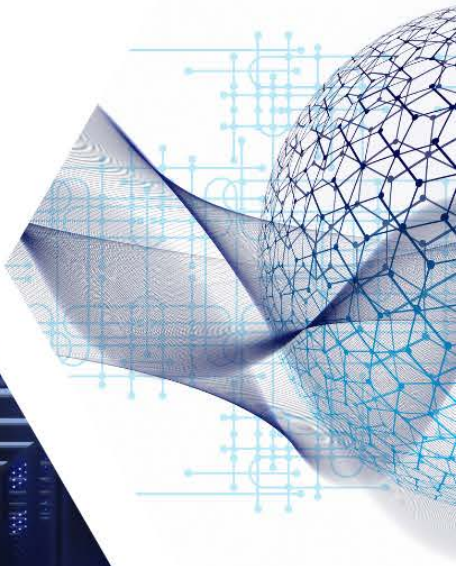
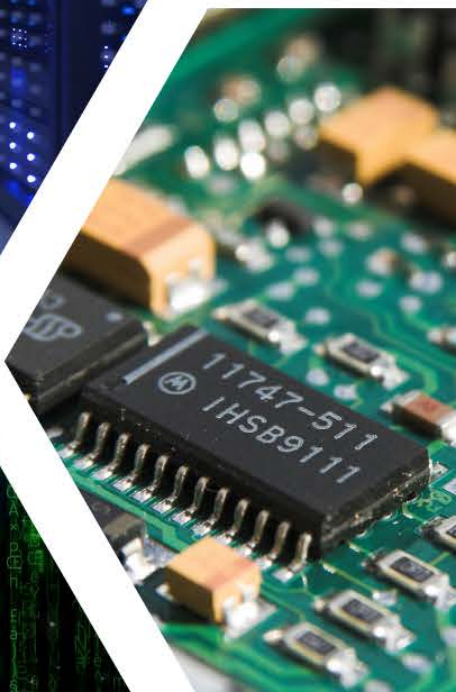
แผนรับมือภัยคุกคามทางไซเบอร์





กองสื่อสารและสารสนเทศ
สำนักงานสภาเกษตรกรแห่งชาติ

สารบัญ

แผนรับมือภัยคุกคามทางไซเบอร์ของสำนักงานสภาเกษตรกรแห่งชาติ

๑. หลักการและเหตุผล

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

๑. แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

๒. แผนรับมือภัยคุกคามทางไซเบอร์

เพื่อดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ สำนักงานสภาเกษตรกรแห่งชาติ (สกช.) จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่มาในรูปแบบไวรัสคอมพิวเตอร์ และ การโจมตีระบบ เครือข่ายคอมพิวเตอร์กลางของ สกช. โดยการดำเนินงานตามแผนจะมุ่งเน้นในการ ตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางให้สามารถใช้งานได้

๒. วัตถุประสงค์

๑. เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒. เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางของ สกช. ให้สามารถใช้งานได้

๓. เพื่อเตรียมความพร้อมด้านบุคลากรของ สกช. ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

๓. รูปแบบภัยคุกคามไซเบอร์

๓.๑ ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือที่เรียกโดยทั่วไปว่ามัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๓.๒ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่ง ที่สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหะ เช่น แฟลชไดร์ฟติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

๓.๓ หนอนคอมพิวเตอร์ (Computer worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัส ตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธี สแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของ แอพพลิเคชั่น จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

๓.๔ ม้าโทรจัน (Trojan horse) เป็นมัลแวร์ชนิดหนึ่ง ที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูล

ดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็น ชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคล อื่น ๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะ ซึ่งอาจมาจากแฟลชไดร์ฟ หรือทางอีเมล์

๓.๕ สปายแวร์(Spyware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บน เครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูลสถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

๓.๖ ซอฟต์แวร์เรียกค่าไถ่ (ransomware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีพฤติกรรมเข้ารหัสไฟล์ต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆได้เลยหาก ไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ

๓.๗ ประตูหลัง (Backdoor) เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบงานคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบงานคอมพิวเตอร์ในภายหลัง

๓.๘ Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบ คอมพิวเตอร์ ทั้งนี้ นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบ ระบบคอมพิวเตอร์ได้ด้วย

๓.๙ การโจมตีแบบ DoS/DDoS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุด ทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตี มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่ หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่า ๑ เครื่องและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่า การโจมตีแบบ Distributed Denial of Service (DDoS)

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

๓.๑๑ Spam Mail หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้า ไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti-spam หรือหากใช้ฟรีอีเมล์ ก็จะมีโปรแกรมคัดกรองอีเมล์ขยะ ในชั้นหนึ่งแล้ว

๓.๑๒ Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทาให้คุณต้องเข้าสู่ระบบและ ใส่ข้อมูลที่ สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

๓.๑๓ Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจาก เครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ผู้บุกรุกระบบนิยมใช้

๓.๑๔ Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัย โปรแกรมด้วยวัตถุประสงค์ต่างๆ กัน ทั้งนี้โดยทั่วไปแล้วการ Hacking เป็นสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตาม หากได้รับ

อนุญาตก็ไม่ใช่สิ่งผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบ เพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

๓.๑๕ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่างๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกคามที่หนัก

๔. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์

เพื่อให้ สกช. มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามที่ระบุในข้อ ๓ สกช. จะดำเนินการเตรียมความพร้อมในด้านต่างๆ ดังนี้

๔.๑ การเตรียมพร้อมด้านอุปกรณ์

เพื่อให้ ระบบเครือข่ายคอมพิวเตอร์กลางของ สกช. สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ สกช. จึงควรจัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็นดังนี้

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

๔.๑.๒ ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของ สกช. รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้ โดยดำเนินการเก็บข้อมูลไว้ที่ฐานข้อมูลของโครงการพัฒนาระบบคลาวด์กลางภาครัฐ (GDCC) ซึ่งมีความปลอดภัยสูงมาก

๔.๑.๓ ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์ แม่ข่าย ของ สกช. ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware ,Computer Virus ,Computer worm ,Trojan ,Spyware ,Ransomware ,BOTNET ,Spam Mail

๔.๒ แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของ สกช. สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มี การพัฒนาขึ้นตลอดเวลา สกช. จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความ มั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งในการ ตรวจสอบและประเมินความเสี่ยงนี้อาจสามารถค้นหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้ จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได้

๔.๓ การเตรียมพร้อมด้านบุคลากร

๔.๓.๑ การให้ความรู้เพื่อให้บุคลากรของ สกช. มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ สกช. จะพิจารณาจ้าง บริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรของ สกช.

