แผนรับมือภัยคุกคามทางไซเบอร์กรมกิจการเด็กและเยาวชน

กองยุทธศาสตร์และแผนงาน กรมกิจการเด็กและเยาวชน ๒๕๖๖

คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอกมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้

กลุ่มสารสนเทศและเทคโนโลยีจึงได้จัดทำ “แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมกิจการเด็กและเยาวชน” เพื่อใช้เป็นแผนในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญด้านเด็กและเยาวชนของกรมกิจการเด็กและเยาวชน (ดย.) ได้อย่างเป็นระบบ มีประสิทธิภาพและทันต่อเหตุการณ์

กองยุทธศาสตร์และแผนงาน
กรมกิจการเด็กและเยาวชน
กันยายน ๒๕๖๖

สารบัญ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมกิจการเด็กและเยาวชน

๑. หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอกมาตรฐานด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วยแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พรบ. การรักษาความ มั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกันและแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ ให้สามารถใช้งานได้

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากภัยคุกคามระบบสารสนเทศ

๒.๒ เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้การปฏิบัติราชการดำเนินไปได้อย่างมีเสถียรภาพ

๒.๔ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมกิจการเด็กและเยาวชน

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของกรมกิจการเด็กและเยาวชนรวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

กลุ่มสารสนเทศและเทคโนโลยีมีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึงคณะทำงานการรักษาความมั่นคงปลอดภัยไซเบอร์กรมกิจการเด็กและเยาวชน

๕. หน้าที่ในการดำเนินการตามแผน

กลุ่มสารสนเทศและเทคโนโลยีมีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย

๑. กองส่งเสริมการพัฒนาและสวัสดิการเด็ก เยาวชน และครอบครัว

๒. กองคุ้มครองเด็กและเยาวชน

๓. สำนักงานเลขานุการกรม

๔. ศูนย์อำนวยการรับเด็กเป็นบุตรบุญธรรม

๕. กองยุทธศาสตร์และแผนงาน

๖. กลุ่มตรวจสอบภายในและกลุ่มพัฒนาระบบบริหาร

๗. ศูนย์ส่งเสริมจริยธรรมและต่อต้านการทุจริต

๖. ความเกี่ยวข้องกับเอกสารอื่น

๖.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ กรมกิจการเด็กและเยาวชน

๖.๒ นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล กรมกิจกิจการเด็กและเยาวชน

๖.๓ ประกาศกรมกิจการเด็กและเยาวชนเรื่องยโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓

๖.๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมกิจการเด็กและเยาวชน พ.ศ. ๒๕๖๔

๗. นิยาม

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

กรมกิจการเด็กและเยาวชนใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	นางสาวดรุณี พจนานุกูลกิจ โทร. ๐ ๒๖๕๑ ๖๘๘๔ (๒๖๒)	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	นายนิรุตต์ รุ่งแจ้ง โทร. ๐ ๒๖๕๑ ๖๘๘๔ (๑๕๖)	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	นายสุธี วังเกล็ดแก้ว โทร. ๐ ๒๖๕๑ ๖๘๘๔ (๒๔๒)	เจ้าหน้าที่รับมือฯ (Incident lead)	ทำหน้าที่ดูแลระบบสารสนเทศกรมกิจการเด็กและเยาวชนให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้

