กรมการปกครอง กระทรวงมหาดไทย

Department Of Provincial Administration

แผนรับมือภัยคุกคามทางไซเบอร์

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง

กรมการปกครอง

มิถุนายน 2567

สารบัญ

คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่อง ประมวลแนวทางปฏิบัติและกรอกมาตรฐานด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ ให้สามารถใช้งานได้

ศูนย์สารสนเทศเพื่อการบริหารงานปกครองจึงได้จัดทำ “แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมการปกครอง กระทรวงมหาดไทย” เพื่อใช้เป็นแผนในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญด้านบริการภาครัฐที่สำคัญ ของกรมการปกครองได้อย่างมีประสิทธิภาพและทันต่อเหตุการณ์

แผนรับมือภัยคุกคามทางไซเบอร์

กรมการปกครอง กระทรวงมหาดไทย

๑. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ **มาตรา ๔๔** กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและ กรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วย แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจ ประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ แผนรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กรมการปกครองจึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่มาในรูปแบบ ไวรัสคอมพิวเตอร์ และการโจมตีระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง โดยการดำเนินงานตามแผนจะมุ่งเน้นในการระบุภัยคุกคาม ตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศให้สามารถใช้งานได้

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากภัยคุกคามระบบสารสนเทศ

๒.๒ เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้การปฏิบัติราชการดำเนินไปได้อย่างมีเสถียรภาพ และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอน

๒.๔ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมการปกครอง

๒.๕ เพื่อป้องกันปัญหาการรั่วไหลของข้อมูลภายในของกรมการปกครองที่มีสาเหตุมาจากภัยคุกคามต่างๆ ที่เกิดขึ้น รวมถึงทำให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ๒๕๖๒ ในการป้องกันไม่ให้ข้อมูลส่วนบุคคลรั่วไหล และเกิดการเปลี่ยนแปลง แก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

๓. รูปแบบภัยคุกคามทางไซเบอร์

๓.๑ มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software หมายถึงซอฟต์แวร์ที่ประสงค์ร้ายต่อคอมพิวเตอร์และเครือข่าย โดยถูกสร้างมาให้บุคคลที่สามสามารถเข้าถึงข้อมูลที่สำคัญ หรือขัดขวางการทำงานบางอย่างของระบบการทำงานภายใน มีหลากหลายรูปแบบที่ต้องระมัดระวัง อาทิเช่น

- ไวรัส (Virus) มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์ และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ โดยไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น

- เวิร์ม (Worm) เป็นมัลแวร์ชนิดที่สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่ายได้ เช่น อีเมล การแชร์ไฟล์

- โทรจัน (Trojan) เป็นมัลแวร์ที่หลอกผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย ทำให้ผู้ใช้เผลอติดตั้ง นำมาสู่ความเสียหายในภายหลัง คล้ายกับกลยุทธ์การรบด้วยม้าโทรจัน ในมหากาพย์อีเลียดเรื่องสงครามเมืองทรอย

- แบคดอร์ (Backdoor) คือ การเปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว เหมือนการเปิดประตูหลังบ้านทิ้งไว้ให้โจร

- รูทคิท (Rootkit) คือการเปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

- สปายแวร์ (Spyware) เป็นมัลแวร์ที่ทำตัวเป็นสปาย แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน

๓.๒ แรนซัมแวร์ (Ransomware) คือ ภัยคุกคามทางไซเบอร์ที่ทำการเข้ารหัส หรือล็อกไฟล์ ไม่ให้ผู้ใช้สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความหาผู้ใช้หรือองค์กร เพื่อ "เรียกค่าไถ่ (Ransom)" แลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา มักพบเจอบ่อยในระดับองค์กร หรือหน่วยงานรัฐบาล

๓.๓ โจมตีแบบดักกลางทาง (Man-in-the-middle attack) คือ การที่บุคคลภายนอกปลอมเป็นคนกลางเข้ามาแทรกสัญญาณในระหว่างที่มีการแลกเปลี่ยนข้อมูลในเน็ตเวิร์ค การโจมตีในรูปแบบนี้มักถูกใช้เพื่อขโมยข้อมูลเกี่ยวกับการเงิน และข้อมูล Sensitive อื่น ๆ

