ประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)
เรื่อง ประมวลแนวปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)
พ.ศ. ๒๕๖๖

เพื่อให้การปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เป็นไปอย่างมีประสิทธิภาพสอดคล้องกับมาตรฐานสากล อาศัยอำนาจมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบเทคโนโลยีดิจิทัลของสถาบันวิจัยและพัฒนาพื้นที่สูง เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีดิจิทัลในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ สถาบันวิจัยและพัฒนาพื้นที่สูง จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เรื่อง ประมวลแนวปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)"

ข้อ ๒ ประมวลแนวปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เป็นไปตามเอกสารแนบท้ายประกาศ

ข้อ ๓ ให้ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนและปรับปรุงประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้มีความทันสมัยเป็นปัจจุบัน และเป็นมาตรฐานที่ยอมรับได้อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒ ตุลาคม พ.ศ. ๒๕๖๖

(นางสาวทินรัตน์ พิทักษ์พงศ์เจริญ)
รองผู้อำนวยการสถาบันวิจัยและพัฒนาพื้นที่สูง ด้านบริหารจัดการ
รักษาการผู้อำนวยการสถาบันวิจัยและพัฒนาพื้นที่สูง

เอกสารแนบท้ายประกาศ

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรือร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือ สวพส. เป็นหน่วยงานที่มุ่งมั่นขับเคลื่อนด้วยข้อมูลและเทคโนโลยีดิจิทัลเพื่อยกระดับคุณภาพชีวิตของประชาชนบนบนพื้นที่สูงให้อยู่ดีมีสุขและเป็นมิตรกับสิ่งแวดล้อม โดยกำหนดเป้าหมายการเพิ่มขีดสมรรถนะขององค์กรด้วยเทคโนโลยีดิจิทัล (High Performance Organization) ด้วยการยกระดับการบริหารจัดการและการบริการสู่องค์กรดิจิทัล มีมาตรการรักษาความมั่นคงปลอดภัยในการเข้าใช้ข้อมูลและระบบงานดิจิทัล เพื่อให้การกำกับดูแลการบริหารงานด้านเทคโนโลยีดิจิทัลเป็นไปอย่างมีประสิทธิภาพ

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน จึงได้จัดทำเอกสารฉบับนี้ เพื่อให้สถาบันวิจัยและพัฒนาพื้นที่สูง (สวพส.) มีรูปแบบรวมถึงขั้นตอนปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ทั้งนี้ เพื่อใช้เป็นแนวทางสำหรับผู้ใช้งานข้อมูล ระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานให้ตะหนักถึงความมั่นคงปลอดภัยไซเบอร์ ปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยที่มีการกำหนดตามเอกสารฉบับนี้

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธสาสตร์และแผน
สถาบันวิจัยและพัฒนพื้นที่สูง (องค์การมหาชน)
ตุลาคม ๒๕๖๖

สารบัญ

	หน้า
๑. บทนำ	๔
๒. วัตถุประสงค์	๔
๓. ขอบเขต	๔
๔. คำนิยาม	๔
๕. การจัดทำประมวลแนวทางปฏิบัติ	๖
องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๗
องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๑๓
องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์	๒๒
๖. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๒๔

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(Guideline and Cybersecurity Framework)

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ

สถาบันวิจัยและพัฒนาพื้นที่สูง (สวพส.) ในฐานนะหน่วยงานของรัฐที่ให้บริการข้อมูล องค์ความรู้และงานวิจัยในการพัฒนาพื้นที่สูงผ่านระบบเทคโนโลยีสารสนเทศ สื่อสังคมออนไลน์ และ Mobile Application จึงจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถือปฏิบัติ โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกากับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สาหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสาคัญทางสารสนเทศ พ.ศ ๒๕๖๔ จาก สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานรัฐปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. วัตถุประสงค์ (PURPOSE)

เพื่อกำหนดกรอบแนวคิดและวิธีปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์นำไปใช้ในการดำเนินงานและการจัดการระบบงานเทคโนโลยีสารสนเทศของ สวพส. ให้มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล และเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. ขอบเขต (SCOPE)

เอกสารนี้ครอบคลุมกรอบและวิธีปฏิบัติสำหรับงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สำหรับสารสนเทศที่สำคัญของ สวพส.

