แนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ของ สนข.

โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร

สนข www.otp.go.th

แนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

แนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ ของสำนักงานนโยบายและแผนการขนส่งและจราจร

๑. บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือหน่วยงานของรัฐแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็วในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของตน และได้กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์พ.ศ. ๒๕๖๖ กำหนดให้นำหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มาบังคับใช้แก่หน่วยงานของรัฐโดยอนุโลม กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของหน่วยงานของรัฐนั้น

ในการนี้ เพื่อให้ **สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.)** ซึ่งเป็นหน่วยงานของรัฐมีแนวทางปฏิบัติที่ชัดเจนในการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ให้เป็นไปตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ และสอดคล้องกับแนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ของ**สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** จึงได้กำหนดแนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ของ สนข. ขึ้นเพื่อเป็นแนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องต่อไป

๒. วัตถุประสงค์

แนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ของ สนข. มีไว้เพื่อเป็นแนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ของ สนข. ที่ควรปฏิบัติตามเมื่อเกิดสถานการณ์เกี่ยวกับกรณีภัยคุกคามทางไซเบอร์

๓. นิยาม

สนข.	หมายถึง	สำนักงานนโยบายและแผนการขนส่งและจราจร
สกมช.	หมายถึง	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กรณีที่เกิดภัยคุกคาม	หมายถึง	เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ปรากฏข้อเท็จจริงแล้วว่าได้เกิดขึ้นและทำให้เกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ และให้หมายความรวมถึงการกระทำอื่นใดที่มีผลในทำนองเดียวกันทางไซเบอร์

ระบบสารสนเทศ	หมายถึง	คอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ซึ่งอยู่ในความดูแลรับผิดชอบของ สนข.
ช่องทางอิเล็กทรอนิกส์	หมายถึง	ไปรษณีย์อิเล็กทรอนิกส์ ต้องทำการเข้ารหัสด้วย PGP (เป็นอย่างน้อย) หรือด้วยวิธีการทางอิเล็กทรอนิกส์อื่นใด ที่มีความปลอดภัยเทียบเท่าหรือสูงกว่า

๔. แนวทางการในการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์

เพื่อเป็นแนวทางในการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์สำหรับ สนข. ซึ่งเป็นหน่วยงานของรัฐที่มิได้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยสอดคล้องกับขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling) **ขั้นตอนที่ ๒ - ๔** ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ดังนี้

๔.๑ การแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ระหว่างขั้นตอนที่ ๒ : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

๔.๑.๑ การแจ้งเหตุภัยคุกคามทางไซเบอร์ ให้ดำเนินการดังนี้

(๑) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของ สนข. ที่ทำให้บริการของหน่วยงานด้อยประสิทธิภาพลง หรือเสียหายจนไม่สามารถทำงานหรือให้บริการได้ หรือทำให้การทำงานของหน่วยงานล้มเหลว หรือมีเหตุอันควรเชื่อได้ว่าการก่อภัยคุกคามทางไซเบอร์นั้นกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม **ให้หน่วยงานของรัฐแจ้งไปยัง สกมช. ภายใน ๒๔ ชั่วโมง** นับแต่ทราบถึงเหตุภัยคุกคามทางไซเบอร์นั้น และแจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด โดยการนำส่ง**เอกสาร ก๑** ข้อมูลที่ต้องแจ้ง หรือนำส่ง**เอกสาร ก๒** แบบรายงานภัยคุกคามทางไซเบอร์ ที่มีข้อมูลครบถ้วนตามที่กำหนดไว้ใน**เอกสาร ก๑** ข้อมูลที่ต้องแจ้ง ทั้งนี้ให้เพิ่มเติมข้อมูลอื่นใดตามที่ระบุใน**เอกสาร ก๒** เท่าที่สามารถกระทำได้ และจัดส่งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตนผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย และให้ดำเนินการรายงานภัยคุกคามทางไซเบอร์ ตามความในข้อ ๔.๑.๒ (๑)

(๒) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของ สนข. แต่ไม่ส่งผลกระทบในทำนองเดียวกันกับกรณีในข้อ ๔.๑.๑ (๑) ให้หน่วยงานดังกล่าวแจ้งไปยัง สกมช. โดยเร็ว และแจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด โดยการนำส่ง**เอกสาร ก๑** ข้อมูลที่ต้องแจ้ง หรือนำส่ง**เอกสาร ก๒** แบบรายงานภัยคุกคามทางไซเบอร์ ที่มีข้อมูลครบถ้วนตามที่สามารถกระทำได้ และจัดส่งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตนผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย และอาจดำเนินการรายงานภัยคุกคามทางไซเบอร์ ตามความในข้อ ๔.๑.๒ (๒)

