ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน
เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์
ของกรมพินิจและคุ้มครองเด็กและเยาวชน

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ และให้จัดทำนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและเชื่อถือได้ สอดคล้องกับการพัฒนาของเทคโนโลยีสารสนเทศในปัจจุบัน กรมพินิจและคุ้มครองเด็กและเยาวชน จึงได้มีการจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ของกรมพินิจและคุ้มครองเด็กและเยาวชน จึงออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน เรื่องมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ของกรมพินิจและคุ้มครองเด็กและเยาวชน”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ ประกาศนี้ให้กรมพินิจและคุ้มครองเด็กและเยาวชน ดำเนินการให้ผู้ที่เกี่ยวข้องและผู้ใช้งานทั้งหมด ได้รับทราบโดยทั่วกันผ่านทางเว็บไซต์ https://www.djop.go.th ของกรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๔ ให้ใช้มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ของกรมพินิจและคุ้มครองเด็กและเยาวชน ที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๗ สิงหาคม พ.ศ. ๒๕๖๗

พันตำรวจโท
(ประวุธ วงศ์สีนิล)
อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน

บัญชีแนบท้ายประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน
เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์
ของกรมพินิจและคุ้มครองเด็กและเยาวชน

สารบัญ

บัญชีแนบท้ายประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน
เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

****

หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ และให้จัดทำนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและเชื่อถือได้

กรมพินิจและคุ้มครองเด็กและเยาวชนฐานะหน่วยงานของรัฐ ได้ให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน จึงดำเนินการจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชน โดยกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ หรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

วัตถุประสงค์

เพื่อจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชน และยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชนในภาพรวมให้ชัดเจนและเป็นไปในทิศทางเดียวกัน

คำนิยาม

หน่วยงาน	หมายถึง	กรมพินิจและคุ้มครองเด็กและเยาวชน
ช่องโหว่ (Vulnerability)	หมายถึง	จุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สิน หรือการควบคุมภายในของกระบวนการ
ความน่าจะเป็น (Likelihood)	หมายถึง	ความน่าจะเป็นที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ สามารถใช้ประโยชน์จากช่องโหว่ที่กำหนด (หรือชุดของช่องโหว่) ความน่าจะเป็นสามารถได้รับจากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ (Reproducibility)
ผลกระทบ (Impact)	หมายถึง	ขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จาก ช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

ส่วนที่ ๑
นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙(๒) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ กำหนดนโยบาย การบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ จัดทำเพื่อเป็นแนวทางการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการดำเนินการ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ใช้หลักการ ตามแนวทางการปฏิบัติที่ดีที่ใช้กันแพร่หลายทั่วโลก รวมถึงประเทศไทย ซึ่งคือ หลักการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) ประกอบด้วย ๓ หลักการ ดังนี้

๑.๑ การกำกับดูแลการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

ปัจจุบันภาครัฐให้ความสำคัญกับความเสี่ยงทางด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ไม่ว่าจะเป็นอุปสรรคที่เกิดจากการจู่โจมทางระบบเทคโนโลยีสารสนเทศจากภายนอก หรือการรั่วไหลของข้อมูลส่วนบุคคลและข้อภายในหน่วยงานรัฐ ความเสี่ยงดังกล่าวสามารถส่งผลกระทบต่อการดำเนินงาน และความปลอดภัยทางข้อมูลส่วนบุคคลของผู้ที่มีส่วนเกี่ยวข้องทั้งภายใน และภายนอกหน่วยงาน ดังนั้น กรมพินิจและคุ้มครองเด็กและเยาวชน จึงมุ่งพัฒนาระบบเพื่อสร้างเกราะกำบังทางระบบสารสนเทศผ่านโครงสร้างการกำกับดูแลที่มั่นคง การปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล การจัดอบรมเพื่อสร้างความมั่นใจ และความรู้ความเข้าใจให้แก่บุคลากรทุกคน

เป้าหมาย

๑. ไม่มีผู้ตกเป็นเหยื่อในการโจมตีหรือการทดสอบการโจมตีหลังจากผ่านการอบรมความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Cybersecurity)

๒. ลดระยะเวลาในการตรวจจับการโจมตีให้ได้เร็วที่สุด

การกำกับดูแลความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Cybersecurity Governance)

กรมพินิจและคุ้มครองเด็กและเยาวชน ได้กำกับและบริหารระบบความมั่นคงปลอดภัยด้านสารสนเทศ และกรอบความมั่นคงปลอดภัยด้านไซเบอร์เพื่อกำหนดทิศทางการทำงานให้ชัดเจน และสร้างความโปร่งใสแก่การบริหารงานเชิงนโยบายตลอดจนระดับปฏิบัติการ โดยสามารถแบ่งลำดับขั้นการบริหารได้ทั้งหมด ๓ ขั้น อันประกอบด้วย (๑) ระดับกำกับดูแล (๒) ระดับบริหารจัดการ และ (๓) ระดับปฏิบัติการ