๔. คำนิยาม

๑) หน่วยงาน หรือ องค์กร	หมายถึง	สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือ สวพส.
๒) คณะกรรมการ	หมายถึง	คณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์
๓) บริการที่สำคัญ	หมายถึง	ภารกิจหรือบริการของหน่วยงาน

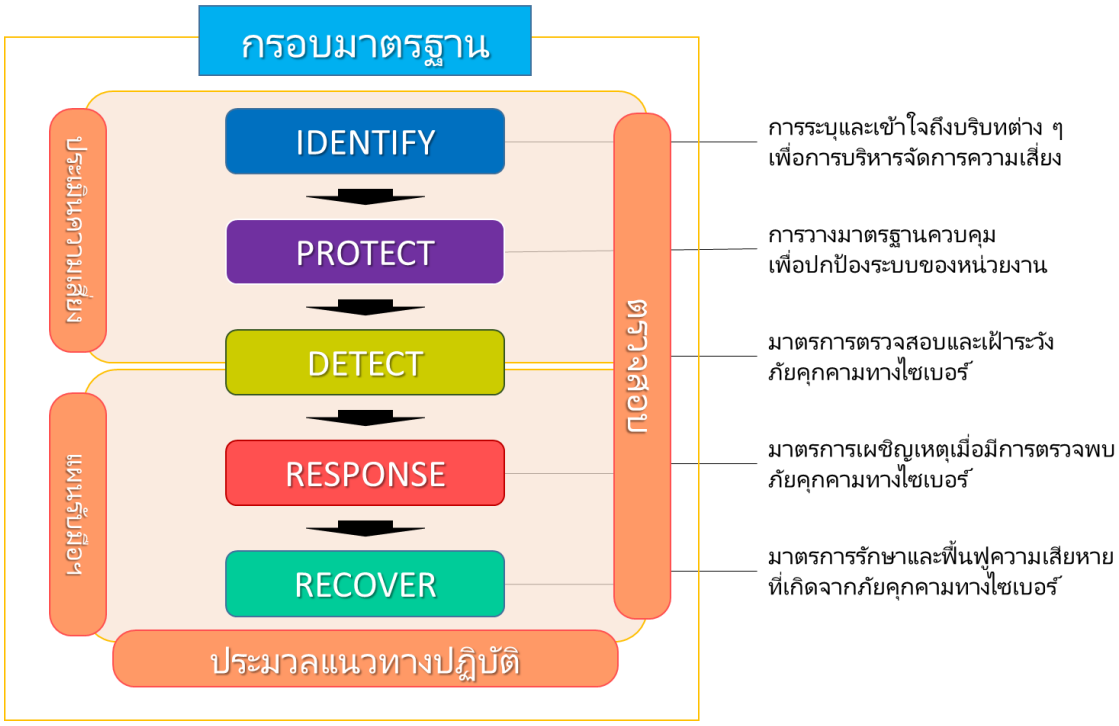
๔) ตัวชี้วัดความเสี่ยงที่สำคัญ	หมายถึง	เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงเพิ่มขึ้นพร้อมทั้งพร้อมทั้งสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย
๕) ผู้ให้บริการภายนอก	หมายถึง	บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของ สวพส. หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของ สวพส. หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดย สวพส. ได้
๖) interface	หมายถึง	การเชื่อมต่อกันระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์ สามารถถ่ายโอนข้อมูลซึ่งกันและกันได้
๗) คอมไพเลอร์ (Compiler)	หมายถึง	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
๘) แพตช์ (Patch)	หมายถึง	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
๙) Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
๑๐) Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๑๑) Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้การดำเนินงานตามภารกิจหยุดชะงัก เพื่อรองรับการดำเนินภารกิจหรือบริการสำคัญอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ระยะเวลาแก้ไขภัยคุกคามให้ทำงานได้ตามปกติให้เร็วที่สุด

๑๒) เหตุการณ์ (Event)	หมายถึง	การเกิดขึ้นที่สังเกตได้ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้
๑๓) เหตุภัยคุกคามทางไซเบอร์ (Cyber incident)	หมายถึง	เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
๑๔) ภัยคุกคามทางไซเบอร์ (Cyber threat)	หมายถึง	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
๑๕) เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ	หมายถึง	เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๕. การจัดทำประมวลแนวทางปฏิบัติ

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ซึ่งจัดทำประมวลแนวทางปฏิบัติ มีองค์ประกอบ ดังนี้

๑) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
๒) การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
๓) แผนการรับมือภัยคุกคามทางไซเบอร์



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

องค์ประกอบที่ ๑ แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

๑.๑ ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยหน่วยงาน เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน โดยมีเกณฑ์การพิจารณามี ๒ ประการ ได้แก่ ความเป็นอิสระและความสามารถที่หน่วยตรวจสอบภายใน หรือทีมงาน (audit firm/team) และผู้ตรวจสอบ (auditors) ที่เสนอจำเป็นต้องปฏิบัติตาม

