แผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)
กรมกิจการสตรีและสถาบันครอบครัว

คำนำ

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้น เพื่อให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอกมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ ให้สามารถได้

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ ประกอบด้วย การวิเคราะห์ความเสี่ยงการระบุภัยคุกคาม การวางมาตรการป้องกัน และการกำหนดขั้นตอนในการตอบสนองต่อเหตุการณ์ ซึ่งการดำเนินงานตามแผนดังกล่าวจะช่วยเสริมสร้างความปลอดภัยในระบบสารสนเทศ ลดความเสี่ยงที่อาจเกิดขึ้น และสร้างความมั่นใจให้กับบุคลากรและผู้เกี่ยวข้องทุกฝ่าย

กลุ่มเทคโนโลยีสารสนเทศ
กองยุทธศาสตร์และแผนงาน
กรมกิจการสตรีและสถาบันครอบครัว

สารบัญ

๑.หลักการและเหตุผล

การจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมกิจการสตรีและสถาบันครอบครัวมีวัตถุประสงค์หลักเพื่อปฏิบัติตามข้อกำหนดของมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งระบุให้หน่วยงานของรัฐต้องจัดทำแผนการรับมือที่สอดคล้องกับนโยบายและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันและจัดการกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ การจัดทำแผนนี้จะช่วยให้กรมกิจการสตรีและสถาบันครอบครัวสามารถเตรียมความพร้อมและรับมือกับเหตุการณ์ทางไซเบอร์ได้อย่างทันท่วงที

การมีแผนรับมือภัยคุกคามทางไซเบอร์จะเสริมสร้างความมั่นคงให้กับระบบสารสนเทศของหน่วยงาน โดยกำหนดแนวทางการป้องกัน การตรวจสอบ และการตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้น นอกจากนี้ยังช่วยลดความเสี่ยงในการสูญเสียข้อมูลสำคัญและการทำลายระบบ ซึ่งเป็นผลดีต่อการให้บริการและสร้างความเชื่อมั่นให้กับประชาชนและผู้ใช้บริการ

การดำเนินการตามแผนนี้จะช่วยให้กรมกิจการสตรีและสถาบันครอบครัวปฏิบัติตามข้อกำหนดทางกฎหมายอย่างครบถ้วน และยังเป็นการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ภายในองค์กร การฝึกฝนและเตรียมความพร้อมของบุคลากรจะช่วยให้เจ้าหน้าที่มีทักษะและความรู้ในการจัดการกับเหตุการณ์ทางไซเบอร์อย่างมีประสิทธิภาพ ส่งผลให้การดำเนินงานของหน่วยงานเป็นไปตามมาตรฐานที่กำหนดและมีประสิทธิภาพสูงสุด

๒.วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในกรมกิจการสตรีและสถาบันครอบครัว โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใต้กรมกิจการสตรีและสถาบันครอบครัว การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของกรมกิจการสตรีและสถาบันครอบครัว

๓. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ใช้สำหรับการจัดการและรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบสารสนเทศและข้อมูลดิจิทัลของกรมกิจการสตรีและสถาบันครอบครัว รวมถึงการคุ้มครองและการตอบสนองต่อภัยคุกคามที่เกิดจากบุคคลหรืออุปกรณ์ใด ๆ ที่มีการเข้าถึงระบบสารสนเทศและข้อมูลดิจิทัลของหน่วยงาน โดยมีขอบเขตครอบคลุม ดังนี้

(๑) การจัดการภัยคุกคามที่เกิดขึ้นกับระบบสารสนเทศต่าง ๆ ที่ใช้ในการดำเนินงานของกรม เช่น ระบบฐานข้อมูล การจัดการเอกสารอิเล็กทรอนิกส์ และระบบเครือข่ายภายใน

(๒) การปกป้องข้อมูลดิจิทัลที่จัดเก็บและใช้ภายในกรม รวมถึงการรักษาความปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลที่เกี่ยวข้องกับการให้บริการประชาชน

(๓) การควบคุมและการรับมือกับภัยคุกคามที่มาจากบุคคลภายในหรือภายนอกที่มีการเข้าถึงระบบสารสนเทศของกรม รวมถึงอุปกรณ์ที่เชื่อมต่อกับระบบสารสนเทศ

ซึ่งการจัดทำแผนนี้จะช่วยให้หน่วยงานสามารถเตรียมความพร้อมและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ลดความเสี่ยงที่อาจเกิดขึ้นต่อการดำเนินงานและข้อมูลสำคัญของหน่วยงาน ทั้งนี้ แผนรับมือเหตุภัยคุกคามทางไซเบอร์ต้องได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตามที่เห็นสมควร

๔. หน้าที่การทบทวนแผน

กองยุทธศาสตร์และแผนงาน กรมกิจการสตรีและสถาบันครอบครัว มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึงผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)

๕. หน้าที่ในการดำเนินการตามแผน

กรมกิจการสตรีและสถาบันครอบครัว มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย กองยุทธศาสตร์และแผนงาน รวมถึง กลุ่มเทคโนโลยีและสารสนเทศ และหน่วยงานภายในกรม ดังนี้ สำนักงานเลขานุการกรม กองส่งเสริมความเสมอภาคระหว่างเพศ กองส่งเสริมสถาบันครอบครัว กองคุ้มครองและพัฒนาอาชีพ กลุ่มพัฒนาระบบบริหาร ศูนย์ส่งเสริมจริยธรรมและต่อต้านการทุจริต กลุ่มตรวจสอบภายใน ศูนย์เรียนรู้การพัฒนาสตรีและครอบครัว ทั้ง ๘ แห่ง และสถานคุ้มครองและพัฒนาอาชีพ ทั้ง ๔ แห่ง

๖. รายละเอียดการบังคับใช้เอกสาร

๖.๑. รายละเอียดการอนุมัติเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	
ชื่อ นางสาวชุตินันท์ พุ่มกลิ่น ตำแหน่ง ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ วันที่	ลงชื่อ ..... (นางสาวชุตินันท์ พุ่มกลิ่น)
ผู้ดำเนินการตามเอกสาร (Owner)	
หน่วยงานภายใต้สังกัดกรมกิจการสตรีและสถาบันครอบครัว	
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	
ชื่อ นางสาวอมรรัตน์ ศรีฉ่ำ ตำแหน่ง ผู้อำนวยการกองยุทธศาสตร์และแผนงาน วันที่	ลงชื่อ ..... (นางสาวอมรรัตน์ ศรีฉ่ำ)
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	
ชื่อ นางจตุพร โรจนพานิช ตำแหน่ง อธิบดีกรมกิจการสตรีและสถาบันครอบครัว วันที่	ลงชื่อ ..... (นางจตุพร โรจนพานิช)
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	

๖.๒. การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
๑.๐			

๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๗.๑ ประมวลแนวทางปฏิบัติ ตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมกิจการสตรีและสถาบันครอบครัว พ.ศ. ๒๕๖๙

๗.๒ นโยบายการคุ้มครองข้อมูลส่วนบุคคล

๗.๓ นโยบายการบริหารจัดการข้อมูลของหน่วยงาน

๗.๔ พระราชบัญญัติข้อมูลว่าด้วยการกระทำความผิดคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๗.๕ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และที่แก้ไขเพิ่มเติม

๗.๖ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๗.๗ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๗.๘ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

๘. นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (Observable occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

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

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ[๑] หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หมายถึง การกระทำโดยมิชอบที่มีผลต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ โดยทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์แล้วแต่กรณี เสียหาย ถูกทำลาย ด้อยประสิทธิภาพหรือไม่สามารถนำมาใช้งานได้และให้หมายความรวมถึงการกระทำอื่นใดที่มีผลในทำนองเดียวกัน

การประทุษร้ายต่อข้อมูล หมายถึง การกระทำโดยมิชอบที่มีผลเป็นการเปลี่ยนแปลงข้อมูล ทำลายข้อมูล ขโมยข้อมูล นำข้อมูลไปใช้โดยไม่ได้รับอนุญาต หรือจำกัดมิให้ผู้เป็นเจ้าของหรือผู้ครอบครองข้อมูลเข้าถึงข้อมูลของตนได้ และให้หมายความรวมถึงการกระทำอื่นใดที่มีผลในทำนองเดียวกัน

---

[๑] เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ มีนิยามตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖

๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

๙.๑. ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ลำดับ	ชื่อ – นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายปิยวุฒิ กษิดิศ (หลัก)	โทร: ๐ ๒๖๕๙ ๖๗๘๙ Email: ict@dwf.go.th	- รับแจ้งเหตุ - คัดกรองและประเมินเหตุการณ์เบื้องต้น - ประสานงานกับหน่วยงานที่เกี่ยวข้อง	- รับแจ้ง และตอบกลับภายในระยะเวลาที่กำหนด - บันทึก และประเมินเหตุ - ดำเนินการเบื้องต้น และแจ้งผู้เกี่ยวข้อง - ติดตามสถานการณ์ - รักษาความลับของข้อมูล
๒	นายปรัชญา ดุลลาดิน (หลัก)	โทร: ๐ ๒๖๕๙ ๖๗๘๙ Email: ict@dwf.go.th	- เฝ้าระวัง ดูแลระบบ - รับแจ้งเหตุ - ประสานงาน	- รับแจ้ง และตอบกลับภายในระยะเวลาที่กำหนด - บันทึก และประเมินเหตุ - ดำเนินการเบื้องต้น และแจ้งผู้เกี่ยวข้อง - ติดตามสถานการณ์ - รักษาความลับของข้อมูล
๓	นายคฤหาสน์ ยงเพชร (รอง)	โทร: ๐ ๒๖๕๙ ๖๗๘๙ Email: ict@dwf.go.th	- รับแจ้งเหตุ และสนับสนุน - ประสานงาน และติดตามสถานการณ์	- ติดตามสถานการณ์ร่วม - สนับสนุนการวิเคราะห์ - จัดทำข้อมูลการทำรายงาน - รักษาความลับของข้อมูล

๙.๒. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

กรมกิจการสตรีและสถาบันครอบครัว ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ (Centralize) โดยหน่วยงานภายใต้กรมกิจการสตรีและสถาบันครอบครัวระบุรายชื่อของกอง กลุ่ม ที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	ผู้บริหารเทคโนโลยีสารสนเทศ (DCIO)	โทร: ๐ ๒๖๕๙ ๖๗๘๙ Email: suda.su@dwf.go.th	หัวหน้าทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
			(Team Manager)	
๒	ผู้อำนวยการกองยุทธศาสตร์และแผนงาน	โทร: ๐ ๒๖๕๙ ๖๗๘๒ Email: tarnroma๑๙@gmail.com	หัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่ หรือไม่สามารถปฏิบัติงานได้
๓	ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ	โทร: ๐ ๒๖๕๙ ๖๗๘๙ Email: c_phoomglin@dwf.go.th	ทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Incident Lead)	ช่วยเหลือ ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ เสนอแนะแนวทางควบคุม และรายงานผล
๔	เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ นายปิยวุฒิ กษิดิศ	โทร: ๐ ๒๖๕๙ ๖๗๘๙ Email: piyawut.ka@dwf.go.th	ทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ด้านเทคนิค (Technical Lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๕	เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ	โทร: ๐ ๒๖๕๙ ๖๗๘๙ Email: ict@dwf.go.th	ทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ด้านเทคนิค (Technical Lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	ผู้อำนวยการกลุ่มกฎหมาย	โทร: ๐ ๒๖๕๙ ๖๗๖๖ Email: Law@dwf.go.th	บริหารจัดการด้านกฎหมายของหน่วยงาน	ทำหน้าที่ควบคุม ดูแล และดำเนินการเกี่ยวกับคดี/ฟ้องร้องที่เกิดขึ้นกับหน่วยงาน
๒	เจ้าหน้าที่กลุ่มกฎหมาย	โทร: ๐ ๒๖๕๙ ๖๗๖๗ Email: Law@dwf.go.th	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ดำเนินการจัดทำข้อมูล/ชี้แจงรายละเอียดข้อเท็จจริงตามเหตุละเมิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ และ พ.ร.บ.

				ความมั่นคงปลอดภัยทางไซเบอร์ฯ
๓	สกมช.	โทร: ๐ ๒๑๑๔ ๓๕๓๑ Email: saraban@ncsa.or.th	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ทดสอบเจาะระบบสารสนเทศของหน่วยงาน พร้อมเสนอแนะแนวทางแก้ไขช่องโหว่ที่ตรวจพบ
๔	ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร	โทร: ๐ ๒๖๕๙ ๖๗๓๔ Email: kaporo ๘๗๗๖@dwf.go.th	บริหารจัดการความเสี่ยง	ทำหน้าที่ดูแลการบริหารจัดการความเสี่ยงให้สอดรับตามนโยบายความมั่นคงปลอดภัยฯ
๕	ผู้อำนวยการกลุ่มสื่อสารองค์กร	โทร: ๐ ๒๖๕๙ ๖๗๗๕ Email: pr.dwf ๑๒๓@gmail.com	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ประชาสัมพันธ์การดำเนินการตามแผน
๖	เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ	โทร: ๐ ๒๖๕๙ ๖๗๙๐ Email: ict@dwf.go.th	ผู้ประสานงาน	ทำหน้าที่ประสานงานในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

๙.๓. หน่วยงานภายนอกที่เกี่ยวข้อง

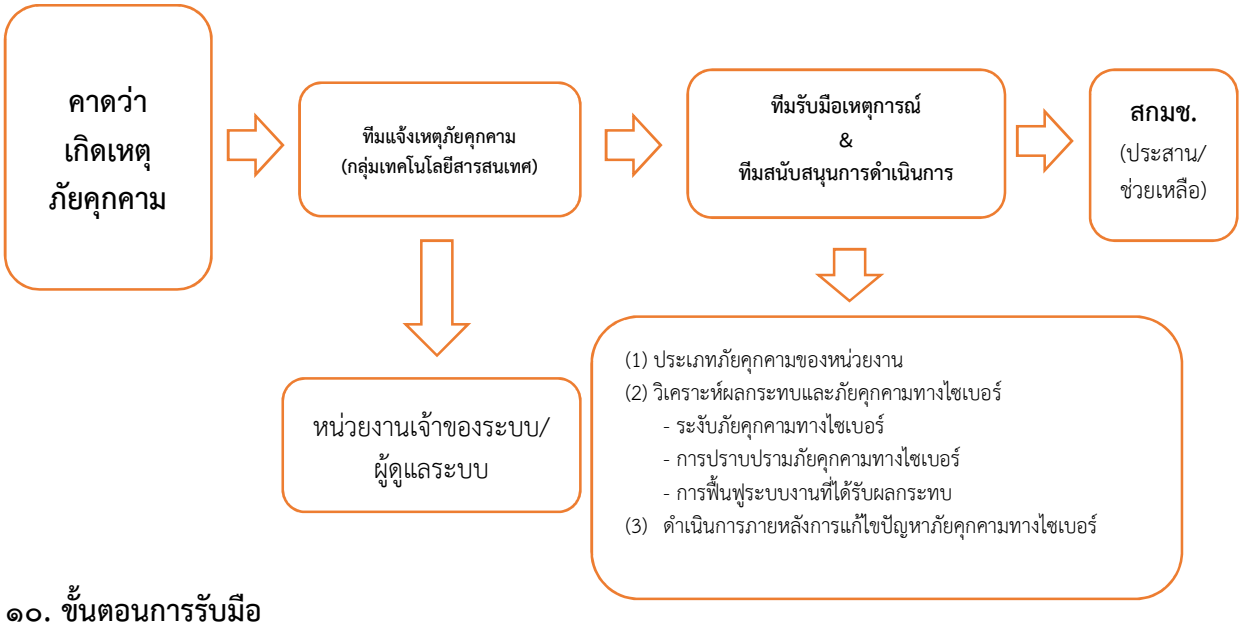
ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	NCSA	โทร: ๐ ๒๑๔๒ ๖๘๘๘ Email : cii@ncsa.or.th	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	แจ้งเหตุภัยคุกคามทางไซเบอร์ ประสานการปฏิบัติงานในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง เพื่อป้องกันและรับมือกับภัยคุกคามทางไซเบอร์

๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป. พม	โทร: ๐ ๒๒๐๒ ๙๐๑๐ Email: ictc@m-society.go.th Line : @๗๓๓aprjl	กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์	หน่วยงานกำกับดูแล
๓	ThaiCERT	โทร: ๐ ๒๒๐๒ ๙๐๑๐ Email: thaicert@ncsa.or.th	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ Thailand Computer Emergency Response Team (ThaiCERT)	เป็นหน่วยงานเฝ้าระวังติดตาม และเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์
๔	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	โทร: ๐ ๒๑๑๑ ๘๘๐๐ Email: saraban@pdpc.or.th	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุละเมิดข้อมูลส่วนบุคคล
๕	บริษัทคู่สัญญาดูแลบำรุงรักษาระบบสารสนเทศ	โทร: ๐ ๒๖๕๒ ๕๔๔๕ Email: info@gmail.gbtech.co.th	บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด	ทำหน้าที่ดูแลและบำรุงรักษาระบบสารสนเทศ
๖	บริษัทคู่สัญญาดูแลบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย ลูกข่าย อุปกรณ์ต่อพ่วง และระบบเครือข่ายสำนักงาน	โทร: ๐ ๒๗๕๓ ๔๒๙๑ Email: opentech.ti@gmail.com	บริษัท โอเพ่น เทคโนโลยี่ จำกัด (มหาชน)	ทำหน้าที่ดูแลและบำรุงรักษาคอมพิวเตอร์ อุปกรณ์ต่อพ่วง และระบบเครือข่าย
๗	บริษัท Data Center	โทร: ๐๙๕ ๒๘๙ ๕๔๙๔ Email: kridtiyak@sitem.co.th	บริษัท ไซเท็ม คอร์ปอเรชั่น จำกัด	ดูแลบำรุงรักษา
๘	บริษัทคู่สัญญาอินเตอร์เน็ต	โทร: ๐๙๕ ๒๘๙ ๕๔๙๔ Email: kridtiyak@sitem.co.th	บริษัท ไซเท็ม คอร์ปอเรชั่น จำกัด	ให้บริการเครือข่ายอินเตอร์เน็ต

๙.๔. โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

เพื่อให้การดำเนินการรับมือเหตุภัยคุกคามทางไซเบอร์ สามารถนำไปปฏิบัติงานได้อย่างมีประสิทธิภาพ กรมกิจการสตรีและสถาบันครอบครัว จึงจัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัย

ไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก รวมถึงกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



๑๐. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ รวมถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ดังนี้

๑๐.๑ ขั้นตอนการเตรียมการ (Preparation)

หน่วยงานจะต้องดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัยการจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ ๙.๒

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ ๙.๔

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และการติดต่อไปยังหน่วยงาน CIRT ต่าง ๆ

(๔) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์, ห้องประชุม War room เป็นต้น

(๕) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของกรมกิจการสตรีและสถาบันครอบครัว (รายละเอียดปรากฏตามภาคผนวก ๑)

นอกจากนี้ กรมกิจการสตรีและสถาบันครอบครัว จะพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๒ ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

กรมกิจการสตรีและสถาบันครอบครัว ดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(๑) กรมกิจการสตรีและสถาบันครอบครัวดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น ดังนี้

ประเภท	คำอธิบาย	วิธีการรับมือ
Malicious Code (โปรแกรมไม่พึงประสงค์)	มัลแวร์ (Malware), Virus, Worm, Trojan, Ransomware และ Spyware ต่าง ๆ ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์	- การใช้ซอฟต์แวร์ป้องกัน: ติดตั้งและอัปเดตโปรแกรมแอนติไวรัสและมัลแวร์ที่เชื่อถือได้เพื่อป้องกันการติดเชื้อ - การสำรองข้อมูล: สำรองข้อมูลสำคัญอย่างสม่ำเสมอและเก็บในที่ปลอดภัย เช่น คลาวด์หรือสื่อเก็บข้อมูลภายนอก - การอัปเดตซอฟต์แวร์: อัปเดตระบบปฏิบัติการและซอฟต์แวร์ทั้งหมดให้ทันสมัยเพื่อปิดช่องโหว่ - การระมัดระวังในการดาวน์โหลด: ดาวน์โหลดซอฟต์แวร์และไฟล์จากแหล่งที่เชื่อถือได้เท่านั้น และหลีกเลี่ยงการเปิดไฟล์แนบที่ไม่ได้รับการตรวจสอบ
Intrusion Attempts, Intrusions (ความพยายามบุกรุกเข้าระบบ)	Login Attempt, Connection Attempt, Brute-force เป็นการดำเนินการเพื่อจะควบคุมหรือทำให้	- การใช้การตรวจสอบตัวตนหลายปัจจัย (MFA): เพิ่มระดับความปลอดภัยโดยการใช้การตรวจสอบตัวตนหลายปัจจัย

ประเภท	คำอธิบาย	วิธีการรับมือ
	เกิดความขัดข้องกับบริการของระบบ	- การตั้งค่าความปลอดภัยของบัญชี: จำกัดจำนวนความพยายามในการเข้าสู่ระบบและตั้งค่าการล็อกบัญชีหลังจากพยายามล้มเหลวหลายครั้ง - การใช้ระบบตรวจจับการบุกรุก (IDS): ติดตั้ง IDS เพื่อตรวจจับและแจ้งเตือนเกี่ยวกับกิจกรรมที่ผิดปกติ - การบันทึกและตรวจสอบ: บันทึกกิจกรรมการเข้าสู่ระบบและตรวจสอบบันทึกเพื่อระบุพฤติกรรมที่ผิดปกติ
Availability (ความพร้อมใช้ของระบบ)	การถูกโจมตีความพร้อมใช้งานของระบบ เช่น DDoS (Denial of Service), Open DNS Resolver, Flood ทำให้เกิดความล่าช้าในการบริการ จนถึงทำให้ระบบไม่สามารถทำงานได้	- การใช้บริการป้องกัน DDoS: ใช้บริการป้องกัน DDoS จากผู้ให้บริการที่เชี่ยวชาญในการจัดการการโจมตี - การปรับขนาดทรัพยากร: เตรียมระบบให้สามารถปรับขนาดตามปริมาณการร้องขอ เช่น การใช้คลาวด์ที่สามารถปรับขนาดอัตโนมัติ - การใช้ Open DNS Resolver: ตั้งค่าคอนฟิก DNS เพื่อป้องกันการใช้งานเป็น Open DNS Resolver - การเฝ้าระวัง: ติดตั้งระบบเฝ้าระวังเพื่อตรวจสอบและตอบสนองต่อการโจมตี
Phishing (การหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้ซึ่งข้อมูล)	การถูกสร้างหน้าเว็บไซต์ปลอม (Web Phishing) หรือหลอกลวงเพื่อให้ได้ข้อมูลผ่านทางอีเมล	- การฝึกอบรม: ให้การฝึกอบรมเกี่ยวกับการระบุฟิชชิ่งและหลีกเลี่ยงการเปิดเผยข้อมูลส่วนตัว - การใช้ฟิลเตอร์อีเมล: ใช้ฟิลเตอร์อีเมลเพื่อกรองและตรวจจับอีเมลฟิชชิ่ง - การตรวจสอบเว็บไซต์: ตรวจสอบ URL ของเว็บไซต์ที่ให้ข้อมูลและตรวจสอบความปลอดภัยของเว็บไซต์ที่เข้าถึง

ประเภท	คำอธิบาย	วิธีการรับมือ
		- การใช้การตรวจสอบความปลอดภัยของเว็บไซต์: ใช้เทคโนโลยีการเข้ารหัสข้อมูล เช่น HTTPS เพื่อปกป้องข้อมูลที่ส่ง
Web Defacement	การถูกปรับเปลี่ยนหน้าเว็บไซต์	- การอัปเดตและแพตช์: อัปเดตระบบจัดการเนื้อหา (CMS) และปลั๊กอินเป็นประจำเพื่อป้องกันช่องโหว่ - การควบคุมการเข้าถึง: จำกัดสิทธิ์การเข้าถึงเนื้อหาเว็บไซต์ให้เฉพาะผู้ที่ได้รับอนุญาต - การตรวจสอบความปลอดภัย: ใช้เครื่องมือสแกนความปลอดภัยเพื่อค้นหาช่องโหว่และปรับปรุง - การสำรองข้อมูล: สำรองข้อมูลของเว็บไซต์และฐานข้อมูลเพื่อให้สามารถกู้คืนได้ในกรณีที่เกิดการถูกปรับเปลี่ยน
SEO attack	เว็บไซต์ถูกโจมตี ด้วยการฝังสคริปต์โฆษณาเว็บไซต์ การพนันออนไลน์	- การตรวจสอบเว็บไซต์: ตรวจสอบเว็บไซต์เป็นประจำเพื่อค้นหาและลบสคริปต์ที่ไม่พึงประสงค์ - การใช้เครื่องมือ SEO: ใช้เครื่องมือ SEO ที่เชื่อถือได้เพื่อตรวจสอบการเปลี่ยนแปลงและป้องกันการโจมตี - การอัปเดตซอฟต์แวร์:อัปเดตระบบจัดการเว็บไซต์และปลั๊กอินเพื่อป้องกันช่องโหว่
Cross-site scripting (XSS)	การโจมตีที่ผู้ไม่ประสงค์ดีแทรกโค้ด JavaScript หรือสคริปต์อื่นๆ เข้าไปในเว็บแอปพลิเคชัน (เช่น จากช่องค้นหา หรือแบบฟอร์ม) เพื่อทำให้สคริปต์นั้นทำงานในเบราว์เซอร์ของผู้ใช้งานคนอื่น เพื่อขโมยข้อมูลส่วนตัว การปลอมแปลงเนื้อหาหน้าเว็บ หรือแม้กระทั่งการดำเนินการอื่น ๆ ในนามของผู้ใช้	- ข้อมูลที่ป้อนเข้ามาควรถูกตรวจสอบอย่างเข้มงวดทันที โดยพิจารณาจากประเภทของเนื้อหา ตัวอย่างเช่น ชื่อส่วนตัวควรประกอบด้วยตัวอักษร มีความยาวไม่มาก ปีเกิดควรประกอบด้วยตัวเลขสี่หลักเท่านั้น ที่อยู่อีเมลควรตรงกับนิยามของ regular expression ที่กำหนดไว้ ข้อมูลที่ไม่ผ่านการตรวจสอบควรถูกปฏิเสธ ไม่ใช่การตรวจสอบและแก้ไขข้อมูล

