กรมการขนส่งทางราง
DEPARTMENT OF RAIL TRANSPORT

แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ ประจำปี ๒๕๖๗

มิถุนายน ๒๕๖๗

สารบัญ

หน้า

แผนรักษาความมั่นคงปลอดภัยไซเบอร์

ชื่อระบบ : ระบบสารสนเทศภายในกรมการขนส่งทางราง (ขร.)
หมายเลขอ้างอิง : DRT_Cyber๐๑

รุ่น Version	วันที่จัดทำ	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
๑.๐	มิถุนายน ๒๕๖๗	มิถุนายน ๒๕๖๗	นายอธิภู จิตรานุเคราะห์ (CISO)	ร่างเอกสาร

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมการขนส่งทางราง (ขร.) ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในหัวข้อที่ ๓ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงสมควรจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อประโยชน์ในการดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๒ วัตถุประสงค์

(๑) เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบเทคโนโลยีและสารสนเทศ

(๒) เพื่อกำหนดกระบวนในการเฝ้าระวัง ตรวจสอบ ติดตาม และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์

๑.๓ ขอบเขต

แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของ ขร.

๑.๔ หน้าที่การทบทวนแผน

ขร. มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย กองยุทธศาสตร์และแผนงาน รวมถึง กลุ่มเทคโนโลยีและสารสนเทศ และหน่วยงานภายในกรมต่อไปนี้ สำนักงานเลขานุการกรม กองกฎหมาย กองมาตรฐานความปลอดภัยและบำรุงทาง กองกำกับกิจการขนส่งทางราง กลุ่มพัฒนาระบบบริหาร และ กลุ่มตรวจสอบภายใน

๑.๕ การจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ ฉบับนี้ประกอบด้วยรายละเอียด ๓ ส่วน ได้แก่

ส่วนที่ ๑ รายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง

ส่วนที่ ๒ การควบคุมความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๓ การบริหารแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

โดยมีรายละเอียดแต่ละส่วน ดังต่อไปนี้

ส่วนที่ ๑ รายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง ประกอบด้วย ๑๑ หัวข้อ ดังนี้

๑.๑ ชื่อและหมายเลขอ้างอิงระบบสารสนเทศ โดยหน่วยงานต้องกำหนดชื่อและหมายเลขอ้างอิงเฉพาะระบบ (Unique Identifier) ให้แก่ระบบสารสนเทศทุกระบบ

๑.๒ คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ ได้แก่ คำอธิบาย การทำงาน (Function) และวัตถุประสงค์ของระบบสารสนเทศ

๑.๓ เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ (Senior Information Security Officer) ให้ระบุรายละเอียดของผู้บริหารระดับสูงของหน่วยงานซึ่งเป็นผู้มีหน้าที่และอำนาจบริหาร

จัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) (หรือ Head of Information Security ในกรณีที่หน่วยงานไม่มี CISO) หรือผู้ที่ได้รับมอบหมายให้รับผิดชอบในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศเป็นผู้มีหน้าที่และอำนาจจัดทำและทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยประสานงานร่วมกับเจ้าของระบบสารสนเทศ เจ้าของสารสนเทศ และผู้ที่เกี่ยวข้องกับระบบสารสนเทศ รวมถึงเป็นผู้ประสานงานกับบุคลากรของหน่วยงานในการกำหนดและตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่มีการใช้งานร่วมกัน โดยต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) ชื่อ
(๒) ตำแหน่ง
(๓) หน่วยงาน/ส่วนงาน
(๔) ที่อยู่สำหรับการติดต่อ
(๕) หมายเลขโทรศัพท์
(๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

๑.๔ เจ้าของระบบสารสนเทศ (Information System Owner) ให้ระบุรายละเอียดของผู้รับผิดชอบระบบสารสนเทศ ซึ่งทำหน้าที่เกี่ยวกับการจัดซื้อ พัฒนา บูรณาการ เปลี่ยนแปลงหรือแก้ไข ดำเนินงาน และบำรุงรักษาระบบสารสนเทศในภาพรวม โดยเจ้าของระบบสารสนเทศเป็นผู้มีส่วนในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ ในการช่วยระบุและตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ รวมถึงดำเนินการตามแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ และหากมีการเปลี่ยนแปลงที่สำคัญที่เกี่ยวข้องกับระบบสารสนเทศเกิดขึ้น เจ้าของระบบสารสนเทศต้องดำเนินการแจ้งเจ้าหน้าที่ระดับอาวุโส ด้านความมั่นคงปลอดภัยของสารสนเทศทราบ โดยต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) ชื่อ
(๒) ตำแหน่ง
(๓) หน่วยงาน/ส่วนงาน
(๔) ที่อยู่สำหรับการติดต่อ
(๕) หมายเลขโทรศัพท์
(๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

๑.๕ เจ้าของสารสนเทศ (Information Owner) ให้ระบุรายละเอียดของผู้มีอำนาจโดยกฎหมายหรือโดยการได้รับมอบหมายให้ดำเนินงานเกี่ยวกับสารสนเทศนั้น หรือรายละเอียดของผู้มีหน้าที่รับผิดชอบกำหนดมาตรการควบคุมสำหรับการสร้าง การรวบรวม การประมวลผล การเผยแพร่ และการทำลายสารสนเทศดังกล่าว โดยเจ้าของสารสนเทศควรมีส่วนในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ ในการให้ข้อมูลเกี่ยวกับความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศ และร่วมพิจารณากำหนดหรืออนุญาตสิทธิและประเภทของสิทธิในการเข้าถึงสารสนเทศให้แก่บุคคล (หรือผู้ดำรงตำแหน่ง) หรือหน่วยงาน รวมทั้งช่วยในการระบุและตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ โดยต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) ชื่อ

(๒) ตำแหน่ง

(๓) หน่วยงาน/ส่วนงาน

(๔) ที่อยู่สำหรับการติดต่อ

(๕) หมายเลขโทรศัพท์

(๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

๑.๖ เจ้าหน้าที่ที่มีอำนาจ (Authorizing Official) ให้ระบุรายละเอียดของผู้บริหารระดับสูงขององค์กรซึ่งมีหน้าที่รับผิดชอบในการดำเนินงานระบบสารสนเทศ ในระดับความเสี่ยง (ต่อการดำเนินงาน ภารกิจ หน้าที่ ภาพลักษณ์ หรือทรัพย์สินของหน่วยงานหรือของบุคคล) ที่หน่วยงานยอมรับได้และมีอำนาจอนุมัติหรือรับรองแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือผู้ที่ได้รับมอบหมาย โดยต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) ชื่อ

(๒) ตำแหน่ง

(๓) หน่วยงาน/ส่วนงาน

(๔) ที่อยู่สำหรับการติดต่อ

(๕) หมายเลขโทรศัพท์

(๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคนให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด

๑.๗ ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ (Other Designated Contact) ให้ระบุรายละเอียดของบุคคลที่มีความเกี่ยวข้องกับระบบสารสนเทศ ดังต่อไปนี้

(๑) ผู้ที่สามารถให้ข้อมูลเกี่ยวกับการดำเนินการและคุณลักษณะของระบบสารสนเทศ

(๒) ผู้ที่มีส่วนร่วมในการดำเนินการพัฒนาและปรับปรุงแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) ผู้ที่ได้รับมอบหมายจากบุคคลตาม (๑) หรือ (๒) ให้กระทำการแทน

รายละเอียดของบุคคลตามวรรคหนึ่ง ต้องมีอย่างน้อยดังต่อไปนี้

(๑) ชื่อ

(๒) ตำแหน่ง

(๓) หน่วยงาน/ส่วนงาน

(๔) ที่อยู่สำหรับการติดต่อ

(๕) หมายเลขโทรศัพท์

(๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

๑.๘ การกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ ให้ระบุรายละเอียดเกี่ยวกับการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ (Security Category) ให้แก่ระบบสารสนเทศจากการประเมินและจัดระดับผลกระทบต่อการดำเนินงานของหน่วยงาน ทรัพย์สินของหน่วยงาน หรือความปลอดภัยของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงาน หรือประชาชน ในกรณีที่มีเหตุการณ์ที่เกี่ยวกับความมั่นคง

ปลอดภัยไซเบอร์หรือเหตุภัยคุกคามทางไซเบอร์เกิดขึ้น โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ของระบบย่อยแต่ละระบบภายใต้ระบบสารสนเทศในเรื่อง (๑) การรักษาความลับ (Confidentiality) (๒) การรักษาความถูกต้องครบถ้วน (Integrity) และ (๓) การรักษาสภาพพร้อมใช้งาน (Availability) และใช้ระดับผลกระทบของประเภทข้อมูลตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ในแต่ละเรื่องที่มีระดับผลกระทบมากที่สุด

การกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศตามวรรคหนึ่ง ให้ดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

๑.๙ สถานะของระบบสารสนเทศ ให้ระบุสถานะของระบบโดยเลือกจากสถานะใดสถานะหนึ่งดังต่อไปนี้

(๑) สถานะอยู่ระหว่างการพัฒนา หมายถึง ระบบใหม่ที่อยู่ระหว่างขั้นตอนการออกแบบพัฒนา หรือทดสอบการใช้งาน

(๒) สถานะดำเนินการ หมายถึง ระบบดำเนินการหรือใช้งานในปัจจุบัน

(๓) สถานะอยู่ระหว่างการปรับปรุง หมายถึง ระบบอยู่ระหว่างการปรับปรุง แก้ไขหรือเปลี่ยนแปลง และไม่มีการใช้งาน

๑.๑๐ การเชื่อมต่อระบบสารสนเทศและการใช้งานข้อมูลร่วมกัน ให้ระบุรายละเอียดที่เกี่ยวข้องกับการเชื่อมต่อกับระบบสารสนเทศอื่นในเรื่อง ดังต่อไปนี้

(๑) ชื่อระบบสารสนเทศที่เชื่อมต่อ ชื่อหน่วยงานของระบบสารสนเทศที่เชื่อมต่อ และชนิดของการเชื่อมต่อ (เช่น ผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น)

(๒) รายละเอียดการให้สิทธิในการเชื่อมต่อ ได้แก่ วันที่ การกำหนดคุณลักษณะของระบบสารสนเทศที่เชื่อมต่อ การรับรองมาตรฐานด้านความมั่นคงปลอดภัยและสถานะการรับรองมาตรฐานด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่เชื่อมต่อ และชื่อและตำแหน่งของผู้ได้รับมอบอำนาจของระบบสารสนเทศที่เชื่อมต่อ

๑.๑๑ นโยบาย ระเบียบ หรือกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศ ให้ระบุนโยบาย ระเบียบ หรือกฎหมายที่ส่งผลโดยตรงกับการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

ส่วนที่ ๒ การควบคุมความมั่นคงปลอดภัยไซเบอร์

ให้ระบุรายละเอียดการดำเนินการที่เป็นมาตรฐานขั้นต่ำสำหรับการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ (Minimum Security Control) ตามหลักเกณฑ์ที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ เพื่อให้เหมาะสมกับการกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศตามข้อ ๑.๘

ส่วนที่ ๓ การบริหารงานแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

๓.๑ วันที่ที่จัดทำและลายมือชื่อผู้จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒ วันที่ที่อนุมัติและลายมือชื่อผู้อนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๓ กำหนดเวลาทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ และชื่อผู้รับผิดชอบในการติดตามการทบทวนแผน

๓.๔ สาเหตุการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเลือกจากสาเหตุใดสาเหตุหนึ่ง ดังต่อไปนี้

(๑) จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับแรก หมายถึง การจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นใหม่เป็นครั้งแรก หรือจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นใหม่ทั้งฉบับแทนฉบับเดิม

(๒) ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ตามรอบที่กำหนด หมายถึง การทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่กำหนดไว้ในแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับที่ใช้บังคับอยู่ในขณะนั้น

(๓) ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์เนื่องจากมีการเปลี่ยนแปลง หมายถึง การทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์เนื่องจากมีการเปลี่ยนแปลงที่สำคัญ โดยต้องระบุความเปลี่ยนแปลงดังกล่าวด้วย

ทั้งนี้ กระบวนการทบทวนแผน ขร. จะดำเนินการทุกปี หรือดำเนินการก่อนรอบหนึ่งปี หากมีการเปลี่ยนแปลงที่สำคัญ เช่น มีการเปลี่ยนแปลงระดับความเสี่ยงเพิ่มขึ้นเกินกว่าระดับความเสี่ยงที่ยอมรับได้ กฎหมายที่เกี่ยวข้องกับการจัดทำหรือดำเนินการตามแผนการรักษาความมั่นคงปลอดภัยไซเบอร์มีการเปลี่ยนแปลงในสาระสำคัญ มีการเปลี่ยนแปลงลักษณะของภัยคุกคามทางไซเบอร์ มีการเปลี่ยนแปลงเกี่ยวกับบุคคลที่เกี่ยวข้องกับแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (เช่น การเปลี่ยนแปลงเจ้าของระบบสารสนเทศ ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ หรือเจ้าหน้าที่ที่มีอำนาจ เป็นต้น) ระบบสารสนเทศมีการเปลี่ยนแปลง สถานะของระบบสารสนเทศมีการเปลี่ยนแปลง หรือการเชื่อมต่อระบบสารสนเทศมีการเปลี่ยนแปลง เป็นต้น

บทที่ ๒
การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์
(Good Governance in Cybersecurity)

ส่วนที่ ๑ รายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง

ชื่อ : เว็บไซต์ของกรมการขนส่งทางราง (https://www.drt.go.th/)	
หมายเลขอ้างอิง : DRT_๐๐๐๑	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ - เป็นเว็บไซต์ที่รับผิดชอบด้านการบริหารงานทางด้านรถไฟและระบบขนส่งทางรางต่าง ๆ ในประเทศไทย รวมถึงการสนับสนุนและพัฒนาการขนส่งทางรางให้เป็นอย่างดี	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com
เจ้าของระบบสารสนเทศ*	
ชื่อ	นายณัฐวีร์ พูลสมบัติภิญโญ
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๑-๗๗๑-๒๗๕๕
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	admin@drt.go.th

เจ้าของสารสนเทศ*	
ชื่อ	นายณัฐวีร์ พูลสมบัติภิญโญ
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๑-๗๗๑-๒๗๕๕
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	admin@drt.go.th
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	นายเรืองเดช มังกรเดชสกุล
ตำแหน่ง	ผู้อำนวยการกองยุทธศาสตร์และแผนงาน
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๙-๑๔๒๖๐๕๗
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	ruengdej.man@drt.go.th
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	คุณกันต์นนท์ จงพีร์เพียร
ตำแหน่ง	-
หน่วยงาน/ส่วนงาน	บริษัท กันโด้ จำกัด
ที่อยู่สำหรับการติดต่อ	๕๘๔/๑ สุขุมวิท ๖๕ ถนนสุขุมวิท แขวงพระโขนงเหนือ เขตวัฒนา กทม.๑๐๑๑๐
หมายเลขโทรศัพท์	๐๙๒-๔๙๕-๓๖๕๑
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	P@gundodigital.com

ชื่อ : ระบบสำนักงานอัตโนมัติ (e-office)

หมายเลขอ้างอิง : DRT_๐๐๐๒

คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ

- ระบบที่ถูกพัฒนาขึ้นเพื่อช่วยให้การทำงานภายในสำนักงานเป็นไปอย่างมีประสิทธิภาพและสะดวกสบายยิ่งขึ้น โดยระบบนี้เป็นระบบอิเล็กทรอนิกส์ที่ใช้เทคโนโลยีสารสนเทศและการสื่อสารในการจัดการข้อมูลและกระบวนการทำงานต่าง ๆ ของสำนักงาน โดยในระบบนี้จะมีระบบบริหารวัสดุ ครุภัณฑ์และสินทรัพย์ถาวร ระบบบริหารงานบุคคล ระบบจองรถยนต์อิเล็กทรอนิกส์ และระบบบริหารการประชุมอิเล็กทรอนิกส์ เป็นต้น

เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*

ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com

เจ้าของระบบสารสนเทศ*

ชื่อ	นายณัฐวีร์ พูลสมบัติภิญโญ
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๑-๗๗๑-๒๗๕๕
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	admin@drt.go.th

เจ้าของสารสนเทศ*	
ชื่อ	นายณัฐวีร์ พูลสมบัติภิญโญ
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๑-๗๗๑-๒๗๕๕
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	admin@drt.go.th
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	นายเรืองเดช มังกรเดชสกุล
ตำแหน่ง	ผู้อำนวยการกองยุทธศาสตร์และแผนงาน
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๙-๑๔๒๖๐๕๗
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	ruengdej.man@drt.go.th
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	คุณพิมพ์รพัชร์ ขัติวงค์
ตำแหน่ง	-
หน่วยงาน/ส่วนงาน	บริษัท K&O Systems and Consulting Co.,Ltd.
ที่อยู่สำหรับการติดต่อ	๑๕ Q-Doc Studio ๑๗ ซ.กรุงธนบุรีซอย ๔ แขวงบางลำพูล่าง เขตคลองสาน กทม. ๑๐๖๐๐
หมายเลขโทรศัพท์	๐๖๑-๔๙๔-๖๕๔๔
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	hrm@ko.in.th