๔	นายสมศักดิ์ หนองจิก โทร. ๐ ๒๖๕๑ ๖๘๘๔ (๒๔๒)	เจ้าหน้าที่รับมือฯ (Incident lead)	ทำหน้าที่ดูแลระบบสารสนเทศกรมกิจการเด็กและเยาวชนให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
๕	นายกอบชัย ตงลิ้ม โทร. ๐ ๒๖๕๑ ๖๘๘๔ (๒๔๒)	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับที่	ชื่อ นามสกุล	หน้าที่	ความรับผิดชอบ
๑	นายชูเกียรติ์ ตั้งกิจไพศาล โทร. ๐๘ ๑๘๐๑ ๒๕๑๘	ผู้ดูแลระบบสารสนเทศกรมกิจการเด็กและเยาวชน	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ และรายงานผล
๒	นางสาวจุไรรัตน์ รุ่งเรือง โทร. ๐ ๒๖๕๑ ๖๘๘๔ (๒๗๕)	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล กรมกิจกิจการเด็กและเยาวชน
๓	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน) โทร. ๐๘ ๑๘๐๑ ๒๕๑๘	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ กรมกิจการเด็กและเยาวชน
๔	นายณรงศักดิ์ ทองสุข โทร. ๐ ๒๖๕๑ ๖๙๗๔ (๒๗๑)	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ตามคำสั่งแต่งตั้งคณะทำงานการรักษาความมั่นคงปลอดภัยไซเบอร์กรมกิจการเด็กและเยาวชน
๕	นางเรณู บุญวัฒน์พุฒิ โทร. ๐ ๒๖๕๑ ๖๘๘๔ (๑๕๖)	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล กรมกิจกิจการเด็กและเยาวชน
๖	นายโอภาส ภูครองนาค โทร. ๐ ๒๒๕๐ ๑๙๔๘ (๑๗๐)	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตาม แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมกิจการเด็กและเยาวชน พ.ศ. ๒๕๖๔

๙. รูปแบบภัยคุกคามไซเบอร์

๙.๑ Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูล ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการ ผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus) เวิร์ม (worms) โทรจัน (Trojans)

๙.๒ Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไข เว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๙.๓ Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๙.๔ Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์และ Web Server หรือ Database Server

๙.๕ Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

๙.๖ DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๙.๗ Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูล ของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบ ไม่ทราบ ซึ่งผู้โจมตีต้องการน าข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

๙.๘ Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

๙.๙ Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัว อยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๙.๑๐ Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

๙.๑๑ Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

๙.๑๒ ผู้บุกรุก (Hacker) ผู้ที่ไม่ได้รับอนุญาตในหารใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหาย จากผู้บุกรุกเป็นภัยคุกคามที่หนัก

๑๐. ขั้นตอนการรับมือ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมกิจการเด็กและเยาวชน ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของ

รัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึง นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์กรมกิจการเด็กและเยาวชน ดังนี้

๑๐.๑ ขั้นการเตรียมการ

เพื่อให้กรมกิจการเด็กและเยาวชน (ดย.) มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามที่ระบุในข้อ ๙ ดย. จึงได้ดำเนินการเตรียมความพร้อม ดังนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๘

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายละเอียดตามข้อ ๖

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) เพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) ดังนี้

ระดับ	แนวปฏิบัติ
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับวิกฤติ	๑. การเตรียมความพร้อมด้านอุปกรณ์ ๑.๑ อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท Dos/DDos BOTNET Phishing Hackers ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหานอกจากความสามารถในการเป็น Firewall แล้วยังต้องมีความสามารถอื่น ๆ เพิ่มเติม ได้แก่ ความสามารถในการตรวจจับผู้บุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซต์อันตราย (Web Filtering) และการควบคุมการใช้งานซอฟต์แวร์ (Application Control) ๑.๒ ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของ ดย. ๑.๓ อุปกรณ์ web app firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ของ ดย. ที่พัฒนาขึ้นมาให้บริการผ่าน web browser ได้แก่ การคุกคามทางไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุกเช่น Cross-site scripting และ sql injection ได้ ๑.๔ ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และการกู้ข้อมูลของระบบเครือข่ายคอมพิวเตอร์ของ ดย. รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้