ประเภท	คำอธิบาย	วิธีการรับมือ
		- ข้อมูลที่ผู้ใช้ป้อนควรเข้ารหัส HTML ทุกครั้งที่มันถูกคัดลอกเข้าไปในการตอบกลับของแอปพลิเคชัน อักขระพิเศษของ HTML ทั้งหมด รวมถึง < > " ' และ = ควรถูกแทนที่ด้วย HTML entity ที่สอดคล้องกัน (< > ฯลฯ) - ตรวจสอบโค้ดอย่างสม่ำเสมอด้วย Security Scanner - อัปเดต Libraries และ Dependencies ให้เป็นเวอร์ชันล่าสุด - ทดสอบความปลอดภัยของแอปพลิเคชันอย่างสม่ำเสมอ - ใช้ HTTPS เพื่อป้องกันการดักจับข้อมูล
Vulnerability	ช่องโหว่ของระบบหรือจุดอ่อนของระบบบริหารจัดการเว็บไซต์	- การจัดการช่องโหว่: ทำการสแกนช่องโหว่และแก้ไขช่องโหว่ที่พบเป็นประจำ - การอัปเดตซอฟต์แวร์: อัปเดตระบบและซอฟต์แวร์ให้ทันสมัยเพื่อลดช่องโหว่ที่รู้จัก - การทดสอบการเจาะระบบ (Penetration Testing): ทำการทดสอบการเจาะระบบเพื่อค้นหาช่องโหว่ที่อาจถูกโจมตี
Abuse	การละเมิดการใช้งานเครือข่าย เช่น Spam, Copyright	- การใช้ฟิลเตอร์สแปม: ใช้ฟิลเตอร์สแปมเพื่อป้องกันการส่งอีเมลที่ไม่พึงประสงค์ - การติดตามและตรวจสอบ: ติดตามการใช้งานเครือข่ายและตรวจสอบการละเมิดลิขสิทธิ์ - การปฏิบัติตามนโยบาย: พัฒนานโยบายการใช้งานเครือข่ายที่ชัดเจนและบังคับใช้อย่างเคร่งครัด

(๒) กรมกิจการสตรีและสถาบันครอบต้องจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น

(๒.๑) เครื่องมือและอุปกรณ์เฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน ประกอบด้วย

- Firewall ระบบรักษาความปลอดภัยไซเบอร์ของเครือข่ายคอมพิวเตอร์ที่สามารถควบคุมคัดกรองข้อมูลที่รับส่งข้อมูลได้

- Web Application Firewall (WAF) ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอปพลิเคชันโดยเฉพาะ เพื่อป้องกันการโจมตีไปยังระบบเว็บแอปพลิเคชันของหน่วยงาน

- IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีโดยเฉพาะที่เกิดขึ้นในระบบเครือข่าย โดยระบบประเภทนี้จะตรวจจับได้เฉพาะสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

- Endpoint Security ซอฟต์แวร์ตรวจจับโปรแกรมประสงค์ร้ายที่พยายามโจมตีต่อระบบคอมพิวเตอร์และเครือข่าย

- Centralized Log Management ระบบจัดเก็บและบริหารจัดการข้อมูล Log File แบบศูนย์กลาง

(๒.๒) แหล่งข้อมูลข่าวสารภัยคุกคามจากภายนอก (Threat intelligence) เช่น Thailand Computer Emergency Response Team (ThaiCERT) [https://www.thaicert.or.th] เป็นต้น

(๓) กรมกิจการสตรีและสถาบันครอบครัว ต้องดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น

(๓.๑) ผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน

ระดับผลกระทบ	**ลักษณะภัยคุกคามทางไซเบอร์**	**การตอบสนองต่อเหตุการณ์**
ไม่ร้ายแรง	การประทุษร้ายต่อคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ดังนี้ (๑) ระบบคอมพิวเตอร์ของหน่วยงาน หรือ (๒) อุปกรณ์หรือระบบงานอื่นที่ใช้สำหรับการให้บริการ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ระบบคอมพิวเตอร์ของหน่วยงาน หรือการให้บริการด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	
ร้ายแรง	การประทุษร้ายต่อคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่ถูกใช้สำหรับให้บริการหลัก ดังนี้ (๑) ระบบคอมพิวเตอร์ (๒) โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว แสดงให้เห็นได้ว่าผู้โจมตีมีความมุ่งหมายที่จะทำให้โครงสร้างพื้นฐานสำคัญประเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้	

ระดับผลกระทบ	ลักษณะภัยคุกคามทางไซเบอร์	การตอบสนองต่อเหตุการณ์
วิกฤต	<u>กรณี (ก)</u> การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่รุนแรงในลักษณะที่เป็นวงกว้างต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าวทำให้ (๑) การทำงานของหน่วยงาน หรือการให้บริการของโครงสร้างพื้นฐานสำคัญที่ให้กับประชาชน ล้มเหลวทั้งระบบจนไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ได้ หรือ (๒) การใช้มาตรการเยียวยาตามปกติ ในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ หรือระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลาย เป็นวงกว้างในระดับประเทศ <u>กรณี (ข)</u> ไม่เจาะจงอุปกรณ์หรือระบบงานที่ได้รับผลกระทบ แต่เมื่อพิจารณาจากพฤติกรรมของผู้โจมตีหรือพฤติการณ์แวดล้อมแล้ว มีเหตุอันควรเชื่อได้ว่าการก่อภัยคุกคามทางไซเบอร์นั้นกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญาการรบหรือการสงคราม	

(๓.๒) ระดับผลกระทบต่อข้อมูลในระบบ

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ	การตอบสนองต่อเหตุการณ์
ไม่ร้ายแรง	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูล ซึ่งส่งผลกระทบทำให้ระบบคอมพิวเตอร์ของหน่วยงาน หรือการให้บริการด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่ สามารถใช้งานได้	
ร้ายแรง	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลที่ใช้สำหรับระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศ ซึ่งส่งผลให้บริการหลักไม่สามารถทำงาน หรือให้บริการได้	
วิกฤต	<u>กรณี (ก)</u> มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลอันมีลักษณะดังนี้	

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ	การตอบสนองต่อเหตุการณ์
	(๑) เป็นข้อมูลที่เกี่ยวข้องกับการทำงานของหน่วยงานหรือการให้บริการที่ให้กับประชาชน หรือ (๒) เป็นข้อมูลที่เกี่ยวข้องกับชีวิตของบุคคลจำนวนมาก หรือเป็นข้อมูลคอมพิวเตอร์จำนวนมากในระดับประเทศ <u>กรณี (ข)</u> มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลใด ๆ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา การรบหรือการสงคราม	

(๓.๓) ผลกระทบต่อผู้รับบริการ

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ	การตอบสนองต่อเหตุการณ์
ไม่ร้ายแรง	ส่งผลหรืออาจส่งผลกระทบต่อผู้ใช้บริการในวงจำกัด	
ร้ายแรง	อาจส่งผลกระทบต่อผู้ใช้บริการทั้งหมด	
วิกฤต	<u>กรณี (ก)</u> ส่งผลกระทบต่อผู้ใช้บริการทั้งหมด หรืออาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต <u>กรณี (ข)</u> ส่งผลหรืออาจส่งผลกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมาย อาญา การรบหรือการสงคราม	