ชื่อ : ระบบสำนักงานอัตโนมัติ (e-office) ระยะที่ ๒	
หมายเลขอ้างอิง : DRT_๐๐๐๓	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ - ระบบที่ถูกพัฒนาขึ้นเพื่อช่วยให้การทำงานภายในสำนักงานเป็นไปอย่างมีประสิทธิภาพและสะดวกสบายยิ่งขึ้น โดยระบบนี้จะแตกต่างจาก E-office แรก โดยภายในจะมีระบบต่าง ๆ เช่น ระบบสารบรรณอิเล็กทรอนิกส์ สลิป/หนังสือรับรอง บริหารโครงการ วัสดุ/ครุภัณฑ์คอมพิวเตอร์ เป็นต้น	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com
เจ้าของระบบสารสนเทศ*	
ชื่อ	นายณัฐวีร์ พูลสมบัติภิญโญ
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๑-๗๗๑-๒๗๕๕
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	admin@drt.go.th

เจ้าของสารสนเทศ*	
ชื่อ	นายณัฐวีร์ พูลสมบัติภิญโญ
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๑-๗๗๑-๒๗๕๕
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	admin@drt.go.th
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	นายเรืองเดช มังกรเดชสกุล
ตำแหน่ง	ผู้อำนวยการกองยุทธศาสตร์และแผนงาน
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๙-๑๔๒๖๐๕๗
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	ruengdej.man@drt.go.th
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	คุณชัยสิริ ธนสถิรชัย
ตำแหน่ง	-
หน่วยงาน/ส่วนงาน	บริษัท CDG Systems Ltd.
ที่อยู่สำหรับการติดต่อ	๒๐๒ อาคารซีดีจีเฮ้าท์ ถนนนางลิ้นจี่ แขวงช่องนนทรี เขตยานนาวา กทม. ๑๐๑๒๐
หมายเลขโทรศัพท์	๐๒-๖๗๘-๐๙๗๘
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	marcom.cdgs@cdg.co.th

ชื่อ : ระบบฐานข้อมูลผู้ประกอบการและการออกใบอนุญาตด้านการขนส่งทางรางผ่านระบบดิจิทัล (e-License R)	
หมายเลขอ้างอิง : DRT_๐๐๐๔	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ - เป็นระบบที่สนับสนุนการดำเนินงานด้านการออกใบอนุญาตที่เกี่ยวข้องกับการดำนินกิจการขนส่งทางราง เช่น เรื่องการขอ/ต่ออายุใบอนุญาตขับรถ ใบอนุญาตโรงเรียนสอนขับรถไฟ ใบอนุญาตตัวรถ เป็นต้น	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com
เจ้าของระบบสารสนเทศ*	
ชื่อ	นายกิจติศักดิ์ รำไพรุจิพงศ์
ตำแหน่ง	วิศวกรเครื่องกลชำนาญการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๙-๙๒๑๖๓๖๓
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	Kittisak_rum@drt.go.th

เจ้าของสารสนเทศ*	
ชื่อ	นายกิจติศักดิ์ รำไพรุจิพงศ์
ตำแหน่ง	วิศวกรเครื่องกลชำนาญการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๙-๙๒๑๖๓๖๓
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	Kittisak_rum@drt.go.th
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	นางสาวจีรวรรณ หงสกุล
ตำแหน่ง	ผู้อำนวยการกองกำกับกิจการขนส่งทางราง
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๑-๘๓๘๘๓๐๙
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	gewunn@yahoo.com
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	อาจารย์ศุภวุฒิ มาลัยกฤษณะชาลี
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	มหาวิทยาลัยเกษตรศาสตร์
ที่อยู่สำหรับการติดต่อ	๕๐ ถนนงามวงศ์วาน แขวงลาดยาว เขตจตุจักร กทม. ๑๐๙๐๐
หมายเลขโทรศัพท์	๐๘๖-๐๘๔-๒๔๔๔
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	-

ชื่อ : ฐานข้อมูลจุดตัดทางรถไฟและระบบแผนที่สารสนเทศออนไลน์ของจุดตัดทางรถไฟทั่วประเทศ (DRT-Crossing)	
หมายเลขอ้างอิง : DRT_๐๐๐๕	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ - เป็นระบบข้อมูลจัดตัดทางรถไฟ อุบัติเหตุบริเวณจุดตัด แจ้งจุดตัดเกิดใหม่(ทางลักผ่าน)	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com
เจ้าของระบบสารสนเทศ*	
ชื่อ	นายพลากร กลัดเจริญ
ตำแหน่ง	วิศวกรไฟฟ้าชำนาญการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๖-๘๕๘-๗๒๓๓
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	phalakorn.kla@drt.go.th

เจ้าของสารสนเทศ*	
ชื่อ	นายพลากร กลัดเจริญ
ตำแหน่ง	วิศวกรไฟฟ้าชำนาญการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๖-๘๕๘-๗๒๓๓
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	phalakorn.kla@drt.go.th
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	นายทยากร จันทรางศุ
ตำแหน่ง	ผู้อำนวยการกองมาตรฐานความปลอดภัย
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๑-๘๔๓-๐๔๕๐
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	tayakorn@hotmail.com
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	อาจารย์ศุภวุฒิ มาลัยกฤษณะชาลี
ตำแหน่ง	-
หน่วยงาน/ส่วนงาน	มหาวิทยาลัยเกษตรศาสตร์
ที่อยู่สำหรับการติดต่อ	๕๐ ถนนงามวงศ์วาน แขวงลาดยาว เขตจตุจักร กทม. ๑๐๙๐๐
หมายเลขโทรศัพท์	๐๘๖-๐๘๔-๒๔๔๔
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	-

ชื่อ : ระบบ BKK-Rail	
หมายเลขอ้างอิง : DRT_๐๐๐๖	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ - ระบบที่รวบรวมข้อมูลการเดินทางจากจุดจากจุดนึงไปอีกจุดนึง เช่น ต้องนั่งรถไฟสายสีอะไรต่อด้วยสีอะไร มีเรียงตามเวลาการเดินทางกับเรียงตามราคา	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com
เจ้าของระบบสารสนเทศ*	
ชื่อ	นายวรรธนิธ สุวรรณรัตน์
ตำแหน่ง	นักวิชาการขนส่งชำนาญการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๗-๔๑๕-๙๖๙๑
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	-

เจ้าของสารสนเทศ*	
ชื่อ	นายวรรธนิธ สุวรรณรัตน์
ตำแหน่ง	นักวิชาการขนส่งชำนาญการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๗-๔๑๕-๙๖๙๑
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	-
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	
ที่อยู่สำหรับการติดต่อ	
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	มหาวิทยาลัยมหิดลฯ
ที่อยู่สำหรับการติดต่อ	๙๙๙ ถนนพุทธมณฑลสาย ๔ ต.ศาลายา อ.พุทธมณฑล จ.นครปฐม ๗๓๑๗๐
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	

ชื่อ : ระบบ Rail-KPI	
หมายเลขอ้างอิง : DRT_๐๐๐๗	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ - ข้อมูลสถิติระบบราง ซึ่งให้ผู้ประกอบการสามารถเข้ามา Login เพื่อกรอกข้อมูล แล้วใช้ Power BI ทำ Dashboard แสดงผลออกมา	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com
เจ้าของระบบสารสนเทศ*	
ชื่อ	นายธัญศักดิ์ นกน้อย
ตำแหน่ง	นักวิชาการขนส่งปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๑-๙๙๔-๕๘๕๘
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	-

เจ้าของสารสนเทศ*	
ชื่อ	นายธัญศักดิ์ นกน้อย
ตำแหน่ง	นักวิชาการขนส่งปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๑-๙๙๔-๕๘๕๘
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	-
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	นางสาวจีรวรรณ หงสกุล
ตำแหน่ง	ผู้อำนวยการกองกำกับกิจการขนส่งทางราง
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๘๑-๘๓๘-๘๓๐๙
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	gewunn@yahoo.com
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	บริษัท เอพซิลอน จำกัด
ที่อยู่สำหรับการติดต่อ	๓๓๕ หมู่ ๓ อาคารเอพซิลอน ถนนบางกรวย-ไทรน้อย ต.ลางรักพัฒนา อ.บางบัวทอง จ.นนทบุรี ๑๑๑๑๐
หมายเลขโทรศัพท์	๐๒-๕๗๑๒-๗๕๑ - ๖๐
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	epsilon@epsilon.co.th

ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	-
ตำแหน่ง	-
หน่วยงาน/ส่วนงาน	บริษัท ยูไนเต็ด แอนนาลิสต์ แอนด์ เอ็นจิเนียริ่ง คอนซัลแตนท์ จำกัด
ที่อยู่สำหรับการติดต่อ	๓ ซอยอุดมสุข ๔๑ ถนนสุขุมวิท แขวงบางจาก เขตพระโขนง กทม.๑๐๒๖๐
หมายเลขโทรศัพท์	๐๒-๗๖๓-๒๘๒๘
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	customersupport@uaeconsultant.com
ชื่อ	-
ตำแหน่ง	-
หน่วยงาน/ส่วนงาน	สถาบันเพิ่มผลผลิตแห่งชาติ
ที่อยู่สำหรับการติดต่อ	อาคารยาคูลท์ ๑๐๒๕ ชั้น ๑๒,๑๔ ถนนพหลโยธิน แขวงพญาไท เขตพญาไท กทม.๑๐๔๐๐
หมายเลขโทรศัพท์	๐๒-๖๑๙-๕๕๐๐
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	-
ชื่อ	-
ตำแหน่ง	-
หน่วยงาน/ส่วนงาน	บริษัท อินฟราทรานส์ คอนซัลแตนท์ จำกัด (สำนักงานใหญ่)
ที่อยู่สำหรับการติดต่อ	๓๑๕/๗ พรีเมียมเพลส ๑๐ (เกษตร-นวมินทร์) ถ.สุคนธสวัสดิ์ แขวงลาดพร้าว เขตลาดพร้าว กทม.๑๐๒๓๐
หมายเลขโทรศัพท์	๐๒-๐๒๙-๙๕๔๒
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	infratrans@infratrans.co.th

ชื่อ : ฐานข้อมูลรถขนส่งทางรางในประเทศไทย (http://traindatabase.drt.go.th/train/)	
หมายเลขอ้างอิง : DRT_๐๐๐๘	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ - เป็นระบบที่รวบรวมข้อมูลสเปคตัวขบวนรถไฟ เช่น รุ่น เครื่อง ชนาด เป็นต้น	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com
เจ้าของระบบสารสนเทศ*	
ชื่อ	นายยรรยงค์ ยิ้มแย้ม
ตำแหน่ง	วิศวกรเครื่องกลปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๔-๖๒๑-๙๓๒๖
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	yanyong.yim@drt.go.th

เจ้าของสารสนเทศ*	
ชื่อ	นายยรรยงค์ ยิ้มแย้ม
ตำแหน่ง	วิศวกรเครื่องกลปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๔-๖๒๑-๙๓๒๖
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	yanyong.yim@drt.go.th
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	นายทยากร จันทรางศุ
ตำแหน่ง	ผู้อำนวยการกองมาตรฐานความปลอดภัย
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	
ที่อยู่สำหรับการติดต่อ	
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	

ชื่อ : ระบบ DRT.gdcatalog	
หมายเลขอ้างอิง : DRT_๐๐๐๙	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ - เป็นระบบสำหรับเผยแพร่ชุดข้อมูลสาธารณะ	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	นายอธิภู จิตรานุเคราะห์
ตำแหน่ง	ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
หน่วยงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	-
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	athibhu@gmail.com
เจ้าของระบบสารสนเทศ*	
ชื่อ	นายณัฐวีร์ พูลสมบัติภิญโญ
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๑-๗๗๑-๒๗๕๕
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	admin@drt.go.th

เจ้าของสารสนเทศ*	
ชื่อ	นายณัฐวีร์ พูลสมบัติภิญโญ
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน่วยงาน/ส่วนงาน	กรมการขนส่งทางราง (ขร.)
ที่อยู่สำหรับการติดต่อ	อาคาร ณ ถลาง ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กทม.๑๐๓๐๐
หมายเลขโทรศัพท์	๐๙๑-๗๗๑-๒๗๕๕
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	admin@drt.go.th
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	
ที่อยู่สำหรับการติดต่อ	
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	-
ตำแหน่ง	-
หน่วยงาน/ส่วนงาน	สำนักงานสถิติแห่งชาติ
ที่อยู่สำหรับการติดต่อ	สำนักงานสถิติแห่งชาติ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา อาคารรัฐประศาสนภักดี ชั้น ๒ ถ.แจ้งวัฒนะ เขตหลักสี่ กทม.๑๐๒๑๐
หมายเลขโทรศัพท์	๐๒-๑๔๑-๗๕๐๐-๗๕๐๓
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	saraban@nso.mail.go.th

กรมการขนส่งทางราง (ขร.) มี ฮาร์ดแวร์ด้านความปลอดภัย ดังนี้

ลำดับ	รายการอุปกรณ์	ยี่ห้อ/รุ่น	สถานที่ติดตั้ง	จำนวน(ชุด)
๑	เครื่องคอมพิวเตอร์แม่ข่าย	Lenovo Think System SR๕๕๐	อาคาร ณ ถลาง	๗
๒	อุปกรณ์ป้องกันเครือข่าย	FortiGate ๖๐๐E	อาคาร ณ ถลาง	๑
๓	หน่วยเก็บข้อมูล	Lenovo DE๒๐๐๐H	อาคาร ณ ถลาง	๑
๔	อุปกรณ์เครือข่าย Core Switch	ARUBA ๒๙๓๐F JL๒๕๓A	อาคาร ณ ถลาง	๑
๕	อุปกรณ์สวิตซ์เครือข่าย	ARUBA ๒๙๓๐F JL๒๕๓A/ JL๒๕๔A	อาคาร ณ ถลาง	๙
๖	อุปกรณ์เราเตอร์	CISCO ๔๓๐๐ Series	อาคาร ณ ถลาง	๑
๗	อุปกรณ์ควบคุม การกระจาย Wireless	ARUBA ๗๐๑๐	อาคาร ณ ถลาง	๑

โดยในแต่ละอุปกรณ์ทาง ขร. ได้กำหนดหมายเลขอ้างอิง ดังนี้

ลำดับ	รายการอุปกรณ์	หมายเลขอ้างอิง
๑	เครื่องคอมพิวเตอร์แม่ข่าย	DRT_๐๐๑๑
๒	อุปกรณ์ป้องกันเครือข่าย	DRT_๐๐๑๒
๓	หน่วยเก็บข้อมูล	DRT_๐๐๑๓
๔	อุปกรณ์เครือข่าย Core Switch	DRT_๐๐๑๔
๕	อุปกรณ์สวิตซ์เครือข่าย	DRT_๐๐๑๕
๖	อุปกรณ์เราเตอร์	DRT_๐๐๑๖
๗	อุปกรณ์ควบคุมการกระจาย Wireless	DRT_๐๐๑๗

๒. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

<u>๒.๑. ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในขร.</u>

ขร. ระบุข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในขร. กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยมีผู้รับแจ้งเหตุฯหลัก รวมถึงช่องทางหลักในการติดต่อ และเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดย ขร. กำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ คลอบคลุมตลอดระยะเวลา ๒๔ ชั่วโมง/ ๗ วัน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	คุณภูวิศ รักษาแก้ว	๐๘.๓๐ – ๑๖.๓๐	๐๘xxxxxxxx	ผู้ประสานงานหลัก	ผู้ประสานด้านความมั่นคงลอดภัยไซเบอร์ของ ขร.
๒	คุณณัฐวีร์ พูลสมบัติภิญโญ	๐๘.๓๐ – ๑๖.๓๐	๐๙๑-๗๗๑-๒๗๕๕	ผู้รับผิดชอบโครงการ	- ดูแลเว็บไซต์ ขร. - ดูแลระบบสำนักงานอัตโนมัติ (E-office) - ดูแลระบบสำนักงานอัตโนมัติ (E-office) ระยะที่ ๒
๓	คุณกิจติศักดิ์ รำไพรุจิพงศ์	๐๘.๓๐ – ๑๖.๓๐	๐๘๙-๙๒๑-๖๓๖๓	ผู้รับผิดชอบโครงการ	E-License R
๔	คุณพลากร กลัดเจริญ	๐๘.๓๐ – ๑๖.๓๐	๐ ๙ ๖ - ๘ ๕ ๘ - ๗๒๓๓	ผู้รับผิดชอบโครงการ	DRT Crossing
๕	คุณภูวิศ รักษาแก้ว	๐๘.๓๐ – ๑๖.๓๐	๐๘xxxxxxxx	ผู้รับผิดชอบโครงการ	ดูแลระบบเครือข่าย ขร.
๖	คุณวรรธนิธ สุวรรณรัตน์	๐๘.๓๐ – ๑๖.๓๐	๐๙๗-๔๑๕-๙๖๙๑	ผู้รับผิดชอบโครงการ	ดูแลระบบ BKK-Rail
๗	คุณธัญศักดิ์ นกน้อย	๐๘.๓๐ – ๑๖.๓๐	๐๘๑-๙๙๔-๕๘๕๘	ผู้รับผิดชอบโครงการ	ดูแลระบบ Rail-KPI
๘	คุณยรรยงค์ ยิ้มแย้ม	๐๘.๓๐ – ๑๖.๓๐	๐๙๔-๖๒๑-๙๓๒๖	ผู้รับผิดชอบโครงการ	ดูแลระบบ Traindatabase

๒.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

กรมการขนส่งทางราง ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	คุณวรกร พุ่มเรือง	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของ ขร.
๒	คุณภูวิศ รักษาแก้ว	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	คุณณัฐวีร์ พูลสมบัติภิญโญ คุณสุกฤษฎิ์ คำหอมกุล คุณมนตรี สุดสาย คุณศรัทธา พันธ์พุทธ คุณธีรพัฒน์ ยิ้มเจริญ คุณธรรมสรณ์ อยู่ไพศาล	เจ้าหน้าที่รับมือฯ (Incident lead)	ทำหน้าที่ช่วยเหลือ ขร. ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
๔	คุณภูวิศ รักษาแก้ว	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับที่	ชื่อ นามสกุล	หน้าที่	ความรับผิดชอบ
๑	คุณวรกร พุ่มเรือง	เจ้าหน้าที่จาก ขร.	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๒	Pentest สกมช.	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.
๓	คุณชนินทร์ ธันดา	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.
๔	คุณขวัญสิรี ช่วงวิไล	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.