ระดับ	แนวปฏิบัติ
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับวิกฤติ	๑.๕ อุปกรณ์จัดเก็บข้อมูลภายนอก (SAN Storage) เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งระบบงานคอมพิวเตอร์ของ ดย. และในการรับมือทางไซเบอร์อุปกรณ์จัดเก็บข้อมูลภายนอกยังสามารถลดผลกระทบที่เกิดจาก Ransomware โดย ดย. จะใช้อุปกรณ์จัดเก็บข้อมูลภายนอกดังกล่าวจัดทำพื้นที่จัดเก็บข้อมูลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากกองต่าง ๆ นำไฟล์สำคัญมาจัดเก็บเอาไว้ที่พื้นที่จัดเก็บข้อมูลส่วนกลางแม่ว่าจะเกิดภัยคุกคามไซเบอร์ประเภท Ransomware ก็สามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาได้ ๑.๖ ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีไม่สามารภกู้ระบบงานคอมพิวเตอร์ขึ้นมาได้ ๑.๗ อุปกรณ์จัดเก็บ Log file ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของ ดย. ๑.๘ อุปกรณ์วิเคราะห์ Log file ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ที่เกิดจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของ ดย. ซึ่งข้อมูลที่ถูกวิเคราะห์ดังกล่าวจะช่วยระบุถึงหมายเลข IP Address ของผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางของ ดย. และใช้ประกอบการทำรายงานให้แก้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ๑.๙ ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่ายของ ดย. ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer worm, Trojan, Ransomware, BOTNET และ Spam Mail ๒. แผนการตรวจสอบการประเมินความเสี่ยงด้านการักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของ ดย. สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา ดย. จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้ อาจสามารถค้นหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได้๓. การเตรียมพร้อมด้านบุคลากร ๓.๑ การให้ความรู้ เพื่อให้บุคลากรของ ดย. มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ดย. จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรของ ดย.

ระดับ	แนวปฏิบัติ
	๓.๒ มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของ ดย. ๔. การเตรียมความพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง ในกรณีภัยคุกคามทางไซเบอร์ ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางของ ดย. อย่างมากจนไม่สามารภทำงานได้เป็นเวลานาน ดย. จะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบคอมพิวเตอร์กลางของ ดย. สามารถใช้งานได้อย่างรวดเร็วที่สุด

๑๐.๒ ดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยกรมกิจการเด็กและเยาวชน ได้ดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ดังนี้

ระดับ	แนวปฏิบัติ
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	๑. กำหนดช่องทางที่จะใช้ในการตรวจจับความผิดปกติได้อย่างเหมาะสมกับสภาพแวดล้อมที่ดูแล โดยสามารถพิจารณา “การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident” ๒. ดำเนินการวิเคราะห์ Incident ได้อย่างรวดเร็วและเหมาะสม ๓. การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident การตรวจจับ Incidentจะขึ้นอยู่กับระบบที่ใช้งานอยู่และรูปแบบของความพยายามในการโจมตีประกอบกับกลไกต่าง ๆ ที่ทำการปกป้องระบบอยู่ เพราะโดยทั่วไประบบการป้องกันจะทำการแจ้งเตือน (Alert) หรือ เก็บบันทึกข้อมูล (Log) เพื่อ ใช้ในการวิเคราะห์หาความผิดปกติด้วย โดยลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น 2 ประเภท • **Precursor** เป็นข้อมูลที่บ่งบอกว่า Incident จะเกิดขึ้นในอนาคต • **Indicator** เป็นข้อมูลที่บ่งบอกว่า Incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่ ซึ่งการเลือกใช้อุปกรณ์ป้องกันและตรวจจับ นอกจากจะต้องพิจารณาความเหมาะสมกับระบบที่ต้องการจะ ป้องกันแล้ว ควรต้องมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ เป็นสำคัญ และถูกต้องมากยิ่งขึ้น ซึ่งเทคนิคในการวิเคราะห์เหตุภัยคุกคามเมื่อได้รับแจ้งมีดังต่อไปนี้