ระดับ	หน้าที่	คณะกรรมการ / หน่วยงาน ที่เกี่ยวข้อง
ระดับกำกับดูแล	กำกับ ดูแล บริหารการดำเนินงาน และกำหนดทิศทางกลยุทธ์และเป้าหมาย	คณะกรรมการกำกับดูแลงานด้านดิจิทัลและเทคโนโลยี สารสนเทศ และคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ
ระดับบริหารจัดการ	จัดการข้อมูลสารสนเทศตามมาตรฐานและติดตามตรวจสอบความถูกต้องและแม่นยำ	หน่วยงาน Cybersecurity และคณะกรรมการบริหารความเสี่ยงระดับองค์กร
ระดับปฏิบัติการ	กำหนดระบบ วิธีปฏิบัติ และบริการ ให้แก่ผู้ใช้งานปฏิบัติตาม และ ประเมินการติดตามผลงานและรายงานความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงระดับองค์กร	หน่วยงาน Cybersecurity

แนวทางและกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Cybersecurity Framework)

๑. ทบทวนนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

๒. ซ้อมแผนรับมือภัยคุกคามจากการโจมตีด้านไซเบอร์และแผนการกู้คืนระบบสารสนเทศในหน่วยงานและประเมินประสิทธิภาพของแผนการดำเนินงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๓. จัดตั้งคณะทำงานที่มีหน้าที่ในการกำหนดแผนและขั้นตอนการดำเนินงาน รวมถึงการประเมินผลการดำเนินงานของหน่วยงานให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

๔. สร้างความตระหนักรู้และเตรียมความพร้อมด้านความปลอดภัยไซเบอร์ให้บุคลากรภายในหน่วยงานอย่างต่อเนื่อง โดยการจัดการอบรมเกี่ยวกับความเสี่ยงจากการโจมตีทางไซเบอร์ การรั่วไหลของข้อมูลสารสนเทศและความรู้ด้าน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

๑.๒ การบริหารความเสี่ยง

มาตราการป้องกันความเสี่ยง (mitigation actions) จากการคุกคามทางไซเบอร์ และการรั่วไหลของข้อมูลสารสนเทศ

๑. ทบทวนนโยบาย ความมั่นคงปลอดภัย ทางเทคโนโลยีสารสนเทศ อย่างต่อเนื่อง

๒. ซ้อมแผนรับมือภัยคุกคาม จากการโจมตีด้านไซเบอร์ และแผนการกู้คืนระบบ สารสนเทศในหน่วยงาน โดยจัดให้มีการทบทวน และประเมินประสิทธิภาพ ของแผนการดำเนินงาน ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ อย่างสม่ำเสมอ

๓. จัดตั้งคณะทำงาน คุ้มครองข้อมูลส่วนบุคคล ที่มีหน้าที่ในการกำหนดแผน และขั้นตอนการดำเนินงาน การประเมินผล การดำเนินงาน ของหน่วยงานให้สอดคล้อง กับ พ.ร.บ. คุ้มครองข้อมูล ส่วนบุคคล

๔. สร้างความตระหนักรู้ และเตรียมความพร้อม ด้านความปลอดภัย ไซเบอร์ให้บุคลากรทุกระดับ โดยจัดการอบรม เกี่ยวกับความเสี่ยงจาก การโจมตีทางไซเบอร์ การรั่วไหลของข้อมูล สารสนเทศ และความรู้ ด้าน พ.ร.บ. คุ้มครอง ข้อมูลส่วนบุคคล

๑.๓ แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แนวปฏิบัติ

๑.๑ จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

(๑) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(๒) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการตามผลการวิเคราะห์ในข้อ (ก)

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

๑.๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการ ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติภายในกำหนด ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในพระราชบัญญัติฯ (มาตรา ๕๔) พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วยทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ให้สำนักงานฯ ประกาศกำหนด

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

(๑) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(๒) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๓.๑

๑.๔ ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๑.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.

องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แนวปฏิบัติ

เพื่อให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 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) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment) ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัย

ไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน 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) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

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

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

๓.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๓.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐและ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒
ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑ แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

๒.๑.๑ แนวปฏิบัติ

๒.๑.๑.๑ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตในการตรวจสอบดังนี้

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติ และคณะกรรมการประกาศกำหนด

๒.๑.๑.๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดตามมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๒.๑.๑.๓ ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑. เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบ โดยดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๓.๑.๓ (ก.)

๒.๑.๑.๔ ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๒.๑.๑.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม.หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.