๕	คุณธีรพัฒน์ ยิ้มเจริญ	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.
๖	คุณภูวิศ รักษาแก้ว	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.

๒.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

ขร. ได้จัดให้มีข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน่วยงานกำกับดูแล (Regulator) THAI – CERT และผู้ให้บริการภายนอกของหน่วยงาน เช่น หน่วยงานผู้ให้บริการด้านการตรวจสอบพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic Investigator) เป็นต้น

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	เบอร์โทรศัพท์ : ๐๒ ๑๔๒ ๖๘๘๘ Email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐ-ประศาสนภักดี (อาคารบี) ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กทม. ๑๐๒๑๐	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	หน่วยงานหลัก
๒	กระทรวงคมนาคม	เบอร์โทรศัพท์ : ๐๒ ๒๘๓ ๓๐๐๐ email : saraban@mot.go.th ที่อยู่ : ๓๘ ถนนราชดำเนินนอก แขวงวัดโสมนัส เขตป้อมปราบศัตรูพ่าย กทม. ๑๐๑๐๐	กระทรวงคมนาคม	หน่วยงานต้นสังกัด
๓	คุณพิมพ์รพัชร์ ขัติวงค์	เบอร์โทรศัพท์มือถือ : ๐๖๑ ๔๙๔ ๖๕๔๔ Email : hrm@ko.in.th ที่อยู่ : ๑๕ Q-Doc Studio ๑๗ ซ.กรุงธนบุรีซอย ๔ แขวงบางลำพูล่าง เขตคลองสาน กทม. ๑๐๖๐๐	K&O Systems and Consulting Co.,Ltd.	E-Office
๔	คุณชัยสิริ ธนสถิรชัย	เบอร์โทรศัพท์ : ๐๒ ๖๗๘ ๐๙๗๘ email : marcom.cdgs@cdg.co.th ที่อยู่ : ๒๐๒ อาคารซีดีจีเฮ้าท์ ถนนนางลิ้นจี่ แขวงช่องนนทรี เขตยานนาวา กทม. ๑๐๑๒๐	CDG Systems Ltd.	E-Office๒
๕	คุณกันต์กมล เสนานนท์	เบอร์โทรศัพท์มือถือ : ๐๘๗ ๗๕๘ ๗๕๐๐ Email : info@npera.co.th ที่อยู่สำนักงาน : ๑๓๘/๔๙ ถนนรังสิต-ปทุมธานี ต.บ้านกลาง อ.เมือง จ.ปทุมธานี ๑๒๐๐๐	บริษัท เอ็นพีร่า จำกัด	MA แม่ข่ายและระบบเครือข่าย

๖	คุณกันต์นนท์ จงพีร์เพียง	เบอร์โทรศัพท์มือถือ : ๐๙๒ ๔๙๕ ๓๖๕๑ Email : P@gundodigital.com ที่อยู่สำนักงาน : ๕๘๔/๑ สุขุมวิท ๖๕ ถนนสุขุมวิท แขวงพระโขนงเหนือ เขตวัฒนา กทม. ๑๐๑๑๐	บริษัท กันโด้ จำกัด	เว็บไซต์กรมฯ
ลำดับ	**ชื่อ - นามสกุล**	**ช่องทางการติดต่อสื่อสาร**	**หน่วยงาน**	**ความเกี่ยวข้อง**
๗	อาจารย์ศุภวุฒิ มาลัยกฤษณะชาลี	เบอร์โทรศัพท์มือถือ : ๐๘๖-๐๘๔-๒๔๔๔ Email : ที่อยู่สำนักงาน : ๕๐ ถนนงามวงศ์วาน แขวงลาดยาว เขตจตุจักร กทม. ๑๐๙๐๐	มหาวิทยาลัยเกษตรศาสตร์	E-License R / DRT Crossing
๘	รองศาสตราจารย์ ดร. วเรศรา วีระวัฒน์	เบอร์โทรศัพท์มือถือ : Email : waressara.wee@mahidol.ac.th ที่อยู่สำนักงาน : คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล	มหาวิทยาลัยมหิดล	BKK Rail
๙	บริษัท เอพซิลอน จำกัด	เบอร์โทรศัพท์มือถือ : ๐๒-๕๗๑๒-๗๕๑ Email : epsilon@epsilon.co.th waressara.wee@mahidol.ac.th ที่อยู่สำนักงาน : ๓๓๕ หมู่ ๓ อาคาร เอพซิลอน ถนนบางกรวย-ไทรน้อย ต.ลาง รักพัฒนา อ.บางบัวทอง จ.นนทบุรี ๑๑๑๑๐	บริษัท เอพซิลอน จำกัด	Rail KPI
๑๐	การรถไฟแห่งประเทศไทย	เบอร์โทรศัพท์ : ๑๖๙๐ Email : sarabanklang@railway.co.th ที่อยู่สำนักงาน : เลขที่ ๑ ถนนรองเมือง แขวงรองเมือง เขตปทุมวัน กทม.๑๐๓๓๐	การรถไฟแห่งประเทศไทย	หน่วยงานที่เกี่ยวข้อง
๑๐	การรถไฟขนส่งมวลชน แห่งประเทศไทย	เบอร์โทรศัพท์ : ๐๒ ๗๑๖ ๔๐๐๐ Email : saraban@mrta.co.th ที่อยู่สำนักงาน : ๑๗๕ ถนนพระราม ๙ เขตห้วยขวาง แขวงห้วยขวาง กทม. ๑๐๓๑๐	การรถไฟขนส่งมวลชน แห่งประเทศไทย	หน่วยงานที่เกี่ยวข้อง
๑๒	บริษัท รถไฟฟ้า ร.ฟ.ท. จำกัด	เบอร์โทรศัพท์ : ๑๖๙๐ Email : cus.redline@srtet.co.th ที่อยู่สำนักงาน : สถานีกลางกรุงเทพ อภิวัฒน์ เลขที่ ๑๐ ถนนกำแพงเพชร แขวงจตุจักร เขตจตุจักร กทม.๑๐๙๐๐	บริษัท รถไฟฟ้า ร.ฟ.ท. จำกัด	หน่วยงานที่เกี่ยวข้อง

๑๓	บริษัท ระบบขนส่งมวลชนกรุงเทพ จำกัด	เบอร์โทรศัพท์ : ๐๒ ๖๑๗ ๗๓๐๐ Email : nuduan@bts.co.th ที่อยู่สำนักงาน : อาคารบีทีเอส ๑๐๐๐ ถนนพหลโยธิน แขวงจอมพล เขตจตุจักร กทม. ๑๐๙๐๐	บริษัท ระบบขนส่งมวลชนกรุงเทพ จำกัด	หน่วยงานที่เกี่ยวข้อง

๒.๔ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

ขร. จัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่า หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (รายละเอียดปรากฏตามภาคผนวก ๑)

บทที่ ๓
การบริหารความเสี่ยง (Risk Management)

ส่วนที่ ๒ การควบคุมความมั่นคงปลอดภัยไซเบอร์

๓.๑ คำนิยาม

ระบบเทคโนโลยีสารสนเทศ หมายถึง เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ อิเล็กทรอนิกส์ อินเทอร์เน็ต อุปกรณ์โทรคมนาคม และบริการทางคอมพิวเตอร์

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า"การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงระดับหน่วยงานของหน่วยงาน โดยการประเมินความเสี่ยง หน่วยงานจะสามารถ:

- ระบุเหตุการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจากการกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในหน่วยงาน การประเมินความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้พนักงานมีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยีและวิธีที่พนักงานดังกล่าวปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

๓.๒ คำนิยามความเสี่ยง

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว ลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงินและการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

การประเมินความเสี่ยง หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

การวิเคราะห์ความเสี่ยง หลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นต่อไปคือ การวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธีเนื่องจากการวัดความเสี่ยงเป็นตัวเลขว่ามีผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก โดยทั่วไปจะวิเคราะห์ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสี่ยง และความถี่ที่จะเกิดหรือโอกาสที่จะเกิดความเสี่ยง

การบริหารความเสี่ยง หมายถึง การบริหารปัจจัยและควบคุมกิจกรรมรวมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดเหตุจากโอกาสที่จะทำให้เกิดความเสียหายจากการดำเนินงานไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายของหน่วยงานเป็นสำคัญ

๓.๓ กระบวนการบริหารจัดการความเสี่ยง

๓.๓.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องของโครงการหรือกิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายในและภายนอกองค์กร

วิธีการระบุความเสี่ยงมีหลายวิธี เช่น

๓.๓.๑.๑ การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๓.๓.๑.๒ การใช้ Checklist

๓.๓.๑.๓ การวิเคราะห์สถานการณ์จากการตั้งคำถาม What-if

๓.๓.๑.๔ การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

ในขั้นตอนนี้ มีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปแบบของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินงานใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จและปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๓.๓.๒ การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมินและการจัดระดับความเสี่ยงประกอบด้วย ๔ ขั้นตอน คือ

๓.๓.๒.๑ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) ซึ่งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต้องกำหนดเกณฑ์ขึ้นซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก (รุนแรงมากที่สุด) สูง (ค่อนข้างรุนแรง) ปานกลาง น้อย และน้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็น ๔ ระดับ (สูง ค่อนข้างสูง ค่อนข้างต่ำ และต่ำ)

๓.๓.๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยที่ระบุไว้มาประกอบโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรง หรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงจะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินผลกระทบ (ความน่าเชื่อถือ/ความพึงพอใจของผู้ใช้บริการ) ดังนี้

ผลกระทบที่จะเกิด	ความเสียหายที่เกิดขึ้น		ระดับคะแนน
	เชิงคุณภาพ	เชิงปริมาณ	
สูงมาก	มีการสูญเสียทรัพย์สินอย่างมาก ผู้บริหารถูกลงโทษทางวินัย	มากกว่า ๑,๐๐๐,๐๐๐ บาท	๕
สูง	มีการสูญเสียทรัพย์สินอย่างมาก ผู้บริหารถูกตำหนิหรือถูกร้องเรียน	มากกว่า ๒๐๐,๐๐๐ บาท ถึง ๑,๐๐๐,๐๐๐ บาท	๔
ปานกลาง	มีการสูญเสียทรัพย์สินมาก เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย	มากกว่า ๕๐,๐๐๐ บาท ถึง ๒๐๐,๐๐๐ บาท	๓
น้อย	มีการสูญเสียทรัพย์สินพอสมควร เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ	มากกว่า ๑๐,๐๐๐ บาท ถึง ๕๐,๐๐๐ บาท	๒
น้อยมาก	มีการสูญเสียทรัพย์สินเล็กน้อย แทบไม่มีผลกระทบเลย	น้อยกว่า ๑๐,๐๐๐ บาท	๑

ที่มา : แผนบริหารความเสี่ยงสถาบันสารสนเทศทรัพยากรน้ำ (องค์การมหาชน) ปีงบประมาณ พ.ศ. 2564

เกณฑ์การประเมินโอกาสของการประเมินความเสี่ยง ดังนี้

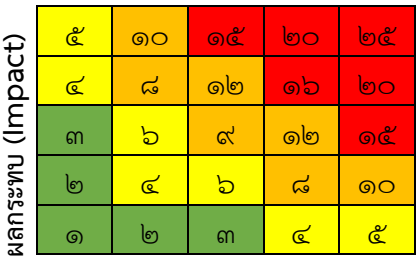
โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้นของความเสี่ยง	ระดับคะแนน
	เชิงปริมาณ	
สูงมาก	มากกว่า ๑ ครั้งต่อเดือน	๕
สูง	ระหว่าง ๑-๖ เดือนต่อครั้ง	๔
ปานกลาง	ระหว่าง ๖-๑๒ เดือนต่อครั้ง	๓
น้อย	มากกว่า ๑ ปีต่อครั้ง	๒
น้อยมาก	มากกว่า ๕ ปีต่อครั้ง	๑

๓.๓.๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงที่จะต้องบริหารจัดการความเสี่ยงก่อน

ระดับความเสี่ยง	ระดับสี	คำอธิบาย	คะแนน
สูง		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	๑๕ - ๒๕

ค่อนข้างสูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป	๘ – ๑๔
ค่อนข้างต่ำ		ระดับที่พอยอมรับได้ แต่ต้องการมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	๔ – ๗
ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม	๑ - ๓

การประเมินความเสี่ยง



๓.๓.๒.๔ การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้แล้ว เลือกความเสี่ยงที่มีระดับสูงหรือค่อนข้างสูงมาจัดทำแผนการบริหารความเสี่ยง

๓.๔ คำนิยามความเสี่ยง

๓.๔.๑ ความเสี่ยง (Risk)

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และ จะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว ลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงินและการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ลักษณะของความเสี่ยง สามารถแบ่งออกได้เป็น ๓ ส่วน ดังนี้

๑) ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง

๒) เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงาน หรือ นโยบาย

๓) ผลกระทบของความเสี่ยง คือ ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

๓.๔.๒ การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

๓.๔.๓ การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุมการยกเลิกและการโอนย้ายหรือแบ่งความเสี่ยง

๓.๔.๔ การควบคุม (Control) หมายถึง นโยบาย แนวทำงานหรือขั้นตอนการปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะและการควบคุมเพื่อการแก้ไข

๓.๔.๕ ทรัพย์สิน (Asset) หมายถึง ทรัพย์สินต่าง ๆ ขององค์แบ่งเป็น ๕ หมวด ได้แก่ หมวดข้อมูล หมวดบุคลากร หมวดฮาร์ดแวร์ หมวดซอฟต์แวร์ และหมวดบริการ

๓.๕ หลักการวิเคราะห์ ประเมิน การจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Tread way Commission) มีดังนี้

๓.๕.๑ การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

เป็นการกำหนดวัตถุประสงค์ของการดำเนินการบริหารจัดการความเสี่ยง ซึ่งจะต้องสอดคล้องกับวิสัยทัศน์ พันธกิจ และยุทธศาสตร์การดำเนินงานขององค์กร ตั้งแต่ระดับองค์กร หน่วยงาน กิจกรรม จนถึงระดับบุคคล เพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าประสงค์ และเพื่อเพิ่มประสิทธิภาพในการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานฯ ที่น่าจะส่งผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย โดยพิจารณาหาแนวทางในการป้องกัน หรือจัดการกับความเสี่ยงเหล่านั้นก่อนที่จะเริ่มปฏิบัติงาน หรือ ดำเนินกิจการตามแผนที่กำหนดไว้ สำหรับวัตถุประสงค์ของการบริหารความเสี่ยงอาจแบ่งออกได้เป็น ๒ ระดับ คือ

๑) วัตถุประสงค์ระดับองค์กร (Corporate Objective) เป็นวัตถุประสงค์ของการดำเนินงานในภาพรวม ตามแผนยุทธศาสตร์และแผนปฏิบัติราชการประจำปีขององค์กร

๒) วัตถุประสงค์ระดับกิจกรรม (Activities Objective) เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจงลงไป สำหรับแต่ละกิจกรรมที่องค์กรกำหนดเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การกำหนดวัตถุประสงค์ที่ชัดเจนช่วยให้การระบุและวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นได้อย่างครบถ้วน ซึ่งวัตถุประสงค์ที่กำหนดขึ้นในแต่ละระดับ ควรมีการกำหนดเป้าหมายและตัวชี้วัดความสำเร็จและสามารถวัดผลได้วัตถุประสงค์ที่ดี (SMART) ควรมีลักษณะ ดังนี้