๔.๑.๒ การรายงานภัยคุกคามทางไซเบอร์ ให้ดำเนินการดังนี้

(๑) ในกรณีที่เหตุภัยคุกคามทางไซเบอร์นั้น เป็นเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของของ สนข. ให้รายงานไปยัง สกมช. ภายใน ๒๔ ชั่วโมง และรายงานไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดโดยการนำส่ง**เอกสาร ก๒** แบบรายงานภัยคุกคามทางไซเบอร์ หน่วยงานอาจระบุข้อมูลเฉพาะเท่าที่ทราบหรือสามารถระบุได้ในขณะนั้นผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย ทั้งนี้หากมิได้มีการแจ้งภัยคุกคามฯ ตามข้อ ๔.๑.๑ ให้ทำการรายงานตามข้อนี้เป็นการแจ้งเหตุภัยคุกคามไปในคราวเดียวกัน

หากไม่อาจหรือไม่สามารถดำเนินการจัดเตรียมข้อมูลและจัดส่งรายงานได้ภายใน ๒๔ ชั่วโมง ให้แจ้งเหตุขัดข้องดังกล่าวแก่ สกมช. ทราบโดยเร็ว แต่ต้องไม่เกินระยะเวลา ๒๔ ชั่วโมง นับแต่ทราบถึงเหตุภัยคุกคามทางไซเบอร์นั้น

(๒) ในกรณีที่เกิดภัยคุกคามที่มีลักษณะตามข้อ ๔.๑.๑ (๒) สนข. อาจแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์โดยรายงานข้อมูลตามที่กำหนดไว้ใน**เอกสาร ก๒** แบบรายงานภัยคุกคามทางไซเบอร์ไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตน ผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย ทั้งนี้ หากมิได้มีการแจ้งภัยคุกคามฯ ตามข้อ ๔.๑.๑ (๒) ให้นำการรายงานตามข้อนี้เป็นการแจ้งเหตุภัยคุกคามไปในคราวเดียวกัน

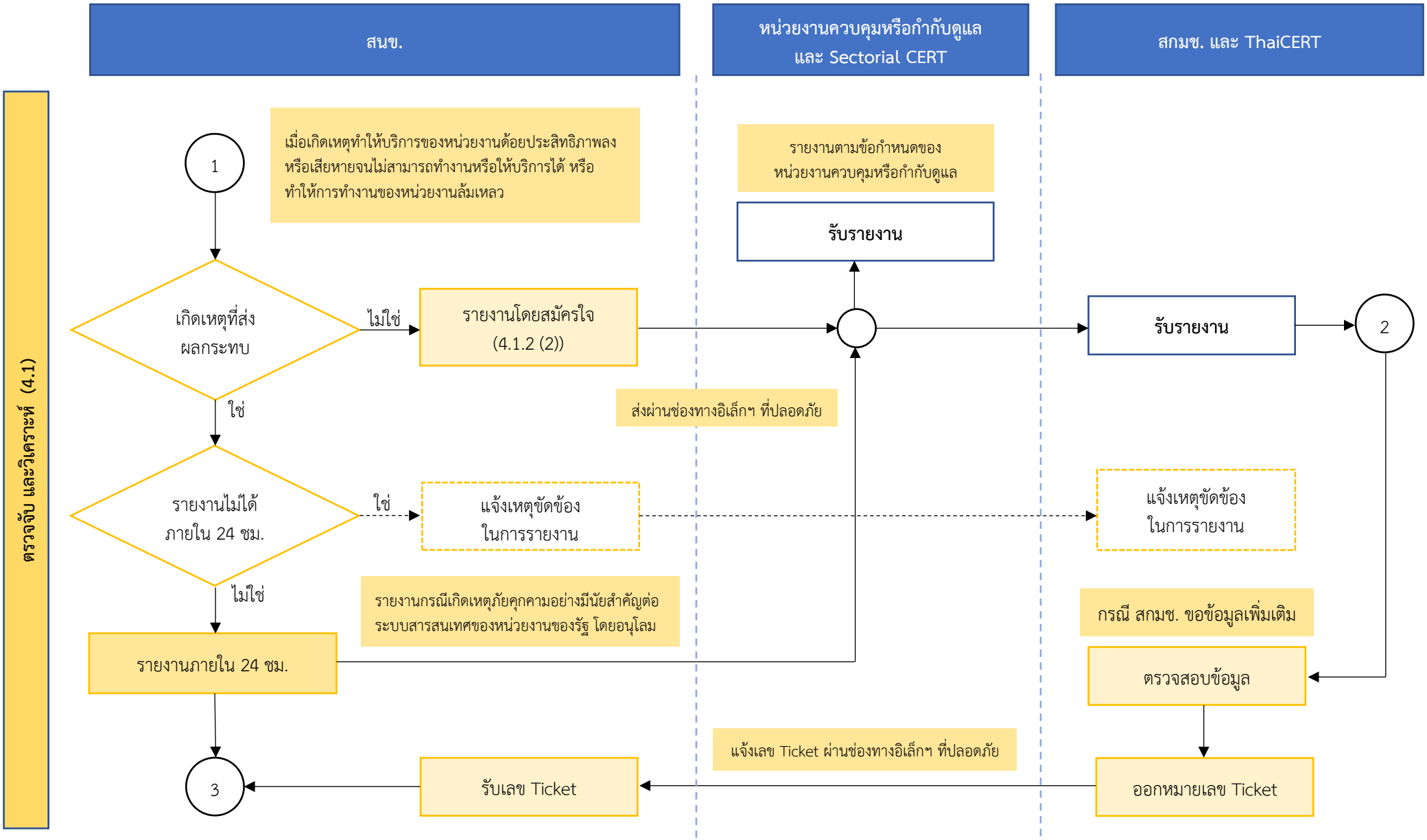
๔.๒ การรายงานเหตุภัยคุกคามทางไซเบอร์เพิ่มเติม ระหว่างขั้นตอนที่ ๓ : การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