หน่วยตรวจสอบภายใน หรือทีมงาน และผู้ตรวจสอบที่ได้รับการแต่งตั้ง:

ก. ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of interest) ใด ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใดที่ผลประโยชน์ของผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์ และ

ข. ควรมีความสามารถทางเทคนิคที่จำเป็น (เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง) เพื่อดำเนินการตรวจสอบ

ในกรณีผู้ตรวจสอบของหน่วยงานที่ได้รับการแต่งตั้งจากหน่วยงานแล้วลาออกจากการเป็นเจ้าหน้าที่ก่อนการดำเนินการตรวจสอบ หรือมีการเปลี่ยนแปลงเจ้าหน้าที่ ให้แจ้งต่อผู้บริหารของหน่วยงาน ภายใน ๓๐ วัน นับจากวันที่การเปลี่ยนแปลงอย่างเป็นทางการ

๑.๒ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

ก. กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)
ข. บริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (๑)
ค. การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใดที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด

๑.๓ ความคาดหวังในการตรวจสอบ (AUDIT EXPECTATIONS) ได้ระบุไว้ ๗ ประการดังนี้

๑.๓.๑ หลักการตรวจสอบ (Principles of Auditing) ควรยึดหลักการต่อไปนี้ เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้ เพื่อช่วยให้ผู้ตรวจสอบซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน

ก. ความซื่อสัตย์ (Integrity): รากฐานของความเป็นมืออาชีพ
   - ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
   - ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ
   - ดำเนินการตรวจสอบอย่างเป็นกลาง
   - ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใดที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

ข. การนำเสนออย่างยุติธรรม (Fair Presentation): หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง
   - ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง
   - รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่าง
   - ทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ
   - ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจนและครบถ้วน

ค. การปฏิบัติอย่างมืออาชีพ (Due Professional Care): การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ
   - ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
   - ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

ง. การรักษาความลับ (Confidentiality): ความมั่นคงปลอดภัยของข้อมูล
   - ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
   - ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ
   - จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

จ. ความเป็นอิสระ (Independence): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบและความเที่ยงธรรมของข้อสรุปการตรวจสอบ
   - ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ
   - ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี
   - รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ

- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (audit evidence) เท่านั้น

๑.๓.๒ วัตถุประสงค์ในการตรวจสอบ

ก. ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

ข. ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๑.๓.๓ ขอบเขตการตรวจสอบ (Audit Scope) ครอบคลุมสิ่งต่อไปนี้:

ขอบเขต (Scope)	**คำอธิบาย (Description)**
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรครอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๑.๓.๔ แนวทางการตรวจสอบ (Audit Approach) ควรใช้ทั้งแนวทางการปฏิบัติตามข้อกำหนด (compliance approach) และตามความเสี่ยง (risk-based approach)

ค. การปฏิบัติตามข้อกำหนด (compliance approach) ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

ง. ตามความเสี่ยง (risk-based approach) ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญและตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๑.๓.๕ ข้อค้นพบการตรวจสอบ (Audit Finding) ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้:

ก. ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

ข. เน้นการค้นหาอย่างเป็นระบบ (systemic finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงานซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

ค. เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (corrective action) แล้วก็ตาม และ

ง. เน้นแนวปฏิบัติที่ดี (good practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบการตรวจสอบไว้อย่างชัดเจน

องค์ประกอบ (Attributes)	คำอธิบาย (Description)
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
เกณฑ์ (Criteria)	มาตรฐาน/ กฎ/ เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ
สาเหตุ (Cause)	สาเหตุที่แท้จริง (root cause) และเหตุผลที่สนับสนุนสำหรับสภาพหรือเงื่อนไขตรวจสอบ
ผลกระทบ (Effect)	ผลกระทบและนัยสำคัญของสภาพหรือเงื่อนไขที่ตรวจสอบ (ทันทีในอนาคตหรือที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบต่อบริการที่จำเป็นของหน่วยงาน ซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและการตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

๑.๓.๖ สรุปผลการตรวจสอบ (Audit Conclusion)

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

ก. ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

ข. ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

๑.๓.๗ รูปแบบรายงานการตรวจสอบ (Audit Report Format) ควรมีอย่างน้อยดังต่อไปนี้:

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน

เนื้อหา	คำอธิบาย
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๑.๓.๒ ของเอกสารนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๑.๓.๓ ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ และบทบาท และความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ: ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ ค. วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๑.๓.๕ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๑.๓.๖ ของเอกสารนี้

๑.๔. ขั้นตอนการปฏิบัติในการตรวจสอบ

๑) ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งเตรียมทรัพยากรที่เกี่ยวข้อง