(๓.๔) ระดับความสามารถในการกู้คืน

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ	การตอบสนองต่อเหตุการณ์
ไม่ร้ายแรง	สามารถกู้คืนระบบคอมพิวเตอร์ หรือทำให้บริการของหน่วยงานกลับมาได้บางส่วน โดยสามารถดำเนินการได้ตามแผนการกู้คืน	
ร้ายแรง	ไม่สามารถกู้คืนระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศที่ใช้สำหรับให้บริการหลักได้ ตามแผนการกู้คืน	
วิกฤต	<u>กรณี (ก)</u>	

	ไม่สามารถกู้คืนการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของรัฐได้ (๒) มีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลาย เป็นวงกว้างในระดับประเทศ <u>กรณี (ข)</u> ไม่สามารถกู้คืนอุปกรณ์หรือระบบงานที่ได้รับผลกระทบได้ และจำเป็นต้องมีมาตรการเร่งด่วนในการกู้คืนอุปกรณ์หรือระบบงานที่เกี่ยวข้อง	

(๓.๕) หมวดหมู่ภัยคุกคาม และลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

หมวดหมู่	**คำอธิบาย**
๐	เหตุการณ์จำลอง และการฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

ประเภท อุปกรณ์เครือข่าย	หมวดหมู่ภัยคุกคาม						
	๑	๒	๓	๔	๕	๖	๗
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชัน	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

ตารางที่ ๑ ตัวอย่างเกณฑ์การประเมินระดับของภัยคุกคาม

ความรุนแรง	คำอธิบาย	การตอบสนองต่อเหตุการณ์
ต่ำ (Low)	ส่งผลกระทบต่อหน่วยงานในวงจำกัด เช่น เกิดการหยุดชะงักของการให้บริการเล็กน้อย หรือกระทบแค่หน่วยงานเดียว สามารถกู้คืนโดยใช้ทรัพยากรที่มีได้ ความเสียหายทางการเงินต่ำ ไม่ส่งผลกระทบต่อชื่อเสียงหรือความเชื่อมั่นของสาธารณะ หรือไม่เกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแล	แก้ไขภายใน ๗๒ ชั่วโมง
ปานกลาง (Medium)	ส่งผลกระทบต่อหน่วยงานในระดับปานกลาง เช่น เกิดการหยุดชะงักของการให้บริการที่ยาวนานขึ้น กระทบหลายหน่วยงาน สามารถกู้คืนได้แต่ต้องมีการจัดหาทรัพยากรเพิ่ม มีความเสียหายทางการเงินมากขึ้น เริ่มส่งผลกระทบต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับไม่ร้ายแรง	แก้ไขภายใน ๔๘ ชั่วโมง
สูง (High)	ส่งผลกระทบอย่างมากต่อหน่วยงาน เช่น ระบบสารสนเทศบางส่วนถูกทำลาย การดำเนินงานหยุดชะงักอย่างมากในช่วงเวลาหนึ่ง เวลาในการกู้คืนไม่สามารถ	แก้ไขภายใน ๒๔ ชั่วโมง

ความรุนแรง	คำอธิบาย	การตอบสนองต่อเหตุการณ์
	คาดการณ์ได้ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก ข้อมูลสำคัญจำนวนมากสูญหาย ความเสียหายทางการเงินสูง ส่งผลกระทบอย่างมากต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงาน ด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับร้ายแรง	
สูงมาก (Extreme)	ส่งผลกระทบอย่างร้ายแรงต่อหน่วยงาน เช่น มีภัยคุกคามต่อชีวิต ระบบสารสนเทศหลักถูกทำลาย การดำเนินงานทั้งหมดหยุดชะงักจนต้องปิดการให้บริการ ไม่สามารถทำการกู้คืนได้ ข้อมูลสำคัญจำนวนมากสูญหายและถูกนำไปเผยแพร่ต่อสาธารณะ ความเสียหายทางการเงินสูงมาก ส่งผลกระทบอย่างรุนแรงต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับวิกฤติ	แก้ไขภายใน ๔ ชั่วโมง

(๔) หน่วยงานจะต้องดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๒)

(๕) หน่วยงานจะต้องจัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ทุกขั้นตอน ตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุ ตลอดถึงระยะเวลาที่ใช้ระงับเหตุด้วย ทั้งนี้ ควรบันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ โดยระบุวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๓)

(๖) กรณีหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการแจ้งตามกฎหมาย หรือนำส่งข้อมูลที่มีรายละเอียดเทียบเท่ากับแบบฟอร์ม ก๑ (รายละเอียดปรากฏตามภาคผนวก ๔) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยัง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

(ค) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๓ ขั้นตอนการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

หน่วยงานจะต้องดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

(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 ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๔. ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

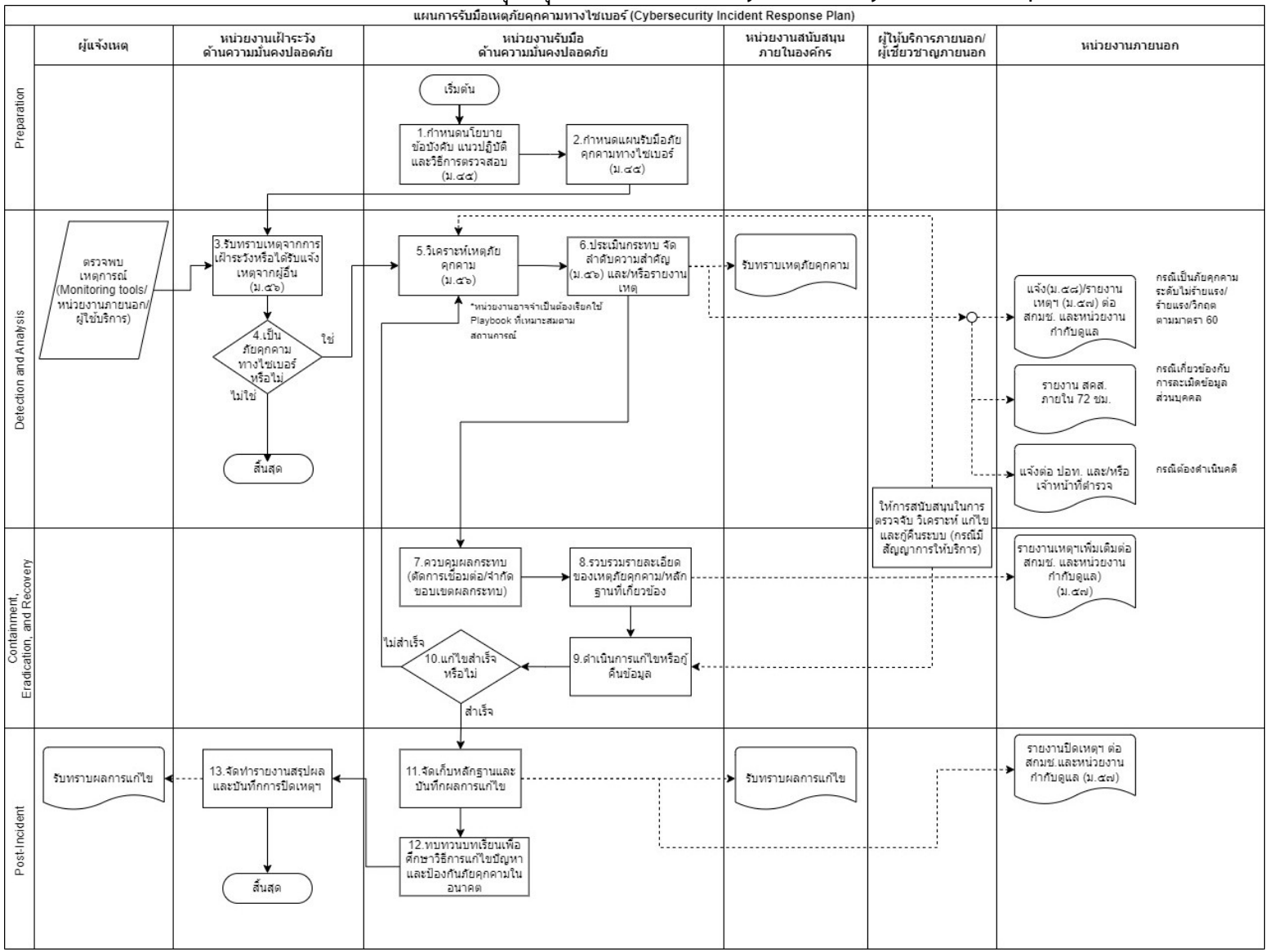
หน่วยงานควรกำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมาและสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นอาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๔ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๕. การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

หน่วยงานจะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก ๕)

ภาคผนวก ๑ แผนการรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรับมือภัยคุกคามแต่ละประเภท

๑. แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)



