DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

ขอเชิญรับฟังและแสดงความคิดเห็นต่อ

(ร่าง) ประกาศ สพร. ตามหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล

DGA DIGITAL GOVERNMENT DEVELOPMENT AGENCY **CII REGULATOR**

ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

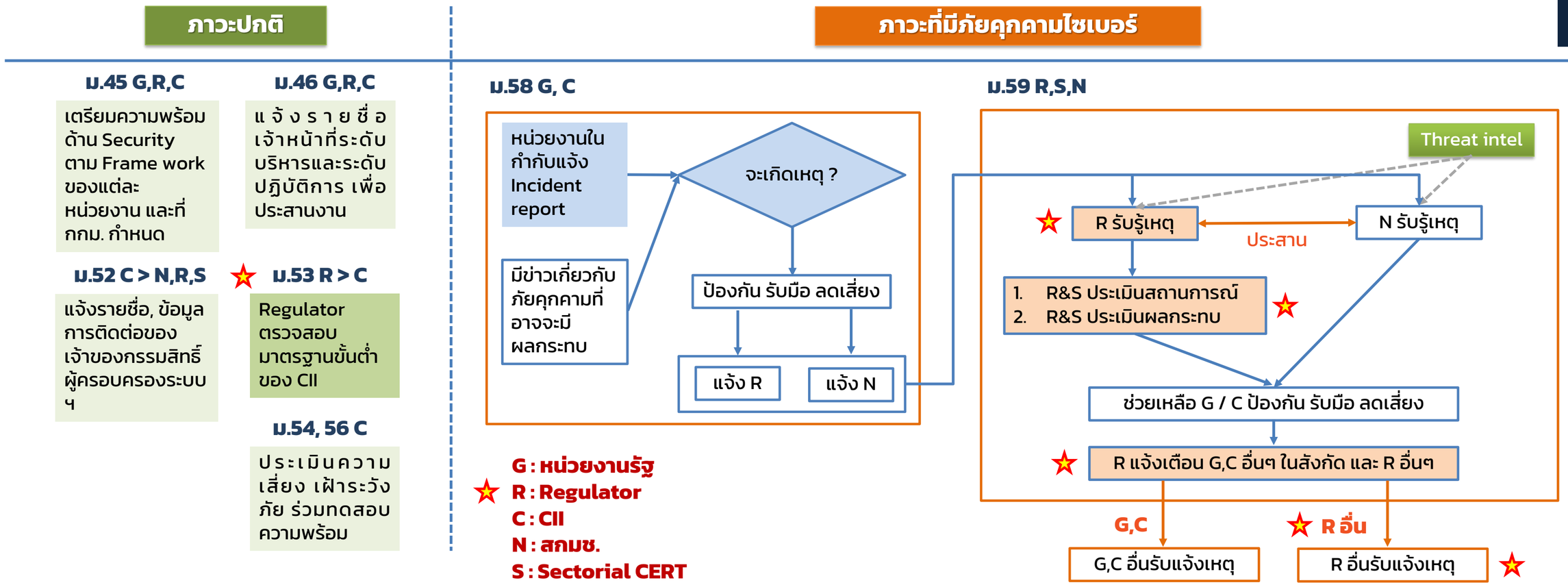
31 ตุลาคม 2566
13.30 - 15.30 น.

กรุณาตอบความคิดเห็นตั้งแต่
20 ตุลาคม - 31 ตุลาคม 2566

Scan QR code เพื่อรับ Link เข้าร่วมการประชุมและศึกษาเอกสารเพิ่มเติม

หน้าที่ของหน่วยงานกำกับดูแล ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

Incident Response Flow ของหน่วยงานกำกับ/หน่วยควบคุม



ภาพแสดงหน้าที่ของหน่วยงานในภาวะปกติ และเกิดภาวะภัยคุกคามทางไซเบอร์

ที่มา : หลักสูตรผู้นำการปฏิบัติ (Lead Implementor) เพื่อให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

หลักการและเหตุผล

ด้วยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้ถูกกำหนดให้เป็นหน่วยงานควบคุมหรือกำกับดูแล ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้หน่วยงานควบคุมหรือกำกับดูแล ต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 44 เพื่อให้บริการภาครัฐมีความมั่นคงปลอดภัยและเป็นไปตามมาตรฐานเดียวกัน

ประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล

พ.ศ. ๒๕๖๔

หมวด ๒

ด้านบริการภาครัฐที่สำคัญ

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีบริการด้านการเงิน	(๑) บริการที่เกี่ยวข้องกับการบริหารการเงินการคลังภาครัฐ (GFMIS)	กระทรวงการคลัง
	(๒) บริการที่เกี่ยวข้องกับการเชื่อมโยงข้อมูลหน่วยงานภาครัฐและภาคธุรกิจสำหรับการนำเข้า - ส่งออกและโลจิสติกส์	กรมศุลกากร
ข้อ ๒ ที่มีการให้บริการโดยตรงแก่ประชาชน	(๑) บริการที่เกี่ยวข้องกับการทะเบียนราษฎร (๒) บริการที่เกี่ยวข้องกับบัตรประจำตัวประชาชน (๓) บริการที่เกี่ยวข้องกับทะเบียนครอบครัว (๔) บริการ Linkage Center (๕) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล (๖) บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง (๗) บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน (๘) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล (๙) บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ	กรมการปกครอง สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ข้อ ๓ ที่มีการให้บริการที่เกี่ยวข้องกับการแจ้งเตือน	(๑) บริการที่เกี่ยวข้องกับการคาดการณ์คุณภาพน้ำและการเตือนภัย (๒) บริการที่เกี่ยวข้องกับการชลประทาน (๓) บริการที่เกี่ยวข้องกับการแพร่ภาพและกระจายเสียงแบบดิจิทัล	กรมชลประทาน

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

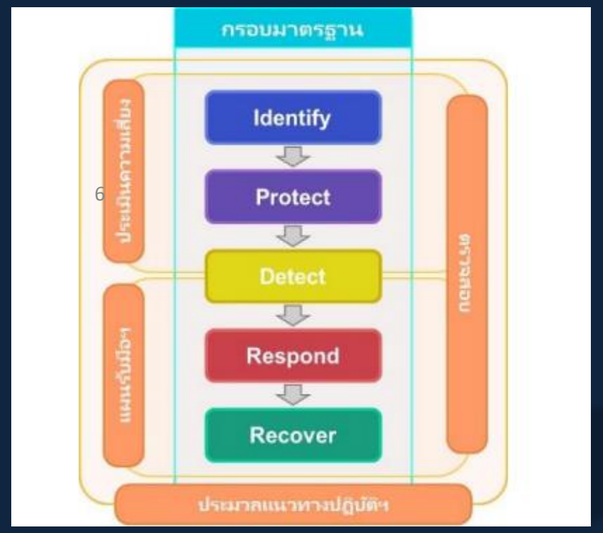
ประกาศประมวลแนวทางปฏิบัติ และ กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

การดำเนินการ

ประกาศว่าประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานควบคุมหรือกำกับดูแล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมวด 2 ด้านบริการภาครัฐที่สำคัญ ลักษณะหน่วยงาน ข้อ 2 ที่มีการให้บริการโดยตรงแก่ประชาชน ภารกิจหรือให้บริการ (Critical Services) (6) บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง (7) บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน (8) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล (9) บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ ถือปฏิบัติ

ประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พ.ศ. ๒๕๖๔



NIST Cybersecurity Framework
NIST SP800-53

(ร่าง) ประกาศแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

(ร่าง) ประกาศแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

หลักการและเหตุผล

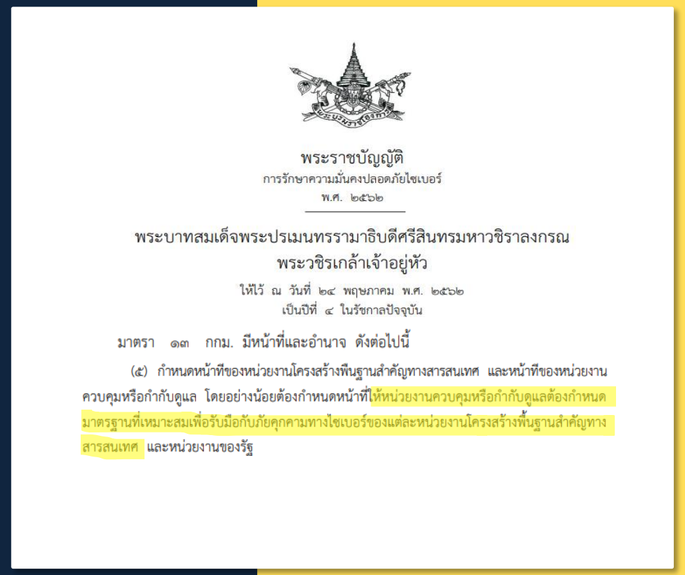
ด้วยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้ถูกกำหนดให้เป็นหน่วยงานควบคุมหรือกำกับดูแล ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้หน่วยงานควบคุมหรือกำกับดูแล ต้องกำหนดมาตรฐานที่เหมาะสม เพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามมาตรา 13 (5)