๒.๑.๒ ความคาดหวังในการตรวจสอบ

๒.๑.๒.๑ มีความถูกต้องแม่นยำการตรวจสอบควรดำเนินการอย่างครอบคลุมและถูกต้องตามมาตรฐานสากลเพื่อให้ได้ข้อมูลที่สะท้อนถึงสถานะของการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรอย่างแท้จริง

๒.๑.๒.๒ มีวัตถุประสงค์ การตรวจสอบควรดำเนินการอย่างเป็นกลางและปราศจากอคติ เพื่อให้ได้ข้อเสนอแนะและคำแนะนำ ที่เป็นประโยชน์ต่อการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

๒.๑.๒.๓ ความทันต่อเหตุการณ์ การตรวจสอบควรติดตามความเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์อยู่เสมอเพื่อให้คำแนะนำที่สอดคล้องกับสถานการณ์ปัจจุบัน

๒.๑.๒.๔ ความสามารถในการตอบสนองต่อภัยคุกคามอย่างรวดเร็วและมีประสิทธิภาพ

๒.๑.๒.๕ ความสามารถในการระบุและแก้ไขช่องโหว่ก่อนที่จะถูกใช้ประโยชน์

๒.๑.๒.๖ ความสามารถในการติดตามพฤติกรรมของผู้โจมตี

๒.๑.๒.๗ ความสามารถในการระบุและประเมินความเสี่ยงด้านความปลอดภัยไซเบอร์ขององค์กร

๒.๑.๓ หลักในการตรวจสอบ

การตรวจสอบควรยึดหลักการต่อไปนี้เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้เพื่อช่วยให้ผู้ตรวจสอบซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน

ก. ความซื่อสัตย์ (Integrity): รากฐานของความเป็นมืออาชีพ

- ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
- ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ
- ดำเนินการตรวจสอบอย่างเป็นกลาง
- ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

ข. การนำเสนออย่างยุติธรรม (Fair Presentation): หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง

- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง
- รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ
- ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจน และครบถ้วน

ค. การปฏิบัติอย่างมืออาชีพ (Due Professional Care): การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ

- ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
- ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

ง. การรักษาความลับ (Confidentiality): ความมั่นคงปลอดภัยของข้อมูล

- ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
- ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ
- จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

จ. ความเป็นอิสระ (Independence): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบ และความเที่ยงธรรมของข้อสรุปการตรวจสอบ

- ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ

• ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี

• รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ

• ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (audit evidence) เท่านั้น

๒.๑.๔ วัตถุประสงค์ในการตรวจสอบ

๒.๑.๔.๑ ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

๒.๑.๔.๒ ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๒.๑.๔.๓ เพื่อระบุช่องโหว่ การตรวจสอบ ควรหาช่องโหว่ต่าง ๆ ของระบบ เพื่อช่วยในการปรับปรุงแก้ไขและปิดเส้นทางในการเข้ามาเจาะระบบ

๒.๑.๔.๔ เพื่อประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล

๒.๑.๔.๕ เพื่อเสนอแนวทางการปรับปรุงความปลอดภัยของข้อมูล

๒.๑.๕ ขอบเขตการตรวจสอบ

การตรวจสอบจะครอบคลุมสิ่งต่อนี้

ขอบเขต (Audit Subject)	คำอธิบาย (Description)
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรคลอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษร ที่เกี่ยวข้อง

๒.๑.๖ แนวทางการตรวจสอบ (Audit Approach) การตรวจสอบควรใช้แนวทางการปฏิบัติตามข้อกำหนด (compliance approach) และตามความเสี่ยง (risk-based approach)

๒.๑.๖.๑ การปฏิบัติตามข้อกำหนด คือ ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๒.๑.๖.๒ ตามความเสี่ยง คือ ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๒.๑.๗ ข้อค้นพบการตรวจสอบ (Audit Finding)

๒.๑.๗.๑ ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

๒.๑.๗.๒ เน้นการค้นหาอย่างเป็นระบบ (systemic finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงานซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

๒.๑.๗.๓ เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (corrective action) แล้วก็ตาม

๒.๑.๗.๔ เน้นแนวปฏิบัติ (good practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบการตรวจสอบอย่างชัดเจน

องค์ประกอบ (Attributes)	คำอธิบาย (Description)
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
เกณฑ์ (Criteria)	มาตรฐาน/กฎ/เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคง ปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือ เงื่อนไขที่ตรวจสอบ
สาเหตุ (Cause)	สาเหตุที่แท้จริง (root cause) และเหตุผลที่สนับสนุนสำหรับสภาพหรือเงื่อนไข ที่ตรวจสอบ
ผลกระทบ (Effect)	ผลกระทบและนัยสำคัญของสภาพหรือเงื่อนไขที่ตรวจสอบ (ทันทีในอนาคตหรือ ที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบ ต่อบริการที่จำเป็นของหน่วยงาน ซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและ การตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการ ดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

๒.๑.๘ สรุปผลการตรวจสอบ (Audit Conclusion) ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

๒.๑.๘.๑ ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

๒.๑.๘.๒ ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

๒.๑.๙ รูปแบบรายงานของการตรวจสอบ (Audit Report Format) รายงานการตรวจสอบควรมีอย่างน้อยดังนี้

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วย คำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบ ที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมิน ความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหาร ควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุม
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๓.๔ ของเอกสารนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๓.๕ ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ และบทบาทความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการ ตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ: ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ ค. วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผล ของการควบคุม)

เนื้อหา	คำอธิบาย
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๓.๗ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๓.๘ ของเอกสารนี้