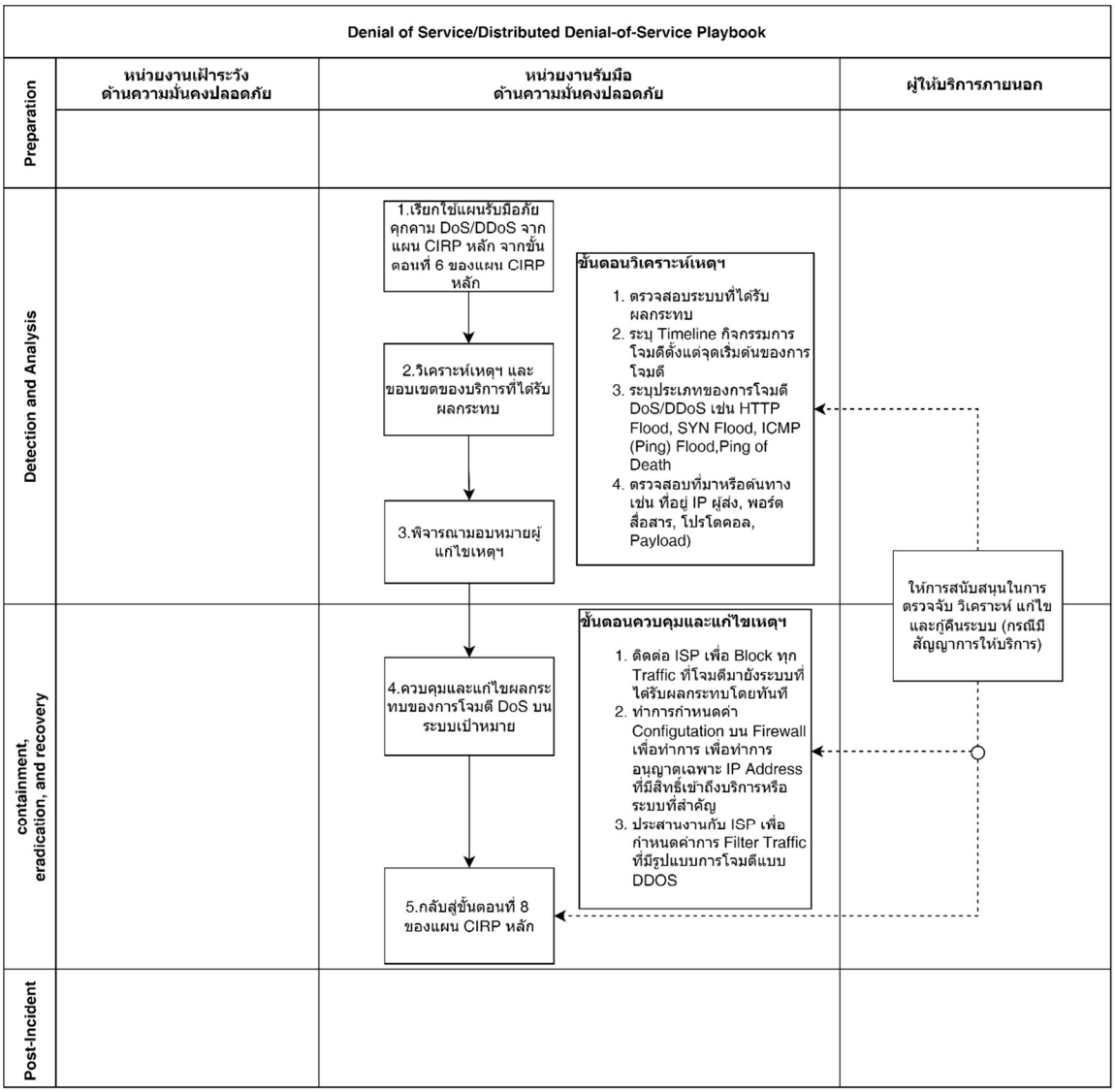
คำอธิบายแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ลำดับ	หัวข้อ	คำอธิบาย
ขั้นตอนการเตรียมการ (preparation)		
๑	กำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบ (ม.๔๕)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย ร่วมกับผู้บริหารของหน่วยงานกำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบด้านความมั่นคงปลอดภัย โดยสอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามมาตรา ๑๓ วรรคหนึ่ง (๔))
๒	กำหนดแผนรับมือภัยคุกคามทางไซเบอร์ (ม.๔๕)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย กำหนดแผนรับมือภัยคุกคามทางไซเบอร์ โดยระบุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน กำหนดขั้นตอนและวิธีการกำหนดผู้รับผิดชอบในแต่ละขั้นตอน และกำหนดให้มีการทดสอบแผนรับมือภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๓	รับทราบเหตุจากการเฝ้าระวังหรือได้รับแจ้งเหตุจากผู้อื่น (ม.๕๖)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ได้รับทราบเหตุจากการเฝ้าระวัง (Monitoring tools) หรือได้รับแจ้งเหตุจากผู้อื่นที่ตรวจพบเหตุการณ์ เช่น หน่วยงานภายนอกหรือผู้ใช้บริการ
๔	เป็นภัยคุกคามทางไซเบอร์หรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัยพิจารณาเหตุการณ์ว่าเป็นภัยคุกคามทางไซเบอร์หรือไม่
๕	วิเคราะห์เหตุภัยคุกคาม	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาประเภทของภัยคุกคาม หมวดหมู่ของภัยคุกคาม รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม ข้อมูล จำนวนระบบ บริการ หรือสินทรัพย์ที่ได้รับผลกระทบ
๖	ประเมินกระทบ และจัดลำดับความสำคัญ (ม.๕๖)	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ดำเนินการประเมินกระทบ และจัดลำดับความสำคัญของเหตุภัยคุกคาม รวมถึงเลือกแนวทางในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ หมายเหตุ: หน่วยงานอาจจำเป็นต้องเรียกใช้ Playbook ที่เหมาะสมตามสถานการณ์

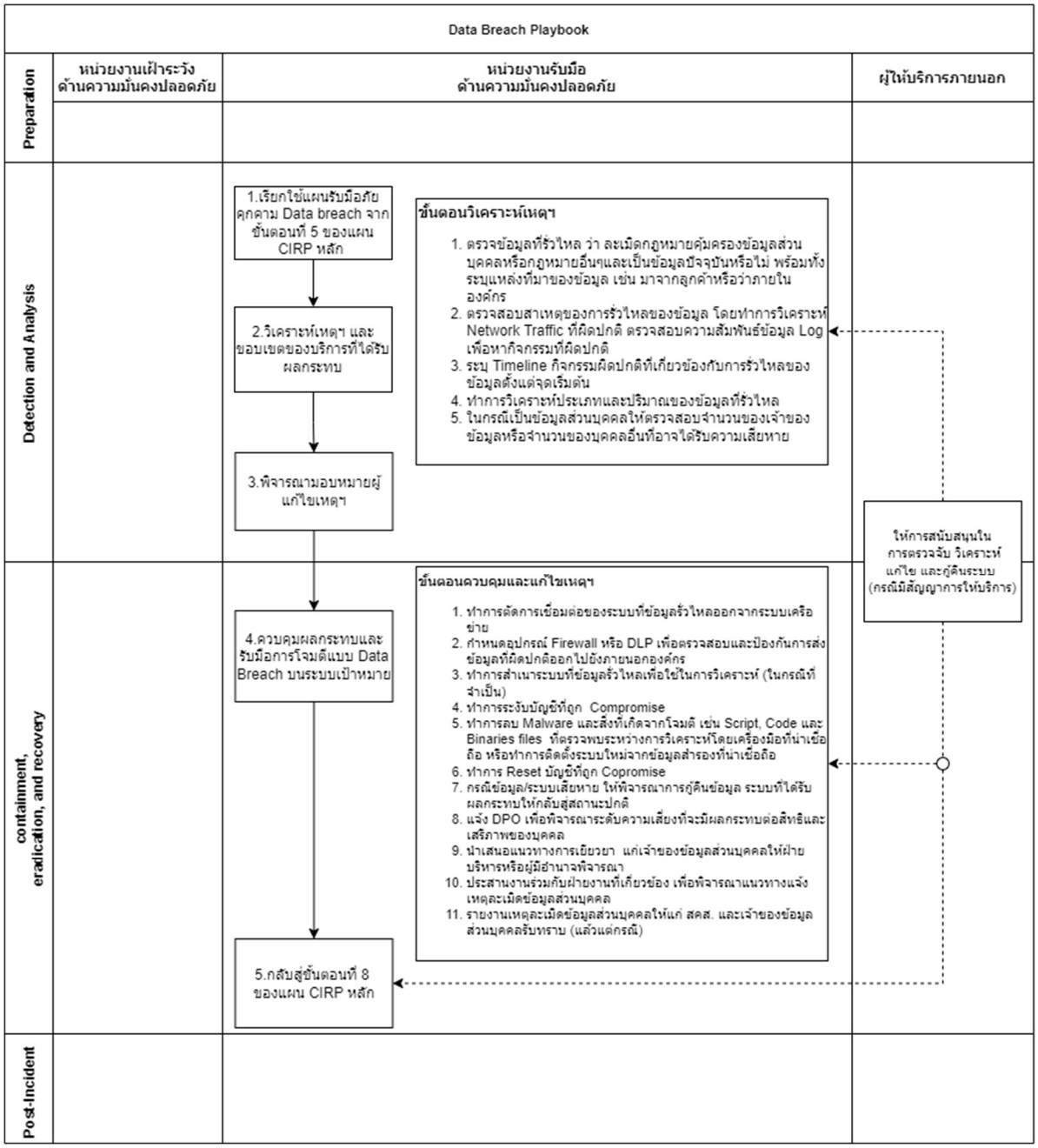
ลำดับ	หัวข้อ	คำอธิบาย
		๒. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงานต่าง ๆ ■ กรณีเป็นภัยคุกคามระดับไม่ร้ายแรง/ร้ายแรง/วิกฤตตามมาตรา ๖๐ หน่วยงานต้องแจ้งเหตุภัยคุกคาม (มาตรา ๕๘) (แบบฟอร์ม ก.๑ หรือมีข้อมูลเทียบเท่า) และ/หรือรายงานเหตุภัยคุกคาม (มาตรา ๕๗) (แบบฟอร์ม ก.๒) ต่อ สกมช. และหน่วยงานกำกับดูแล ■ กรณีเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล หน่วยงานอาจต้องแจ้งไปยัง สคส. ■ กรณีมีความจำเป็นต้องดำเนินคดีเนื่องจากเหตุนั้นเหตุนั้นเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง หน่วยงานอาจต้องแจ้งไปยัง ปอท. และ/หรือเจ้าหน้าที่ตำรวจ เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น
ขั้นตอนการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๗	ควบคุมผลกระทบ (ตัดการเชื่อมต่อ/จำกัดขอบเขตผลกระทบ)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ควรจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ทำการกำจัดสาเหตุ (Eradicate the incident) กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่น ๆ
๘	รวบรวมรายละเอียดของเหตุภัยคุกคาม/หลักฐานที่เกี่ยวข้อง	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย บันทึกเหตุการณ์ และดำเนินการจัดเก็บรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน ๒. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุการณ์เพิ่มเติมต่อ สกมช. และหน่วยงานกำกับดูแล (ม.๕๗) (แบบฟอร์ม ก.๒)

