ประมวลแนวทางปฏิบัติ และกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำนักงานปลัดกระทรวงการพัฒนาสังคม และความมั่นคงของมนุษย์ (สป.พม.)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

มิถุนายน 2567

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.)
มิถุนายน 2567

คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วย งานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็วมีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจึงได้จัดทำเอกสารฉบับนี้ เพื่อให้สำนักงานปลัดกระทรวงการพัฒนาสังคมและ ความมั่นคงของมนุษย์ มีรูปแบบรวมถึงขั้นตอนปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ทั้งนี้ เพื่อใช้เป็นแนวทางสำหรับผู้ใช้งานข้อมูล ระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานให้ตระหนักถึงความมั่นคงปลอดภัยไซเบอร์ ปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนด

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

สารบัญ

หน้า

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(Guideline and Cybersecurity Framework)

1. วัตถุประสงค์

เพื่อกำหนดกรอบแนวคิดและวิธีปฏิบัติของระบบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์นำไปใช้กับการดำเนินงานและการจัดการระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

2. ขอบเขต

กำหนดกรอบและวิธีปฏิบัติสำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework) สำหรับสารสนเทศที่สำคัญของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

3. คำนิยาม

หน่วยงาน หมายถึง สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

คณะกรรมการ หมายถึง คณะกรรมการควบคุมและกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจหรือให้บริการที่เกี่ยวข้อง

กกม. หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

สำนักงาน หมายถึง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายถึง คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายถึง หน่วยงานของรัฐหรือหน่วยงานเอกชนซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หน่วยงานควบคุมหรือกำกับดูแล หมายถึง หน่วยงานของรัฐ หน่วยงานเอกชน หรือ บุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของ หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

บริการที่สำคัญ หมายถึง ภารกิจหรือบริการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 49

ตัวชี้วัดความเสี่ยงที่สำคัญ หมายถึง เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้หน่วยงานมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

บุคคลภายนอก (Third Party) หมายถึง บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงานหรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานหรือข้อมูลของลูกค้าที่ควบคุมโดยหน่วยงานได้

Interface หมายถึง การเชื่อมต่อกันระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์ สามารถถ่ายโอนข้อมูลซึ่งกันและกันได้

Compiler หมายถึง โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

patch หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายเผยแพร่ patch ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่ Patch ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update

Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืน

Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

Maximum Tolerance Period of Disruption (MTPD)หมายถึง ระยะเวลาสูงสุดที่ยอมให้ระบบหยุดชะงัก เพื่อรองรับการดำเนินงานอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

Asset Management หมายถึง การจัดการสินทรัพย์ เช่น ข้อมูล บุคลากร อุปกรณ์ ระบบและสิ่งอำนวยความสะดวกที่ช่วยให้หน่วยงานบรรลุวัตถุประสงค์ การระบุและจัดการให้สอดคล้องกับความสำคัญที่สัมพันธ์กับวัตถุประสงค์และกลยุทธ์ความเสี่ยงของหน่วยงาน

Business Environment หมายถึง สภาพแวดล้อมการดำเนินงาน ภารกิจ วัตถุประสงค์ ผู้มีส่วนได้ ส่วนเสีย และกิจกรรมของหน่วยงานได้รับการเข้าใจและจัดลำดับความสำคัญ ข้อมูลนี้ใช้เพื่อแจ้งบทบาทความปลอดภัยทางไซเบอร์ ความรับผิดชอบ และการตัดสินใจในการจัดการความเสี่ยง

Governance หมายถึง นโยบาย ขั้นตอน และกระบวนการในการจัดการและติดตามข้อกำหนดของหน่วยงาน กฎหมาย ความเสี่ยง สิ่งแวดล้อม และการดำเนินงาน เป็นที่เข้าใจและแจ้งการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

Risk Assessment หมายถึง การประเมินความเสี่ยง หน่วยงานเข้าใจถึงความเสี่ยงด้านความปลอดภัยทางซเบอร์ต่อการดำเนินงานของหน่วยงาน (รวมถึงภารกิจ หน้าที่ ภาพลักษณ์หรือชื่อเสียง) ทรัพย์สินของหน่วยงาน และบุคคล

Risk Management Strategy หมายถึง ลำดับความสำคัญของหน่วยงาน ข้อจำกัดความเสี่ยงที่ยอมรับได้ และข้อสมมติของหน่วยงานได้รับการกำหนดและใช้เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงด้านปฏิบัติการ

Access Control หมายถึง การควบคุมการเข้าถึงทรัพย์สินและสิ่งอำนวยความสะดวกที่ได้รับอนุญาตที่เกี่ยวข้องนั้นจำกัดเฉพาะผู้ใช้ กระบวนการ หรืออุปกรณ์ที่ได้รับอนุญาต และเฉพาะกิจกรรมและธุรกรรม

Awareness and Training หมายถึง การรับรู้และการฝึกอบรม บุคลากรและพันธมิตรของหน่วยงานได้รับการศึกษาด้านความตระหนักด้านความปลอดภัยทางไซเบอร์และได้รับการฝึกอบรมอย่างเพียงพอเพื่อปฏิบัติหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลโดยสอดคล้องกับนโยบาย ขั้นตอน และข้อตกลงที่เกี่ยวข้อง

Data Security หมายถึง การรักษาความปลอดภัยข้อมูล ข้อมูลและบันทึก (ข้อมูล) ได้รับการจัดการที่สอดคล้องกับกลยุทธ์ความเสี่ยงของหน่วยงานเพื่อปกป้องความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล

Information Protection Processes and Procedures หมายถึง กระบวนการและขั้นตอนการคุ้มครองข้อมูล นโยบายความปลอดภัย (ที่กล่าวถึงวัตถุประสงค์ ขอบเขต บทบาท ความรับผิดชอบความมุ่งมั่นในการจัดการ และการประสานงานระหว่างหน่วยงานขององค์กร) กระบวนการและชั้นตอนต่างๆ ได้รับการดูแลและใช้เพื่อจัดการการป้องกันระบบข้อมูลและทรัพย์สิน

Maintenance หมายถึง การบำรุงรักษาและการซ่อมแซมการควบคุมระบบสารสนเทศและส่วนประกอบระบบสารสนเทศดำเนินการให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติ

Protective Technology หมายถึง การรักษาความปลอดภัยทางเทคนิคได้รับการจัดการเพื่อให้มั่นใจในความปลอดภัยและความยืดหยุ่นของระบบและทรัพย์สิน สอดคล้องกับนโยบาย ขั้นตอนและข้อตกลงที่เกี่ยวข้อง

Anomalies and Events หมายถึง การตรวจพบกิจกรรมผิดปกติในเวลาที่เหมาะสมและเข้าใจผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์

Security Continuous Monitoring หมายถึง การตรวจสอบความปลอดภัยอย่างต่อเนื่องของระบบข้อมูลและทรัพย์สินได้รับการตรวจสอบเป็นระยะเพื่อระบุเหตุการณ์ความปลอดภัยทางไซเบอร์และตรวจสอบประสิทธิภาพของมาตรการป้องกัน

Detection Processes หมายถึง กระบวนการและขั้นตอนการตรวจจับได้รับการบำรุงรักษาและทดสอบเพื่อให้แน่ใจว่ามีการรับรู้เหตุการณ์ผิดปกติในเวลาที่เหมาะสมและเพียงพอ

Response Planning หมายถึง กระบวนการและขั้นตอนการตอบสนองจะได้รับการดำเนินการและบำรุงรักษา เพื่อให้แน่ใจว่าตอบสนองต่อเหตุการณ์การรักษาความปลอดภัยทางไซเบอร์ที่ตรวจพบได้ทันท่วงที

Communications หมายถึง กิจกรรมตอบสนองได้รับการประสานงานกับผู้มีส่วนได้ส่วนเสียภายในและภายนอกตามความเหมาะสมเพื่อรวมการสนับสนุนภายนอกจากหน่วยงานบังคับใช้กฎหมาย

Analysis หมายถึง การวิเคราะห์ดำเนินการเพื่อให้แน่ใจว่ามีการตอบสนองที่เพียงพอและสนับสนุนกิจกรรมการกู้คืน

Mitigation หมายถึง มีการดำเนินกิจกรรมเพื่อป้องกันการขยายเหตุการณ์ ลดผลกระทบและกำจัดเหตุการณ์

Improvements หมายถึง กิจกรรมการตอบสนองของหน่วยงานได้รับกรปรับปรุงโดยการรวมบทเรียนที่เรียนรู้จากกิจกรรมการตรวจจับ/การตอบสนองในปัจจุบันและก่อนหน้า

Recovery Planning หมายถึง กระบวนการและขั้นตอนการกู้คืนจะได้รับการดำเนินการและบำรุงรักษาเพื่อให้แน่ใจว่าระบบหรือทรัพย์สินที่ได้รับผลกระทบจากเหตุการณ์ความปลอดภัยทางไซเบอร์สามารถกู้คืนได้ทันเวลา

Improvements หมายถึง การวางแผนและกระบวนการฟื้นฟูได้รับการปรับปรุงโดยนำบทเรียนที่เรียนรู้ไปใช้กับกิจกรรมในอนาคต

Communications หมายถึง กิจกรรมการฟื้นฟูได้รับการประสานงานกับฝ่ายภายในและภายนอก เช่น ศูนย์ประสานฯ NCERT สำนักงาน ผู้ให้บริการอินเทอร์เน็ต เจ้าของระบบที่ถูกโจมตี และผู้มีส่วนได้ส่วนเสีย

4. ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประกอบด้วย 3 ประมวลแนวทางปฏิบัติ ดังนี้

4.1 แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้ง โดยผู้ตรวจสอบภายในหรือภายนอกหน่วยงาน โดยมีขอบเขตของการตรวจสอบ ดังนี้

4.1.1 ตรวจสอบการปฏิบัติของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย คำสั่ง แนวปฏิบัติ ข้อปฏิบัติ ที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

4.1.2 ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

4.1.3 ตรวจสอบบริการที่สำคัญของหน่วยงาน ทั้งกรณีที่หน่วยงานเป็นเจ้าของ และใช้บริการจากผู้ให้บริการภายนอก

4.2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้งเพื่อเป็นการเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น รวมถึงให้มีแนวทางในการดำเนินงานการกำกับดูแลในช่วงสถานการณ์ที่เกิดขึ้น และให้สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

4.2.1 การประเมินความเสี่ยง (Risk Assessment)

- การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคาม และช่องโหว่ต่างๆ

- การวิเคราะห์ความเสี่ยง (Risk Analysis) เป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น และผลกระทบ (Impact) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

- การประเมินความเสี่ยง (Risk Evaluation) ต้องมีการกำหนดและจัดลำดับความสำคัญของความเสี่ยง

4.2.2 การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ค่าความเสี่ยงอยู่ในระดับที่ยอมรับได้

4.2.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีการติดตามและทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ค่าความเสี่ยงอยู่ในระดับที่ยอมรับได้

4.2.4 การรายงานความเสี่ยง (Risk Report)

ต้องมีการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงให้ผู้บริหารทราบ

4.3 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

หน่วยงานต้องดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ โดยกำหนดขั้นตอนการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยมีรายละเอียดอย่างน้อย หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อระบบบริการสำคัญของหน่วยงาน

5. กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ซึ่งสามารถสรุปกิจกรรมการดำเนินการต่าง ๆ ดังต่อไปนี้

รูปที่ 1 กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กิจกรรมตามกรอบมาตรฐาน รายละเอียดของแต่ละกิจกรรมมีดังนี้

1) Identify คือ การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง ที่จะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

2) Protect คือ การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน

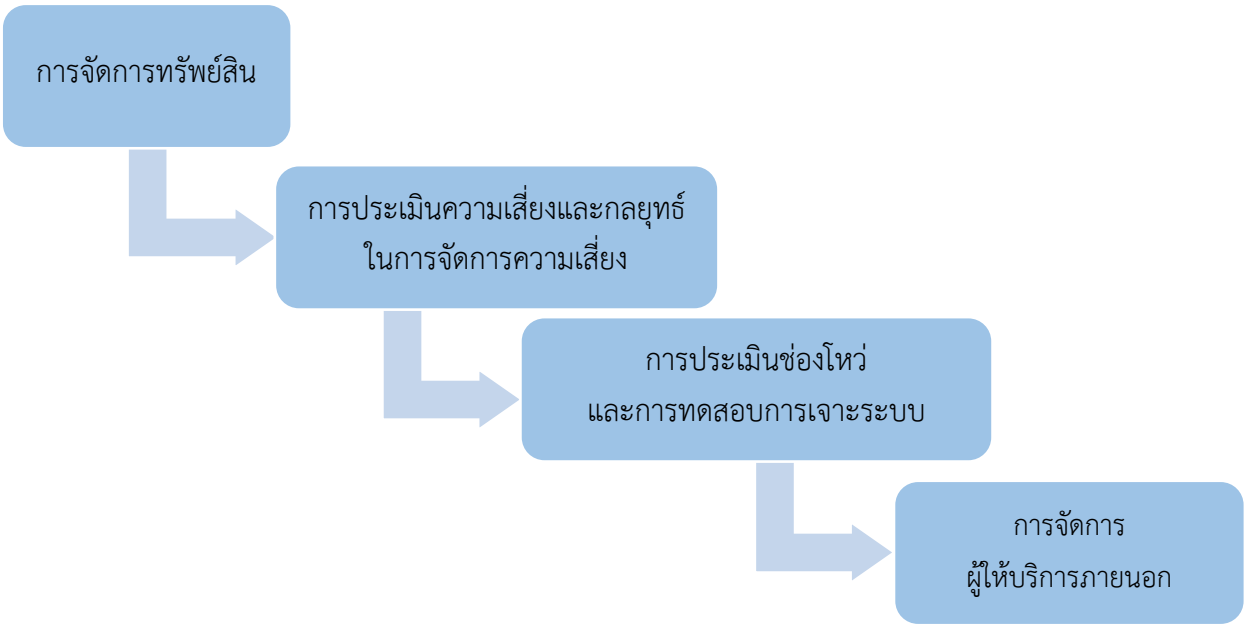
3) Detect คือ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

4) Response คือ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

5) Recover คือ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

กิจกรรมการระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)

เพื่อให้หน่วยงานสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ หน่วยงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานให้ครอบคลุมเรื่องโครงสร้างองค์การและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง ประกอบด้วยกระบวนการ 4 ขั้นตอน ดังนี้



รูปที่ 2 การระบุความเสี่ยง (Identify)

5.1 การจัดการทรัพย์สิน (Asset Management)

5.1.1 ต้องจัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และทบทวนทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

- ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญ
- ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญ
- ตำแหน่งทางกายภาพของทรัพย์สิน ของบริการที่สำคัญ
- การระบุและการจัดลำดับความสำคัญของทรัพย์สิน ของบริการที่สำคัญ
- การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญ บนระบบเครือข่ายภายใน และ/หรือภายนอก

5.1.2 ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

5.1.3 ต้องมีการตรวจสอบและปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หากมีการเปลี่ยนแปลงใดๆ กับทรัพย์สิน ของบริการที่สำคัญ

5.1.4 ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สิน อย่างน้อยปีละ 1 ครั้ง

5.2 การประเมินความเสียงและกลยุทธิ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

5.2.1 การประเมินความเสี่ยง (Risk Assessment)

- การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากรหรือปัจจัยภายนอก

- การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

- การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินงานของหน่วยงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

5.2.2 ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการฯ ประกาศกำหนด

5.2.3 ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- วันที่ระบุความเสี่ยง (Date the Risk is Identified)
- คำอธิบายของความเสี่ยง (Description of the Risk)
- โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- การจัดการความเสี่ยง (Risk Treatment)
- เจ้าของความเสี่ยง (Risk Owner)
- สถานะของการจัดการความเสี่ยง (Status of the Treatment)
- ความเสี่ยงที่เหลือ (Residual Risk)

5.2.4 การจัดการความเสี่ยง (Risk Treatment) ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินงาน ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

5.2.5 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

5.2.6 การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยงและผลกระทบการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการกำกับและดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจ

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

5.3 การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

5.3.1 ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ อ้างอิงตามหลักการบริหารความเสี่ยงเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยไซเบอร์และการควบคุม โดยครอบคลุมบริการที่สำคัญ

- Information Technology System
- Industrial Control System

5.3.2 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

- Host Security Assessment
- Network Security Assessment
- Architecture Security Assessment

5.3.3 ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆกับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

5.3.4 ควรดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ต ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

5.3.5 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ

5.3.6 ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีการรับรองและได้รับประกาศนียบัตรที่เป็นที่ยอมรับในอุตสาหกรรมและเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

5.3.7 ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

5.3.8 ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

5.3.9 หากได้รับการรับรองจาก กกม. หรือสำนักงาน ต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ดังกล่าวไปยังสำนักงานภายในกำหนด 30 วัน นับแต่วันที่ได้รับหนังสือ

5.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

5.4.1 ต้องรับผิดชอบ (Responsible) และมีการรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญ

5.4.2 ต้องกำหนดแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียด ดังต่อไปนี้

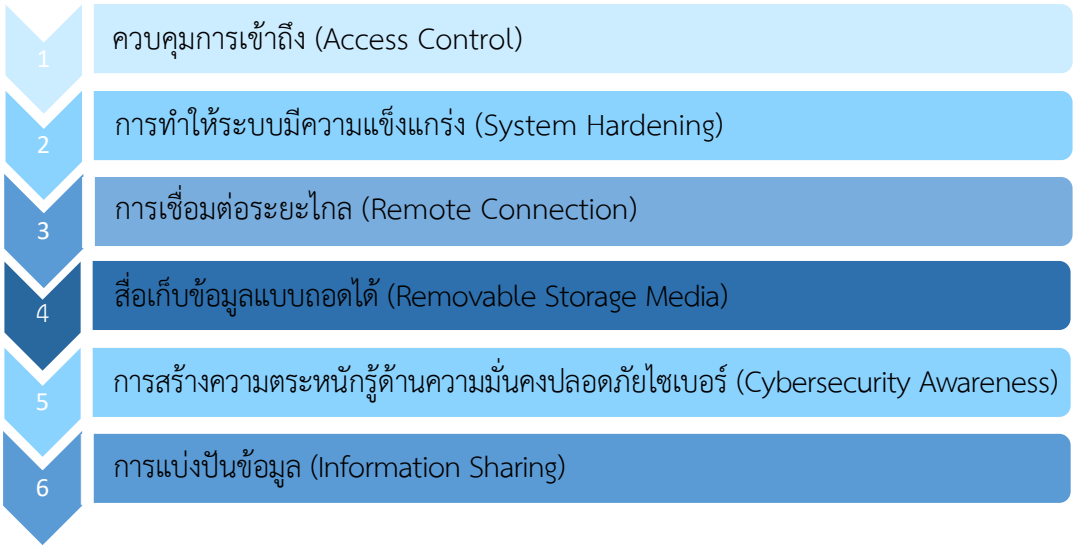
ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญ ตามความต้องการ

- ทางธุรกิจของหน่วยงานและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของหน่วยงานจากภัยคุกคาม
- ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์สิทธิ์ของหน่วยงาน

ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

กิจกรรมการวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)

รายละเอียดของกิจกรรมนี้ ประกอบด้วยกระบวนการ 6 ขั้นตอน ดังต่อไปนี้



รูปที่ 3 การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน (Protect)

5.5 การควบคุมการเข้าถึง (Access Control)

5.5.1 ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงาน ถูกจำกัดไว้ที่

- บุคลากร และกิจกรรมที่ได้รับอนุญาต
- อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

5.5.2 ในส่วนที่เกี่ยวกับภาระหน้าที่การตรวจสอบการเข้าถึงบริการที่ สำคัญของหน่วยงาน ต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตมีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหนดการเข้าถึงบริการที่สำคัญ

5.5.3 ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Log of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงาน และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ความสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

5.5.4 ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ เช่น USB, Serial Port และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดย

- ทำภายใต้กำกับดูแลของหน่วยงาน
- ดำเนินการในสถานที่ หากเป็นไปได้

5.6 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

5.6.1 ต้องสร้างมาตรฐานกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของหน่วยงาน

5.6.2 มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

- สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
- การแบ่งแยกหน้าที่ (Separation of Duties)
- การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
- การลบบัญชีที่ไม่ได้ใช้งาน
- การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)
- การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
- การป้องกันมัลแวร์ (Malware)
- การปรับปรุงซอฟต์แวร์และแพตซ์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

5.6.3 ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใดๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

5.6.4 ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงาน อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

5.6.5 ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

5.7 การเชื่อมต่อระยะไกล (Remote Connection)

5.7.1 ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของหน่วยงานมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

5.7.2 สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงาน ต้องปฏิบัติตามแนวทางปฏิบัติ ดังนี้

- ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยังไซต์ระยะไกล เมื่อจำเป็นเท่านั้น
- ในกรณีที่ เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
- ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, sh, scp เป็นต้น
- ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Command) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญหน่วยงาน เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการใช้งาน
- จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

5.8 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

5.8.1 ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น โน้ตบุ๊ก) กับบริการที่สำคัญของหน่วยงาน โดยมีมาตรการอย่างน้อย ดังนี้

- ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพาและเปิดใช้งานเมื่อจำเป็นเท่านั้น
- ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตจากหน่วยงานเท่านั้น
- ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน

5.8.2 ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงาน บนสื่อบันทึกข้อมูลแบบถอดได้

5.9 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

5.9.1 ต้องให้ความสำคัญกับแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์(Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอก บุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่
  - พนักงานใหม่ (New employees)
  - ผู้ใช้และระดับบริหาร (User and Management)
  - เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT
  - ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendor, Contractor and Service Provider)
- การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการสำคัญของหน่วยงาน
- การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบ

5.9.2 ต้องทบทวนแผนงานในการสร้างความระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

5.10 การแบ่งปันข้อมูล (Information Sharing)

ต้องมีการกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล ที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการป้องกันผลกระทบใดๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุมคามที่เกิดขึ้นกับบุคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ เช่น ผู้ใช้งาน ผู้ให้บริการ เจ้าของคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ที่มีความจำเป็นต้องเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน เพื่อให้สามารถใช้เป็นแนวทางและรูปแบบในการแบ่งปันข้อมูลเพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานกำหนด

กิจกรรมกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

5.11 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

5.11.1 ต้องสร้างกลไกและกระบวนการเพื่อตรวจรับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน และการจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน

5.11.2 ต้องดำเนินการทบทวนกลไกและกระบวนการอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

กิจกรรมการกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 3 ขั้นตอน ดังต่อไปนี้

รูปที่ 4 การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)

5.12 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ต้องมีการจัดทำ การสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

5.13 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

5.13.1 ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์

5.13.2 ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

- จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต
- ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง
- ระบุกลุ่มเป้าหมาย และผู้ที่มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
- ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนของหน่วยงานเมื่อกล่าวแถลงกับสื่อมวลชน
- ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

5.13.3 ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

5.13.4 ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้องปีละ 1 ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงที และมีประสิทธิภาพในช่วงวิกฤต อันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

5.14 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

5.14.1 หน่วยงานต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ ดังกล่าว

5.14.2 ต้องปฏิบัติตามคำขอของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้ รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของหน่วยงาน

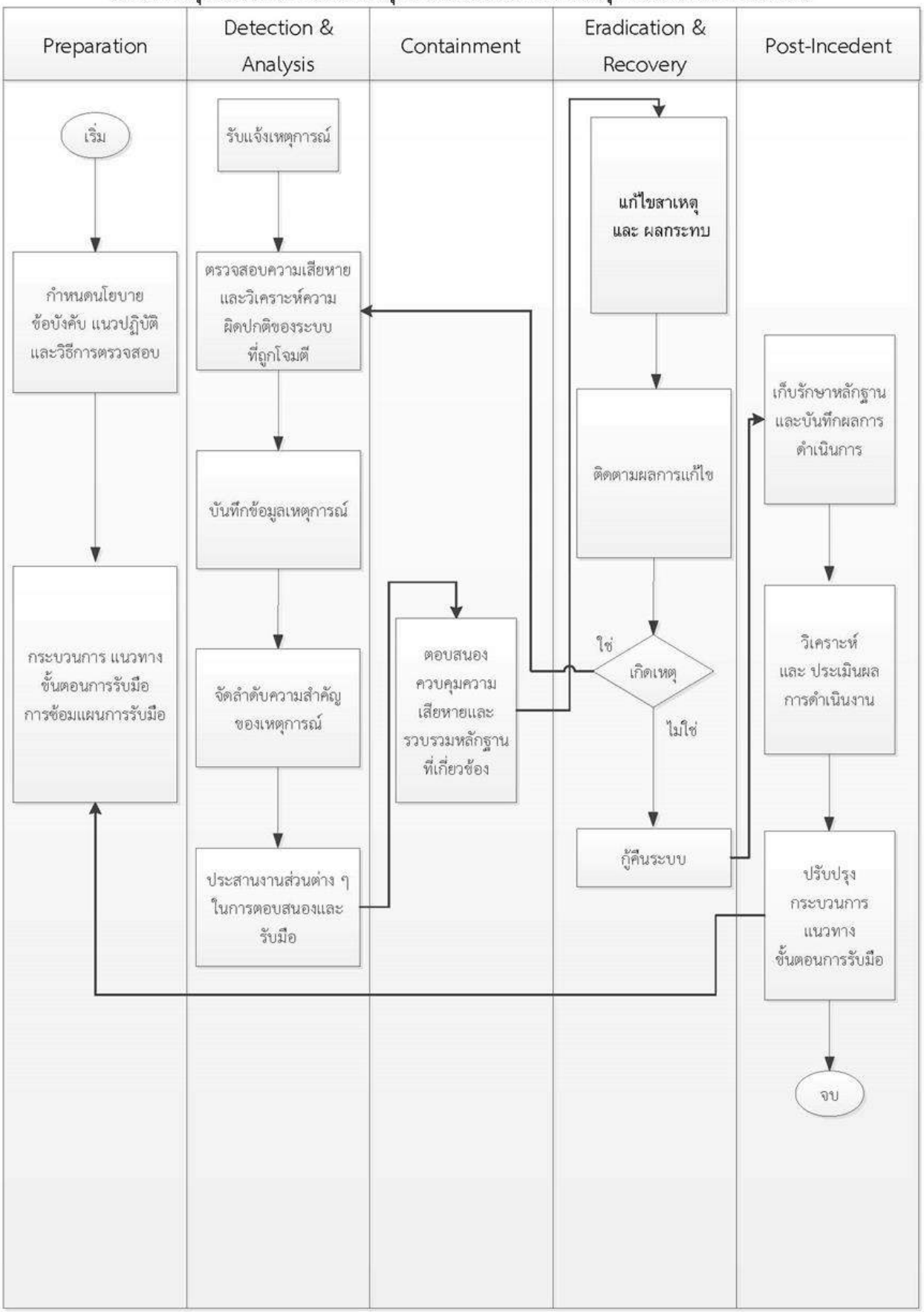
กิจกรรมการกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

5.15 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

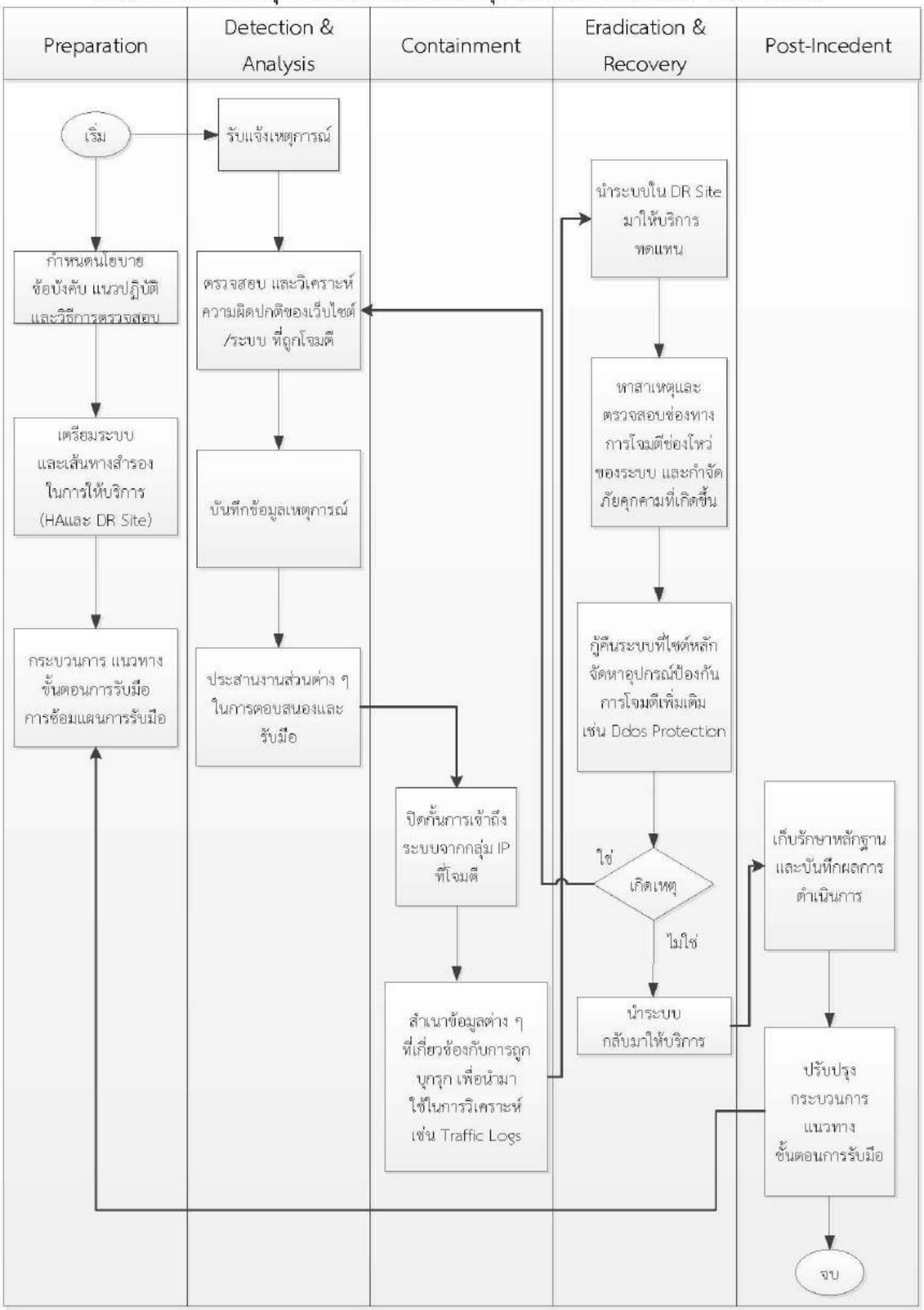
5.15.1 ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงาน สมารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกับขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ เช่น Maximum Tolerance Period of Disruption (MTPD) Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

