื่อให้ผู้ดูแลข้อมูลถือปฏิบัติ	การยอมรับ (Take)	(ทุกกลุ่มที่ดูแลระบบงานต่างๆ) ศส.
19) ความเสี่ยงจากการไม่สำรองข้อมูลและไม่สามารถกู้คืนระบบฐานข้อมูล	1.เกิดการสูญหายของข้อมูล และกระทบต่อการทำงานตามปกติ 2.ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้สนับสนุนการปฏิบัติงานได้	1	3	3	1. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน 2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) ทุกสัปดาห์	การยอมรับ (Take)	(ทุกกลุ่มที่ดูแลระบบงานต่างๆ) ศส.
20) ความเสี่ยงจากการโจมตีระบบฐานข้อมูล	1.ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ 2. ข้อมูลที่สำคัญสูญหายและถูกทำลาย	1	4	4	1. ตรวจสอบระบบป้องกันการบุกรุกและระบบตรวจสอบและเฝ้าระวังเครือข่าย เป็นประจำทุกวัน 2. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกและระบบเฝ้าระวังเครือข่าย เป็นประจำทุกวัน	การยอมรับ (Take)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย ศส.