



ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ที่ ๑ /๒๕๖๙

เรื่อง แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) (ฉบับที่ ๒)

.....

ตามที่ได้มีประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ๑๓/๒๕๖๖ เรื่อง แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ลงวันที่ ๑๙ ธันวาคม พ.ศ. ๒๕๖๖ เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๒ ด้านบริการภาครัฐที่สำคัญ ลักษณะหน่วยงาน ข้อ ๒ ที่มีการให้บริการโดยตรงแก่ประชาชน ภารกิจหรือให้บริการ (Critical Services) (๖) บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง (๗) บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน (๘) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล และ (๙) บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ ได้ถือปฏิบัติ โดยมีรายละเอียด ขั้นตอน กรอบระยะเวลา และแบบฟอร์มการแจ้งเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงานควบคุมหรือกำกับดูแล และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ปรากฏตามเอกสารแนบท้ายประกาศดังกล่าว นั้น

เนื่องจากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) มีการเปลี่ยนแปลงส่วนงานที่รับผิดชอบการรับรายงานภัยคุกคามทางไซเบอร์ จึงจำเป็นต้องแก้ไขเพิ่มเติมช่องทางการติดต่อให้สอดคล้องกัน

อาศัยอำนาจตามความในมาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ ประกอบกับมาตรา ๑๓ (๕) และมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัลจึงเห็นควรให้ยกเลิกความในตารางที่ ๑ การกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์ ของเอกสารแนบท้ายประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ๑๓/๒๕๖๖ เรื่อง แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ลงวันที่ ๑๙ ธันวาคม พ.ศ. ๒๕๖๖ และให้ใช้ความต่อไปนี้แทน

ตารางที่ ๑ การกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

ลักษณะภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์)	การส่งรายงานให้ สกมช. (ภายในเวลา หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์)
ระดับไม่ร้ายแรง	๒๔ ชั่วโมง	๓๐ วัน	๓๐ วัน
ระดับร้ายแรง	๓๐ นาที	๔ ชั่วโมง	๒๔ ชั่วโมง
ระดับวิกฤติ	๑๕ นาที	๑ ชั่วโมง	๖ ชั่วโมง
ช่องทาง การติดต่อ	โทรศัพท์ : ๐ ๒๖๑๒ ๖๐๐๐ Contact Center: ๐ ๒๖๑๒ ๖๐๖๐ Email: sd-g4_division@dga.or.th	Email: sd-g4_division@dga.or.th ระดับชั้นข้อมูล “ลับมาก” เข้ารหัสข้อมูลแบบ PGP	Email: saraban@ncsa.or.th ระดับชั้นข้อมูล “ลับมาก” เข้ารหัสข้อมูลแบบ PGP

จึงประกาศให้ทราบ และถือปฏิบัติอย่างเคร่งครัดโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ กุมภาพันธ์ พ.ศ. ๒๕๖๙



(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการ รักษาการแทน

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล



ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ที่ ๑๓ /๒๕๖๖

เรื่อง แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)

.....

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ ที่ออกโดยอาศัยอำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เป็นหน่วยงานควบคุมหรือกำกับดูแล ที่ได้รับมอบหมายให้ดำเนินการควบคุมหรือกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านบริการภาครัฐที่สำคัญ ลักษณะหน่วยงานที่มีการให้บริการโดยตรงแก่ประชาชน ในภารกิจหรือให้บริการ (Critical Services) ได้แก่ บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล และบริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ ทั้งนี้ เพื่อให้การรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๘ (๙) มาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ ประกอบกับมาตรา ๑๓ (๕) และมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จึงออกประกาศเรื่อง แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๒ ด้านบริการภาครัฐที่สำคัญ ลักษณะหน่วยงานข้อ ๒ ที่มีการให้บริการโดยตรงแก่ประชาชน ภารกิจหรือให้บริการ (Critical Services) (๖) บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง (๗) บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน (๘) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล และ (๙) บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ ได้ถือปฏิบัติ โดยมีรายละเอียด ขั้นตอน กรอบระยะเวลา และแบบฟอร์มการแจ้งเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงานควบคุมหรือกำกับดูแล และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ปรากฏตามเอกสารแนบท้ายประกาศนี้

จึงประกาศให้ทราบ และถือปฏิบัติอย่างเคร่งครัดโดยทั่วกัน

ประกาศ ณ วันที่ ๑๙ ธันวาคม พ.ศ. ๒๕๖๖



(นายสุพจน์ เขียวรุฒิ)
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

เอกสารแนบท้ายประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เรื่อง แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)

การแจ้งเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงานควบคุมกำกับดูแล และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ซึ่งมีขั้นตอน และกรอบระยะเวลาดำเนินการแจ้งเหตุภัยคุกคามทางไซเบอร์โดยสังเขป ดังนี้