๓.๔ ฟิชชิ่ง (Phishing) คือ ภัยคุกคามที่ใช้เทคนิคทางวิศวกรรมสังคม (Social engineering) ซึ่งคือการหลอกลวง ล่อหลอกผู้อื่น ใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล ตัวอย่างเช่นผู้โจมตีส่งอีเมลที่ดูน่าเชื่อถือให้ผู้ใช้งานกดคลิกลิงก์ และเข้าไปกรอกข้อมูลบัตรเครดิต หรือข้อมูล Sensitive อื่น ๆ ในหน้าเพจที่ทำปลอมขึ้นมาอย่างแนบเนียน หรือให้ผู้ใช้ดาวน์โหลดไฟล์ที่แนบมากับอีเมลแล้วติดตั้ง มัลแวร์ หรือ แรมซัมแวร์ ในคอมพิวเตอร์ขององค์กร เป็นต้น

๓.๕ Spam Mail หรืออีเมลขยะ เป็น e-mail ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ Anti-Spam หรือหากใช้ฟรีอีเมลก็จะมีโปรแกรมคัดกรองอีเมลขยะในชั้นหนึ่งแล้ว หรือใช้ฟรีอีเมลที่เป็นที่นิยมและมีการรักษาความปลอดภัยสูง เช่นHotmail Gmail หรือ Mailภาครัฐ (WorkD) เป็นต้น

๓.๖ การโจมตีโดยปฏิเสธการให้บริการ (Distributed Denial of Service: DDOS) คือ การที่แฮกเกอร์จะทำการส่ง Traffic หรือคำขอเข้าถึงข้อมูลจากอุปกรณ์จำนวนมาก และหลากหลายแหล่งที่มา ไปยังเว็บไซต์ที่ต้องการโจมตีพร้อม ๆ กัน ทำให้เว็บไซต์นั้นมีปริมาณ Traffic มากเกินกว่าที่เครื่องแม่ข่าย (Server) จะสามารถรองรับได้ ส่งผลให้เว็บไซต์ไม่สามารถใช้งานได้ หรือ เว็บไซต์ล่ม โดยแฮกเกอร์จะใช้ Robot Network ซึ่งคือเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่มีการติดตั้งมัลแวร์ที่เคยปล่อยไปตามช่องทางต่าง ๆ เช่น อีเมล เว็บไซต์ รวมถึงโซเชียลมีเดีย เมื่ออุปกรณ์เหล่านั้นติดมัลแวร์ จะทำให้แฮกเกอร์สามารถควบคุม หรือนำไปสร้างเส้นทาง (Traffic) เพื่อใช้โจมตีเว็บไซต์ต่าง ๆ จากระยะไกลได้

๓.๗ ภัยคุมคามจากภายใน (Insider threat) ภัยคุกคามชนิดนี้มีลักษณะตรงตามชื่อเรียก กล่าวคือเป็นภัยที่มาจากบุคคลภายในองค์กรที่ตั้งใจมุ่งประสงค์ร้ายต่อระบบความปลอดภัยขององค์กร โดยใช้อำนาจหน้าที่หรือสวมรอยอำนาจหน้าที่เพื่อเข้าถึงระบบคอมพิวเตอร์ และทำให้ระบบการป้องกันภัยคุกคามอ่อนแอลง

๓.๘ Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ผู้บุกรุกระบบนิยมใช้

๓.๙ Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่าง ๆ กัน ทั้งนี้โดยทั่วไปแล้วการ Hacking เป็นสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตามหากได้รับอนุญาตก็ไม่ใช่สิ่งผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบเพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายของหน่วยงาน

๓.๑๐ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่อาจมีผลกระทบรุนแรงต่อระบบงานบริการต่างๆ ได้

๔. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์

เพื่อให้กรมการปกครอง มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามที่ระบุในข้อ ๓ ข้างต้น กรมการปกครอง จะดำเนินการเตรียมความพร้อมในด้านต่าง ๆ ดังนี้

๔.๑ การเตรียมพร้อมด้านอุปกรณ์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ จึงควรจัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็นดังนี้