S	: Specific	หมายถึง	มีการกำหนดเป้าหมายที่ชัดเจน
M	: Measurable	หมายถึง	สามารถวัดผลหรือประเมินผลได้
A	: Achievable	หมายถึง	สามารถปฏิบัติให้บรรลุผลได้

R	: Reasonable	หมายถึง	สมเหตุผล มีความเป็นไปได้
T	: Time constrained	หมายถึง	มีกรอบเวลาที่ชัดเจนและเหมาะสม

๓.๕.๒ การระบุความเสี่ยงต่าง ๆ (Event Identification)

นอกจากการกำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารตามแนวทางของ COSO ออกเป็น ๘ ประเภทแล้ว การระบุความเสี่ยงยังต้องนำหลักธรรมาภิบาลมาเป็นปัจจัยในการวิเคราะห์และระบุความเสี่ยง เพื่อให้เป็นไปตามแนวทางการบริหารกิจการบ้านเมืองที่ดี ประกอบด้วย ๑๐ ประการ ดังนี้

๑) หลักประสิทธิผล (Effectiveness) หมายถึง ผลการปฏิบัติราชการที่บรรลุวัตถุประสงค์และเป้าหมายของแผนปฏิบัติราชการที่ได้รับงบประมาณมาดำเนินการ โดยการปฏิบัติราชการจะต้องมีทิศทางยุทธศาสตร์ และเป้าประสงค์ที่ชัดเจน มีกระบวนการปฏิบัติงาน และระบบงานที่เป็นมาตรฐาน รวมถึงการติดตาม ประเมินผล และพัฒนาปรับปรุงอย่างต่อเนื่องและเป็นระบบ

๒) หลักประสิทธิภาพ (Efficiency) หมายถึง การบริหารราชการตามแนวทางการกำกับดูแลที่ดี มีการออกแบบกระบวนการปฏิบัติงาน โดยการใช้เทคนิคและเครื่องมือการบริหารจัดการที่เหมาะสม ให้องค์กรสามารถใช้ทรัพยากรทั้งด้านต้นทุน แรงงาน และระยะเวลาให้เกิดประโยชน์สูงสุดต่อการพัฒนาขีดความสามารถในการปฏิบัติราชการตามภารกิจ เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกกลุ่ม

๓) หลักการตอบสนอง (Responsiveness) หมายถึง การให้บริการที่สามารถดำเนินการได้ภายในระยะเวลาที่กำหนดและสร้างความเชื่อมั่น ความไว้วางใจ รวมถึง ตอบสนองตามความคาดหวัง/ความต้องการของประชาชนผู้รับบริการ และผู้มีส่วนได้ส่วนเสียที่มีความหลากหลายและมีความแตกต่าง

๔) หลักภาระรับผิดชอบ (Accountability) หมายถึง การแสดงความรับผิดชอบในการปฏิบัติหน้าที่ และผลงานต่อเป้าหมายที่กำหนดไว้ โดยความรับผิดชอบนั้นควรอยู่ในระดับที่สนองต่อ ความคาดหวังของสาธารณะ รวมทั้งการแสดงถึงความสำนึกในการรับผิดชอบต่อปัญหาสาธารณะ

๕) หลักความโปร่งใส (Transparency) หมายถึง กระบวนการเปิดเผยอย่างตรงไปตรงมา ชี้แจงได้เมื่อมีข้อสงสัย และสามารถเข้าถึงข้อมูลข่าวสารอันไม่ต้องห้ามตามกฎหมายได้อย่างเสรีโดยประชาชนสามารถรู้ทุกขั้นตอนในการดำเนินกิจกรรม หรือกระบวนการต่าง ๆ และสามารถตรวจสอบได้

๖) หลักการมีส่วนร่วม (Participation) หมายถึง กระบวนการที่ข้าราชการ ประชาชน และผู้มีส่วนได้ส่วนเสียทุกกลุ่มมีโอกาสได้เข้าร่วมรับรู้ เรียนรู้ ทำความเข้าใจ ร่วมแสดงทักษะ ร่วมเสนอปัญหา/ประเด็นที่สำคัญที่เกี่ยวข้อง ร่วมคิดแนวทาง ร่วมการแก้ไขปัญหา ร่วมในกระบวนการตัดสินใจ และร่วมกระบวนการพัฒนาในฐานะหุ้นส่วนพัฒนา

๗) หลักการกระจายอำนาจ (Decentralization) หมายถึง การถ่ายโอนอำนาจการตัดสินใจ การมอบอำนาจและความรับผิดชอบในการตัดสินใจ และการดำเนินการให้แก่บุคลากร โดยมุ่งเน้นการสร้างความพึงพอใจในการให้บริการต่อผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย การปรับปรุงกระบวนการเพิ่มผลิตภาพเพื่อผลการดำเนินงานที่ดีของส่วนราชการ

๘) หลักนิติธรรม (Rule of Law) หมายถึง การใช้อำนาจของกฎหมาย กฎระเบียบข้อบังคับในการบริหารราชการด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของผู้มีส่วนได้ส่วนเสีย

๙) หลักความเสมอภาค (Equity) หมายถึง การได้รับการปฏิบัติ และได้รับบริการอย่างเท่าเทียมกัน โดยไม่มีการแบ่งแยกด้านชาย/หญิง ถิ่นกำเนิด เชื้อชาติ ภาษา เพศ อายุ ความพิการ สภาพทางกายหรือสุขภาพ สถานะบุคคล ฐานะทางเศรษฐกิจและสังคม ความเชื่อทางศาสนา การศึกษา และอื่น ๆ

๑๐) หลักมุ่งเน้นฉันทามติ (Consensus Oriented) หมายถึง การหาข้อตกลงทั่วไปภายในกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ซึ่งเป็นข้อตกลงที่เกิดจากการใช้กระบวนการ เพื่อหาข้อคิดเห็นจากกลุ่มบุคคลที่รับ

ประโยชน์ และเสียประโยชน์ โดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง ซึ่งต้องไม่มีข้อคัดค้านที่ยุติไม่ได้ในประเด็นที่สำคัญ โดยฉันทามติไม่จำเป็นต้องหมายความว่าเป็นความเห็นพ้องโดยเอกฉันท์

๓.๖ การประเมินความเสี่ยง (Risk Assessment)

เป็นขั้นตอนในการใช้หลักเกณฑ์การให้คะแนนจากระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) มาเป็นเครื่องมือในการประเมินความเสี่ยง และกำหนดกลยุทธ์ที่ใช้จัดการกับความเสี่ยง โดยแบ่งการจัดระดับความเสี่ยง (Degree of Risk) ออกเป็น ๔ ระดับ ตามระดับคะแนน ได้แก่ ระดับความเสี่ยงต่ำ ระดับความเสี่ยงปานกลาง ระดับความเสี่ยงสูง และระดับความเสี่ยงสูงมาก ซึ่งการจัดทำแผนผังระดับความเสี่ยง (Risk Matrix) จะช่วยในการตัดสินใจในการวางแผนความเสี่ยงได้อย่างเหมาะสม และสามารถจัดลำดับความสำคัญในการจัดการได้ ซึ่งการประเมินความเสี่ยงด้วยวิธีการแบ่งการจัดระดับความเสี่ยงมีขั้นตอนดังนี้

๑) การประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood : L) เป็นขั้นตอนการประเมินความเป็นไปได้ความถี่ หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง แล้วจัดแบ่งระดับของโอกาสที่เกิดความเสี่ยง (Likelihood) ออกเป็น ๕ ระดับ ตามตารางที่ ๑

ระดับโอกาส	คำนิยาม
๑	นาน ๆ ครั้ง (แทบไม่เกิดขึ้นเลย)
๒	ไม่บ่อย (อาจเกิดขึ้นได้ทุก ๕ ปี)
๓	ปานกลาง (อาจเกิดขึ้นได้ทุกปี)
๔	บ่อย (อาจเกิดขึ้นได้ทุกเดือน)
๕	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

ตารางที่ ๑ โอกาสจะเกิดความเสี่ยง

๒) การประเมินความรุนแรงของผลกระทบ (Impact : I) เป็นขั้นตอนการประเมินขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง ซึ่งสามารถจัดแบ่งออกเป็นระดับต่าง ๆ ได้จากผลกระทบที่แตกต่างกันซึ่งแสดงตามตารางที่ ๒

ผลกระทบ	คำนิยาม
๑	- เกิดเหตุที่ไม่มีความสำคัญ - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการน้อยมาก (แทบไม่มีผลกระทบเลย)
๒	- เกิดเหตุที่แก้ไขได้ - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการน้อย (เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ)
๓	- ระบบ IT มีปัญหา และมีความสูญเสียไม่มาก - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)
๔	- เกิดปัญหากับระบบ IT ที่สำคัญและระบบความปลอดภัย ซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน

	- กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการมาก (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)
๕	- เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูล - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการมากที่สุด (ผู้บริหารถูกลงโทษทางวินัย)

ตารางที่ ๒ ผลกระทบจากความเสี่ยง

๓) การจัดระดับความเสี่ยง (Degree of Risk) เป็นขั้นตอนการนำผลการประเมินความเสี่ยงที่ประมวลจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) เข้าด้วยกัน (ระดับความเสี่ยง = ระดับโอกาส x ระดับผลกระทบ) แล้วจัดทำแผนผังระดับความเสี่ยง (Risk Matrix)

๓.๗ กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

เป็นการวิเคราะห์ทางเลือกกลยุทธ์ในการจัดการความเสี่ยง เพื่อช่วยในการตัดสินใจของบุคคลหรือองค์กรใด ๆ ในอันที่จะหาวิธีการที่ดีที่สุดในการตัดสินใจแก้ไขปัญหาต่าง ๆ ที่อาจเกิดขึ้นในอนาคต ทั้งนี้เพื่อลดผลกระทบหรือความเสียหายที่อาจเกิดขึ้นให้น้อยที่สุด โดยมีค่าใช้จ่ายน้อยที่สุด ซึ่งมีวิธีการจัดการ ดังนี้

๑) การยอมรับความเสี่ยง (Take/Risk Acceptance) หมายถึง การไม่กระทำใด ๆ เพิ่มเติม กรณีนี้ใช้กับความเสี่ยงที่มีน้อย มีความน่าจะเกิดน้อย หรือเห็นว่ามีต้นทุนในการบริหารความเสี่ยงสูง โดยขออนุมัติหลักการรับความเสี่ยงไว้

๒) การลด (Treat/Risk Reduction) หมายถึง การลดโอกาสที่จะเกิดความเสี่ยง การป้องกันการเกิดความสูญเสีย หรือลดผลกระทบจากเหตุการณ์ที่อาจเกิดขึ้นในอนาคต โดยการจัดระบบการควบคุม การกำหนดแผนสำรองในเหตุฉุกเฉิน การวิเคราะห์ข้อมูลในอดีต ปัจจุบัน ซึ่งรวมถึงการคาดการณ์ในอนาคตประกอบการตัดสินใจ

๓) การหลีกเลี่ยงความเสี่ยง (Terminate/Risk Avoidance) หมายถึง การหยุด หรือ การเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น การงดทำขั้นตอนที่ไม่จำเป็นและจำนำมาซึ่งความเสี่ยง หรือการปรับเปลี่ยนรูปแบบการทำงานและลดขอบเขตการดำเนินการ เป็นต้น

๔) การกระจาย (Transfer/Risk Sharing) หรือโอนความเสี่ยง (Risk Spreading) หมายถึง การลดโอกาสความน่าจะเกิดหรือลดความเสียหายโดยการแบ่งโอน การหาผู้รับผิดชอบในความเสี่ยง การจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน แลการจัดประกันภัย เป็นต้น

๕) การลดความเสี่ยง (Risk Mitigate) หมายถึง การวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง : การใช้ไฟร์วอลล์เพื่อจำกัดทราฟฟิกเครือข่ายเป็นตัวอย่างในการลดความเสี่ยงของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในหน่วยงานจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกเป็นทางการและตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

แนวทางปฏิบัติที่ดีที่สุดสำหรับการลดความเสี่ยง (Best Practices For Risk Mitigation)

- Cybersecurity training programs

- Updating Software
- Privileged access management solutions
- Multi-factor access Authentification
- Dynamic data backup

๓.๘ กิจกรรมการบริหารความเสี่ยง (Control Activities)

เป็นขั้นตอนดำเนินการกำหนดกิจกรรม หรือมาตรการในการจัดการความเสี่ยงให้หมดไป หรือควบคุมความเสี่ยงให้ลดลงในระดับที่ยอมรับได้ โดยกิจกรรมที่กำหนดต้องเป็นกิจกรรมที่ยังไม่เคยปฏิบัติ หรือเป็นกิจกรรมที่กำหนดขึ้นเพิ่มเติมจากกิจกรรมเดิมที่เคยปฏิบัติอยู่แล้ว แต่กิจกรรมนั้นไม่สามารถควบคุมความเสี่ยงได้ นอกจากนี้ยังต้องกำหนดระยะเวลาที่ใช้ในการดำเนินการแต่ละกิจกรรม ตลอดจนหน่วยงานผู้รับผิดชอบ ดังนั้น กิจกรรมการบริหารความเสี่ยงต่าง ๆ ที่กำหนดขึ้นจึงมีเป้าหมายเพื่อควบคุมความเสี่ยง (Risk Control) ซึ่งสามารถแบ่งประเภทของการควบคุมความเสี่ยงออกเป็น ๔ ประเภท ดังนี้

๑) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

๒) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว

๓) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

๔) การควบคุมเพื่อแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขใหม่ไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

ทั้งนี้ การดำเนินกิจกรรมการควบคุมควรต้องคำนึงถึงความคุ้มค่าในด้านค่าใช้จ่าย ต้นทุน และผลประโยชน์ที่คาดว่าจะได้รับ โดยกิจกรรมการควบคุมควรมีองค์ประกอบ ดังนี้

๑) วิธีการดำเนินงาน ซึ่งประกอบด้วยขั้นตอนและกระบวนการ

๒) การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น ซึ่งควรพิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน และพิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

๓) กำหนดระยะเวลาแล้วเสร็จของงาน

๓.๙ ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

เป็นขั้นตอนและกระบวนการโดยมีวัตถุประสงค์เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง มีการเปิดช่องทางการสื่อสาร และรับทราบข้อมูลด้านการบริหารความเสี่ยงให้กับผู้บริหารและบุคลากรขององค์กรได้เข้าถึง โดยผ่านช่องทางต่าง ๆ เช่น ระบบอินทราเน็ต หนังสือเวียน การประชุมชี้แจงโดยผู้บริหาร หรือการฝึกอบรม เป็นต้น ซึ่งการสื่อสารที่มีประสิทธิผลนั้น ต้องให้มั่นใจได้ว่า

๑) ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา

๒) ผู้บริหารสามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่ได้ทันท่วงที

๓) มีการติดตามแผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กรและจัดากรความเสี่ยงต่าง ๆ เพื่อให้องค์กรมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด

๓.๑๐ การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

การติดตาม และเฝ้าระวังความเสี่ยง โดยการกำหนดให้มีการติดตาม และประเมินผลว่าแต่ละหน่วยงานมีการประเมินประสิทธิผลของการจัดการความเสี่ยงที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ เพื่อให้เกิดความมั่นใจว่ามาตรการในการปรับปรุงความเสี่ยงที่วางไว้มีความเพียงพอ เหมาะสม มีประสิทธิภาพประสิทธิผลและมีการปฏิบัติจริง สามารถลดหรือป้องกันความเสี่ยงที่อาจเกิดขึ้น นับเป็นขั้นตอนสุดท้ายและเป็นปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง ซึ่งควรพิจารณาประเด็นต่อไปนี้

๑) การรายงาน และสอบทานขั้นตอนตามกระบวนการบริหารความเสี่ยง เช่น การรายงานและติดตามผลระหว่างการดำเนินงาน (On Going Monitoring) เพื่อสังเกต ติดตาม รายงานความคืบหน้า รวมทั้งสอบทานหรือยืนยันผลระหว่างการปฏิบัติงาน

๒) ความชัดเจนและสม่ำเสมอของการมีส่วนร่วม และความมุ่งมั่นของผู้บริหารระดับสูง

๓) บทบาทของผู้นำในการสนับสนุน และติดตามการบริหารความเสี่ยง

๔) การประยุกต์ใช้เกณฑ์การประเมินผลการดำเนินงานที่เกี่ยวกับการบริหารความเสี่ยง เช่น การประเมินผลอิสระ (Independent Evaluation) ซึ่งเป็นการประเมินผลที่เกิดขึ้นในช่วงเวลาที่แล้วแต่จะกำหนด หรือการประเมินโดยผู้ที่ไม่มีส่วนเกี่ยวข้อง หรือการประเมินการควบคุมด้วยตนเอง (Control Self Assessment : CSA) ซึ่งเป็นการจัดประชุมเชิงปฏิบัติร่วมกัน ระหว่าง ผู้บริหาร ผู้ปฏิบัติงาน ผู้มีความรู้ด้านการควบคุม และผู้อื่นที่มีส่วนเกี่ยวข้อง เป็นต้น

๓.๑๑ ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ขร. ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๘ ประเภท ดังนี้

๓.๑๑.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

๓.๑๑.๒ ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งนั้น

๓.๑๑.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan และ Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

๓.๑๑.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

๓.๑๑.๕ ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้ความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่ต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

๓.๑๑.๖ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่าง ๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

๓.๑๑.๗ ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

๓.๑๑.๘ ความเสี่ยงด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยง เนื่องจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

๓.๑๒ การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุกาณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยง

ความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้น การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่าย เมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๓.๑๓ ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของกรมการขนส่งทางราง ได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๑.๖ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่าง ๆ จากผู้ใช้ภายใน ขร.