๑. กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ ต่อระบบสารสนเทศของหน่วยงานของรัฐ หรือ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ^๑
 - (๑) ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อม
 - (๒) ประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ เป็นภัยคุกคามระดับใด
 - (๓) ดำเนินการ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของตน
 - (๔) แจ้งข้อมูลดังกล่าว ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติโดยเร็ว และให้แจ้งภัยคุกคามนั้นไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดไว้ด้วย ทั้งนี้ ให้แจ้งข้อมูลเบื้องต้น และส่งรายงาน ที่กำหนดตามแบบ เอกสาร ก๑ ที่ปรากฏท้ายเอกสารนี้ส่งภายในระยะเวลาและช่องทางที่กำหนดในตารางที่ ๑ โดยการแจ้ง การรายงาน และการรายงานสรุปตามประกาศฯ จะทำเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้
๒. กรณีที่มีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ ต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ^๒

ให้หน่วยงานดังกล่าวจัดทำและส่งรายงานเหตุภัยคุกคามทางไซเบอร์นั้น ตามแบบที่กำหนดใน **เอกสาร ก๒** ที่ปรากฏท้ายเอกสารนี้ ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติภายในระยะเวลา ๒๔ ชั่วโมง หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์ดังกล่าวแล้ว พร้อมทั้งให้จัดส่งรายงานดังกล่าว ไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาและช่องทางที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดใน ตารางที่ ๑ โดยการแจ้ง การรายงาน และการรายงานสรุปตามประกาศฯ จะทำเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้

๓. การรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี^๓

ให้หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จัดทำและส่งรายงาน สรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตน ในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดใน**เอกสาร ก๓** แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี โดยการแจ้ง การรายงาน และการรายงานสรุปตามประกาศฯ จะทำเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้

^๑ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ข้อ ๔

^๒ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ข้อ ๕

^๓ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ข้อ ๖

ตารางที่ ๑ การกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

ลักษณะภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์)	การส่งรายงานให้ สกมช. (ภายในเวลา หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์)
ระดับไม่ร้ายแรง	๒๔ ชั่วโมง	๓๐ วัน	๓๐ วัน
ระดับร้ายแรง	๓๐ นาที	๔ ชั่วโมง	๒๔ ชั่วโมง
ระดับวิกฤติ	๑๕ นาที	๑ ชั่วโมง	๖ ชั่วโมง
ช่องทางการติดต่อ	โทรศัพท์ : ๐ ๒๖๑๒ ๖๐๐๐ Contact Center: ๐ ๒๖๑๒ ๖๐๖๐ ไลน์กลุ่ม Regulator & CII	Email: sd-g2_division@dgga.or.th ระดับชั้นข้อมูล “ลับมาก” เข้ารหัสข้อมูลแบบ PGP	Email: saraban@ncsa.or.th ระดับชั้นข้อมูล “ลับมาก” เข้ารหัสข้อมูลแบบ PGP

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น																	
<p>๑. ข้อมูลการประสานงาน</p> <p>ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม: โปรตระบุ</p> <p>วันที่และเวลาที่แจ้ง: โปรตระบุ</p>																	
<p>๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม</p> <p>ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรตระบุ</p> <p>ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรตระบุ</p>																	
<p>๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม</p> <p>ชื่อ-นามสกุล: โปรตระบุ ตำแหน่งงาน: โปรตระบุ</p> <p>ชื่อหน่วยงาน: โปรตระบุ อีเมล: โปรตระบุ</p> <p>โทรศัพท์ (ที่ทำงาน / มือถือ): โปรตระบุ</p>																	
<p>๔. ความต่อเนื่องของเหตุภัยคุกคาม</p> <p><input type="checkbox"/> เหตุภัยคุกคามใหม่ <input type="checkbox"/> การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม</p>																	
<p>๕. ลักษณะภัยคุกคามทางไซเบอร์</p> <p>ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่</p> <p>เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์^๔ ในระดับใด (มาตรา ๖๐)</p> <p><input type="checkbox"/> ไม่ร้ายแรง <input type="checkbox"/> ร้ายแรง <input type="checkbox"/> วิกฤต (ก) <input type="checkbox"/> วิกฤต (ข)</p> <p><input type="checkbox"/> ยังไม่สามารถระบุได้</p>																	
<p>๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)</p> <table border="1"> <thead> <tr> <th>หมวดหมู่*</th> <th>คำอธิบาย</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๒</td> <td>การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๓</td> <td>การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๔</td> <td>การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๕</td> <td>การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๖</td> <td>การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๗</td> <td>การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๘</td> <td>เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)</td> </tr> </tbody> </table>		หมวดหมู่*	คำอธิบาย	<input type="checkbox"/> หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	<input type="checkbox"/> หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)	<input type="checkbox"/> หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	<input type="checkbox"/> หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	<input type="checkbox"/> หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	<input type="checkbox"/> หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	<input type="checkbox"/> หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
หมวดหมู่*	คำอธิบาย																
<input type="checkbox"/> หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)																
<input type="checkbox"/> หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)																
<input type="checkbox"/> หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)																
<input type="checkbox"/> หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)																
<input type="checkbox"/> หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)																
<input type="checkbox"/> หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)																
<input type="checkbox"/> หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)																
<p>* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคาม ทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)</p>																	