๒) ผู้ตรวจสอบและคณะทำงานของหน่วยงาน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

- เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ
- การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ
- การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร
- การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ
- ยืนยันแผนการตรวจสอบ

๓) ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔) ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

- ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ
- ระดับความไม่สอดคล้องของข้อตรวจพบ
- ข้อเสนอแนะในการปรับปรุง
- สรุปผลการตรวจสอบ
- กำหนดการตรวจติดตาม (ถ้ามี)

๕) ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๖) คณะทำงานรับทราบผลการตรวจสอบ

๗) ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงาน

๘) ความไม่สอดคล้อง (Non-conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษาความลับในการตรวจสอบ

๙) คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๑๐) คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๑๑) ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

เพื่อให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ กำหนดความเสี่ยง (Define Risk)

มีคำจำกัดความมากมายเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนั้น ก่อนที่จะกำหนดรายละเอียดเพิ่มเติมเกี่ยวกับการประเมินความเสี่ยง สิ่งสำคัญคือต้องกำหนดคำนิยามทั่วไป ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับวัตถุประสงค์ของแนวทางฉบับนี้ ความเสี่ยงถูกกำหนดให้เป็นผลลัพธ์ของ ๒ ปัจจัย คือ (๑) ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน และ (๒) ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (**Likelihood**, **Impact**)

ปัจจัยเสี่ยงแต่ละประการที่กล่าวถึงในคำจำกัดความได้อธิบายไว้ด้านล่าง

เหตุการณ์ภัยคุกคาม (Threat Event) หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor)[๑] ใช้เวกเตอร์ ภัยคุกคาม (การกระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย (เรียกว่า เวกเตอร์การโจมตี (Threat Vector)[๒]) กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP) ที่ใช้โดยผู้คุกคาม

ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สิน หรือการควบคุมภายในของกระบวนการ

ความน่าจะเป็น (Likelihood) หมายถึง ความน่าจะเป็นที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ สามารถใช้ประโยชน์จากช่องโหว่ที่กำหนด (หรือชุดของช่องโหว่) ความน่าจะเป็นสามารถได้รับจากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ (Reproducibility)

[๑] ผู้คุกคาม หมายถึง บุคคล หรือองค์กร หรือภาครัฐที่รับผิดชอบต่อเหตุการณ์ที่อาจส่งผลเสียหายต่อองค์กร

[๒] เวกเตอร์ภัยคุกคาม หมายถึง เส้นทางหรือเส้นทางที่ผู้คุกคามใช้เพื่อโจมตีเป้าหมาย

ผลกระทบ (Impact) หมายถึง ขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

๒.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)[๓] หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ของหน่วยงานที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ:

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตัวอย่างของตารางการยอมรับความเสี่ยงและต้องปรับแต่งตามแต่ละรายการเพื่อให้เหมาะสมกับบริบทของหน่วยงาน

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
High	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็น**ต้องยุติลงทันที** ทางเลือกที่เป็นไปได้ คือ กลยุทธ์การลดระดับความเสี่ยงหรือการถ่ายโอนความเสี่ยง จำเป็นต้องดำเนินการทันที
Medium	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้ **กลยุทธ์การรักษาที่มุ่งลดระดับความเสี่ยง** ควรได้รับการพัฒนาและดำเนินการใน ๓ - ๖ เดือนข้างหน้า
Low	ความเสี่ยงระดับนี้**สามารถยอมรับได้หากไม่มีกลยุทธ์การจัดการความเสี่ยง**ที่สามารถดำเนินการได้ง่ายและประหยัด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม

[๓] แหล่งข้อมูล เช่น ISACA นิยามการยอมรับความเสี่ยง (risk tolerance) ว่าเป็น “ระดับความแปรผันที่ยอมรับได้ (acceptable level) ซึ่งผู้บริหารเต็มใจที่จะยอมให้กับความเสี่ยงใด ๆ โดยเฉพาะเมื่อองค์กรดำเนินการตามวัตถุประสงค์” และใช้คำว่าความเสี่ยงที่ยอมรับได้ (risk appetite) เพื่ออ้างถึง "ปริมาณความเสี่ยงบนระดับกว้างที่กิจการยินดีรับตามพันธกิจ” เอกสารแนวทางฉบับนี้ไม่ได้แยกความแตกต่างระหว่างการยอมรับความเสี่ยง (risk tolerance) และความเสี่ยงที่ยอมรับได้ (risk appetite) เนื่องจากพิจารณาว่าทั้งสองอย่างนี้มีความหมายกว้างๆ เหมือนกัน (เช่น ความเสี่ยงที่องค์กรยินดียอมรับ)