ลำดับ	หัวข้อ	คำอธิบาย
๙	ดำเนินการแก้ไขหรือกู้คืนข้อมูล	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เรียกใช้งานกระบวนการกู้คืน (Recovery Process)
๑๐	แก้ไขสำเร็จหรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัยพิจารณาว่าระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งานแล้วหรือไม่ หากยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ ให้ดำเนินการต่อที่ขั้นตอนที่ ๑๑ หากยังไม่สามารถแก้ไขได้ ให้ดำเนินการขั้นตอนที่ ๕ ซ้ำเพื่อวิเคราะห์ภัยคุกคามทางไซเบอร์อีกครั้ง
ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๑๑	จัดเก็บหลักฐานและบันทึกผลการแก้ไข	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ๒. บันทึกผลการแก้ไขเหตุภัยคุกคามและวิธีการแก้ไขเพื่อจัดเก็บเป็นบทเรียน ๓. รายงานปิดเหตุการณ์ต่อ สกมช. และหน่วยงานกำกับดูแล (ม.๕๗) (แบบฟอร์ม ก.๒)
๑๒	ทบทวนบทเรียนเพื่อศึกษาวิธีการแก้ไขปัญหา และป้องกันภัยคุกคามในอนาคต	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว และกำหนดแนวทางในการป้องกันการเกิดเหตุซ้ำ หรือป้องกันภัยคุกคาม อื่น ๆ ที่มีลักษณะคล้ายคลึงกันในอนาคต
๑๓	จัดทำรายงานสรุปผลและบันทึกการปิดเหตุฯ	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดทำรายงานสรุปผลและบันทึกการปิดเหตุการณ์ รวมถึงแจ้งผลการแก้ไขไปยังผู้เกี่ยวข้องให้รับทราบ

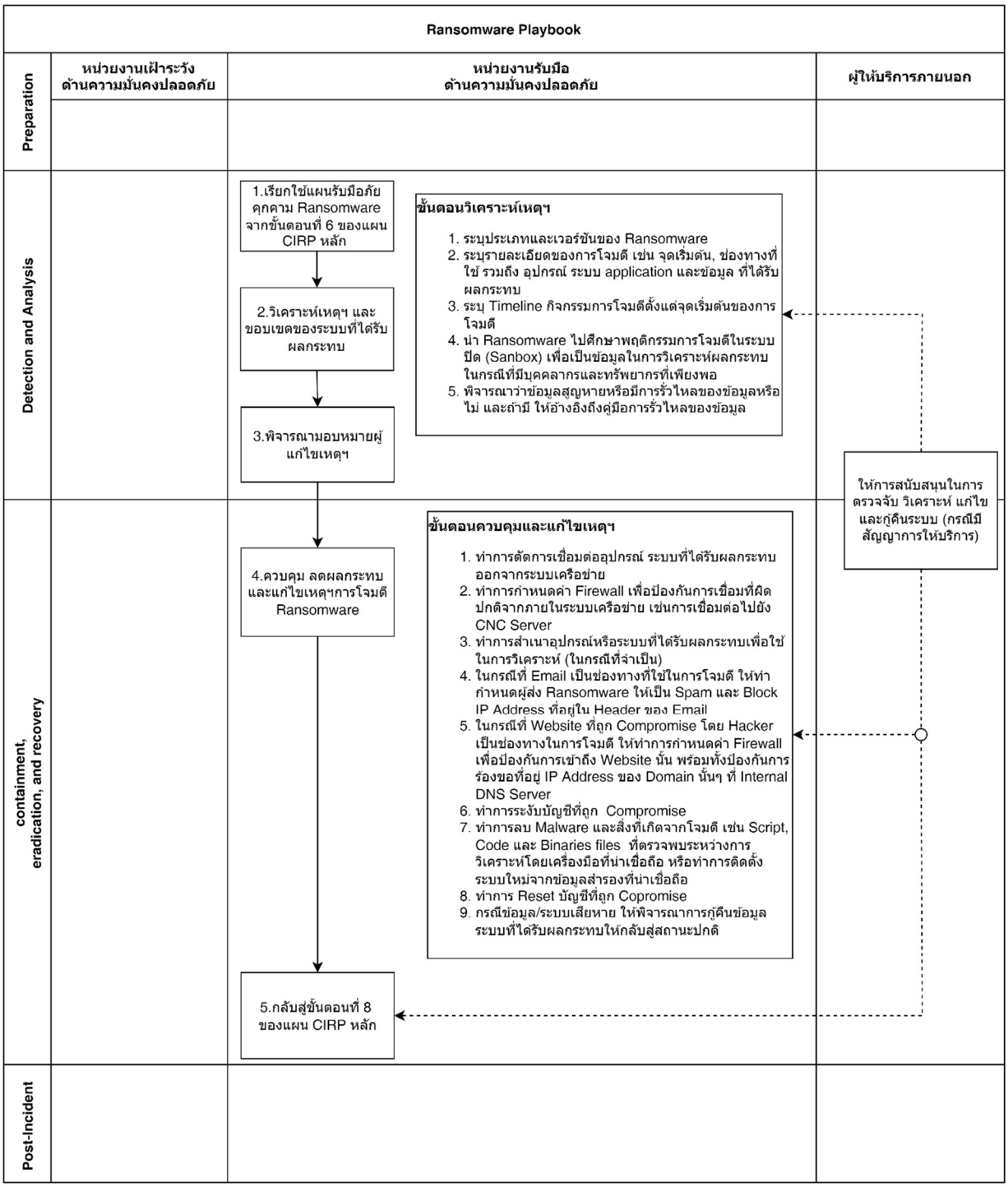
๒. ขั้นตอนการรับมือภัยคุกคามแบบ Denial of Service/Distributed Denial-of-Service (DoS/DDoS Playbook)