กรณี สนข. มีความคืบหน้าหรือมีข้อมูลเพิ่มเติมในระหว่างการระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ อันนอกเหนือจากการรายงานภัยคุกคามทางไซเบอร์ตามกรณี ข้อ ๔.๑.๒ ให้หน่วยงานปรับปรุง**เอกสาร ก๒** แบบรายงานภัยคุกคามทางไซเบอร์ฉบับที่ได้จัดส่งต่อ สมกช. และหน่วยงานควบคุมหรือกำกับดูแลของตน ตามข้อ ๔.๑.๒ ให้สอดคล้องกับข้อมูลที่หน่วยงานได้สืบทราบเพิ่มมากขึ้นในระหว่างการดำเนินการรับมือและแก้ไขภัยคุกคามทางไซเบอร์และจัดส่งรายงานที่ได้ปรับปรุงเพิ่มเติมไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตน ผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย

๔.๓ การรายงานปิดเหตุภัยคุกคามทางไซเบอร์ ระหว่างขั้นตอนที่ ๔ : การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

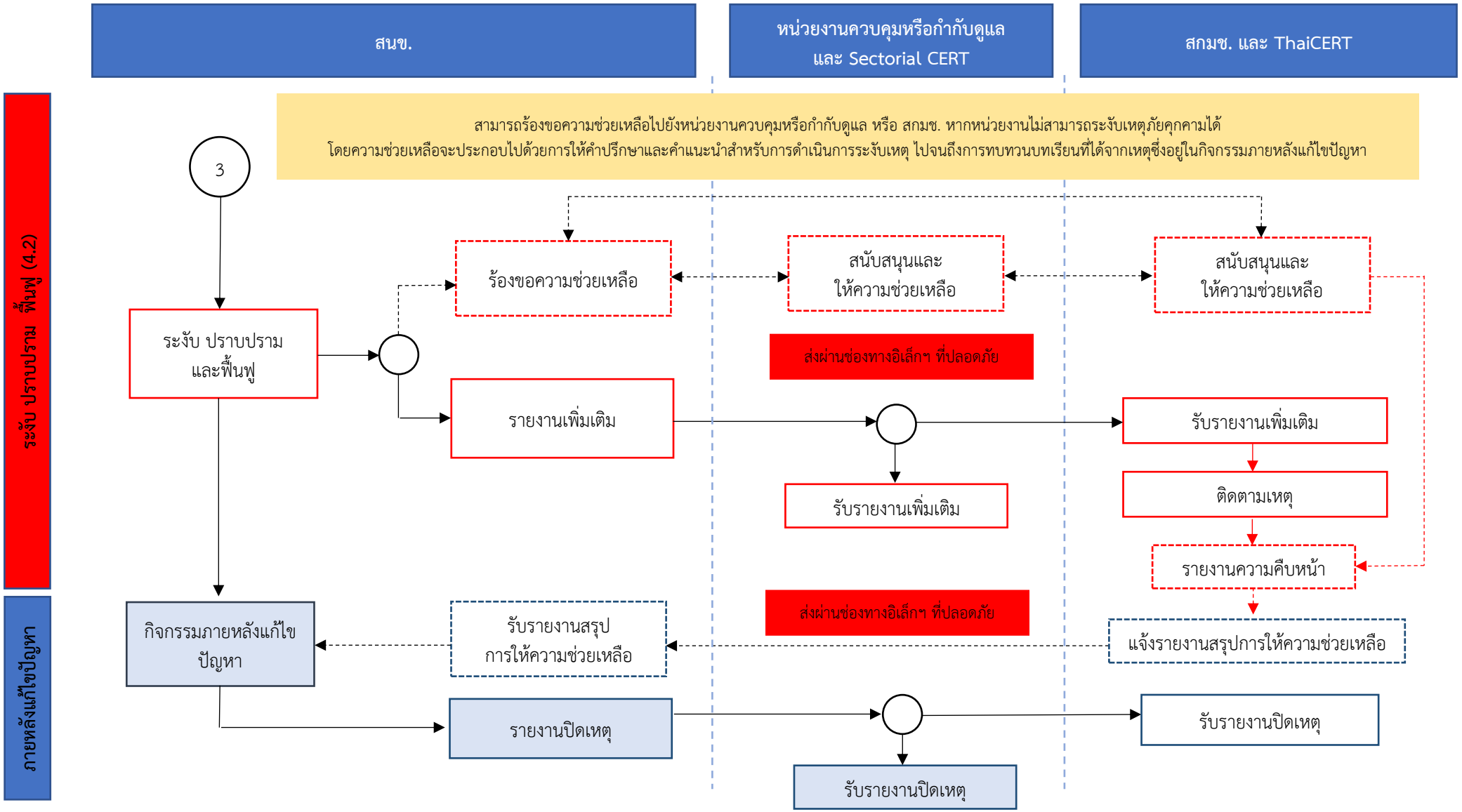
เมื่อเหตุภัยคุกคามทางไซเบอร์ตามกรณีข้อ ๔.๑.๒ สิ้นสุดลง ให้ สนข. เพิ่มเติมข้อมูลลงใน**เอกสาร ก๒** แบบรายงานภัยคุกคามทางไซเบอร์ฉบับที่ได้จัดส่งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตนตามข้อ ๔.๑.๒ ให้ครบถ้วน และจัดส่งรายงานที่ปรับปรุงสมบูรณ์แล้วไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตน ผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย

๕. กระบวนการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์สำหรับหน่วยงานของรัฐ



แนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ ของสำนักงานนโยบายและแผนการขนส่งและจราจร

๕. กระบวนการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์สำหรับหน่วยงานของรัฐ (ต่อ)