๒.๓ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหายใช้งานไม่ได้ หรือหยุดการทำงาน

๓.๑๔ การประเมินความเสียหาย

๓.๑๔.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๓.๑๔.๒ ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๓.๑๕ การติดตามและรายงานผล

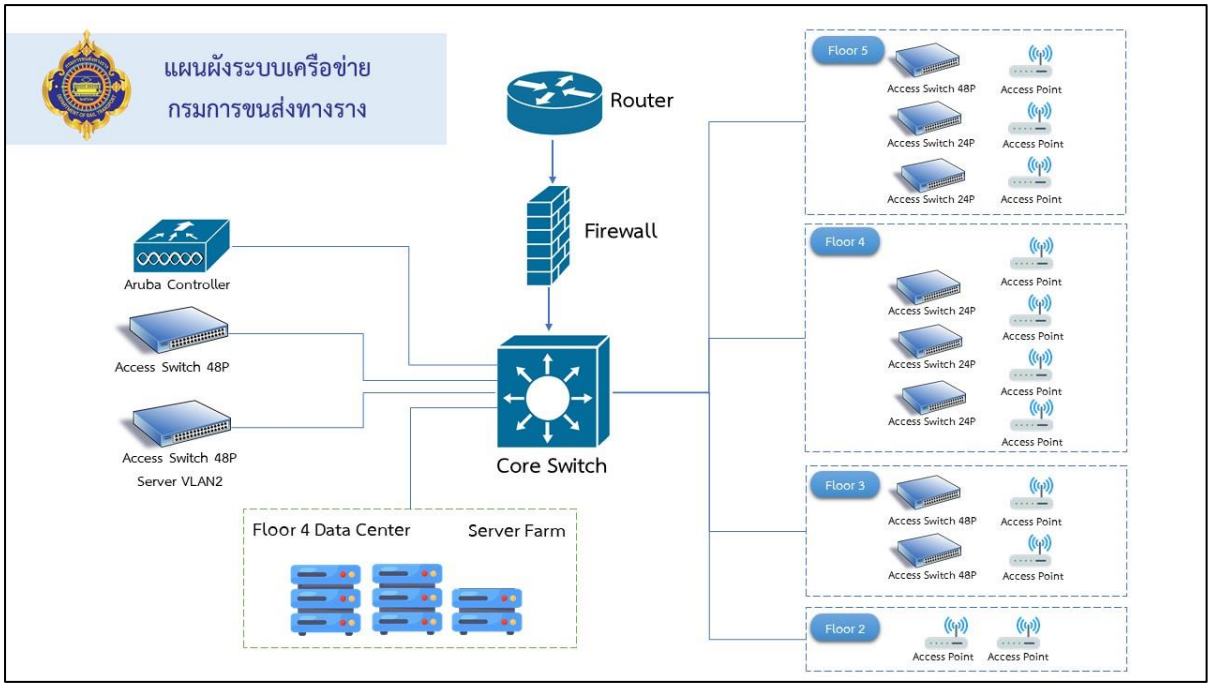
กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

๓.๑๖ ระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของ ขร.

ระบบเครือข่ายคอมพิวเตอร์ของ ขร. ได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) ของ ขร. ตั้งอยู่ที่ อาคาร ณ ถลาง ชั้น ๔ เลขที่ ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กรุงเทพมหานคร และมีเครือข่ายเชื่อมโยงไปยังหน่วยงานในส่วนกลางกระทรวงคมนาคม เพื่อการสื่อสารข้อมูลคอมพิวเตอร์หรือการสื่อสารรูปแบบอื่นในอนาคต

ระบบเครือข่ายคอมพิวเตอร์ของ ขร. มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังระบบเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ในการกรองกลุ่มของข้อมูล (Package Filter) ที่ผ่านเข้ามาภายในระบบเครือข่ายคอมพิวเตอร์ส่วนกลางของ ขร. จากเครือข่ายภายนอก เช่น เครือข่ายของสำนักงานปลัดกระทรวงคมนาคม เครือข่ายอินเทอร์เน็ต เป็นต้น นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ที่ดูแลเครื่องแม่ข่ายทั้งหมดของ ขร. ให้บุคคลภายนอกเข้าถึงได้ เช่น Web Server และ Mail Server เป็นต้น รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของ ขร. เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ระบบเครือข่ายหลักของ ขร. (Core Network) ตั้งอยู่ที่กองยุทธศาสตร์และแผนงาน เป็นศูนย์กลางการเชื่อมต่อทำหน้าที่เชื่อมโยงระบบเครือข่ายภายในระดับสำนัก/กอง/กลุ่ม ในความเร็วระดับ ๑,๐๐๐ Mbps และระบบเครือข่ายภายนอก เช่น อินเทอร์เน็ตเข้าด้วยกัน เป็นต้น

ผังระบบเครือข่ายกรมการขนส่งทางราง

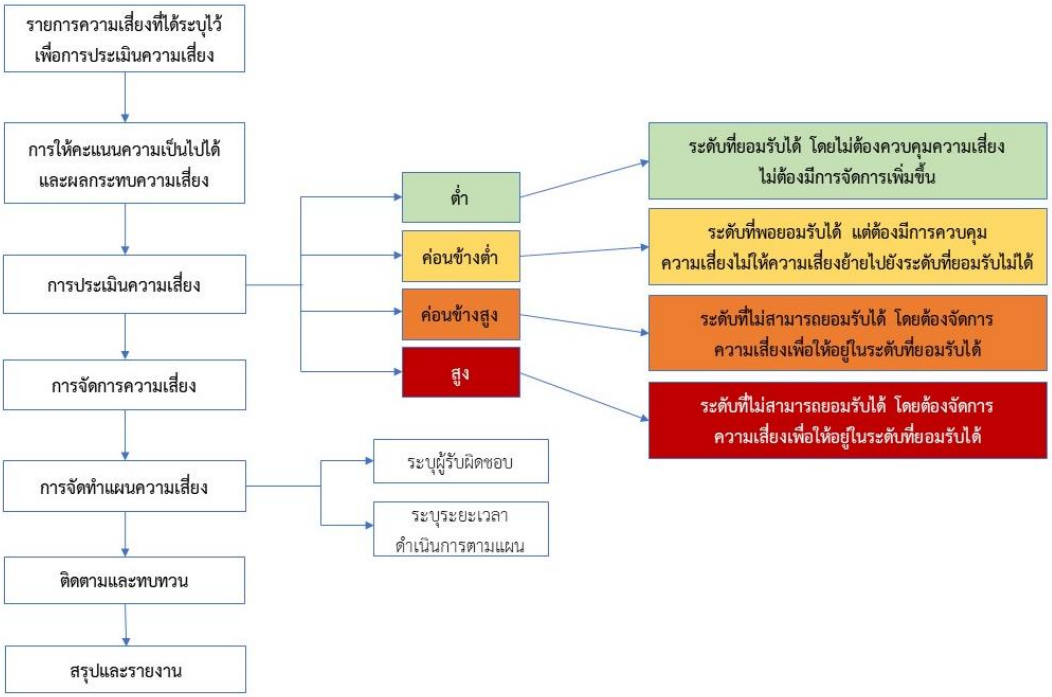

แผนผังระบบเครือข่าย
กรมการขนส่งทางราง
Router
Firewall
Aruba Controller
Access Switch 48P
Access Switch 48P
Server VLAN2
Core Switch
Floor 4 Data Center
Server Farm
Floor 5
Access Switch 48P
Access Point
Access Switch 24P
Access Point
Access Switch 24P
Access Point
Floor 4
Access Point
Access Switch 24P
Access Point
Access Switch 24P
Access Point
Access Switch 24P
Access Point
Floor 3
Access Switch 48P
Access Point
Access Switch 48P
Access Point
Floor 2
Access Point
Access Point

บทที่ ๔

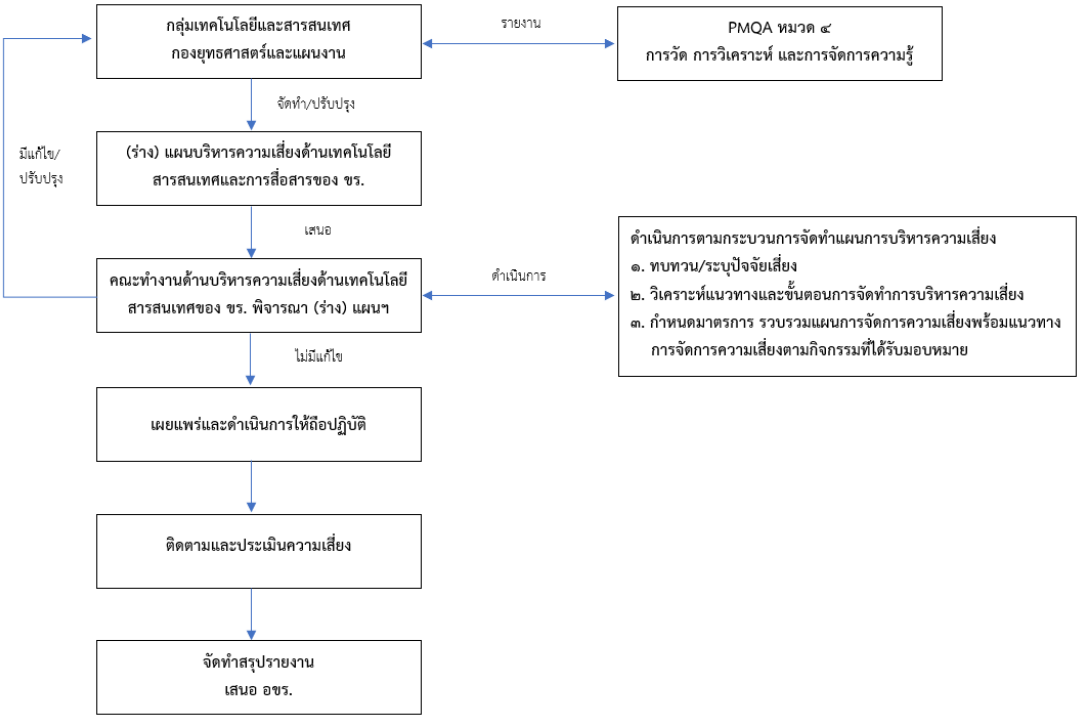
นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

กรมการขนส่งทางราง ได้ตระหนักถึงความสำคัญของข้อมูลที่อยู่ภายใต้การดูแลของหน่วยงานที่อาจเกิดความเสียหายจากปัจจัยต่าง ๆ จึงได้มอบหมายให้กลุ่มเทคโนโลยีและสารสนเทศ (ยส.) จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของ ขร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ – ๒๕๖๘ โดยกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เริ่มต้นจากการรวบรวมข้อมูลกิจกรรมและปัจจัยเสี่ยงที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและทำการศึกษาข้อมูลระดมความคิดเห็นกับเจ้าหน้าที่ผู้ปฏิบัติงานด้านกิจกรรมต่าง ๆ ดังนี้

๔.๑ ขั้นตอนการดำเนินการบริหารจัดการความเสี่ยง



๔.๒ กระบวนการจัดทำแผนบริหารจัดการความเสี่ยง



๔.๓ การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk Identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่ ขร. เผชิญอยู่ โดยมีการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินความเป็นไปได้และผลกระทบ มีดังนี้

ระดับความเสี่ยง	ระดับสี	คำอธิบาย	คะแนน
สูง		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	๑๕ - ๒๕
ค่อนข้างสูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป	๘ – ๑๔
ค่อนข้างต่ำ		ระดับที่พอยอมรับได้ แต่ต้องการมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	๔ – ๗
ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม	๑ - ๓

การประเมินความเสี่ยง

ผลกระทบ (Impact)					
๕	๑๐	๑๕	๒๐	๒๕	
๔	๘	๑๒	๑๖	๒๐	
๓	๖	๙	๑๒	๑๕	
๒	๔	๖	๘	๑๐	
๑	๒	๓	๔	๕	
		โอกาสเกิด			

๔.๓.๑ ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สามารถกำหนดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร จำนวน ๕ ด้าน ดังนี้