๔.๓.๒ การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๔๖ กำหนดให้ หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดย สกช. จะกำหนดระดับภัยคุกคามทางไซเบอร์ตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๕๐ และจะแจ้งรายชื่อผู้เจ้าหน้าที่เพื่อประสานงานด้านการรักษาความปลอดภัยไซเบอร์ในระดับต่างๆ

๔.๓.๓ มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และ ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของ สกช. (ดูแลโดย GDCC)

๔.๔ การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรองในกรณีที่ภัยคุกคามทางไซเบอร์ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางของ สกช. อย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน สกช. จะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการ กู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ กลางของ สกช. สามารถใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้แนวทางในการกู้คืนข้อมูล และ การใช้ระบบ คอมพิวเตอร์สำรองจะกำหนดอยู่ในแอกสารแผนสำรองและกู้คืนระบบ ของ สกช.

๕. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์

ตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็วแต่เนื่องจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ยังไม่ได้ประกาศนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ในการนี้ สกช. จึงจัดทำขั้นตอนการปฏิบัติเมื่อเกิดภัย คุกคามทางไซเบอร์ซึ่งเป็นการดำเนินการเบื้องต้น และเมื่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกาศนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แล้ว สกช. จะดำเนินการปรับปรุงขั้นตอนการปฏิบัติให้สอดคล้องกับแผนดังกล่าว ทั้งนี้ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ของ สกช. มีขั้นตอนดังนี้

ลำดับ	ขั้นตอน	รายละเอียด
๑	ตรวจพบภัยคุกคามทางไซเบอร์	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอร์ได้ จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่างๆ ตามที่ กำหนดในข้อ ๓.๑ ซึ่งจะช่วยให้ สกช. สามารถตรวจพบการคุกคาม ทางไซเบอร์อย่างรวดเร็ว
๒	ตรวจสอบภัยคุกคามทางไซเบอร์	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัย คุกคามตามที่กำหนดใน พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๐
๓	การควบคุมภัยคุกคามทางไซเบอร์	ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่ เร่งด่วน สกช. จะทำการ ปิดระบบ หรือ ตัดการเชื่อมต่อของระบบ คอมพิวเตอร์ชั่วคราว
๔	แก้ได้ / แก้ไม่ได้ — แก้ไขปัญหา	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นในทันที
๕	ติดต่อศูนย์ประสานการรักษาความมั่นคง ปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อศูนย์ประสาน การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ
๖	แก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกัน การเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม	หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว สกช. จะดำเนินการแก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกัน ตรวจหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย หรือ การเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม เครื่องมืออื่น ๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ใน ลักษณะเดิม
๗	สมบูรณ์ / ไม่สมบูรณ์ — ทดสอบระบบ	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของ สกช. ว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน
๘	กู้คืนระบบ	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรอง และกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ สกช.จะพิจารณาเปิดใช้ ระบบงานคอมพิวเตอร์สำรอง และ เร่งกู้ระบบงานคอมพิวเตอร์หลัก
๙	ระบบสามารถใช้งานได้ตามปกติ	เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของ สกช. สามารถ ทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่าย ระบบสารสนเทศของ สกช. จะดำเนินการสรุปผลในการดำเนินการ รับมือภัยคุกคามไซเบอร์
๑๐	สรุปผลในการดำเนินการรับมือภัยคุกคามฯและจัดทำรายงาน	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการ ดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการกอง ผู้บริหารระดับสูงด้านสารสนเทศ

๖. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของเจ้าหน้าที่ สกช.

เมื่อเกิดการคุกคามทางไซเบอร์แล้ว ในบางครั้งผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ สกช. ทำงานผิดพลาดหรือล่าช้าลง หรือส่งผลให้ไฟล์ข้อมูลที่ถูกจัดเก็บเอาไว้ใน เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้นเจ้าหน้าที่ของ สกช. ควร ดำเนินการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ดังนี้

๖.๑ ดำเนินการตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

๖.๒ ดำเนินการตามนโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และ นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างเคร่งครัด โดยสำนักงาน สกช. จะดำเนินการสนับสนุนการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ของเจ้าหน้าที่ สกช. ดังนี้

๑) ดำเนินการจัดหาซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ให้เพียงพอต่อจำนวนเจ้าหน้าที่ของ สกช.

๒) ดำเนินการจัดเตรียมพื้นที่จัดเก็บข้อมูลส่วนกลาง โดยกำหนดให้แต่ละกองมีพื้นที่จัดเก็บข้อมูล ๕๐๐ GB และจะมีการสำรองข้อมูลจากพื้นที่จัดเก็บข้อมูลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากกองต่างๆ นำไฟล์ สำคัญมาจัดเก็บเอาไว้ที่พื้นที่จัดเก็บข้อมูลส่วนกลางแล้วแม้ว่าจะเกิดภัยคุกคาม ไซเบอร์ประเภท Ransomware ก็จะสามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาได้

****