๒.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในการประเมินความเสี่ยง ได้แก่

หัวหน้าหน่วยงาน (Head of Organization)

เจ้าหน้าที่ระดับสูงสุด (Highest-level Senior Official) ภายในหน่วยงานที่มีภาระหน้าที่และความรับผิดชอบโดยรวม (Responsibility and Accountability) ในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของหน่วยงาน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

เจ้าของกระบวนการหลัก (Business Owner)

เจ้าหน้าที่ระดับสูงสุดของสำนักหรือเทียบเท่า (Business Unit) ที่รับผิดชอบในการตรวจสอบให้แน่ใจว่ากิจกรรมตามภารกิจหรือบริการบรรลุเป้าหมาย/เป้าประสงค์ของสำนัก หรือแบ่งปันข้อกังวล หรือข้อสังเกตเกี่ยวกับผลกระทบที่มีต่อการดำเนินงานตามเป้าหมายในกรณีที่ระบบมีการหยุดชะงัก

ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งหน่วยงาน ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและเจ้าของกระบวนการหลักในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุนการทำงานของระบบที่สนับสนุนกิจกรรมตามภารกิจหรือบริการ ควรรู้จักทรัพย์สินของระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

๒.๔ การประเมินความเสี่ยง (Risk Assessment)

ก. การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

งาน A: ระบุทรัพย์สิน (Identify Assets)

เป็นสิ่งแรกที่ควรดำเนินการ โดยระบุและสร้างทะเบียนทรัพย์สินทางกายภาพและทางตรรกะทั้งหมดที่ประกอบกันเป็นระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยง ดังนี้

- **ทรัพย์สินสำคัญ** มีความสำคัญต่อการบรรลุวัตถุประสงค์ของหน่วยงานโดยรวม และมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์ เช่น ในระบบควบคุมแบบกระจาย (Distributed Control System (DCS)) ของโรงไฟฟ้า โปรแกรมควบคุมลอจิกแบบตั้งโปรแกรมได้ (Programmable Logic Controller (PLC)) ที่ควบคุมระบบไฟฟ้ามักจะ

ได้รับการพิจารณาว่าเป็นทรัพย์สินสำคัญ เนื่องจากมีผลโดยตรงต่อการผลิตไฟฟ้า ซึ่งเป็นวัตถุประสงค์ทางธุรกิจโดยรวมของโรงไฟฟ้า ผู้โจมตีที่ต้องการขัดขวางการผลิตไฟฟ้า มีแนวโน้มที่จะโจมตีและควบคุมตรรกะภายใน PLC

- **ทรัพย์สินที่เกี่ยวข้อง** เป็นทรัพยากรที่ผู้โจมตีต้องการควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ เช่น ในสภาพแวดล้อม Windows ทั่วไป เซิร์ฟเวอร์ Active Directory (AD) ที่เก็บรักษาหรือตรวจสอบข้อมูลรับรองการเข้าสู่ระบบของผู้ใช้ไปยังเซิร์ฟเวอร์หลายเครื่องมักจะได้รับการพิจารณาว่าเป็นทรัพย์สินที่เกี่ยวข้อง เนื่องจากเป็นสะพานเชื่อมให้ผู้โจมตีเปลี่ยนเข้าสู่เซิร์ฟเวอร์เหล่านี้

ใช้รายการทรัพย์สินที่รวมเข้าด้วยกันเพื่อสร้างแผนผังสถาปัตยกรรมเครือข่ายที่แสดงภาพของเส้นทางการเชื่อมต่อระหว่างกันและการสื่อสารระหว่างทรัพย์สิน ระบุจุดเข้าทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายในระบบ รวมถึงทรัพย์สินที่เกี่ยวข้องและทรัพย์สินสำคัญ สิ่งนี้จะช่วยอำนวยความสะดวกในงานต่อไปในการระบุภัยคุกคาม

งาน B: การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)

มีขั้นตอนต่อไปนี้

๑) **การระบุขอบเขตและการจำแนกระบบ** เป็นข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคามที่แนะนำในงาน A

๒) **การระบุภัยคุกคาม** หน่วยงานควรใช้แนวทางที่เป็นระบบเพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

๓) **การสร้างแบบจำลองการโจมตี** หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว หน่วยงานควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้หน่วยงานสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

งาน C: สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป สถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก ๔ ประการ ต่อไปนี้

๑) ทรัพย์สิน (Asset) สิ่งที่มีค่าที่ได้รับการระบุในงาน A

๒) เหตุการณ์ภัยคุกคาม (Threat event) เหตุการณ์การโจมตีที่ระบุในงาน B

๓) ช่องโหว่ (Vulnerability) จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง

๔) ผลที่ตามมา (Consequence) ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

ข. การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น; และ
(๒) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

งาน A: กำหนดโอกาส (Determine Likelihood)

เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา เพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจไม่เหมาะสม โดยความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับการประเมินจากภัยคุกคามและช่องโหว่ ซึ่งพิจารณาปัจจัยดังนี้

- **ความสามารถในการค้นพบ (Discoverability)** สามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่
- **ความสามารถในการใช้ประโยชน์ (Exploitability)** เป็นการใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี
- **ความสามารถในการทำซ้ำ (Reproducibility)** สามารถสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

ตัวอย่างตารางการประเมินเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำตามขั้นตอนต่อไปนี้

- ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น ๓ ระดับ (ระดับ ๑ – ๓)
- เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด
- คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสี่ยง โดยระดับ ๓ คือ “มีแนวโน้มสูง” และ ๑ คือ “เป็นไปได้ยาก”

Likelihood Rating	ความสามารถในการค้นพบ (Discoverability)	ความสามารถในการใช้ประโยชน์ (Exploitability)	ความสามารถในการทำซ้ำ Reproducibility
High (๓)	ช่องโหว่ของเป้าหมาย: ☐ สามารถค้นพบได้โดยการค้นหา/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, ExploitDB)	การโจมตี: ☐ สามารถดำเนินการได้โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย	การโจมตี: ☐ สามารถทำซ้ำได้ตามต้องการโดยไม่มีการกำหนดค่า (Configuration)[๔] หรือเงื่อนไขของเหตุการณ์

[๔] การกำหนดค่า หมายถึง การตั้งค่าในฮาร์ดแวร์ ซอฟต์แวร์ หรือเฟิร์มแวร์ที่สามารถเปลี่ยนแปลงได้ ซึ่งส่งผลต่อท่าทางการรักษาความมั่นคงปลอดภัยและ/หรือการทำงานของระบบ ตัวอย่างเช่น การเปิดใช้งานบริการ Telnet

Likelihood Rating	ความสามารถในการค้นพบ (Discoverability)	ความสามารถในการใช้ประโยชน์ (Exploitability)	ความสามารถในการทำซ้ำ Reproducibility
	☐ สามารถถูกค้นพบและถูกโจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	☐ สามารถทำได้ด้วยเครื่องมือที่หาได้ทั่วไป โดยไม่ต้องมีความรู้ด้านเทคนิค	(Event Condition)[๕] ☐ สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่
Medium (๒)	ช่องโหว่ของเป้าหมาย: ☐ สามารถค้นพบได้โดยการตรวจสอบการตอบสนอง พฤติกรรม และการสื่อสารของเป้าหมาย (เช่น การฟัซ (Fuzzing) กับแพ็กเก็ตเครือข่าย การดักจับเครือข่าย (Network Sniffing)) ☐ สามารถถูกค้นพบและโจมตีจากภายในเครือข่ายย่อยหรือส่วนเครือข่ายเดียวกัน	การโจมตี: ☐ สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) ของเป้าหมาย (เช่น Admin/SYSTEM/ Root) ☐สามารถดำเนินการได้ด้วยเครื่องมือที่เปิดเผยต่อสาธารณะ ซึ่งต้องใช้ความรู้ด้านเทคนิคในระดับกลาง	การโจมตี: ☐ สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์ที่คาดเดาได้บางอย่าง ☐ สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย
Low (๑)	ช่องโหว่ของเป้าหมาย: ☐ สามารถค้นพบได้โดยการดำเนินการและโต้ตอบกับการตั้งค่าปัจจุบันหรือที่คล้ายกันของเป้าหมาย ☐ สามารถถูกค้นพบและโจมตีด้วยการเข้าถึงแบบลอจิคัลโลคัล	การโจมตี: ☐ สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin / SYSTEM / Root) ☐ สามารถดำเนินการได้ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะซึ่งต้องการความรู้ด้านเทคนิคขั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน	การโจมตี: ☐ สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุ่มบางอย่าง ☐ สามารถทำซ้ำได้ในทางทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่

[๕] เงื่อนไขของเหตุการณ์ หมายถึง สถานการณ์/สภาพแวดล้อมของคอมพิวเตอร์ที่ต้องมีอยู่เพื่อให้ได้ผลลัพธ์ที่ต้องการ ตัวอย่างเช่น งานแบทช์เฉพาะกิจ (ad-hoc batch job) จำเป็นต้องทำงานเพื่อให้การโจมตีดำเนินการได้