๒.๑.๑๐ ขั้นตอนปฏิบัติในการตรวจสอบ (Audit Process)

๒.๑.๑๐.๑ วิธีการประชุมก่อนตรวจประเมิน (Opening meeting)

๒.๑.๑๐.๑.๑ ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๒.๑.๑๐.๑.๒ ผู้ตรวจสอบและคณะทำงานของ กรมพินิจและคุ้มครองเด็กและเยาวชน ร่วมการประชุมเปิดการตรวจสอบโดยมีวัตุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

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

๒.๑.๑๐.๑.๓ ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานหน้าที่ตอบข้อซักถามและจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑.๑๐.๑.๔ ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

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

๒.๑.๑๐.๑.๕ ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๒.๑.๑๐.๑.๖ คณะทำงานรับทราบผลการตรวจสอบ

๒.๑.๑๐.๑.๗ ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษารักษาความลับ ในการตรวจสอบระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และที่แก้ไขเพิ่มเติม

๒.๑.๑๐.๑.๘ คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๒.๑.๑๐.๑.๙ คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๒.๑.๑๐.๑.๑๐ ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

๒.๑.๑๐.๒ วิธีการเก็บหลักฐานการตรวจสอบ (Audit evidence) ผู้ตรวจสอบมีสิทธิ์ที่จะยืนยันในการเข้าถึงแหล่งข้อมูลทั้งหมดที่มีอยู่ในองค์กรที่ได้รับการตรวจสอบเพื่อให้สามารถประเมินการควบคุมที่ประกาศได้อย่างเพียงพอ ตัวอย่างบางส่วนของแหล่งข้อมูล :

- บันทึก (Records) : บันทึกการเข้าใช้ห้องเซิร์ฟเวอร์ที่มอบให้โดยการเข้าถึงระบบบัตรแม่เหล็ก บันทึกผู้เข้าชม
- เอกสาร (Documents) : นโยบายความปลอดภัย คู่มือพนักงาน
- การสัมภาษณ์ (Interviews) : การสัมภาษณ์ผู้ดูแลระบบเครือข่าย การสัมภาษณ์กลุ่มบุคลากร
- ฐานข้อมูลและเว็บไซต์ (Database and website) : ฐานข้อมูลพนักงานขององค์กรและอินทราเน็ต
- ตัวบ่งชี้ (Indicators) : แดชบอร์ดเกี่ยวกับตัวบ่งชี้เกี่ยวกับเหตุการณ์ด้านความปลอดภัย
- การกำหนดค่าระบบ (System configurations) : การกำหนดค่าไฟร์วอลล์ที่แสดงว่าการเข้าถึงเว็บไซต์ต้องห้ามถูกปิดกั้น
- การสังเกต (Observation) : การสังเกตว่าห้องเซิร์ฟเวอร์ถูกล็อค โดยมีการควบคุม

๒.๑.๑๑ ทักษะของการเป็นผู้ตรวจสอบ (Auditing Skills)

๒.๑.๑๑.๑ สมบัติของผู้ตรวจสอบ (Personal behavior)

- มีใบรับรองตามมาตรฐานสากลที่เกี่ยวข้อง เช่น Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), IRCA ISO/IEC ๒๗๐๐๑ Lead Auditor, Certified Information Security Manager (CISM) , CompTIA Security+ , SANS/GIAC Certified (Various)
- มีจริยธรรม เช่น ยุติธรรม จริงใจ ซื่อสัตย์
- ใจกว้าง เช่น เปิดเปิดรับฟังความคิดเห็นต่างของผู้อื่น
- มีชั้นเชิง เช่น มีไหวพริบในการติดต่อบุคคล
- ช่างสังเกต เช่น การสังเกตสภาพแวดล้อมต่าง ๆ
- เฉลียวฉลาด เช่น สามารถเข้าใจสถานการณ์ต่าง ๆ ได้
- รอบรู้ เช่น พร้อมปรับตัวเข้ากับสถานการณ์ต่าง ๆ ได้
- ยืนหยัด เช่น แน่วแน่ และมุ่งมั่นที่จะบรรลุวัตถุประสงค์
- เฉียบขาด เช่น สามารถทำข้อสรุปต่าง ๆ ได้ทัน
- พึ่งพาตนเองได้ เช่น ทำหน้าที่ได้อย่างเป็นอิสระ
- ดำเนินงานด้วยความอดทน เช่น สามารถดำเนินงานได้อย่างมีความรับผิดชอบ มีจริยธรรม

- เปิดรับการปรับปรุง เช่น ยินดีที่จะเรียนรู้สิ่งใหม่ ๆ
- มีความอ่อนไหวทางวัฒนธรรม เช่น เชื่อฟัง ยอมรับในวัฒนธรรมของผู้รับตรวจ
- ให้ความร่วมมือ เช่น มีปฏิสัมพันธ์กับผู้อื่น

๒.๑.๑๑.๒ ความรู้และทักษะของผู้ตรวจสอบ (Knowledge and skills)