^๔ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบเขตใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์																			
ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม วันที่ : <input type="text"/> โปรตระบุ เวลา : <input type="text"/> โปรตระบุ วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม วันที่ : <input type="text"/> โปรตระบุ เวลา : <input type="text"/> โปรตระบุ																			
ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ <input type="checkbox"/> ยังไม่ได้แจ้ง <input type="checkbox"/> แจ้งแล้ว																			
ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ) <table border="1"> <thead> <tr> <th>หมวดหมู่*</th> <th>คำอธิบาย</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๒</td> <td>การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๓</td> <td>การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๔</td> <td>การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๕</td> <td>การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๖</td> <td>การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๗</td> <td>การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</td> </tr> <tr> <td><input type="checkbox"/> หมวดหมู่ที่ ๘</td> <td>เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)</td> </tr> <tr> <td><input type="checkbox"/> อื่น ๆ</td> <td><input type="text"/> โปรตระบุ</td> </tr> </tbody> </table>		หมวดหมู่*	คำอธิบาย	<input type="checkbox"/> หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	<input type="checkbox"/> หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)	<input type="checkbox"/> หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	<input type="checkbox"/> หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	<input type="checkbox"/> หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	<input type="checkbox"/> หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	<input type="checkbox"/> หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	<input type="checkbox"/> อื่น ๆ	<input type="text"/> โปรตระบุ
หมวดหมู่*	คำอธิบาย																		
<input type="checkbox"/> หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)																		
<input type="checkbox"/> หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)																		
<input type="checkbox"/> หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)																		
<input type="checkbox"/> หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)																		
<input type="checkbox"/> หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)																		
<input type="checkbox"/> หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)																		
<input type="checkbox"/> หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)																		
<input type="checkbox"/> อื่น ๆ	<input type="text"/> โปรตระบุ																		
* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทาง ไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๘ ไม่เข้าข่ายเป็นภัยคุกคามที่ต้องรายงาน)																			
ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ: สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง): <input type="text"/> โปรตระบุ ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ : <input type="text"/> โปรตระบุ บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน): <input type="text"/> โปรตระบุ ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่อง คอมพิวเตอร์): <input type="text"/> โปรตระบุรายละเอียด มีผลกระทบต่อการใช้งาน (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): <input type="text"/> โปรตระบุ รายละเอียดอื่น ๆ: <input type="text"/> โปรตระบุ																			

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

- | | |
|--|--|
| <input type="checkbox"/> เพิ่งพบเหตุการณ์ | <input type="checkbox"/> อยู่ในขั้นตอนการขอความช่วยเหลือ |
| <input type="checkbox"/> อยู่ในขั้นตอนการสอบสวน | <input type="checkbox"/> กำลังลุกลาม |
| <input type="checkbox"/> อยู่ในขั้นตอนการระงับภัย | <input type="checkbox"/> สามารถระงับภัยได้แล้ว |
| <input type="checkbox"/> รายงานปิดเหตุการณ์ภัยคุกคามแล้ว | <input type="checkbox"/> อื่น ๆ: โปรดระบุ |

ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

- | | |
|---|--|
| <input type="checkbox"/> ยังไม่ได้ดำเนินการแก้ไขใด ๆ | <input type="checkbox"/> ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว |
| <input type="checkbox"/> ตรวจสอบข้อมูลจราจร (Log) แล้ว | <input type="checkbox"/> ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว |
| <input type="checkbox"/> กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว | |
| <input type="checkbox"/> รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ | |

ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ ๒
หมวด ง : รายละเอียดภัยคุกคาม
ง๑. ข้อมูลการตรวจจับและการวิเคราะห์
ง๑.๑ วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access) วันที่: <input type="text"/> / <input type="text"/> / <input type="text"/> เวลา: <input type="text"/> : <input type="text"/> : <input type="text"/> ไม่ทราบ: <input type="checkbox"/>
ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์ รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของ ระบบ, ภัยธรรมชาติ, การโจรกรรม, ความผิดพลาดจากคนนอกองค์กร): <input type="text"/> บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ): <input type="text"/> รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด): <input type="text"/>
ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล) จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): <input type="text"/> ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: <input type="text"/> จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): <input type="text"/> มูลค่าความเสียหาย (โดยประมาณ): <input type="text"/> ในกรณีที่มีข้อมูลที่ระบุตัวบุคคลได้ร่วไหล (หรือถูกขโมย): จำนวนบุคคลที่เป็นเจ้าของข้อมูล: <input type="text"/> ชนิดของข้อมูล (เลือกทุกข้อที่ใช้): <input type="checkbox"/> ข้อมูลไปโอเมตริกซ์ <input type="checkbox"/> ข้อมูลการติดต่อ <input type="checkbox"/> ข้อมูลการเงิน <input type="checkbox"/> ข้อมูลบุคลากรของรัฐ <input type="checkbox"/> หมายเลขบัตรประชาชน <input type="checkbox"/> ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ <input type="checkbox"/> ข้อมูลทางการแพทย์ <input type="checkbox"/> อื่น ๆ: <input type="text"/> จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: <input type="text"/> ผลกระทบอื่น ๆ ที่เกิดขึ้น: <input type="text"/>

<p>๑๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</p> <p>หมายเลข CVE: <input type="text" value="โปรดระบุ"/></p> <p>ช่องโหว่ที่ถูกใช้โจมตี: <input type="text" value="โปรดระบุ"/></p> <p>การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อโจมตีขยายผลไปยังระบบหรือเครื่องอื่น:</p> <p><input type="text" value="โปรดระบุ"/></p> <p>อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)</p> <p><input type="checkbox"/> ระบบล่ม <input type="checkbox"/> รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ</p> <p><input type="checkbox"/> บัญชีผู้ใช้ถูกสร้างขึ้นใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ</p> <p><input type="checkbox"/> การโจมตีด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่ล่าช้าและไม่ล่าช้า</p> <p><input type="checkbox"/> ประสิทธิภาพของระบบด้อยลง (ซึ่งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)</p> <p><input type="checkbox"/> การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ</p> <p><input type="checkbox"/> การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ</p> <p><input type="checkbox"/> การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย</p> <p><input type="checkbox"/> การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง</p> <p><input type="checkbox"/> การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก</p> <p><input type="checkbox"/> การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย</p> <p><input type="checkbox"/> รูปแบบการใช้งานที่ผิดปกติ <input type="checkbox"/> การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ</p> <p><input type="checkbox"/> ความพยายามที่จะเขียนไฟล์ของระบบ <input type="checkbox"/> การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ</p> <p><input type="checkbox"/> การแก้ไขหรือลบข้อมูลที่ผิดปกติ <input type="checkbox"/> การโจมตีให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)</p> <p><input type="checkbox"/> ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ <input type="checkbox"/> การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ไม่ปกติ</p> <p><input type="checkbox"/> การแก้ไขหน้าเว็บ <input type="checkbox"/> การสร้างเพิ่มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น</p> <p><input type="checkbox"/> การเปลี่ยนแปลงในไดเรกทอรีและเพิ่มข้อมูลของระบบปฏิบัติการที่ผิดปกติ</p> <p><input type="checkbox"/> การตรวจพบโปรแกรมเจาะระบบ (Crack utility)</p> <p><input type="checkbox"/> สิ่งผิดปกติไปจากเดิมอื่น ๆ: <input type="text" value="โปรดระบุ"/></p>		
<p>๑๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การโจมตีครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการโจมตี, Attack vector, เทคนิคหรือเครื่องมือที่ผู้โจมตีใช้ ฯลฯ)</p> <p><input type="text" value="โปรดระบุ"/></p>		
<p>๑๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม:</p> <p><input type="text" value="โปรดระบุ"/></p>		
<p>๑๒. ข้อมูลการระงับ ปรามปราม และฟื้นฟู : <input type="text" value="โปรดระบุ"/></p>		
<p>๑๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม:</p> <p><input type="text" value="โปรดระบุ"/></p>		
<p>๑๒.๒ การคาดการณ์ความสามารถฟื้นฟู</p> <p><input type="text" value="โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู"/></p>		
<p>๑๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)</p>		
๑๓.๑	วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด	วันที่: <input type="text" value="โปรดระบุ"/> เวลา: <input type="text" value="โปรดระบุ"/>
<p>๑๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: <input type="text" value="โปรดระบุ"/></p>		
<p>๑๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: <input type="text" value="โปรดระบุ"/></p>		

เอกสาร ก๓ แบบรายงานสรุปลักษณะภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์^๖

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกซ้อมของหน่วยงาน (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)	
สวิตช์ (Switch) / เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์^๗

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

^๖ หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคาม ทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔

^๗ ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