๔.๑.๑ อุปกรณ์ป้องกันระบบเครือข่าย (Firewall) เป็นซอฟต์แวร์หรือฮาร์ดแวร์ชนิดหนึ่ง ที่มีหน้าที่ตรวจสอบแพ็คเกจที่ผ่านเข้า-ออกระบบเครือข่าย คัดกรองข้อมูลที่เข้ามาว่าเป็นข้อมูลอะไร มาจากที่ไหน และจะส่งไปที่ใด เพื่อเป็นการป้องกันว่าข้อมูลที่จะส่งผ่านเข้ามานั้นมีความปลอดภัยหรือไม่ ด้วยการตั้งกฎ (Rule) หรือนโยบาย (Policy) ของผู้ดูแลระบบสารสนเทศ หากแพ็คเกจ (Package) ไม่ตรงตามกฎที่ตั้งไว้แม้เพียงข้อเดียว Firewall ก็จะไม่ให้ผ่าน Firewall เข้าไปได้

๔.๑.๒ ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง

๔.๑.๓ ซอฟต์แวร์ Web Application Firewall (WAF) เป็นซอฟต์แวร์หรือบริการสำหรับปกป้อง Web Application ที่เหนือชั้นกว่า Firewall ทั่วไป ด้วยความสามารถในการตรวจจับทุกกิจกรรมการใช้งาน Web Application ของ User ต่าง ๆ และป้องกันได้ทุกภัยคุกคามบน Web Application ที่ได้รับการจัดอันดับความร้ายแรง ๑๐ อันดับแรกใน OWASP Top ๑๐ เช่น Cross-site scripting และ SQL injection ได้

๔.๑.๔ ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และ การกู้ข้อมูล ของระบบสารสนเทศบนเครือข่ายคอมพิวเตอร์ของกรมการปกครอง รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้

๔.๑.๕ อุปกรณ์จัดเก็บข้อมูลภายนอก (SAN Storage) เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งระบบงานสารสนเทศของกรมการปกครอง และในการรับมือทางไซเบอร์อุปกรณ์จัดเก็บข้อมูลภายนอก ยังสามารถลดผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ได้ โดยกรมกรมการปกครองจะใช้อุปกร์จัดเก็บข้อมูลภายนอก (SAN Storage) ดังกล่าว จัดทำพื้นที่สำหรับจัดเก็บข้อมูลสารสนเทศในส่วนกลาง และจะมีการสำรองข้อมูลดังกล่าวอย่าง

สม่ำเสมอ เมื่อเกิดภัยคุกคามทางไซเบอร์ ก็จะสามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลสารสนเทศกลับมาได้

๔.๑.๖ อุปกรณ์จัดเก็บ Log file ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานระบบสารสนเทศบนเครืออข่ายคอมพิวเตอร์ของกรมการปกครอง

๔.๑.๗ อุปกรณ์วิเคราะห์ Log file ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานสารสนเทศบนเครือข่ายคอมพิวเตอร์ของกรมการปกครอง ซึ่งข้อมูลที่ถูกวิเคราะห์ดังกล่าวจะช่วยระบุถึงหมายเลข IP Address ของผู้โจมตี อุปกรณ์คอมพิวเตอร์ที่เป็นเป้าหมาย และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์ และใช้ประกอบการทำรายงานให้แก่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือหน่วยงานรัฐที่มีหน้าที่ตรวจสอบ Log file ได้

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

๔.๒ แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา กรมการปกครองได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศขึ้น และพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง

๔.๓ การเตรียมพร้อมด้านบุคลากร

๔.๓.๑ การให้ความรู้เพื่อให้บุคลากรของกรมการปกครองตระหนักถึงภัยคุกคามทางไซเบอร์ โดยจะต้องดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรภายในเพื่อลดความเสี่ยงจากภัยไซเบอร์

๔.๓.๒ การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๔๖ กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) โดยกรมการปกครองจะต้องแจ้งรายชื่อเจ้าหน้าที่เพื่อประสานงานด้านการรักษาความปลอดภัยไซเบอร์ในระดับต่าง ๆ ให้ทาง สกมช. ในการประสานงาน

๔.๓.๓ มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และ ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง

๔.๓.๔ การให้ความรู้ และฝึกอบรมเฉพาะทางด้านความปลอดภัยทางไซเบอร์ (Cyber Security) ให้กับบุคลากรที่ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และ ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง

๔.๔ การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์

ในกรณีที่ภัยคุกคามทางไซเบอร์ ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานอย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน กรมการปกครองจะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง สามารถใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้แนวทางในการสำรอง และกู้คืนข้อมูลจะกำหนดอยู่ในเอกสารแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการปกครอง

๕. แนวทางปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ทั้งนี้ทางกรมการปกครองได้ดำเนินการจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการปกครองขึ้นตามข้อกำหนด มาตรา ๔๔ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และได้มีมาตรการสำหรับรับมือกับภัยคุกคามทางไซเบอร์ตามกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity Framework สามารถจำแนกได้เป็น ๕ ด้าน ได้แก่ การระบุ (Identify), การป้องกัน (Protect), การตรวจสอบ (Detect), การตอบสนอง (Respond) และการคืนสภาพ (Recover) เพื่อช่วยในการบริหารความเสี่ยง และการบรรเทาผลกระทบของภัยคุกคาม

๕.๑ มาตรการระบุภัยคุกคามทางไซเบอร์ (Identify) มีขั้นตอนดังนี้

๕.๑.๑ การจัดการทรัพย์สิน (Asset Management)

- ต้องจัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และต้องทบทวนทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยมีรายละเอียดอย่างน้อยดังนี้ ชื่อ/คำอธิบายของทรัพย์สิน ฟังก์ชั่นที่สำคัญของทรัพย์สิน การระบุ และจัดความสำคัญของทรัพย์สิน
- ต้องมีการตรวจสอบ และปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง

๕.๑.๒ การประเมินความเสี่ยง

- ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง
- ต้องดำเนินการปรับปรุงทะเบียนความเสี่ยง โดยมีรายละเอียดอย่างน้อยดังนี้ วันที่ระบุความเสี่ยง คำอธิบายความเสี่ยง โอกาสที่จะเกิดได้ ความรุนแรง เจ้าของความเสี่ยง สถานะของการจัดการความเสี่ยง เป็นต้น

๕.๑.๓ การประเมินช่องโหว่ และการทดสอบเจาะระบบ (Vulnerability Assessment And Penetration Testing)

- ดำเนินการประเมินช่องโหว่ เพื่อประเมินช่องโหว่ของบริการที่สำคัญของกรมการปกครอง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย สำหรับการดำเนินการทดสอบระบบเก่า และระบบใหม่ใดๆ ที่เกี่ยวข้องกับบริการที่สำคัญ

- ดำเนินการเจาะระบบ (Penetration Testing) ของบริการที่สำคัญ รวมถึงเจาะระบบในส่วนของโฮสต์ เครือข่าย และระบบสารสนเทศของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง

- ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง

๕.๑.๔ การจัดการผู้ใช้ภายนอก (Third Party Management) ต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดความเสี่ยงที่เกี่ยวข้องในการเข้าถึง จัดเก็บ การสื่อสาร และการดำเนินการต่างๆ ของผู้ให้บริการภายนอก ในส่วนของข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดจะต้องคำนึงถึงรายละเอียดอย่างน้องดังนี้ ประเภทผู้ให้บริการภายนอกที่สามารถเข้าถึงทรัพย์สิน/บริการของกรมการปกครอง ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องข้อมูลที่เป็นของบริการสำคัญ และสิทธิ์ของหน่วยงานในการเข้าจรวจสอบความมั่นคงปลอดภัยของผู้ให้บริการภายนอก

๕.๒ มาตรการในการป้องกันความเสี่ยงที่เกิดขึ้น (Protect) ประกอบด้วย ๕ ขั้นตอน ดังนี้

๕.๒.๑ การควบคุมการเข้าถึง (Access Control) เพื่อตรวจสอบให้แน่ใจว่าการเข้าถึงระบบบริการที่สำคัญของกรมการปกครองถูกจำกัดเฉพาะ บุคลากรที่อนุญาต อุปกรณ์ที่ได้รับอนุญาต และมีการเก็บบันทึกการเข้า-ออกทั้งหมด