๕. ช่องทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์

ลำดับ	หน่วยงาน	ช่องทางการติดต่อสื่อสาร	ความเกี่ยวข้อง
๑	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	เบอร์โทรศัพท์ : ๐ ๒๑๔๒ ๖๘๘๘ email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคารซี) ชั้น ๑๐ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐	หน่วยงานกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ภายในประเทศ
๒	นายจิระพงศ์ เทพพิทักษ์ รองปลัดกระทรวงคมนาคม กระทรวงคมนาคม	เบอร์โทรศัพท์ : ๐ ๒๒๘๓ ๓๑๓๐ email : saraban@mot.go.th ที่อยู่สำนักงาน : ๓๘ ถนนราชดำเนินนอก แขวงวัดโสมนัส เขตป้อมปราบศัตรูพ่าย กรุงเทพฯ ๑๐๑๐๐	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (MCIO) ประจำกระทรวงคมนาคม และหน่วยงานกำกับดูแล
๓	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT)	เบอร์โทรศัพท์ : ๐ ๒๑๔๒ ๓๕๓๑ email : info@turnonsolution.co.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคารซี) ชั้น ๑๐ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐	หน่วยงานเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

ผู้จัดทำร่าง

๑. นายพิสิฏฐ์ ป้อมทอง
นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

๒. นายทรงเกียรติ ตะเภาทอง
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

ที่ปรึกษา

๑. นางสาวจิรังรัก ห้วยหงษ์ทอง
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

๒. นายนฤทธิ์ มัยรัตน์
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร