

## แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

### องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แนวปฏิบัติ

๑.๑ จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้งโดยมีขอบเขตของการตรวจสอบ ดังนี้

(๑) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(๒) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นเจ้าของและใช้บริการตามผลการวิเคราะห์ในข้อ (ก)

(๓) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติมาตรฐานการปฏิบัติงาน และที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนด

๑.๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการ ตรวจสอบ ด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติภายในกำหนด ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในพระราชบัญญัติฯ (มาตรา ๕๔) พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย ทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ให้สำนักงานฯ ประกาศกำหนด

๑.๓ ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑ เว้นแต่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ วันนับจากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(๑) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(๒) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๓.๑

๑.๔ ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๑.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.



## องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แนวปฏิบัติ

เพื่อให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

### ๒.๑ การประเมินความเสี่ยง (Risk Assessment)

(๑) การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(๒) การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(๓) การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการทำงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

### ๒.๒ การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับนอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำเร็จและความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

### ๒.๓ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

## ๒.๔ การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

### องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์แนวปฏิบัติ

๓.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(๑) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

(๒) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๕) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๖) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๗) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๘) ระเบียบวิธีมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ

(๙) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ



๓.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๓.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐและ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์