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงด้านกายภาพและสภาพแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ				
O๑ ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center)	ความเสี่ยงจากภัย หรือสถานการณ์ฉุกเฉิน	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร หรือการวางเพลิง - ภัยที่เกิดจากธรรมชาติฟ้าผ่า	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูล ถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบคอมพิวเตอร์แม่ข่ายและลูกข่ายหยุด ประมวลผลทั้งระบบ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๒ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ	ความเสี่ยงจากภัย หรือสถานการณ์ฉุกเฉิน	- แหล่งที่ให้บริการกระแสไฟฟ้า ขัดข้อง - แรงดันไฟฟ้าขัดข้อง	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่าย ไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๓ การควบคุมอุณหภูมิ/ ความชื้นภายในห้องปฏิบัติการ ศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	ความเสี่ยงด้านเทคนิค หรือความเสี่ยงจากผู้ปฏิบัติงาน	ควบคุมอุณหภูมิและความชื้น ที่ไม่เหมาะสม	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ ในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๔ ไม่มีแผนต่อเนื่องกรณีเกิด สถานการณ์ภัยพิบัติ/ความไม่สงบ ทางการเมือง/ชุมนุมประท้วง	ความเสี่ยงจากภัย หรือ สถานการณ์ฉุกเฉิน	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	- เจ้าหน้าที่ไม่สามารถเข้าไปปฏิบัติงานได้ตามปกติ เนื่องจากถูกปิดล้อมสถานที่ทำงาน - หน่วยงานถูกตัดกระแสไฟฟ้าทำให้ระบบงาน หยุดทำงานไม่สามารถให้บริการได้ เนื่องจาก ไม่สามารถเข้าระบบจากระยะไกล (Remote) ได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
๒. ความเสี่ยงด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดขึ้นกับระบบเครือข่ายเทคโนโลยีสารสนเทศต่าง ๆ เช่น ระบบเครือข่ายอินเทอร์เน็ต ไวรัสคอมพิวเตอร์ การเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ภัยคุกคามทางคอมพิวเตอร์ต่าง ๆ				
O๕ ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ไม่มีการควบคุมบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
O๖ ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ ขร.	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ไม่มีกำหนดแผนรองรับอุปกรณ์เครือข่าย และระบบแม่ข่ายของ ขร.	ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
O๗ ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งาน	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ไม่มีการควบคุมสิทธิการใช้งานอุปกรณ์เทคโนโลยีสารสนเทศ	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งานได้ - ไม่สามารถหาผู้กระทำความผิดได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
O๘ ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	ความเสี่ยงด้านเทคนิคหรือความเสี่ยงจากผู้ปฏิบัติงาน	- การขัดข้องจากทางผู้ให้บริการอินเตอร์เน็ต - IP Address ไม่เพียงพอสำหรับผู้ใช้งาน - ปริมาณการรับ-ส่งข้อมูล (Bandwidth) ไม่เพียงพอสำหรับการใช้งาน	- เสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote) ได้ - ผู้ใช้งานไม่สามารถเชื่อมต่ออินเทอร์เน็ต	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบระบบสารสนเทศ
O๙ ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่มีการควบคุมอุปกรณ์ที่เชื่อมต่อกับเครือข่ายของหน่วยงาน - จำนวนบุคลากรเพิ่มขึ้น	- ไม่สามารถระบุตัวตนผู้ใช้งานได้ - ไม่สามารถหาผู้กระทำความผิดได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
O๑๐ ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ครุภัณฑ์ อุปกรณ์ ไม่ได้มาตรฐาน การติดตั้งใช้งานไม่สมบูรณ์	- เกิดความเสียหายจากการจัดหาครุภัณฑ์อุปกรณ์ที่ไม่ได้มาตรฐาน - การติดตั้งที่ไม่ได้มาตรฐาน	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
๓. ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล หมายถึง ความเสี่ยงที่เกิดจากการทำงานของระบบสารสนเทศและการจัดเก็บฐานข้อมูลสารสนเทศ ที่อาจเกิดความเสียหายจากการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ ไม่มีการอัปเดตโปรแกรมให้ทันสมัยเพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไข เปลี่ยนแปลงคำสั่ง และการถูกผู้ไม่หวังดีทำลายระบบ (Hacker) ตลอดจนความเสี่ยงจากการถูกบุกรุกข้อมูลการสูญหายของข้อมูลความถูกต้องน่าเชื่อถือของข้อมูลและรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ				
O๑๑ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	ความเสี่ยงด้านเทคนิค หรือความเสี่ยงจากผู้ปฏิบัติงาน	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ไม่มีอำนาจ เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) - ขาดการป้องกันและตรวจจับไวรัสคอมพิวเตอร์ - ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลและระบบฐานข้อมูล - เกิดช่วงโหว่ของซอฟต์แวร์ - ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan)	- ข้อมูลถูกเปลี่ยนแปลงหรือถูกทำลาย - ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๑๒ การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	ความเสี่ยงด้านเทคนิค หรือความเสี่ยงจากผู้ปฏิบัติงาน	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ไม่มีอำนาจ เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) - ขาดการป้องกันและตรวจจับไวรัสคอมพิวเตอร์	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการระบบฯ ต่อประชาชนและผู้ใช้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
		- ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลและระบบฐานข้อมูล - เกิดช่วงโหว่ของซอฟต์แวร์ - ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan)		
O๑๓ การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ไม่มีการกำหนดวิธีการรักษาความปลอดภัยจากการปฏิบัติงานจากระยะไกล	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายได้ต่อระบบ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย
O๑๔ พื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย (Server Storage) หรือระบบฐานข้อมูล (Database) ไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่มีการวางแผนการดำเนินโครงการและอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน - ผู้ใช้งานไม่ปรับปรุงข้อมูลให้เป็นปัจจุบัน	- ไม่มีการวางแผนการดำเนินโครงการและอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน - ผู้ใช้งานไม่ปรับปรุงข้อมูลให้เป็นปัจจุบัน	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๑๕ เกิดช่องโหว่ของซอฟต์แวร์ ขาดการบำรุงรักษา หรือเกิดช่องโหว่ของโปรแกรม	- ความเสี่ยงด้านเทคนิค - ความเสี่ยงจากการดำเนินงานหรือความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่มีการอัปเดตซอฟต์แวร์ให้เป็นปัจจุบัน - ไม่มีการบำรุงรักษาโปรแกรมอย่างต่อเนื่อง	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้ - อาจเกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้อันเกิดจากไม่มีการอัปเดตเวอร์ชั่นใหม่ ๆ อย่างสม่ำเสมอทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง/ในเวลาที่ต้องการ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
O๑๖ ละเมิดลิขสิทธิ์โปรแกรม อรรถประโยชน์ (Utilities Program)	ความเสี่ยงด้านเทคนิค หรือความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับ ในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย
๔. ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ				
O๑๗ การนำเข้าข้อมูลผิดพลาด ไม่ครบถ้วน หรือ ไม่เป็นปัจจุบัน	- ความเสี่ยงด้านการบริหาร จัดการ หรือความเสี่ยง จากเจ้าหน้าที่ผู้ปฏิบัติงาน - ความเสี่ยงด้านการบริหาร จัดการ หรือความเสี่ยง จากเจ้าหน้าที่ผู้ปฏิบัติงาน	- การนำข้อมูลที่ไม่ถูกต้องเข้าสู่ระบบ - ระบบมีความผิดพลาด - การนำข้อมูลที่ไม่ถูกต้องเข้าสู่ระบบ - ไม่มีการตรวจสอบและปรับปรุง ข้อมูลให้เป็นปัจจุบัน	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถออกรายงานได้ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้ถูกต้อง และเป็นปัจจุบัน	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๑๘ การจ้างบุคคลภายนอก ที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษา ระบบ/พัฒนาระบบ	ความเสี่ยงด้านการบริหารจัดการ หรือความเสี่ยงจากเจ้าหน้าที่ ผู้ปฏิบัติงาน	การจ้างบุคคลภายนอก ที่ขาดความรู้ความชำนาญเกี่ยวกับ ระบบที่รับผิดชอบ	ระบบมีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไขทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	- ผู้ใช้งาน - ผู้ดูแลระบบ
O๑๙ บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยี ฯ ไม่เพียงพอ	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ขาดการอบรมบุคลากรด้านไอที - หน่วยงานขาดบุคลากรด้านไอที	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่อง และอาจเกิดความเสียหายทั้งระบบได้ งบประมาณที่ใช้ในการบำรุงรักษามีปริมาณ เพิ่มขึ้นทุกปี	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
O๒๐ ผู้ใช้งาน/Users ไม่มีความรู้ ความชำนาญ และทักษะ การใช้งานระบบ	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่มีการอบรมการใช้งานระบบ แก่ผู้ใช้งาน - ระบบมีความซับซ้อน ยากต่อการใช้งาน	- การใช้ระบบงานไม่เป็นไปตาม Workflow ที่กำหนด ทำให้เกิดข้อขัดข้อง ไม่สามารถ แก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
			- ความล่าช้าในการปฏิบัติงานและเพิ่มปริมาณงานให้กับผู้ดูแลระบบ - ไม่มีการใช้งานทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ/ข้อมูลไม่ถูกนำไปใช้งาน	
O๒๑ การเชื่ออีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- การเปิดไฟล์ หรือ URL ที่แนบมากับอีเมลที่น่าสงสัย - การหลงเชื่อเว็บไซต์ปลอมให้ข้อมูลส่วนตัว หรือลงโปรแกรมที่มาจากแหล่งที่ไม่น่าเชื่อถือ	- โดนหลอกลวงเพื่อขอรหัสผ่าน ข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับ - โดนหลอกเพื่อติดตั้งไวรัสลงบนคอมพิวเตอร์หรือคอมพิวเตอร์แม่ข่าย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๒๒ การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- การเข้าใช้งานระบบจากระยะไกลด้วยเครือข่ายที่ไม่น่าเชื่อถือ - การให้บุคคลที่น่าสงสัยมาใช้งานเครือข่ายเดียวกัน	- โดนดักเก็บข้อมูลการดำเนินการ เช่น รหัสผ่าน ข้อมูลที่เป็นความลับ - เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๒๓ ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ผู้ใช้งานลืมออกจากระบบ - ผู้ใช้งานละเลยเรื่องความปลอดภัยของระบบ	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
๕. ความเสี่ยงในด้านการบริหารจัดการ หมายถึง ความเสี่ยงเนื่องมาจากการได้รับสนับสนุนงบประมาณไม่เพียงพอ การบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี และการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา				
O๒๔ งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	- โดนตัด/ปรับลดโครงการตามนโยบายการปรับลดเงินเป็นร้อยละ	- ลดระยะเวลา ลดคุณภาพและประสิทธิภาพการให้บริการ	หน่วยงานซึ่งเป็นหน่วยรับงบประมาณ

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
		- ทำให้โครงการที่จำเป็นต้องดำเนินการ โดนตัด/ปรับลดไปด้วย	- การประชุมผ่านสื่ออิเล็กทรอนิกส์ไม่สามารถรองรับผู้เข้าร่วมประชุมจำนวนมากเนื่องจากข้อจำกัดของ Package ที่ซื้อ - โครงการที่จำเป็นต้องดำเนินการ โดนตัด/ปรับลดงบประมาณ - งวดเงิน และงวดงาน ไม่สอดคล้องกัน	
O๒๕ ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนปฏิบัติราชการ ขร.	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามตามแผนปฏิบัติราชการ ขร. ได้	- ผู้บริหารปรับลดระยะเวลาดำเนินโครงการ - ไม่สามารถดำเนินงานให้บรรลุเป้าหมายและตัวชี้วัดที่กำหนด	- สำนัก/กอง/กลุ่ม
O๒๖ กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า	ความเสี่ยงจากการดำเนินงานหรือความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่สามารถดำเนินงานได้อย่างต่อเนื่องทันที - การดำเนินการโครงการล่าช้า - การเปลี่ยนแปลงวิธีการระหว่างการดำเนินการ	- เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง - อนุมัติโครงการล่าช้า - ไม่สามารถหาผู้รับจ้างได้ตามแผนดำเนินการ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปี ส่งผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน
O๒๗ ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	ความเสี่ยงจากการออกกฎหมาย/ระเบียบที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ	- กฎหมาย/ระเบียบที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีผลบังคับใช้ - ไม่สามารถดำเนินการตามกฎหมาย/ระเบียบที่เกี่ยวข้องได้ทันภายในระยะเวลาที่กฎหมายกำหนด	- การดำเนินงานไม่สามารถรองรับการปฏิบัติงานตามกฎหมาย/ระเบียบที่บังคับใช้ได้ - ไม่มีระบบสารสนเทศรองรับการดำเนินงานตามที่กฎหมายกำหนด	- สำนัก/กอง/กลุ่ม

๔.๓.๒ ผลประเมินความเสี่ยงและจัดการความเสี่ยง ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

ขร. มีการประเมินผลการควบคุมภายในระดับส่วนราชการ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ดังนี้

ลำดับ	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	คะแนน
๑	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๓	๓	๙
๒	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนปฏิบัติราชการ ขร.	๒	๔	๘
๓	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	๒	๓	๖
๔	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๒	๓	๖
๕	เกิดช่องโหว่ของซอฟต์แวร์	๒	๕	๖
๖	ผู้ใช้งาน/Users ไม่มีความรู้ ความชำนาญ และทักษะ การใช้งานระบบ	๒	๓	๖
๗	การเชื่ออีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	๓	๒	๖
๘	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า	๒	๓	๖
๙	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center)	๑	๑	๕
๑๐	ไม่มีแผนต่อเนื่องกรณีเกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑	๕	๕
๑๑	ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลของข้อมูลและระบบฐานข้อมูลครบถ้วน	๑	๕	๕
๑๒	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑	๕	๕
๑๓	ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	๑	๕	๕
๑๔	ขาดการป้องกันหรือตรวจจับไวรัส	๑	๕	๕
๑๕	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๕	๑	๕
๑๖	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๑	๔	๔
๑๗	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	๒	๒	๔
๑๘	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	๑	๓	๓
๑๙	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	๑	๓	๓
๒๐	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ ขร.	๑	๓	๓
๒๑	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งาน	๑	๓	๓
๒๒	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่าย คอมพิวเตอร์ ขร. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	๑	๓	๓
๒๓	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑	๓	๓
๒๔	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	๑	๓	๓
๒๕	พื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย(Server Storage) หรือระบบฐานข้อมูล(Database) ไม่เพียงพอ	๓	๑	๓
๒๖	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลหรือฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	๑	๓	๓

ลำดับ	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	คะแนน
๒๗	ไม่มีการกำหนดสิทธิ์การเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)	๑	๓	๓
๒๘	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	๑	๓	๓
๒๙	การนำเข้าข้อมูลผิดพลาดทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	๑	๓	๓
๓๐	การนำเข้าข้อมูลไม่ครบถ้วน และไม่เป็นปัจจุบัน	๑	๓	๓
๓๑	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓
๓๒	ผู้บริหารไม่ให้ความสำคัญ ต่อความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร	๑	๓	๓
๓๓	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	๑	๒	๒

จากผลประเมินความเสี่ยงและจัดการความเสี่ยง ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ พบว่ามีปัจจัยเสี่ยงทั้งสิ้น ๓๓ ปัจจัย โดยแบ่งเป็น ปัจจัยเสี่ยงที่มีคะแนนอยู่ในระดับค่อนข้างสูงอยู่ ๒ รายการ ปัจจัยเสี่ยงระดับค่อนข้างต่ำ ๑๕ รายการ และปัจจัยเสี่ยงระดับต่ำ ๑๖ รายการ ต้องจัดการความเสี่ยงดังนี้ ความเสี่ยงระดับค่อนข้างสูง เป็นระดับที่ไม่สามารถยอมรับได้ต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ จึงจำเป็นต้องมีการจัดการความเสี่ยงต่อในปี ๒๕๖๖ - ๒๕๖๘ ความเสี่ยงระดับค่อนข้างต่ำเป็นระดับที่สามารถยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ และความเสี่ยงระดับต่ำเป็นระดับที่สามารถยอมรับได้โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

๔.๔ การประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘

ในปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘ ขร. ได้ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ขร. จำนวน ๒๗ กิจกรรม ดังนี้

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
๑. ความเสี่ยงด้านกายภาพและสภาพแวดล้อม	O๑	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center)	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบคอมพิวเตอร์แม่ข่ายและลูกข่ายหยุดประมวลผลทั้งระบบ	๑	๕	๕	ควบคุมความเสี่ยง	ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะ พร้อมใช้งาน และตรวจสอบระบบดับเพลิงอัตโนมัติ เป็นการจ้างบริษัทดำเนินการบำรุงรักษาเนื่องจากมีความเชี่ยวชาญเฉพาะด้าน
	O๒	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้	๒	๓	๖	ควบคุมความเสี่ยง	ติดตั้งและตรวจสอบระบบสำรองไฟฟ้า (UPS) /แบตเตอรี่สำรองไฟสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และลูกข่าย
	O๓	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	๑	๓	๓	ควบคุมความเสี่ยง	ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้นมีการตรวจสอบสภาพแวดล้อมในห้องและระบบควบคุมอุณหภูมิ/ความชื้นผ่านระบบควบคุมอย่างสม่ำเสมอ
	O๔	ไม่มีแผนต่อเนื่องกรณีเกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	- เจ้าหน้าที่ไม่สามารถเข้าไปปฏิบัติงานได้ตามปกติเนื่องจากถูกปิดล้อมสถานที่ทำงาน - หน่วยงานถูกตัดกระแสไฟฟ้าทำให้ระบบงานหยุดทำงานไม่สามารถ	๑	๔	๔	ควบคุมความเสี่ยง	- จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan) - ปรับปรุงแผน/ใช้แผนบริหารความต่อเนื่อง Business

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
			ให้บริการได้ เนื่องจากไม่สามารถเข้าระบบจากระยะไกล (Remote) ได้					Continuity Plan (BCP) ของ ขร. ให้เป็นปัจจุบัน
๒. ความเสี่ยงด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ	O๕	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย	๑	๓	๓	ควบคุมความเสี่ยง	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์ของ ขร.
	O๖	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ ขร.	ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้ เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	๑	๓	๓	ควบคุมความเสี่ยง	- มีแผนการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตาม และสรุปผลการปฏิบัติงานทุก ๖ เดือน - จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ - ทดสอบการโจมตีตามแผนที่กำหนดจริง
	O๗	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งาน	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งานได้ - ไม่สามารถหาผู้กระทำความผิดได้	๑	๓	๓	ควบคุมความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ มีการทบทวนสิทธิ์เป็นประจำทุก ๖ เดือน โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
								- มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก ๖ เดือน
	O๘	ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	- เสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote) ได้ - ผู้ใช้งานไม่สามารถเชื่อมต่ออินเทอร์เน็ต	๓	๓	๙	ควบคุมความเสี่ยง	- ระบุข้อกำหนด/ข้อตกลงระดับการให้บริการที่ชัดเจนกับผู้ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล - มีสัญญาการบำรุงรักษาและการแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนทุกครั้งที่ขัดข้องเพื่อให้แก้ปัญหาได้ทันที - กำหนดช่วง IP Address สำหรับอุปกรณ์ที่เชื่อมต่อเครือข่ายไร้สาย - ทำการติดตั้งสายสายสัญญาณให้เพียงพอต่อการใช้งาน
	O๙	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน	๑	๓	๓	ควบคุมความเสี่ยง	- มีการยืนยันตัวตนเมื่อมีการเข้าใช้งานเครือข่าย - มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
	O๑๐	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	- เกิดความเสียหายจากการจัดหาครุภัณฑ์ อุปกรณ์ที่ไม่ได้มาตรฐาน - การติดตั้งที่ไม่ได้มาตรฐาน	๑	๓	๓	ควบคุมความเสี่ยง	- ทำการตรวจสอบลักษณะของงานเพื่อจัดหาอุปกรณ์ที่เหมาะสม - ตรวจสอบมาตรฐานของอุปกรณ์
๓. ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล	O๑๑	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	๓	๓	๙	ควบคุมความเสี่ยง	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - ติดตั้ง Patch ของระบบ ปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผลทุก ๓ เดือน

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
	O๑๒	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการระบบฯ ต่อประชาชนและผู้ใช้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	๑	๔	๔	ควบคุมความเสี่ยง	- ติดตั้งโปรแกรมป้องกันไวรัสและ Patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศทุก ๖ เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - จัดทำการสำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมออย่างน้อยเดือนละ ๑ ครั้ง
	O๑๓	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายได้ต่อระบบ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้	๑	๕	๕	ควบคุมความเสี่ยง	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง
	O๑๔	พื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย (Server Storage)	- ไม่มีการวางแผนการดำเนินโครงการและอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน	๓	๑	๓	ควบคุมความเสี่ยง	- คอยตรวจสอบพื้นที่คงเหลือของฐานข้อมูล และคอมพิวเตอร์แม่ข่าย