ระดับ	แนวปฏิบัติ
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	๔. การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติควรมีความถูกต้องแม่นยำและประสิทธิภาพ เพื่อให้การ ดำเนินการในขั้นตอนต่อไปสามารถดำเนินการได้เร็ว ๔.๑ **Profiling (Baselining) Networks and Systems & Understand Normal Behavior** ข้อมูลสถานะการทำงาน การตั้งค่า และการใช้งานปกติของระบบจะทำให้ทราบ ได้เร็วขึ้นเมื่อมีพฤติกรรมผิดปกติเกิดขึ้นในระบบ ๔.๒ **Log Retention Policy Log** จากอุปกรณ์ต่าง ๆ เช่น IPDS, Workstation, Servers, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และ บันทึกเหตุการณ์เก็บไว้เพื่อหลักฐานทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมี การเก็บรักษาและป้องกันอย่างดี รวมถึงเก็บไว้เป็นระยะเวลาที่เหมาะสม ตอบ โจทย์ในด้านของการตอบสนองและเป็นไปตามกฎหมายข้อบังคับ ๔.๓ **Perform Event Correlation** การโจมตีโดยทั่วไปมักจะมีเส้นทางการเข้าถึงระบบเป้าหมายที่ผ่านอุปกรณ์ต่าง ๆ บนเครือข่าย ดังนั้นการวิเคราะห์ก็จำเป็นที่จะต้องใช้ข้อมูลจากทุกอุปกรณ์ที่คาดว่า จะเกี่ยวข้องร่วมกัน (Correlation) เพื่อให้เห็นถึงเส้นทางการโจมตี และสาเหตุที่ แท้จริงที่ทำให้การบุกรุกประสบผลสำเร็จ ๔.๔ **Clock Synchronization** อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ตรงกันอยู่เสมอ ไม่เช่นนั้นแล้วการ Correlate Event จะทำได้ยากหรือไม่สามารถทำได้ ๔.๕ **Sniff and Analyze Network Data** ในหลาย ๆ กรณีการดักจับข้อมูลทางเครือข่ายขณะเกิดเหตุเพื่อนำมาร่วมการ วิเคราะห์สามารถที่จะให้ข้อมูลเบาะแสที่สำคัญได้ ๔.๖ **Seek Assistance** เมื่อใดที่ทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ Incident เพื่อหาสาเหตุที่ แท้จริงเพื่อกำจัดผู้บุรุกออกจากระบบได้ ก็สามารถใช้บริการให้คำแนะนำปรึกษา จากภายนอกตามสมควรได้ เช่น CERT ต่าง ๆ หรือบริการจากที่ปรึกษาภายนอก เป็นต้น ๕. การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม ดย. มีการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม ซึ่งจะช่วยให้การ รับมือและตอบสนองภัยคุกคามมีประสิทธิภาพและเป็นระบบมากขึ้น โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้น ตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคาม ซึ่งการบันทึกข้อมูลอาจจัดเก็บในโปรแกรมประยุกต์หรือฐานข้อมูล เช่น ระบบติดตามปัญหา (Issues Tracking System) เพื่อประโยชน์ในการติดตามเหตุการณ์

ระดับ	แนวปฏิบัติ
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ขั้นตอนการจัดการ และแก้ไขเหตุ ภัยคุกคามเพื่อให้มั่นใจได้ว่าเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม ๖. การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์ เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่อย่างจำกัดของหน่วยงานและลดผลกระทบทางธุรกิจให้น้อยลงที่สุด ๗. การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์ เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่อย่างจำกัดของบริษัท และ ลดผลกระทบทางธุรกิจให้น้อยลงที่สุด ๘. กรมกิจการเด็กและเยาวชนสามารถพิจารณาปัจจัยในเรื่องดังต่อไปนี้ประกอบการพิจารณาเพื่อกำหนด แนวทางในการติดต่อประสานงานและแจ้งข้อมูลให้กับผู้ที่เกี่ยวข้อง • เป็นผู้ได้รับผลกระทบจาก Incident • เป็นผู้ที่มีหน้าที่ตัดสินใจในการดำเนินการที่เกี่ยวข้องกับ Incident • เป็นผู้ที่มีหน้าที่รับผิดชอบกำหนดในนโยบายและแผน • เป็นผู้ที่มีหน้าที่รับผิดชอบตามที่กฎหมายกำหนด **การแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์แก่ผู้ที่เกี่ยวข้อง** บุคลากรหรือหน่วยงานที่ควรได้รับการ แจ้งเหตุภัยคุกคาม มีดังต่อไปนี้ • ผู้บริหาร (Top Management) • ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) • ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (CISO) หรือ หัวหน้าหน่วยงานการรักษาความ มั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (Head of Information Security) • ทีมรับมือและตอบสนองต่อเหตุการณ์อื่น ๆ ของ ดย. • ทีมรับมือและตอบสนองต่อเหตุการณ์ภายนอกบริษัท (ตามความเหมาะสม) • เจ้าของระบบงาน (System Owner) • ฝ่ายทรัพยากรบุคคล (Human Resources) • ฝ่ายสื่อสารองค์กร (สำหรับเหตุการณ์ที่จำเป็นต้องให้การประชาสัมพันธ์) • ฝ่ายกฎหมาย (สำหรับเหตุการณ์ที่อาจมีข้อเกี่ยวข้องทางกฎหมาย)