- เข้าใจถึงประเภทของความเสี่ยงที่เกี่ยวข้องกับการตรวจสอบ
- วางแผน และจัดการงานอย่างมีประสิทธิผล
- ตรวจสอบภายในตามตารางเวลาที่กำหนด
- จัดลำดับความสำคัญ และให้ความสำคัญในเรื่องต่าง ๆ
- สื่อสารอย่างมีประสิทธิผล ทั้งทางวาจา และลายลักษณ์อักษร
- เก็บข้อมูลผ่านการสัมภาษณ์ การฟัง การสังเกตการณ์ และการทบทวนเอกสาร
- เข้าใจความเหมาะสมของการใช้เทคนิคการสุ่ม
- รักษาความลับของข้อมูล

๒.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๒.๑ บทนำ

๒.๒.๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ด้วยความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็ว ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนไป และความเป็นดิจิทัลที่เพิ่มขึ้น หน่วยงานต่างๆ อาจเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบในทางลบต่อหน่วยงานและวัตถุประสงค์ทางธุรกิจ ดังนั้นจึงมีความจำเป็นสำหรับ กรมพินิจและคุ้มครองเด็กและเยาวชนในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้ อย่างมีประสิทธิภาพ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า "การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยง ระดับหน่วยงานของกรมพินิจและคุ้มครองเด็กและเยาวชน โดยการประเมินความเสี่ยง กรมพินิจและคุ้มครองเด็กและเยาวชนจะสามารถ: - ระบุเหตุการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจาก การกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์

- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญความเข้าใจที่ดี เกี่ยวกับระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอเพื่อจัดการ กับความเสี่ยงที่มีลำดับความสำคัญสูงสุด

- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในกรมพินิจและคุ้มครองเด็กและเยาวชน การประเมิน ความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้บุคลากรมีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยี และวิธีที่บุคลากรปรับให้สอดคล้องกับวัตถุประสงค์ที่กำหนด

๒.๒.๑.๒ ปัญหาทั่วไปที่สังเกตได้ ในขณะที่หน่วยงานต่าง ๆ ตระหนักดีว่าการประเมินความเสี่ยงเป็นส่วนสำคัญของแนวทางปฏิบัติ ในการประเมินความเสี่ยงของหน่วยงาน (Enterprise Risk assessment Practice) แต่หน่วยงานหลายแห่ง ก็ประสบปัญหากับกระบวนการในการประเมินความเสี่ยงที่เหมาะสม ช่องว่างทั่วไปบางส่วนที่สังเกตเห็น ได้แก่

ก. การระบุสถานการณ์ความเสี่ยงที่ไม่ดี (Poor Articulation of Risk Scenarios) สถานการณ์ ความเสี่ยงที่อธิบายถึงเหตุการณ์ “สิ่งที่อาจผิดพลาดได้(What Could Go Wrong)” มักจะคลุมเครือและ เป็นเรื่องทั่วไป โดยไม่ได้ระบุเหตุการณ์ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมาที่เฉพาะเจาะจง เป็นผลให้การเข้าใจขอบเขตของความเสี่ยง การเชื่อมโยงกับบริบทของหน่วยงาน หรือการระบุมาตรการ เป้าหมายเพื่อจัดการกับความเสี่ยง กระทำได้ยาก

ข. การระบุความเสี่ยงโดยใช้วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบ (Identification of Risks Using a Compliance-oriented Approach) หลายหน่วยงานระบุความเสี่ยงจากจุดที่ประเมินการควบคุม ความมั่นคงปลอดภัย (หรือขาดไป) คล้ายกับการดำเนินการตรวจสอบการปฏิบัติตามหรือการวิเคราะห์ช่องว่าง เทียบกับชุดของมาตรฐานที่กำหนดไว้ วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบเพื่อประเมินความเสี่ยง ทำให้ เกิดพฤติกรรม “รายการตรวจสอบ (Checklist)” ทำให้เกิดความเข้าใจผิดเกี่ยวกับความมั่นคงปลอดภัย ว่าหน่วยงานจะไม่มีความเสี่ยงใด ๆ ตราบใดที่ปฏิบัติตามข้อกำหนดทั้งหมด

ค. การขาดการยอมรับความเสี่ยง (Absence of Risk Tolerance) หน่วยงานมักจะไม่บูรณาการ แผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เข้ากับโปรแกรมการจัดการความเสี่ยง ของหน่วยงาน ด้วยเหตุนี้ การยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับหน่วยงานจึงมักถูกละเลย และผู้บริหารต้องเผชิญกับความยากลำบากในการตัดสินใจเลือกระดับความเสี่ยงที่เหมาะสม ที่จะนำมาใช้ในขณะที่ดำเนินการตามวัตถุประสงค์ทางธุรกิจของหน่วยงาน ๔