งาน B: กำหนดผลกระทบ (Determine Impact)

สถานการณ์ความเสี่ยงอาจส่งผลต่อการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และ/หรือความพร้อมใช้งาน (Availability) ของทรัพย์สิน (เช่น ข้อมูล อุปกรณ์ การดำเนินงาน) การโจมตีใด ๆ ของทรัพย์สินจะแปลเป็นผลกระทบในสาม (๓) ระดับต่อไปนี้

- ระดับชาติ (National) ผลกระทบอาจเป็นอันตรายต่อความมั่นคงและเศรษฐกิจของประเทศ
- หน่วยงาน (Organisational) ผลกระทบอาจเกิดการหยุดชะงักในการดำเนินงาน ความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน
- บุคคล (Individual) ผลกระทบอาจเกิดการสูญเสียชีวิตและการบาดเจ็บ

ตัวอย่างตารางประเมินเพื่อพิจารณาผลกระทบของความเสี่ยงในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” และ ๑ คือ “เล็กน้อย”) คำอธิบายที่ระบุในตารางตัวอย่างด้านล่างเป็นข้อมูลทั่วไป หน่วยงานควรตรวจสอบและปรับแต่งคำอธิบายสำหรับการจัดอันดับผลกระทบแต่ละรายการ

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	**ผลกระทบที่อาจเกิดขึ้น (potential impact)***		
	ต่ำ	**กลาง**	**สูง**
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)	มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)	มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)
ด้านการรักษาความถูกต้องครบถ้วน (Integrity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบ	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบ	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบ

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
	น้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	อย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	อย่างร้ายแรงมาก (Severe or Catastrophic)และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ตารางตัวอย่างเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
การเงินหรือรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินสิบล้านบาท	เกินกว่าสิบล้านบาทขึ้นไป
อันตรายต่อชีวิต ร่างกายหรืออนามัย	ไม่มีผู้ใช้บริการ หรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย	ผู้ใช้บริการ หรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยไม่เกินหนึ่งพันคน	ผู้ใช้บริการ หรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน
ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับ ความเสียหายนอกจากอันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	ไม่มีผลกระทบ หรือมีผลกระทบต่อการดำเนินการตามหน้าที่ของหน่วยงานเพียงเล็กน้อย	การดำเนินการตามหน้าที่หลักของหน่วยงานด้อยประสิทธิภาพลงมากแต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	การดำเนินการตามหน้าที่หลักของหน่วยงานต้องหยุดชะงัก ไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน
ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายใน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐต้องหยุดชะงัก ไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตาม

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
		ระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	แผนกู้คืนระบบของหน่วยงาน เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้

ค. การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินงานของหน่วยงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒.๕ การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๒.๖ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๗ การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย

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

องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือ สวพส. ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง ๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่ง (๑) ครั้ง และ ๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) พ.ศ. ๒๕๖๕ และนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) พ.ศ. ๒๕๖๕ ด้วย

วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในหน่วยงาน โดยเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใต้หน่วยงาน การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของหน่วยงาน

แนวปฏิบัติ

๓.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจน และมีรายละเอียดการติดต่อ

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	ผู้อำนวยการสำนักยุทธศาสตร์และแผน *๐๕๓-๓๒๘๔๙๖-๘ ต่อ ๑๓๐๖*	หัวหน้าทีมรับมือเหตุการณ์ ฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	หัวหน้าศูนย์ข้อมูลและสารสนเทศ *๐๕๓-๓๒๘๔๙๖-๘ ต่อ ๑๒๑๑*	รองหัวหน้าทีมรับมือเหตุการณ์ ฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	เจ้าหน้าที่ศูนย์ข้อมูลที่ได้รับมอบหมาย *๐๕๓-๓๒๘๔๙๖-๘ ต่อ ๑๓๐๕*	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

- **ขั้นการเตรียมการ** เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

  (๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ (ก)

  (๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- **ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์** เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

- **ขั้นการระงับภัยคุกคามทางไซเบอร์** การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เป็นการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

  (๑) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ รายละเอียดตามข้อ (ฌ)

(๒) ดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

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

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ เช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ

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

๓.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๓.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๖. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย ๕ หัวข้อหลัก

๖.๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

(๑) การจัดการทรัพย์สิน (Asset Management)

(๒) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(๓) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(๔) การจัดการผู้ให้บริการภายนอก (Third Party Management)