ระดับ	แนวปฏิบัติ
	• ทีมบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Team) • ทีมรับมือและตอบสนองต่อเหตุการณ์วิกฤต (Crisis Management Team) • หน่วยงานกำกับ (Regulators) / ทีม TI-CERT • หน่วยงาน CERT (Computer Emergency Response Team) • หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง (Law Enforcer)

๑๐.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เป็นการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าวควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น เพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

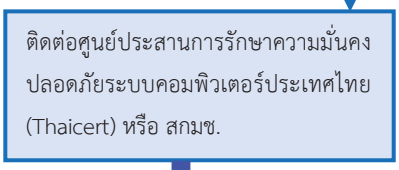
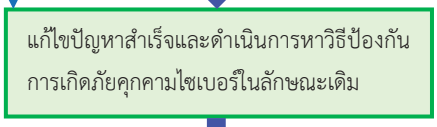
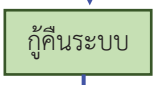
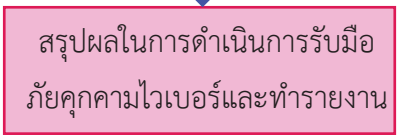
(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

(๖) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ทั้งนี้ ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ของ ดย. มีขั้นตอนดังนี้

ขั้นตอน	รายละเอียด
	มีการแจ้งเหตุจากผู้ใช้งานหรือตรวจจับการคุกคามทางไซเบอร์ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่าง ๆ ตามที่กำหนดในข้อ ๑๐.๑ ซึ่งจะช่วยให้ ดย. สามารถตรวจพบภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว
	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๐
	ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วน ดย. จะดำเนินการปิดระบบ หรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว
	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์เบื้อต้นในทันที
	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อข้อคำแนะนำหรือขอความช่วยเหลือ
	หลังจากการแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว ดย. จะดำเนินการตรวจหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่น ๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม
	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของ ดย. ว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน
	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบบในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ ดย. จะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์สำรอง และเร่งกู้ระบบงานคอมพิวเตอร์หลัก
	เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ ดย. สามารภทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศของ ดย. จะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์
	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการกอง ผู้บริหารระดับสูงด้านสารสนเทศ

๙.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์(Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวของเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ตอไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง นอกจากนี้ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกขหรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปใน ระหว่างที่ตองระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตีเมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคาม ทางไซเบอร์โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะ ดังกล่าวขึ้นอีกในอนาคต

หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมี ดังนี้

๑. Assessment	การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลัง รับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น
๒. Acquisition	ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้ ๑. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker ๒. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของ หลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก ๓. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด ๔. ต้องทำการบันทึกหลักฐาน (Chain of Custody)
๓. Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับ ต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD๕, SHA๑, SHA๒๕๖
๔. Analysis & Report	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือ เพื่อค้นหาสาเหตุของการเกิด Incident
๕. Archive	จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย

กรมกิจการเด็กและเยาวชน
Department of Children and Youth