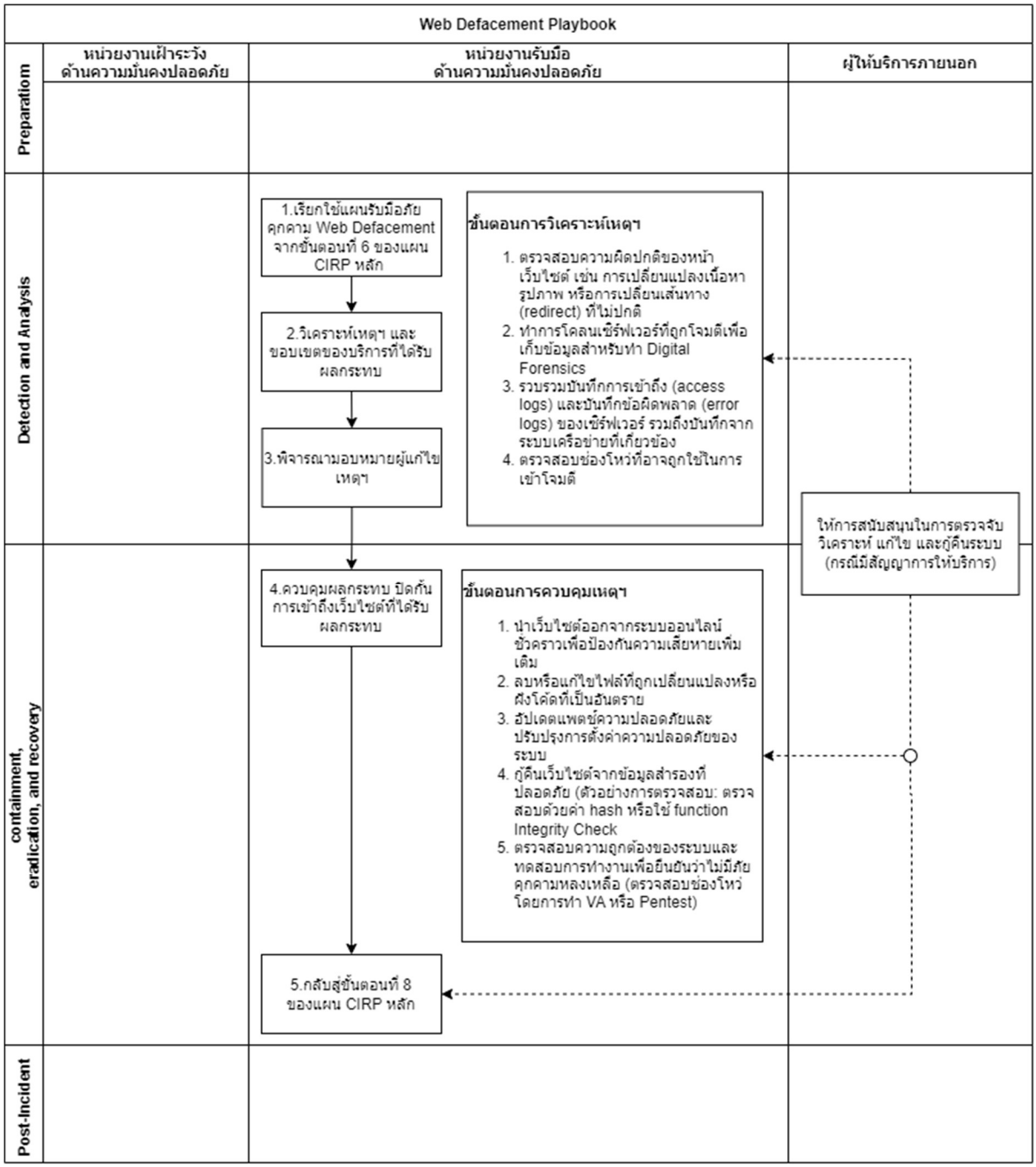
๓. ขั้นตอนการรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook)



๔. ขั้นตอนการรับมือภัยคุกคามแบบ Ransomware (Ransomware Playbook)



๕. ขั้นตอนการรับมือภัยคุกคามแบบ Web Defacement (Web Defacement Playbook)


Web Defacement Playbook
Preparation
Detection and Analysis
containment, eradication, and recovery
Post-Incident
หน่วยงานเฝ้าระวัง ด้านความมั่นคงปลอดภัย
หน่วยงานรับมือ ด้านความมั่นคงปลอดภัย
ผู้ให้บริการภายนอก
1.เรียกใช้แผนรับมือภัยคุกคาม Web Defacement จากขั้นตอนที่ 6 ของแผน CIRP หลัก
2.วิเคราะห์เหตุฯ และขอบเขตของบริการที่ได้รับผลกระทบ
3.พิจารณามอบหมายผู้แก้ไขเหตุฯ
ขั้นตอนการวิเคราะห์เหตุฯ
1. ตรวจสอบความผิดปกติของหน้าเว็บไซต์ เช่น การเปลี่ยนแปลงเนื้อหา รูปภาพ หรือการเปลี่ยนเส้นทาง (redirect) ที่ไม่ปกติ
2. ทำการโคลนเซิร์ฟเวอร์ที่ถูกโจมตีเพื่อเก็บข้อมูลสำหรับทำ Digital Forensics
3. รวบรวมบันทึกการเข้าถึง (access logs) และบันทึกข้อผิดพลาด (error logs) ของเซิร์ฟเวอร์ รวมถึงบันทึกจากระบบเครือข่ายที่เกี่ยวข้อง
4. ตรวจสอบช่องโหว่ที่อาจถูกใช้ในการเข้าโจมตี
ให้การสนับสนุนในการตรวจจับ วิเคราะห์ แก้ไข และกู้คืนระบบ (กรณีมีสัญญาการให้บริการ)
4.ควบคุมผลกระทบ ปิดกั้นการเข้าถึงเว็บไซต์ที่ได้รับผลกระทบ
ขั้นตอนการควบคุมเหตุฯ
1. นำเว็บไซต์ออกจากระบบออนไลน์ชั่วคราวเพื่อป้องกันความเสียหายเพิ่มเติม
2. ลบหรือแก้ไขไฟล์ที่ถูกเปลี่ยนแปลงหรือฝังโค้ดที่เป็นอันตราย
3. อัปเดตแพตช์ความปลอดภัยและปรับปรุงการตั้งค่าความปลอดภัยของระบบ
4. กู้คืนเว็บไซต์จากข้อมูลสำรองที่ปลอดภัย (ตัวอย่างการตรวจสอบ: ตรวจสอบด้วยค่า hash หรือใช้ function Integrity Check
5. ตรวจสอบความถูกต้องของระบบและทดสอบการทำงานเพื่อยืนยันว่าไม่มีภัยคุกคามหลงเหลือ (ตรวจสอบช่องโหว่โดยการทำ VA หรือ Pentest)
5.กลับสู่ขั้นตอนที่ 8 ของแผน CIRP หลัก

ภาคผนวก ๒

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :		

ภาคผนวก ๓

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)
ตัวอย่าง ๑๒/๑/๖๖ – ๐๙.๐๐ น.	*ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน*

ภาคผนวก ๔

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
๑. ข้อมูลการประสานงาน ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง
๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม
๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)
๔. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
๕. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๒] ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

[๒] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑

หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ
หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ
วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม
ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ

ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม
ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ
ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ
โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ

ก๓. ความต่อเนื่องของเหตุภัยคุกคาม
☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

ก๔. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน

☐ ใช่ ☐ ไม่ใช่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๓] ในระดับใด (มาตรา ๖๐)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

[๓] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ

☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม

☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว

☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ

ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว

☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว

☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว

☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ ๒

หมวด ง : รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

วันที่: เลือกวันที่ **เวลา:** โปรดระบุ **ไม่ทราบ:** ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

๑.๔ <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ
☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ
☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ
☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)
☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ
☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ
☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย
☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง
☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก
☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย
☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ
☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ
☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)
☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ
☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น
☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ
☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)
☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)

โปรดระบุ

๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

๒.๒ การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[๔]

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตซ์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

[๔] หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ.๒๕๖๔

[๕] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ภาคผนวก ๕

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๑	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
๑.๑	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
๑.๒	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
๑.๓	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
๑.๔	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นตอนการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
๗.๑	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
๗.๒	กำจัด หรือ ลบมัลแวร์ และสาเหตุภัยคุกคามอื่น ๆ	
๗.๓	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
๘	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
๘.๑	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
๘.๒	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
๘.๓	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.๒๕๖๔
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทาง ไซเบอร์ พ.ศ.๒๕๖๖
- NIST SP ๘๐๐-๖๑r๒ Computer Security Incident Handling Guide
- ACSC Cyber Incident Response Plan Guidance