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
		หรือระบบฐานข้อมูล (Database) ไม่เพียงพอ	- ผู้ใช้งานระบบไม่นำข้อมูลที่ไม่ได้ใช้งานออกจากระบบ					- กำหนดขนาดพื้นที่การจัดเก็บไฟล์ของผู้ใช้งาน
	O๑๕	เกิดช่องโหว่ของซอฟต์แวร์ขาดการบำรุงรักษาหรือเกิดช่องโหว่ของโปรแกรม	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้ - อาจเกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้ อันเกิดจากไม่มีการอัปเดตเวอร์ชันใหม่ ๆ อย่างสม่ำเสมอทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง/ในเวลาที่ต้องการ	๒	๒	๔	ควบคุมความเสี่ยง	-ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่าง ๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง - ทำแผนการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่อง
	O๑๖	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	๑	๓	๓	ควบคุมความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศและการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง จัดทำและส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
๔. ความเสี่ยงด้านบุคลากร	O๑๗	การนำเข้าข้อมูลผิดพลาด ไม่ครบถ้วน หรือ ไม่เป็นปัจจุบัน	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถออกรายงานได้ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	๑	๓	๓	ควบคุมความเสี่ยง	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลของ ขร. เพื่อควบคุมคุณภาพข้อมูล ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ
	O๑๘	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	มีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไขทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	๑	๓	๓	ควบคุมความเสี่ยง	- มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน - มีการจัดทำแผนงาน ขั้นตอนการทำงานที่ชัดเจน และควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้ - มีการติดตามเพื่อป้องกันการผิดพลาดและให้เกิดการแก้ไขปัญหาได้ทันที โดยมีการประชุมทุกสัปดาห์
	๑๙	บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้เพิ่มค่าใช้จ่ายในการบำรุงรักษามากยิ่งขึ้น	๑	๒	๒	ควบคุมความเสี่ยง	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้างบุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน เพื่อจัดอบรมให้กับบุคลากร

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
								- มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรในตำแหน่งที่ว่าง
	๒๐	ผู้ใช้งาน/Users ไม่มีความรู้ความชำนาญและทักษะการใช้งานระบบ	- การใช้ระบบงานไม่เป็นไปตาม Workflow ที่กำหนด ทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้ การปฏิบัติงานติดขัด - ความล่าช้าในการปฏิบัติงานเพิ่มภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งานทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ	๒	๓	๖	ควบคุมความเสี่ยง	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีระบบ Call Center สำหรับให้คำปรึกษา เกี่ยวกับการใช้งานระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุงหรือตามความต้องการของ User
	O๒๑	การเชื่ออีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	- โดนหลอกลวงเพื่อขอรหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับ - โดนหลอกเพื่อติดตั้งไวรัสลงบนคอมพิวเตอร์หรือคอมพิวเตอร์แม่ข่าย	๓	๒	๖	ควบคุมความเสี่ยง	- จัดอบรมให้ความรู้แก่บุคลากรในองค์กร - คอยแจ้งข่าวสารให้บุคลากรในองค์กรทราบเมื่อพบอีเมล หรือหน้าเว็บไซต์ปลอม
	O๒๒	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	- โดนดักเก็บข้อมูลการดำเนินการ เช่น รหัสผ่าน ข้อมูลที่เป็นความลับ - เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้	๑	๒	๒	ควบคุมความเสี่ยง	จัดอบรมให้ความรู้แก่บุคลากรในองค์กร

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
	O๒๓	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้	๕	๑	๕	ควบคุมความเสี่ยง	- ให้ระบบดำเนินการออกจากระบบเมื่อผู้ใช้ไม่มีการเคลื่อนไหวในระยะเวลาที่กำหนด
๕. ความเสี่ยงในด้านการบริหารจัดการ	O๒๔	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	- ลดระยะเวลา ลดคุณภาพและประสิทธิภาพการให้บริการ - ไม่รองรับการประชุมเมื่อมีผู้ขอเข้าประชุมจำนวนมากของโปรแกรมประชุมทางไกล - โครงการที่จำเป็นต้องดำเนินการโดนตัด/ปรับลดงบประมาณ - งวดเงิน และงวดงาน ไม่สอดคล้องกัน	๓	๒	๖	ควบคุมความเสี่ยง	- หน่วยงานวิเคราะห์งบประมาณต้องมีการดำเนินการตัดปรับลดโดยมีการจัดทำความเสี่ยงและการให้น้ำหนักของความสำคัญของโครงการที่ใช้หมวดเงินประเภทเดียวกัน - ปรับลดโครงการตามลำดับความสำคัญและลดปริมาณหน่วยบริการ - ปรับแผนการดำเนินงานตามแผนการใช้จ่ายงบประมาณตามงวดงานที่ได้รับ
	O๒๕	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนปฏิบัติราชการ ขร.	- ผู้บริหารไม่อนุมัติให้ดำเนินโครงการเนื่องจากมีความเห็นว่าเป็นระยะเวลาที่จะสิ้นสุดปีงบประมาณ - ไม่สามารถอบรมให้บรรลุเป้าหมายและตัวชี้วัดที่กำหนด - การดำเนินงานไม่สัมฤทธิผล	๑	๒	๒	ควบคุมความเสี่ยง	- บรรจุโครงการแผนปฏิบัติการให้ผู้บริหารเห็นชอบแผน - กำหนดกรอบเวลาให้ชัดเจนและอยู่ในกรอบเวลาที่สามารถดำเนินการได้ - กำหนดกลุ่มเป้าหมายที่ชัดเจน

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
	O๒๖	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน	- เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง - อนุมัติโครงการล่าช้า - ไม่สามารถหาผู้รับจ้างได้ตามแผนดำเนินการ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปี ส่งผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	๒	๓	๖	ควบคุมความเสี่ยง	- จัดทำแผนปฏิบัติการและดำเนินการ ให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการอย่างจริงจัง กรณีผู้บริหารอนุมัติโครงการล่าช้า ต้องขอวาระชี้แจงเหตุผลความจำเป็นและจัดลำดับความสำคัญ/ความเร่งด่วน - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด
	O๒๗	ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	- การดำเนินงานไม่สามารถรองรับการปฏิบัติงานตามกฎหมาย/ระเบียบที่บังคับใช้ได้ - ไม่มีระบบสารสนเทศรองรับการดำเนินงานตามที่กฎหมายกำหนด	๒	๔	๘	ควบคุมความเสี่ยง	- ติดตามประกาศ/กฎหมาย/ระเบียบที่เกี่ยวข้อง - จัดลำดับความสำคัญและวางแผนการดำเนินงาน

๔.๕ แผนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘

จากการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘ สามารถนำมาจัดทำแผนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘ โดยพิจารณาจากระดับคะแนนความเสี่ยงสูง มีระยะเวลาดำเนินการระหว่างเดือนตุลาคม ๒๕๖๕ – กันยายน ๒๕๖๘ ได้ดังนี้

ประเด็นความเสี่ยง/กิจกรรม	กิจกรรมตามแนวทางการจัดการความเสี่ยง	เป้าหมาย/ผลสำเร็จของการดำเนินการกิจกรรมตามแนวทางการจัดการความเสี่ยง	ปี ๒๕๖๕	ปี ๒๕๖๖				ปี ๒๕๖๗				ปี ๒๕๖๘			ผู้รับผิดชอบ
			ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	
ด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รหัส ๐๘ ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	- ดำเนินการขอเพิ่มปริมาณการรับ-ส่งข้อมูล (Bandwidth) ของเครือข่ายให้เพียงพอสำหรับผู้ใช้งาน - ติดตั้งสายสัญญาณให้ทั่วถึง - กำหนดจำนวนการเชื่อมต่ออุปกรณ์ต่อผู้ใช้งาน	- ระบบเครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพความเสถียร - ระบบเครือข่ายสามารถรองรับการใช้งานของผู้ใช้งานทั้งองค์กร	←											→	ยส.

ประเด็นความเสี่ยง/กิจกรรม	กิจกรรมตามแนวทางการจัดการความเสี่ยง	เป้าหมาย/ผลสำเร็จของการดำเนินการกิจกรรมตามแนวทางการจัดการความเสี่ยง	ปี ๒๕๖๕	ปี ๒๕๖๖				ปี ๒๕๖๗				ปี ๒๕๖๘			ผู้รับผิดชอบ
			ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	
ด้านระบบสารสนเทศและฐานข้อมูล รหัส ๐๑๑ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ติดตั้งโปรแกรมป้องกันไวรัสบนเครื่องแม่ข่าย - ติดตามแก้ไขช่องโหว่ของซอฟต์แวร์เป็นประจำ - มีการยืนยันตัวตนและกำหนดสิทธิผู้ใช้งานก่อนการใช้งานเครือข่าย	- ระบบเครือข่ายของ ขร. มีความปลอดภัย - ผู้ใช้งานมีความมั่นใจในการใช้งานเครือข่าย	←											→	ยส.
ความเสี่ยงในด้านการบริหารจัดการ รหัส ๐๒๗ ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	- ติดตามประกาศ/กฎหมาย/ระเบียบที่เกี่ยวข้อง - จัดลำดับความสำคัญและวางแผนการดำเนินงาน	ขร. มีการปฏิบัติงานที่สอดคล้องตามกฎหมาย/ระเบียบที่เกี่ยวข้อง	←											→	สำนัก/กอง/กลุ่ม

บทที่ ๕

แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Cycle)

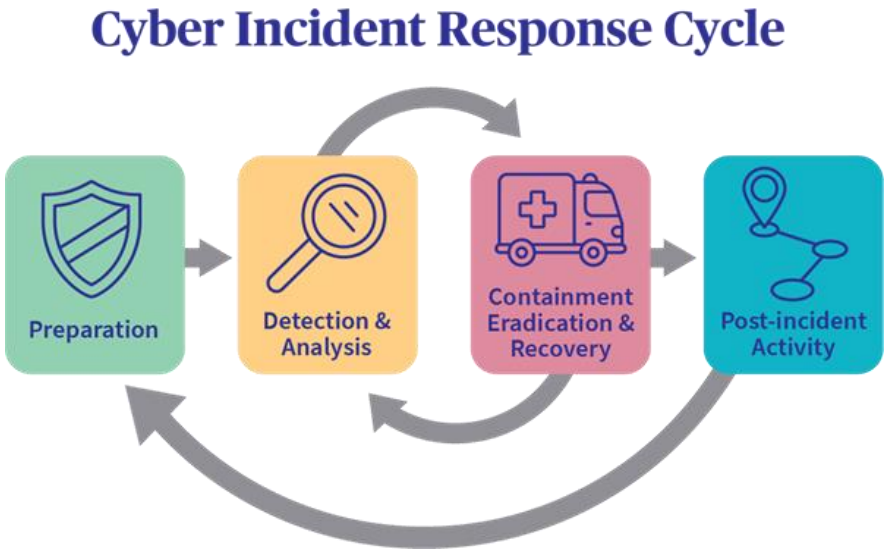
ขร.ได้กำหนดขั้นตอนการดำเนินงาน รวมทั้งการดำเนินงานด้านเทคนิคเพื่อให้สามารถดำเนินงานตามแผน และได้ผลลัพธ์ตามที่กำหนด ดังต่อไปนี้

๑) การเตรียมความพร้อม (Preparation)

๒) การตรวจจับและวิเคราะห์ (Detection & Analysis)

๓) การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคามและการกู้คืน (Containment,Eradication & Recovery)

๔) การดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity)



วัฏจักรของการตอบสนองต่อเหตุการณ์

๑. ขั้นตอนการรับมือ

แผนรับมือฯ นี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกันรับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.๒๕๖๔ และประกาศคณะกรรมการการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ รวมถึงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร .ดังนี้

๑.๑ ขั้นการเตรียมการ (preparation)

ขร. จะต้องดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ ๒.๒

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ ๒.๔

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

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

(๕) จัดเตรียมอุปกรณ์ ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของ ขร. โดย ขร.ได้ทำการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ไว้ (รายละเอียดปรากฏตามภาคผนวก ๑)

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

๑.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

ขร. จะต้องดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้ ขร. สามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(๑) ขร. จะต้องดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น มีตัวอย่าง ดังนี้

ประเภท	อธิบาย	วิธีการรับมือ
External/Flash drive	การโจมตีที่ดำเนินการจากอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง ตัวอย่างเช่น โค้ดที่เป็นอันตรายแพร่กระจายไปยังระบบจากแฟลชไดร์ฟที่ติดไวรัส	ดำเนินการถอนการติดตั้งอุปกรณ์แบบถอดได้ที่เป็นสาเหตุของภัยคุกคามออกจากอุปกรณ์และระบบเครือข่ายของหน่วยงาน และตรวจสอบสาเหตุและประเภทของภัยคุกคามว่าเป็นภัยคุกคามประเภทใด

(๒) ขร. ต้องดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

(๓) ขร. ต้องดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องเช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น

(๔) ขร. ต้องดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๒)

(๕) ขร. ต้องจัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดย ขร. บันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ด้วย บันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ควรลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสมโดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์ม (รายละเอียดปรากฏตามภาคผนวก ๓)

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

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

(ค) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปีภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

นอกจากนี้ ขร.พิจารณาดำเนินการตามเอกสารแนบท้าย ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

<u>๑.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication and recovery)</u>

ขร. จะต้องดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึก การยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

นอกจากนี้ ขร. พิจารณาดำเนินการตามเอกสารแนบท้าย ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

<u>๑.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)</u>

ขร. กำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้ ขร.สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมาและสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้ ขร. ต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) การทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๒) ดำเนินการตามเอกสารแนบท้าย ตารางที่ ๒.๔ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

ขร. ได้จัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่ ขร. เกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดย ขร. สามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก ๕)

๑.๖ ขั้นตอนการทำงานการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยจากหน่วยงานภายใน/ภายนอกใน ขร.

ตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยจากระบบเฝ้าระวังฯ หากพบเหตุการณ์ด้านความมั่นคงปลอดภัยที่ผิดปกติ หรือ ได้รับการแจ้งเตือนพบเหตุการณ์ผิดปกติจากหน่วยงานภายนอก ขร. ให้เริ่มดำเนินการตามกระบวนการทำงาน ดังนี้

๑.๑ บันทึกข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยที่ผิดปกติที่ได้ตรวจสอบพบหรือได้รับการแจ้งเตือนลงในระบบรายงานฯ

๑.๒ รวบรวมข้อมูลต่าง ๆ ที่เกี่ยวข้องกับภัยคุกคามที่ตรวจพบ หรือ ได้รับการแจ้งเตือนจากหน่วยงานภายนอก จากอุปกรณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๑.๓ วิเคราะห์ข้อมูลภัยคุกคามที่ตรวจสอบพบเป็นการโจมตีประเภทใด

๑.๔ บันทึกข้อมูลลงในระบบรายงานฯ

๑.๕ จัดระดับความเร่งด่วนในการแก้ไขปัญหาภัยคุกคาม ดังรายละเอียดดังนี้

๑.๕.๑ เร่งด่วน : มีความเสี่ยงส่งผลกระทบในวงกว้างทั่วทั้ง ขร.