๕.๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) มีการกำหนดมาตรฐานกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับระบบปฏิบัติการ แอปพลิเคชั้น และอุปกรณ์เครือข่ายทั้งหมดที่เกี่ยวข้องกับงานบริการ โดยมาตรฐานกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยที่กรมการปกครองกำหนด มีรายการอย่างน้อยดังนี้ สิทธิ์ในการเข้าถึง การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน การลบบัญชีที่ไม่ได้ใช้งาน การลบหรือยกเลิกระบบสารสนเทศที่ไม่จำเป็น การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน การปรับปรุงแพตช์ (Patch) ของซอฟต์แวร์ให้มีความปลอดภัยของระบบอย่างเหมาะสม

๕.๒.๓ การเชื่อมต่อระยะไกล (Remote Connection) มีการตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังเครื่องแม่ข่ายงานบริการของกรมการปกครอง มีมาตรการรักษาความปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยมีแนวทางปฏิบัติดังนี้ เปิดการเชื่อมต่อที่จำเป็นเท่านั้น ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่าย เช่น Https , ssh และไม่เชื่อมต่อทางไกลจากซอฟท์แวร์ที่ไม่ได้รับอนุญาต

๕.๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removeable Storage Media) มีการตรวจสอบว่าการเชื่อต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับเครื่องแม่ข่ายของกรมการปกครองมีมาตรการอย่างน้อยดังนี้ มีการตรวจสอบสื่อบันทึกข้อมูลแบบถอดได้ทั้งหมดไม่มีมัลแวร์ก่อนการเชื่อมต่อเครื่องแม่ข่าย สื่อบันทึกข้อมูลแบบถอดได้ต้องได้รับอนุญาตจากกรมการปกครองเท่านั้น

๕.๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Awareness) มีการฝึกอบรมด้านตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับ ผู้บริหาร ข้าราชการ พนักงาน และลูกจ้างเป็นประจำอย่างน้อยปีละ ๑ ครั้ง

๕.๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) โดยกรมการปกครองดำเนินการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ด้วยการสร้างกลไกและกระบวนการในการ

- ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของกรมการปกครอง

- การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

- การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับงานบริการของกรมการปกครอง หรือไม่ และดำเนินการทบทวนกลไก และกระบวนการอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่างๆ ยังคงมีประสิทธิภาพ

๕.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) มีดังนี้

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

๕.๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีการดำเนินการดังนี้

- ระบุสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

- ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

- ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต และดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง

๕.๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) โดยกรมการปกครองต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำ โดยคณะกรรมการการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว และอาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน กรมการปกครองต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกข้อมความมั่นคงปลอดภัยไซเบอ์ดังกล่าว และต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการฯ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญกรมการปกครอง เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการของกรมการปกครอง

๕.๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

๕.๕.๑ ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมการปกครอง สามารถให้บริการที่ จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะที่สำคัญ Maximum

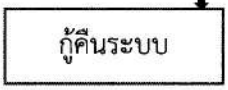
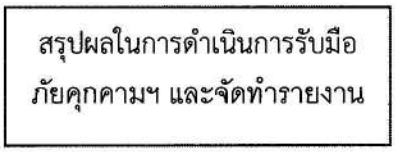
Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๕.๕.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BPC อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕.๕.๓ กำหนดขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแนวทางปฏิบัติสำรองและกู้คืนข้อมูล

กรมการปกครอง ได้จัดทำขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ซึ่งเป็นการดำเนินการเบื้องต้น ดังนี้

ขั้นตอน	รายละเอียด
ตรวจพบภัยคุกคามทางไซเบอร์	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอร์ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่าง ๆ ตามที่กำหนดในข้อ ๔.๑ ซึ่งจะช่วยให้กรมการปกครองสามารถตรวจพบการคุกคามทางไซเบอร์อย่างรวดเร็ว
ตรวจสอบภัยคุกคามทางไซเบอร์	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๒
การควบคุมภัยคุกคามทางไซเบอร์	ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุดและป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วนกรมการปกครองจะทำการปิดระบบ หรือการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว
แก้ไขปัญหา แก้ได้ / แก้ไม่ได้	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นทันที และทำการทดสอบการใช้งานระบบงานหรือแอปพลิเคชันก่อนเปิดให้บริการ
ประสานสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.)	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ
แก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม	หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว กรมการปกครองจะดำเนินการตรวจหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่น ๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคามทางไซเบอร์ในลักษณะเดิม