ง. การกำหนดโอกาสเสี่ยงตามเหตุการณ์ที่เกิดขึ้นในอดีตหรือที่คาดไว้ (Determining Risk Likelihood Based on Historical or Expected Occurrences) หน่วยงานต่าง ๆ มักจะใช้การวัดเวลาหรือ ความถี่ (เช่น เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดไว้) เพื่อประเมินโอกาสเสี่ยงของตน แนวทางนี้อาจไม่ ถูกต้องเมื่อพิจารณาจากจำนวนครั้งที่เหตุการณ์เกิดขึ้นก่อนหน้านี้ โดยเฉพาะอย่างยิ่งเมื่อไม่มีข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมา ในบริบทของความมั่นคงปลอดภัยไซเบอร์ ความน่าจะเป็นของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์นั้นไม่ขึ้นกับความถี่ของการเกิดขึ้นในอดีต

จ. จัดการกับความเสี่ยงด้วยการควบคุมหรือมาตรการที่ไม่เกี่ยวข้อง (Treating Risks With Irrelevant controls/measures) หน่วยงานอาจใช้แนวทางกว้าง ๆ ในการหามาตรการเพื่อลดความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุ ซึ่งส่งผลให้การดำเนินการควบคุมนั้นไม่ได้ระบุถึงสาเหตุที่แท้จริงอย่าง สมบูรณ์ ซึ่งมักเกิดจากความเข้าใจหรือการอธิบายสถานการณ์ความเสี่ยงที่ไม่ดีพอ

๒.๒.๒ วัตถุประสงค์ กลุ่มเป้าหมาย และขอบเขต (PURPOSE, AUDIENCE & SCOPE)

๒.๒.๒.๑ เพื่อให้คำแนะนำแก่สำนัก/กอง/กลุ่ม เกี่ยวกับวิธีดำเนินการประเมิน ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม เอกสารฉบับนี้จะระบุถึงความคาดหวังที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติจำเป็นต้องรับทราบ เมื่อทำการประเมินความเสี่ยง

๒.๒.๒.๒ กลุ่มเป้าหมายและขอบเขต (Audience & Scope) ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ต่อไปนี้

- ผู้มีส่วนได้ส่วนเสีย (Stakeholders) : ผู้บริหารกรมพินิจและคุ้มครองเด็กและเยาวชน ผู้ดูแลระบบตาม ภารกิจหลัก/ภารกิจสนับสนุน

- ที่ปรึกษาภายนอกหรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของกรมพินิจและคุ้มครองเด็กและเยาวชน

- ขอบเขตของแนวทางนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความเสี่ยง อยู่นอกเหนือขอบเขตของแนวทางนี้

๒.๒.๓ สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT) การกำหนดบริบทของความเสี่ยงเป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับการประเมินความเสี่ยง ขั้นตอนนี้ทำให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมิน ความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

๒.๒.๓.๑ กำหนดความเสี่ยง (Define Risk) มีคำจำกัดความมากมายเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนั้น ก่อนที่จะ กำหนดรายละเอียดเพิ่มเติมเกี่ยวกับการประเมินความเสี่ยง สิ่งสำคัญคือต้องกำหนดคำนิยามทั่วไป ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับวัตถุประสงค์ของแนวทางฉบับนี้ ความเสี่ยง ถูกกำหนดให้เป็นผลลัพธ์ของ ๒ ปัจจัย คือ: ๕

- ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน; และ

- ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (Likelihood, Impact)

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

ช่องโหว่ (Vulnerability) หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สิน หรือการควบคุมภายในของกระบวนการ

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

ผลกระทบ (Impact) ผลกระทบหมายถึงขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จาก ช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

๑ ผู้คุกคามหมายถึงบุคคลหรือองค์กรที่รับผิดชอบต่อเหตุการณ์ที่อาจก่อให้เกิดอันตราย
๒ เวกเตอร์ภัยคุกคามหมายถึงเส้นทางหรือเส้นทางที่ผู้คุกคามใช้เพื่อโจมตีเป้าหมาย

๒.๒.๓.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance) ความเสี่ยงที่ยอมรับได้ (Risk Tolerance)[๓] หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้ บรรลุวัตถุประสงค์ทางธุรกิจที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุ ได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด การยอมรับความเสี่ยงที่ชัดเจนควรระบุ:

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตารางการยอมรับควาเสี่ยง

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
High	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรม ที่เกี่ยวข้องจำเป็นต้องยุติลงทันที ทางเลือกที่เป็นไปได้ คือ กลยุทธ์การลดระดับความเสี่ยง หรือการถ่ายโอนจำเป็น ต้องดำเนินการทันที
Medium	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้ กลยุทธ์การรักษาที่มุ่งลดระดับความเสี่ยงควรได้รับ การพัฒนาและดำเนินการใน ๓ - ๖ เดือนข้างหน้า
Low	ความเสี่ยงระดับนี้สามารถยอมรับได้หากไม่มีกลยุทธ์การจัดการความเสี่ยงที่สามารถดำเนินการได้ง่ายและประหยัด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม

ตัวอย่างการแสดงการยอมรับความเสี่ยง

สิ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติ: ในรายงานการประเมินความเสี่ยงกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องกำหนดระดับการยอมรับ ความเสี่ยงให้ชัดเจน ทั้งนี้ อาจพิจารณาใช้ระดับความน่าจะเป็น ผลกระทบที่เกิดขึ้น และความเสี่ยงที่ยอมรับได้ ที่แตกต่างกันไปตามที่กำหนด