๖.๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

(๑) การควบคุมการเข้าถึง (Access Control)
(๒) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)
(๓) การเชื่อมต่อระยะไกล (Remote Connection)
(๔) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)
(๕) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
(๖) การแบ่งปันข้อมูล (Information Sharing)

๖.๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

(๑) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๖.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

(๑) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
(๒) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
(๓) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๖.๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

(๑) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

หัวข้อหลักที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

กรอบมาตรฐาน

๑.๑ การจัดการทรัพย์สิน (Asset Management)

๑.๑.๑ ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(ก) ชื่อ/คำอธิบายของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
(ข) ฟังก์ชันที่สำคัญของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
(ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สิน บริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
(ง) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
(จ) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่ละรายการ และ

(ฉ) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน และ/หรือภายนอก

๑.๑.๒ ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๓ ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละหนึ่ง (๑) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๑.๔ ตามมาตรา ๕๔ ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ อย่างน้อยปีละหนึ่ง (๑) ครั้ง

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑.๒.๑ ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง (๑) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด

๑.๒.๒ ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) วันที่ระบุความเสี่ยง (Date the Risk is Identified)
(ข) คำอธิบายของความเสี่ยง (Description of the Risk)
(ค) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
(ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
(จ) การจัดการความเสี่ยง (Risk Treatment)
(ฉ) เจ้าของความเสี่ยง (Risk Owner)
(ช) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ
(ซ) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๑.๓.๑ ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงานเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งเป็น

(ก) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)

(ข) ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

๑.๓.๒ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

(ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
(ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) และ
(ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๓ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๔ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๑.๓.๕ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๑.๓.๖ ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๑.๓.๗ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระ จากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

๑.๓.๘ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

๑.๓.๙ ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

๑.๓.๑๐ หากได้รับการร้องขอจาก กกม. หรือสำนักงาน หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว ไปยังสำนักงานภายในกำหนด ๓๐ (สามสิบ) วัน นับแต่วันที่ได้รับหนังสือด้วย

ทั้งนี้ รูปแบบรายงานสรุปผลการทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๑.๔. การจัดการผู้ให้บริการภายนอก (Third Party Management)

๑.๔.๑ ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอก จะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์
(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ และ
(ง) สิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

หัวข้อหลักที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

กรอบมาตรฐาน

๒.๑ การควบคุมการเข้าถึง (Access Control)

๒.๑.๑ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถูกจำกัดไว้ที่

(ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต และ
(ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๒.๑.๒ ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ ๒.๑.๑ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk

Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๑.๓ ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒.๑.๔ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดย

(ก) ทำภายใต้การดูแลของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้น และ
(ข) ดำเนินการในสถานที่ หากเป็นไปได้

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
(ข) การแบ่งแยกหน้าที่ (Separation of Duties)
(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
(ง) การลบบัญชีที่ไม่ได้ใช้
(จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)
(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
(ช) การป้องกันมัลแวร์ (Malware) และ
(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบ อย่างทันการณ์และเหมาะสม

๒.๒.๓ ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๒.๔ ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละหนึ่ง (๑) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๕ ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒.๓.๑ ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น
(ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
(ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น
(ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ และ
(จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยใช้มาตรการอย่างน้อย ดังนี้

(ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น
(ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ ๒.๑.๑ (ข) เท่านั้น และ
(ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมด ไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๔.๒ ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๕.๑ ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สาม ที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่
- พนักงานใหม่ (New Employees)
- ผู้ใช้และระดับบริหาร (Users and Management)
- เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS และ
- ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

(ข) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ

(ง) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

๒.๕.๒ ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง (๑) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

หัวข้อหลักที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

กรอบมาตรฐาน

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๓.๑.๑ ต้องสร้างกลไกและกระบวนการเพื่อ

(ก) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และ

(ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือไม่

๓.๑.๒ ต้องดำเนินการทบทวนกลไกและกระบวนการภายในข้อ ๓.๑.๑ อย่างน้อยปีละหนึ่ง (๑) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อหลักที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

กรอบมาตรฐาน

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๔.๑.๑ ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง (๑) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

(ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

(ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

(ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

(ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าว แถลงกับสื่อมวลชน และ

(จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๔.๒.๓ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละหนึ่ง (๑) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๔.๓.๑ ตามมาตรา ๒๒ วรรคหนึ่ง (๑๓) หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว อาจดำเนินการได้ ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

๔.๓.๒ ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามข้อ ๔.๑ และข้อ ๔.๒ ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญ ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หัวข้อหลักที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

กรอบมาตรฐาน

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๕.๑.๑ ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) แ ล ะ Recovery Point Objective (RPO) เป็นต้น

การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไป ตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๕.๑.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละหนึ่ง (๑) ครั้ง ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์