๑.๕.๒ มาก : มีความเสี่ยงส่งผลกระทบต่อ ขร. ตั้งแต่ ๒ กองขึ้นไป

๑.๕.๓ ปานกลาง : มีความเสี่ยงส่งผลกระทบต่อ ขร. ที่โดนโจมตีเท่านั้น

๑.๕.๔ ปกติ : ยังมิได้มีผลกระทบเกิดขึ้น แต่หากไม่ดำเนินการจะส่งผลกระทบในอนาคต

๑.๖ บันทึกข้อมูลลงในระบบรายงานฯ

๑.๗ เตรียมแนวทางการแก้ไขปัญหา หากมีข้อมูลเดิมที่ได้จัดทำไว้แล้ว ให้นำข้อมูลดังกล่าวนำส่งต่อไป หากยังไม่มีแนวทางการแก้ไขปัญหา ต้องค้นคว้าหาข้อมูลแนวทางการแก้ไขปัญหาเพิ่มเติม

๑.๘ ตรวจสอบข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยที่ตรวจสอบพบนั้นเป็นของกองไหนหรือผู้ใช้งานใด

๑.๙ แจ้งปัญหาพร้อมทั้งแนะนำแนวทางการแก้ไขปัญหา ไปยังกองที่เกี่ยวข้อง ตามระดับความเร่งด่วน รายละเอียดดังนี้

๑.๙.๑ เร่งด่วน : โทรแจ้งทันที พร้อมทั้งแจ้งอีเมล

๑.๙.๒ มาก : โทรแจ้งภายใน ๓๐ นาที พร้อมทั้งแจ้งอีเมล

๑.๙.๓ ปานกลาง : โทรแจ้งภายใน ๑ ชั่วโมง พร้อมทั้งแจ้งอีเมล

๑.๙.๔ ปกติ : แจ้งผ่านทางอีเมล

๑.๑๐ บันทึกข้อมูลลงในระบบรายงานฯ

๑.๗ หลักเกณฑ์ในการพิจารณาระดับผลกระทบ

ระดับผลกระทบ	หลักเกณฑ์ในการพิจารณาระดับผลกระทบ
สูง	- เกิดความเสียหายต่อองค์กรในระดับสูง - ส่งผลให้ความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่าร้อยละ ๕๐ - ส่งผลกระทบต่อชื่อเสียงและความมั่นใจในระดับกรม
ปานกลาง	- เกิดความเสียหายต่อองค์กรในระดับปานกลาง - ส่งผลให้ความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่าร้อยละ ๒๕ - ๕๐ - ส่งผลกระทบต่อชื่อเสียงและความมั่นใจในระดับหน่วยงาน
ต่ำ	- เกิดความเสียหายต่อองค์กรในระดับต่ำ - ส่งผลให้ความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่าร้อยละ ๒๕ - ส่งผลกระทบต่อชื่อเสียงและความมั่นใจในระดับบุคคล

โดยกระบวนการหลักที่มีความสำคัญและจำเป็นต้องดำเนินงานให้บริการได้ภายในระยะเวลาที่กำหนด ประกอบด้วย ระบบสารสนเทศ เช่น เว็บไซต์หน่วยงาน ระบบสารบรรณ ระบบเครือข่ายสารสนเทศ เช่น การให้บริการ Internet เครื่องคอมพิวเตอร์แม่ข่าย (Server), Firewall, Router, Swithch เป็นต้น การดูแลและบำรุงรักษาระบบสารสนเทศ/คอมพิวเตอร์และอุปกรณ์ต่อพ่วง เช่น คอมพิวเตอร์ เครื่องพิมพ์ การให้การช่วยเหลือแก้ไขปัญหาด้าน IT เป็นต้น

กระบวนการหลัก	ระดับผลกระทบ	ระยะเวลาที่ยอมรับได้ในการกู้คืนให้กลับสู่สภาวะปกติ	ปริมาณข้อมูลสูญหายที่ยอมรับได้ในช่วงเวลาหนึ่ง	ระยะเวลาสูงสุดที่ยอมรับได้ในการกู้คืน (หากพ้นจากระยะนี้มีผลต่อการดำเนินงานในระดับสูงสุด)
(๑) ระบบสารสนเทศ เช่น เว็บไซต์หน่วยงาน ระบบสารบรรณ (e-saraban) เป็นต้น	สูง	๒๔ ชั่วโมง	๓ วัน	๑ สัปดาห์
(๒) ระบบเครือข่ายสารสนเทศ เช่น Internet เครื่องคอมพิวเตอร์แม่ข่าย (Server) Firewall Router Swithch เป็นต้น	สูง	๒๔ ชั่วโมง	๒๔ ชั่วโมง	๔๘ ชั่วโมง
(๓) การดูแลและบำรุงรักษาระบบสารสนเทศ/ คอมพิวเตอร์และอุปกรณ์ต่อพ่วง เช่น คอมพิวเตอร์ เครื่องพิมพ์ การให้การช่วยเหลือแก้ไขปัญหาด้าน IT เป็นต้น	ปานกลาง	๑ วัน	๓ วัน	๑ สัปดาห์

เอกสารแนบท้าย

ตาราง ที่ ๒.๑ การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	(๑) จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคลหรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใดที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น (๒) จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคาม ทางไซเบอร์ (๓) ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศดังกล่าว (๔) จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย(Network diagrams) เป็นต้น (๕) พิจารณาซ่อนบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น (๖) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) (๗) กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง (๘) จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทำการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์สำหรับการเข้าถึงระบบต่าง ๆ (cryptography / key managements) เป็นต้น (๙) ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ (๑๐) ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (incident respond capability testing) (๑๑) รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence) (๑๒) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ เพื่อดำเนินการทดสอบการเจาะระบบเป็นประจำและสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อพบช่องโหว่หรือ จุดอ่อนต่าง ๆ (ถ้าหน่วยงานมีความพร้อม) (๑๓) กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ (๑๔) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลง ค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไกที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร การแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มีกลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๑๕) จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว (๑๖) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการ ภัยคุกคามทางไซเบอร์

ตาราง ที่ ๒.๒ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับ ร้ายแรง	(๑) จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น (๒) จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ (๓) จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัย ด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงานที่มีความสำคัญมากขึ้น (๔) วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่าย และ ระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรมการใช้งานในช่วงเวลาปกติ (normal behaviors) ทำการศึกษาวิจัยและค้นหา ความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation) (๕) ทันทีที่พบว่ามีหรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหา และ รวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ในการ โจมตี, สถานการณ์ของการโจมตี(อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ, โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลา ประทับ ข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และ ข้อมูลจราจรทาง คอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguard incident data) ให้มีความปลอดภัย เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำาเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (๖) ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าว จะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในข้อ ๒ ของภาคผนวกแนบท้ายนี้ (๗) จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และ ความสามารถในการกู้คืน (recoverability effort) เป็นต้น (๘) ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์ รวมถึงจุดอ่อนของระบบที่ถูกโจมตี (๙) ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูลเพื่อให้บุคคล ดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (๑๐) รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต	ขร. ดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น (๒) จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจัดเก็บและ วิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ (ถ้า ขร. มีความพร้อม) (๓) จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบงานหลักที่สูงผิดปกติ หรือ เมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น (๔) วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูลในระบบเพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ตาราง ที่ ๒.๓ การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	(๑) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้แนวทางดังกล่าวรวมถึง (๑.๑) การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทาง นิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น (๑.๒) การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น (๑.๓) การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด (๒) ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้ เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในกระบวนการ ทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี (๓) ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น (๔) ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้องตลอดจนผู้ที่อาจได้รับผลกระทบอย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยังบุคคลหรือ หน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ในหมวดหมู่ที่ ๑, ๒, ๔, ๕ และ ๗ ตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ทั้งนี้ ในการแจ้งหรือรายงานสถานการณ์นั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสมและปลอดภัย และดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับ ดูแลกำหนด หรืออาจเทียบเคียงจากตามที่ระบุในข้อ ๓ ของภาคผนวก แนบท้ายนี้ แล้วแต่กรณี (๕) ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้งลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐานและดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ เป็นต้น (๖) ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น (๗) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ให้หน่วยงานดำเนินการตามข้อ ๑ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) หากมีความจำเป็นให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (alternate processing) การจัดเก็บข้อมูล (storage site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) (๒) ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยัง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (๓) ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และเนื้อหาที่ต้องรายงาน ลำดับชั้นการรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือ ที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ(ถ้าหน่วยงานมีความพร้อม) (๔) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติหน่วยงานควบคุมหรือกำกับดูแล พนักงาน เจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ ตามกฎหมาย (๕) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติในการรับมือหรือสนับสนุนการรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (automated incident handling processes) (ถ้าหน่วยงานมีความพร้อม)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถ ให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของหน่วยงานทำได้อย่างรวดเร็ว

ตาราง ที่ ๒.๔ การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณาดำเนินการดังนี้ (๑) นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคาม ทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้าง พื้นฐานของบริการ นโยบายและกระบวนการ การฝึกบุคลากร การระบุผู้มีอำนาจดำเนินงานและเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกัน การเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง (๒) รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน (๓) ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสมและเป็นปัจจุบัน (๔) เก็บรักษาข้อมูลและหลักฐานที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดีตามแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

ตารางที่ ๑ ลักษณะภัยคุกคามทางไซเบอร์แต่ละระดับและแนวทางการพิจารณาผลกระทบ

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๑.ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ดังนี้ (๑) ระบบคอมพิวเตอร์ของหน่วยงาน ขร. หรือ (๒) อุปกรณ์หรือระบบงานอื่นที่ใช้สำหรับการให้บริการของรัฐ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ระบบคอมพิวเตอร์ของ ขร. หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกใช้สำหรับให้บริการหลัก ดังนี้ (๑) ระบบคอมพิวเตอร์ (๒) โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว แสดงให้เห็นได้ว่าผู้โจมตีมีความมุ่งหมายที่จะทำให้โครงสร้างพื้นฐานสำคัญของประเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่รุนแรงในลักษณะที่เป็นวงกว้างต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าวทำาให้ (๑) การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชน ล้มเหลวทั้งระบบจนรัฐไม่สามารถ ควบคุมการทำงานส่วนกลางของำระบบคอมพิวเตอร์ของรัฐได้ หรือ (๒) การใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ หรือระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่เจาะจงอุปกรณ์หรือระบบงานที่ได้รับผลกระทบ แต่เมื่อพิจารณาจากพฤติกรรมของผู้โจมตีหรือพฤติการณ์แวดล้อมแล้วมีเหตุอันควรเชื่อได้ว่าการก่อภัยคุกคามทางไซเบอร์นั้นกระทบ หรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๒. ลักษณะ ผลกระทบต่อข้อมูลในระบบ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้าย ต่อข้อมูล ซึ่งส่งผลกระทบทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่ สามารถใช้งานได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลที่ใช้สำหรับระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศ ซึ่งส่งผลให้บริการหลักไม่สามารถทำงาน หรือให้บริการได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลอันมีลักษณะดังนี้ (๑) เป็นข้อมูลที่เกี่ยวข้องกับการทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชน หรือ (๒) เป็นข้อมูลที่เกี่ยวข้องกับชีวิตของบุคคลจำนวนมาก หรือเป็นข้อมูลคอมพิวเตอร์จำนวนมากในระดับประเทศ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลใด ๆ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา การรบ หรือการสงคราม
๓. แนวโน้มในการกู้คืนระบบ	สามารถกู้คืนระบบคอมพิวเตอร์ หรือ ทำให้บริการของรัฐกลับมาได้บางส่วน โดยสามารถดำเนินการได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศ ที่ใช้สำหรับให้บริการหลักได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศได้ตามแผนการกู้คืนทำให้ (๑) รัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ (๒) มีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่สามารถกู้คืนอุปกรณ์หรือระบบงานที่ได้รับผลกระทบได้ และจำเป็นต้องมีมาตรการเร่งด่วนในการกู้คืนอุปกรณ์หรือระบบงานที่เกี่ยวข้อง

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๔. ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ	ส่งผลหรืออาจส่งผลกระทบต่อผู้ใช้บริการในวงจำกัด	อาจส่งผลกระทบต่อผู้ใช้บริการทั้งหมด	ส่งผลกระทบต่อผู้ใช้บริการทั้งหมด หรืออาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต	ส่งผลหรืออาจส่งผลกระทบต่อความสงบเรียบร้อยของประชาชน หรือ เป็นภัยต่อความมั่นคงของรัฐ หรือ อาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมาย อาญา การรบหรือการสงคราม

ภาคผนวก

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม 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)

ข้อ ๒ ลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

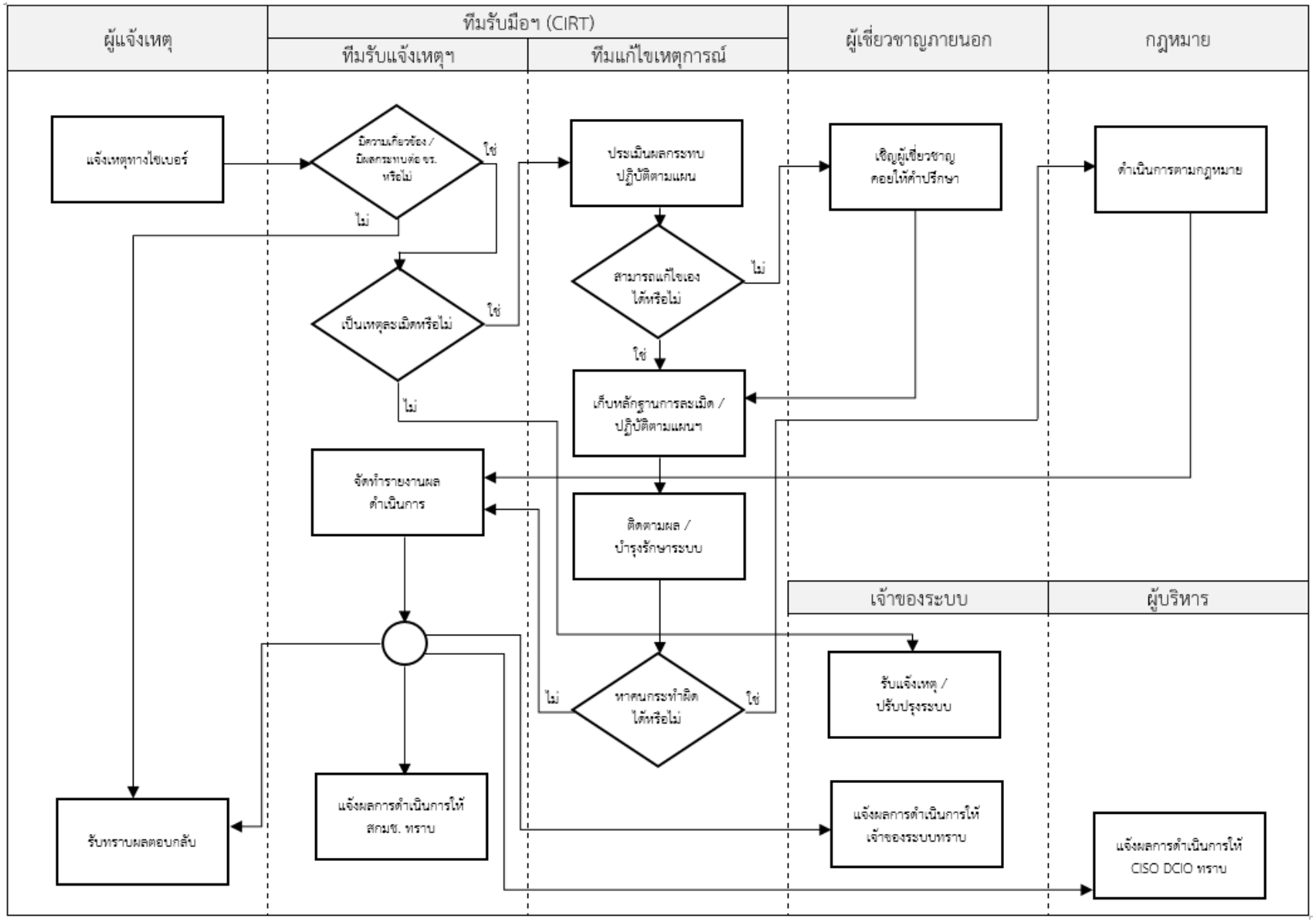
	หมวดหมู่ภัยคุกคาม						
ประเภทอุปกรณ์เครือข่าย	๑	๒	๓	๔	๕	๖	๗
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือ ดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชั่น	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

ข้อ ๓ กำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	ทุกเหตุการณ์	๓๐ นาที	๔ ชั่วโมง
๒	ทุกเหตุการณ์	ตาม ขร. กำหนด	ตาม ขร. กำหนด
๓	ทุกเหตุการณ์	๓๐ นาที	๘ ชั่วโมง
๔	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	ตาม ขร. กำหนด	ตาม ขร. กำหนด
๕	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๔ ชั่วโมง
๖	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๔ ชั่วโมง
๗	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๑๐ นาที	๑ ชั่วโมง
	ไม่ร้ายแรง	ตาม ขร. กำหนด	ตาม ขร. กำหนด
๘	-	๒๐ นาที	๔ ชั่วโมง
๙	-	-	๑๒ ชั่วโมง

ภาคผนวก ๑

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



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 ในระดับใด (มาตรา ๖๐)

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

☐ ยังไม่สามารถระบุได้

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 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)

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

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)	
สวิตช์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

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

ภาคผนวก ๕

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

	รายการตรวจสอบการจัดการเหตุการณ์	Complete
	ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (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	
	ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)	
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
๗.๑	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
๗.๒	กำจัด หรือลบมัลแวร์ 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	
	การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)	
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

ส่วนที่ ๓ การบริหารงานแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

สาเหตุในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์	
☐ จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับแรก ☐ ครั้งแรก ☐ แทนฉบับเดิม..... ☐ ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ตามรอบที่กำหนด ☐ ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ เนื่องจากมีความเปลี่ยนแปลงที่สำคัญ (ระบุ).....	
ผู้จัดทำแผน	
วันที่	**ลายมือชื่อผู้จัดทำแผน**
ผู้ตรวจสอบเอกสาร	
วันที่	**ลายมือชื่อผู้จัดทำแผน**
ผู้อนุมัติแผน	
วันที่	**ลายมือชื่อผู้อนุมัติแผน**
การทบทวนแผน	
ทบทวนภายในวันที่	**ผู้รับผิดชอบในการดำเนินการทบทวนแผน** ชื่อ ..... ตำแหน่ง ..... หน่วยงาน/ส่วนงาน..... ที่อยู่สำหรับการติดต่อ..... เบอร์โทรศัพท์ ..... ไปรษณีย์อิเล็กทรอนิกส์ (e-mail).....