5.15.2 ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

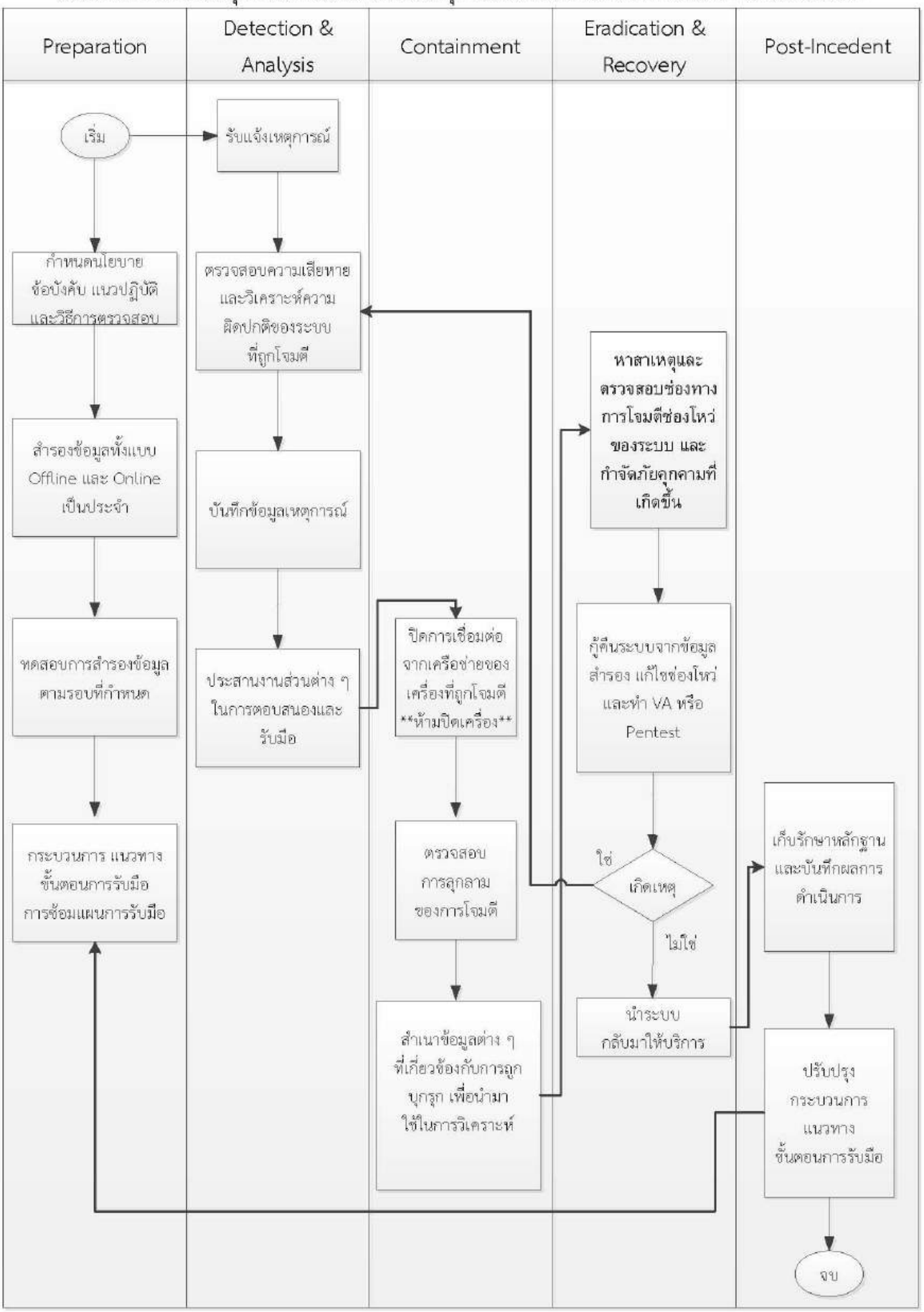
แผนภาพสรุปแนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์



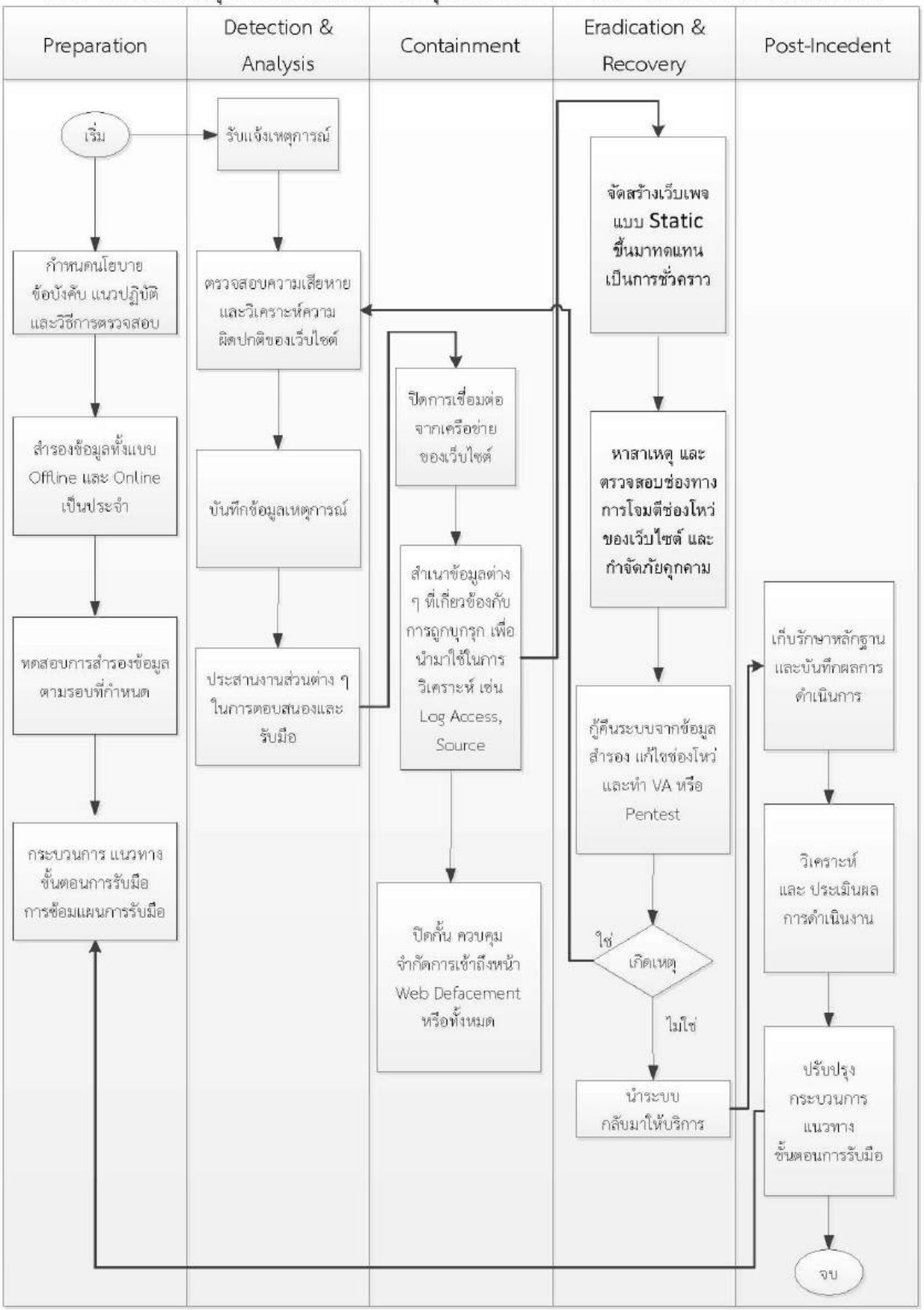
แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ประเภท DDoS