หน้า ๑๔
เล่ม ๑๓๘ ตอนพิเศษ ๑๙๔ ง ราชกิจจานุเบกษา ๒๓ สิงหาคม ๒๕๖๔

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔

หมวด ๒
ด้านบริการภาครัฐที่สำคัญ

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
	(๖) บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง (๗) บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน (๘) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล (๙) บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)



พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

มาตรา ๑๓ กกม. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๕) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

(ร่าง) ประกาศแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

การดำเนินการ (ต่อ)

ประกาศแผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ที่เป็นมาตรฐานที่เหมาะสม ตามที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด โดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) **เสนอให้เป็นไปตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์** เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 **องค์ประกอบที่ 3 แผนการรับมือภัยคุกคามทางไซเบอร์ โดยมีเนื้อหาอย่างน้อยตาม**

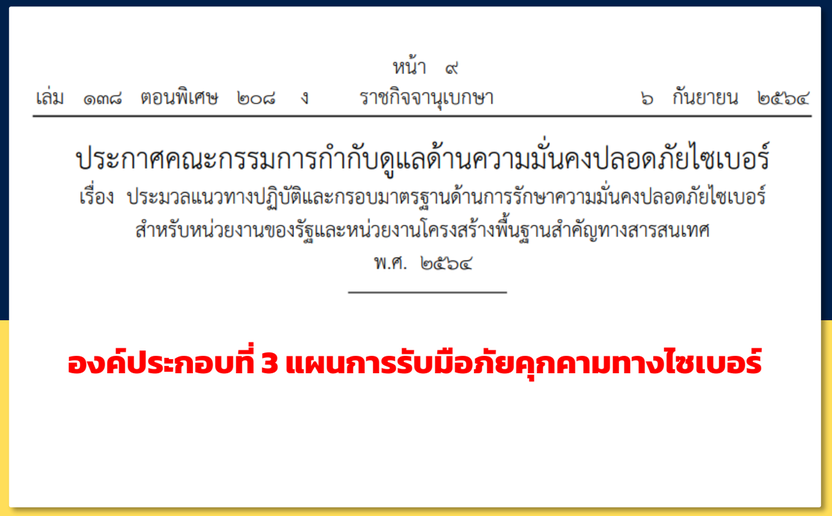
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 และ

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566

(ร่าง) ประกาศแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

การดำเนินการ (ต่อ)

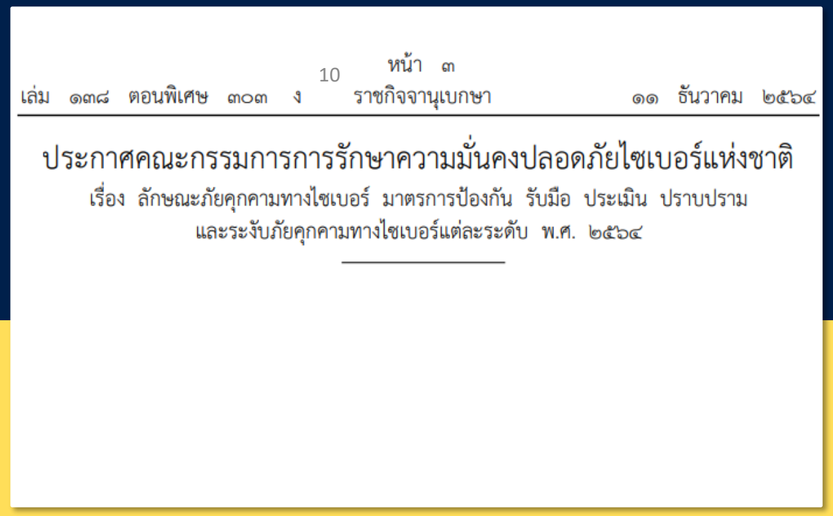
ขอบเขตการกำกับดูแลตามแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมวด 2 ด้านบริการภาครัฐที่สำคัญ ลักษณะหน่วยงาน ข้อ 2 ที่มีการให้บริการโดยตรงแก่ประชาชน ภารกิจหรือให้บริการ (Critical Services) (6) บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง (7) บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน (8) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล (9) บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ ถือปฏิบัติ