๒.๒.๓.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities) เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในการประเมินความเสี่ยง ได้แก่

หัวหน้าหน่วยงาน (Head of Organization) เจ้าหน้าที่อาวุโสระดับสูงสุด (Highest-level Senior Official) ภายในหน่วยงานที่มีภาระหน้าที่ และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับ การจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของหน่วยงาน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

เจ้าของกระบวนการธุรกิจ (Business Owner) เจ้าหน้าที่อาวุโสระดับสูงสุดของหน่วยธุรกิจ (Business Unit) ที่รับผิดชอบในการตรวจสอบ ให้แน่ใจว่ากิจกรรมทางธุรกิจบรรลุเป้าหมายทางธุรกิจหรือแบ่งปันข้อกังวลเกี่ยวกับผลกระทบที่มีต่อธุรกิจใน กรณีที่ระบบมีการหยุดชะงัก

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)

ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function) บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งหน่วยงาน ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและธุรกิจในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยง ที่สอดคล้องกัน

ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน (Technology and Operations Function) บุคลากรภายในกรมพินิจและคุ้มครองเด็กและเยาวชนหรือผู้รับจ้าง ที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุน การทำงานของระบบที่สนับสนุนกิจกรรมตามภารกิจกรมพินิจและคุ้มครองเด็กและเยาวชน ควรรู้จักทรัพย์สินของ ระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิค สำหรับระบบที่ถูกบุกรุกได้

ฟังก์ชั่นความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function) บุคลากรภายในกรมพินิจและคุ้มครองเด็กและเยาวชนหรือผู้รับจ้าง ที่รับผิดชอบในการดำเนินการและ การบำรุงรักษาการควบคุมความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมตามภารกิจกรมพินิจและคุ้มครองเด็กและเยาวชน โดยบุคคลดังกล่าวควรระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ กำหนดแนวคิดเกี่ยวกับ สถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการ ที่เหมาะสมเพื่อจัดการกับภัยคุกคามหรือการโจมตีที่ระบุ

สิ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติ: ในรายงานการประเมินความเสี่ยงกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องระบุบทบาทและ ความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการดำเนินการประเมินความเสี่ยงอย่างชัดเจน

๒.๒.๔ ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT) การประเมินความเสี่ยงนั้นเกี่ยวกับการระบุความเสี่ยงที่เฉพาะเจาะจงกับสภาพแวดล้อม และการกำหนดระดับของความเสี่ยงที่ระบุ ขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินความเสี่ยง (Risk Evaluation)

รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๒.๒.๔.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

งาน A: ระบุทรัพย์สิน (Identify Assets) การระบุและสร้างทะเบียนทรัพย์สินทางกายภาพและทางตรรกะทั้งหมดที่ประกอบกันเป็นระบบ ที่อยู่ภายในขอบเขตการประเมินความเสี่ยง เมื่อระบุทรัพย์สิน สิ่งสำคัญคือต้องจดบันทึกทรัพย์สินเหล่านั้น

ทรัพย์สินสำคัญ (Crown Jewels) - ทรัพย์สินเหล่านี้มีความสำคัญต่อการบรรลุวัตถุประสงค์ ทางธุรกิจโดยรวม และมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์ Step ๑: Risk Identification Step ๒: Risk Analysis Step ๓: Risk Evaluation

ทรัพย์สินที่เกี่ยวข้อง (Stepping Stones) - ทรัพย์สินเหล่านี้เป็นทรัพยากรที่ผู้โจมตีต้องการ ควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ

งาน B: การสร้างแบบจำลองภัยคุกคาม (Threat Modelling) ด้วยรายการทะเบียนทรัพย์สินและไดอะแกรมสถาปัตยกรรมเครือข่าย ควรระบุเหตุการณ์ ภัยคุกคามที่อาจใช้ประโยชน์จากช่องโหว่ของทรัพย์สินแต่ละรายการเพื่อการวิเคราะห์เชิงลึก เทคนิคประการหนึ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนควรใช้คือการสร้างแบบจำลองภัยคุกคาม โดยการสร้างแบบจำลองภัย คุกคามเป็นกระบวนการที่มีโครงสร้างสำหรับการระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับระบบ เพื่อให้กรมพินิจและคุ้มครองเด็กและเยาวชนสามารถสร้างการป้องกันที่มุ่งเน้นมากขึ้นเพื่อปกป้องระบบ

การสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้

๑. การระบุขอบเขตและการจำแนกระบบ (ScopeIdentification and System Decomposition) – สิ่งเหล่านี้เป็นข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคามที่แนะนำ ในงาน A

๒. การระบุภัยคุกคาม (Threat Identification) – สำนัก/กอง/กลุ่ม ควรใช้แนวทางที่เป็นระบบ เพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

๓. การสร้างแบบจำลองการโจมตี (Attack Modelling) – หลังจากระบุเหตุการณ์ภัยคุกคามที่ เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว หน่วยงานควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่ เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้หน่วยงานสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