ขั้นตอน	รายละเอียด
	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมการปกครอง ว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน
	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ กรมการปกครองจะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์สำรอง และ เร่งกู้ระบบงานคอมพิวเตอร์หลัก
	เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมการปกครอง สามารถทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศของกรมการปกครอง จะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์
	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการศูนย์สารสนเทศเพื่อการบริหารงานปกครอง ผู้บริหารระดับสูงด้านสารสนเทศ

๖. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของเจ้าหน้าที่กรมการปกครอง

เมื่อเกิดการคุกคามทางไซเบอร์แล้ว ในบางครั้งผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ของเจ้าหน้าที่กรมการปกครอง ทำงานผิดพลาดหรือล่าช้าลง หรือส่งผลให้ไฟล์ข้อมูลที่ถูกจัดเก็บเอาไว้ในเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้นเจ้าหน้าที่ของกรมการปกครองควรดำเนินการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ดังนี้

๖.๑ ดำเนินการตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการปกครองสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด ในเรื่องแนวทางปฏิบัติของผู้ใช้บริการ เพื่อให้ผู้ใช้บริการมีความรู้ในการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายอย่างปลอดภัย และปฏิบัติตามอย่างเคร่งครัด

๖.๒ ต้องดำเนินการปรับปรุงซอฟท์แวร์ต่างๆ บนเครื่องคอมพิวเตอร์ส่วนบุคคล และ เครื่องคอมพิวเตอร์แบบพกพา เช่น ระบบปฏิบัติการ ซอฟท์แวร์ Antivirus และ ซอฟท์แวร์ที่เกี่ยวข้องในการปฏิบัติงานต่างๆ ให้มีความปลอดภัยใช้งานอย่างสม่ำเสมอ

๗. การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้ง การใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง นอกจากนี้ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี เมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

หลักการบริหารจัดการหลักฐานทางดิจิทัลที่สำคัญมีดังนี้

รายการ	คำอธิบาย
การประเมินหลักฐาน (Assessment)	การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของภัยคุกคามที่กำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device หรือ Network Connection เป็นต้น
การได้มาซึ่งข้อมูล (Acquisition)	ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication / Bit-for-bit Copy) โดยให้ตรงกับต้นฉบับทุกประการด้วยเครื่องมือที่เหมาะสมโดย ๑. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้เทคโนโลยี Write Blocker เพื่อป้องกันการเปลี่ยนแปลงของหลักฐาน หรือเขียนทับข้อมูลดิจิทัลต้นฉบับ ๒. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับต้นๆ ๓. ต้องบันทึกกิจกรรมในการทำสำเนาหลักฐานพร้อมภาพถ่ายอย่างละเอียด ทั้งก่อน ระหว่าง และหลังการจัดเก็บหลักฐาน ๔. ต้องทำการบันทึกหลักฐาน ว่าหลักฐานมีการถูกเข้าถึงโดยใครเมื่อไหร่อย่างไร ด้วยเหตุผลอะไร
การรับรองความถูกต้อง (Authentication)	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD๕, SHA๑, SHA๒๕๖ , CRC-๓๒ ของหลักฐานทั้งสองชุดแล้วนำมาเปรียบเทียบกัน
การจัดเก็บหลักฐานทางดิจิทัล (Archive)	จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึกขั้นตอนการเก็บหลักฐาน การควบคุมการเข้าถึง การส่งต่อ-รับมอบ ในกรณีที่มีการปฏิบัติงานร่วมกับหน่วยงานอื่น ไปจนถึงการทำลายหลักฐาน โดยในทุกขั้นตอนต้องมีการบันทึกการดำเนินงานอย่างละเอียด และมีการลงชื่อผู้รับผิดชอบเพื่อเป็นหลักฐาน
การวิเคราะห์และรายงานผล (Analysis & Report)	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิดภัยคุกคาม และจัดทำรายงานเพื่อนำเสนอผลต่อผู้ที่มีส่วนได้ส่วนเสียในกรณีนั้น ๆ