หน้า ๙
เล่ม ๑๓๘ ตอนพิเศษ ๒๐๘ ง ราชกิจจานุเบกษา ๖ กันยายน ๒๕๖๔

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พ.ศ. ๒๕๖๔

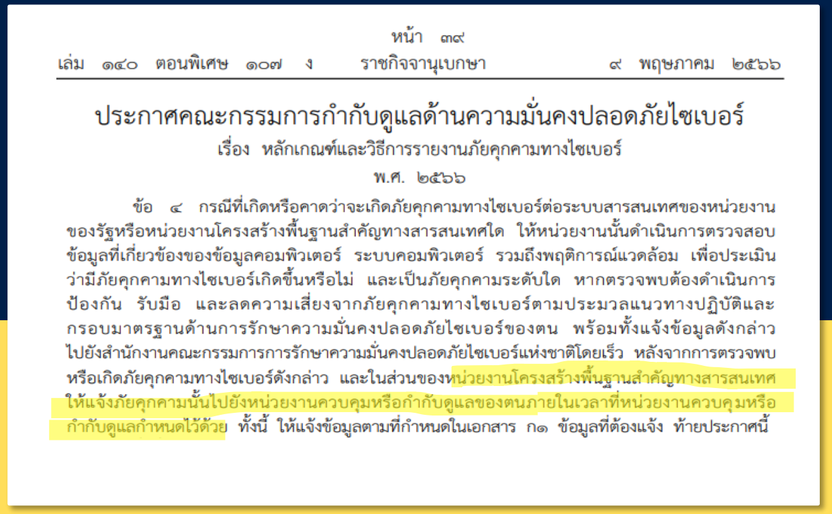
องค์ประกอบที่ 3 แผนการรับมือภัยคุกคามทางไซเบอร์



10

หน้า ๓
เล่ม ๑๓๘ ตอนพิเศษ ๓๐๓ ง ราชกิจจานุเบกษา ๑๑ ธันวาคม ๒๕๖๔

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔



หน้า ๓๙
เล่ม ๑๔๐ ตอนพิเศษ ๑๐๗ ง ราชกิจจานุเบกษา ๙ พฤษภาคม ๒๕๖๖

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์
พ.ศ. ๒๕๖๖

ข้อ ๔ กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ และเป็นภัยคุกคามระดับใด หากตรวจพบต้องดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของตน พร้อมทั้งแจ้งข้อมูลดังกล่าวไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติโดยเร็ว หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์ดังกล่าว และในส่วนของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้แจ้งภัยคุกคามนั้นไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดไว้ด้วย ทั้งนี้ ให้แจ้งข้อมูลตามที่กำหนดในเอกสาร ก๑ ข้อมูลที่ต้องแจ้ง ท้ายประกาศนี้

(ร่าง) ประกาศแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

เอกสารแนบท้ายประกาศ: การกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

ระยะเวลาการแจ้งตามช่องทางที่กำหนดเพื่อพิจารณา

ลักษณะภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา...หลังการแจ้งเบื้องต้น)	การส่งรายงานให้สกมช. (ภายในเวลา...หลังการแจ้งเบื้องต้น)
ระดับไม่ร้ายแรง	24 ชั่วโมง	30 วัน	30 วัน
ระดับร้ายแรง	30 นาที	1 ชั่วโมง	2 ชั่วโมง
ระดับวิกฤติ	15 นาที	30 นาที	1 ชั่วโมง
ช่องทางการติดต่อ	โทรศัพท์ : 0 2612 6000 Contact Center : 0 2612 6060 ไลน์กลุ่ม Regulator & CII	Email: sd-g2_division@dga.or.th ระดับชั้นข้อมูล “ลับมาก” เข้ารหัสข้อมูลแบบ PGP	Email: saraban@ncsa.or.th ระดับชั้นข้อมูล “ลับมาก” เข้ารหัสข้อมูลแบบ PGP

ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์ – ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

อ้างถึง – ภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกซ้อม 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)[๔]
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๒	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๓	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๘ ชั่วโมง
๔	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๕	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๖	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๗	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๑๐ นาที	๑ ชั่วโมง	๑ ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๘	-	๒๐ นาที	ตามเวลาที่ต้องใช้ในการสืบสวน	๔ ชั่วโมง
๙	-	-	๔ ชั่วโมง	๑๒ ชั่วโมง

THANK YOU