

## แบบประเมินความสอดคล้อง ของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คำชี้แจง :

๑. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย ประมวลแนวทางปฏิบัติ จำนวน ๓ ข้อ และกรอบมาตรฐาน จำนวน ๑๕ ข้อ
๒. เนื่องจากมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้สอดคล้องกับประกาศดังกล่าว ทั้งในส่วนของประมวลแนวทางปฏิบัติ จำนวน ๓ ข้อ และกรอบมาตรฐาน จำนวน ๑๕ ข้อ ซึ่งอาจมีเอกสารที่ต้องดำเนินการเป็นจำนวนมาก สำนักงานจึงกำหนดให้หน่วยงานเริ่มดำเนินการในส่วนของประมวลแนวทางปฏิบัติทั้ง ๓ ข้อก่อน โดยให้แล้วเสร็จภายในวันที่ ๑๕ กันยายน ๒๕๖๖ ทั้งนี้ สำนักงานจะได้พิจารณาแจ้งให้หน่วยงานได้ดำเนินการจัดทำในส่วนของกรอบมาตรฐานเป็นลำดับต่อไป
๓. แบบประเมินนี้ มีวัตถุประสงค์เพื่อช่วยให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นำไปใช้ในการประเมินว่าประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน มีความสอดคล้องกับประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน ๓ ข้อ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ หรือไม่
๔. การประเมินความสอดคล้องนี้ หน่วยงานจำเป็นต้องอ้างอิงถึงหลักฐานที่ชัดเจนว่าได้มีการดำเนินการอย่างไร พร้อมแนบหลักฐานดังกล่าวมายังสำนักงาน ทั้งนี้ หน่วยงานของท่านอาจพิจารณาปิด (Masking) ส่วนของข้อมูลที่มีความอ่อนไหว (Sensitive data) ได้ และการประเมินโดยหน่วยงานของท่านเป็นเพียงการประเมินขั้นต้นเท่านั้น ยังไม่ถือว่าได้มีการจัดทำแผนรับมือฯ สอดคล้องกับประกาศดังกล่าวข้างต้น จนกว่าสำนักงานจะได้ตรวจสอบแล้วเสร็จ และแจ้งเป็นหนังสือรับรองกลับไปยังหน่วยงานเป็นลายลักษณ์อักษร แล้วเท่านั้น

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน
		มี	ไม่มี	
	<b>แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์</b>			
๑๗.๑	ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบดังนี้			
	(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)			
	(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)			
	(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด			
๑๗.๒	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย		✓	
๑๗.๓	ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑๗.๑ เว้นแต่ กทม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้		✓	
	(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ		✓	
	(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๑๗.๓ (ก)		✓	
๑๗.๔	ในกรณีที่ กทม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กทม. กำหนด พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย		✓	
๑๗.๕	๑๗.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กทม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กทม.		✓	

	การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
	หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้			
๑๘.๑	การประเมินความเสี่ยง (Risk Assessment)			
	(ก) การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก	✓		
	(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม	✓		
	(ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการทำงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)	✓		
๑๘.๒	การจัดการความเสี่ยง (Risk Treatment)			
	ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ	✓		
	นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง	✓		
๑๘.๓	การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)			

	ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้	✓		
๑๘.๔	การรายงานความเสี่ยง (Risk Reporting)			
	ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย	✓		
	ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น			
	<b>แผนการรับมือภัยคุกคามทางไซเบอร์</b>			
๑๙.๑	ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้			
	(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	✓		
	(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	✓		
	(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT	✓		
	(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	✓		
	(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	✓		
	(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	✓		
	(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	✓		
	(ซ) ระเบียบวิธีมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการ	✓		

	ติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการ บังคับใช้กฎหมายเพื่อดำเนินคดี และ			
	(ณ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	✓		
๑๙.๒	ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสาร อย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของ หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	✓		
๑๙.๓	ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ	✓		
๑๙.๔	ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมี นัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของ หน่วยงานของรัฐและ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ ข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์	✓		

ลงชื่อ .....

( )

\*หลักฐานที่หน่วยงานอ้างอิง จะต้องนำส่งมายังสำนักงานด้วยวิธีการแบบปลอดภัย โดยอาจนำส่งโดยผู้นำสาร หรือด้วยวิธีการทางอิเล็กทรอนิกส์ (PGP) ตามคู่มือที่  
ส่งมาด้วย ทั้งนี้ หน่วยงานของท่านอาจพิจารณาปิด (Masking) ส่วนของข้อมูลที่มีความอ่อนไหว (Sensitive data) ได้

\*\*ผู้ลงชื่อ หมายถึง ผู้ที่ทำหน้าที่ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief Information Security Officer : CISO) หรือ ผู้บริหารด้านการรักษา  
ความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือ ผู้บริหารที่ได้รับมอบอำนาจจากผู้บริหารสูงสุดของหน่วยงานให้รับผิดชอบด้านการรักษา  
ความมั่นคงปลอดภัยไซเบอร์