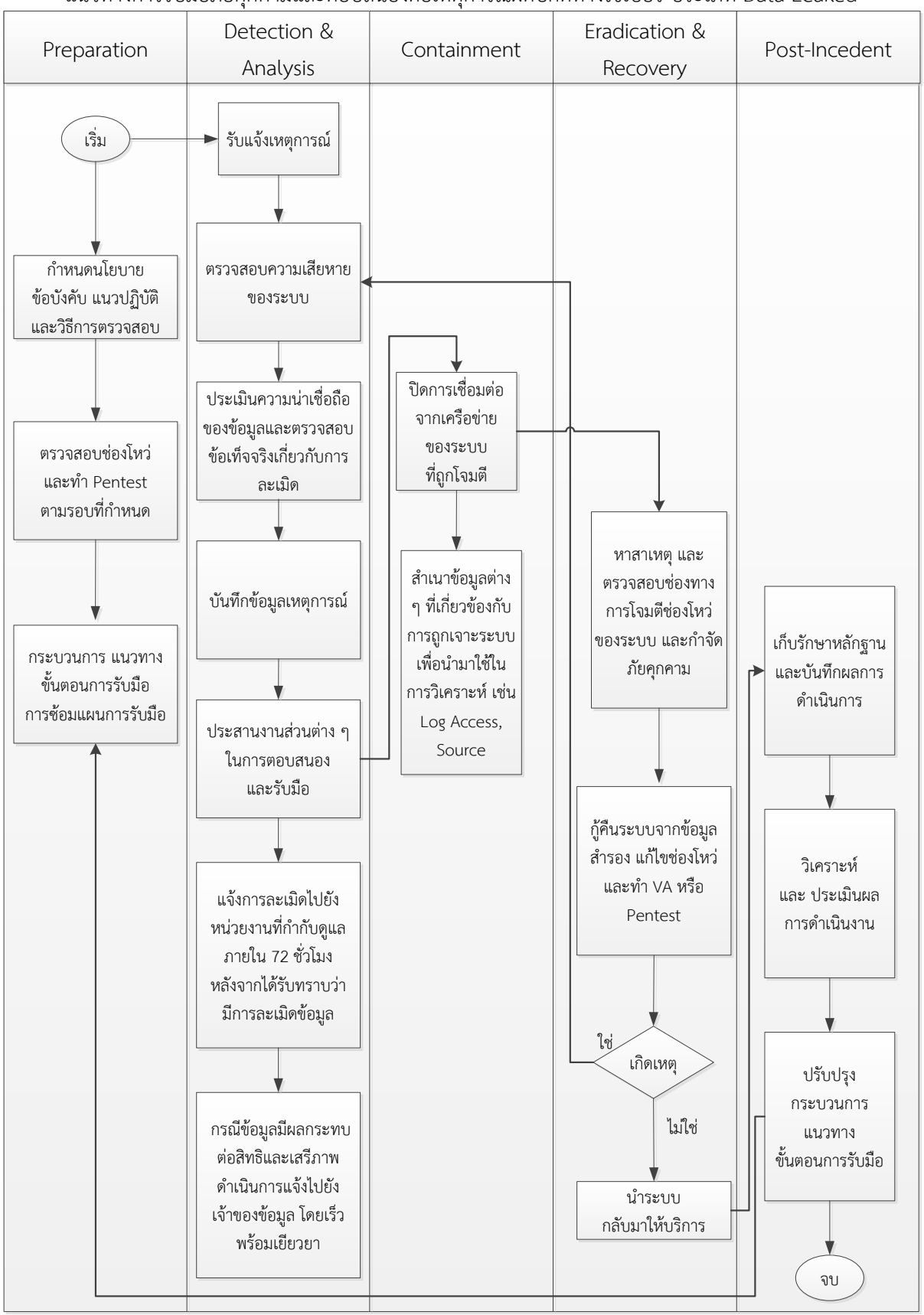
แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ประเภท Ransomeware



แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ประเภท Web Defacement



แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ประเภท Data Leaked



ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ICTC.M-SOCIETY.GO.TH

ธันวาคม 2566

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ICTC.M-SOCIETY.GO.TH

มิถุนายน 2567