งาน C: สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios) การสร้างสถานการณ์ความเสี่ยงเป็นงานสุดท้ายในการดำเนินการขั้นตอนการระบุความเสี่ยง ให้เสร็จสมบูรณ์ งานนี้มีเป้าหมายเพื่อสร้างสถานการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ที่ให้มุมมองที่สมจริงและสัมพันธ์กันของความเสี่ยงตามบริบททางธุรกิจ สภาพแวดล้อมของระบบ และภัยคุกคาม ที่เกี่ยวข้อง

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้ ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป สถานการณ์ความเสี่ยงควรระบุ องค์ประกอบหลัก ๔ ประการ ต่อไปนี้:

- ทรัพย์สิน (Asset) - สิ่งที่มีค่าที่ได้รับการระบุในงาน A
- เหตุการณ์ภัยคุกคาม (Threat event)
- เหตุการณ์การโจมตีที่ระบุในงาน B

- ช่องโหว่ (Vulnerability) - จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถ ใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือ การทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง

- ผลที่ตามมา (Consequence) [๔] – ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

สิ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติ: ในรายงานการประเมินความเสี่ยงกรมพินิจและคุ้มครองเด็กและเยาวชน สถานการณ์ความเสี่ยงต้องมี องค์ประกอบของเหตุการณ์ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมา

๒.๒.๔.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis) เป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยง แต่ละสถานการณ์เพื่อกำหนด

(๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น

(๒) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

งาน A: กำหนดโอกาส (Determine Likelihood) เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าว เพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัต ของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าจะไม่ถูกบุกรุกในอนาคต

ตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับ การประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้ [๕]

- ความสามารถในการค้นพบ (Discoverability) – ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่

- ความสามารถในการใช้ประโยชน์ (Exploitability) – ฝ่ายตรงข้ามจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี

- ความสามารถในการทำซ้ำ (Reproducibility) – ฝ่ายตรงข้ามจะสามารถสร้างการโจมตี ทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่ จำเป็นในการดำเนินการโจมตี

๔ คำว่า "ผลที่ตามมา (consequence)" และ "ผลกระทบ (consequence)" มักใช้แทนกันได้ อย่างไรก็ตามมีความหมาย ต่างกันและไม่ควรสับสน ในขณะที่ "ผลที่ตามมา" เป็นผลโดยตรงจากเหตุการณ์ภัยคุกคาม (เช่น ไฟดับ การหยุดชะงักของ บริการ การสูญเสียข้อมูลที่เป็นความลับ) "ผลกระทบ" คือระดับที่ผลที่ตามมาจะส่งผลกระทบต่อธุรกิจ การดำเนินงาน ฯลฯ (เช่น ขนาดของอันตราย)

๕ ปัจจัย (Discoverability, Exploitability and Reproducibility) ถูกดัดแปลงมาจากโมเดล DREAD ของ Microsoft สำหรับการประเมินภัยคุกคาม

ตารางการประเมินแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยให้คะแนนความเป็นไปได้ของสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(i) ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น ๓ ระดับ (เช่น ๑ – ๓)

(ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

(iii) คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสี่ยง โดยระดับ ๓ คือ “มีแนวโน้มสูง” และ ๑ คือ “เป็นไปได้ยาก”

Likelihood Rating	Discoverability	Exploitability	Reproducibility
High (๓)	ช่องโหว่ของเป้าหมาย: • สามารถค้นพบได้โดยการ ค้นหา/สแกนโดเมน สาธารณะสำหรับข้อมูลที่ เผยแพร่ (เช่น Shodan, ExploitDB) • สามารถถูกค้นพบและถูก โจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	การโจมตี: • สามารถดำเนินการได้ โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย • สามารถทำได้ด้วย เครื่องมือที่หาได้ทั่วไป โดยไม่ต้องมีความรู้ ด้านเทคนิค	การโจมตี: • สามารถทำซ้ำได้ ตามต้องการ โดยไม่มี การกำหนดค่า (Configuration) [๖] หรือ เงื่อนไขของเหตุการณ์ (Event Condition) [๗] • สามารถทำซ้ำได้ตาม ต้องการ โดยไม่ต้อง ปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่
Medium (๒)	ช่องโหว่ของเป้าหมาย: • สามารถค้นพบได้โดยการตรวจสอบการตอบสนอง พฤติกรรม และการสื่อสาร ของเป้าหมาย (เช่น การฟัซ (Fuzzing) กับแพ็กเก็ตเครือข่าย การดักจับเครือข่าย (Network Sniffing)) • สามารถถูกค้นพบและ โจมตีจากภายในเครือข่าย ย่อยหรือส่วนเครือข่าย เดียวกัน	การโจมตี: • สามารถดำเนินการได้ ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) ของเป้าหมาย (เช่น Admin/SYSTEM/ Root) • สามารถดำเนินการได้ ด้วยเครื่องมือที่เปิดเผย ต่อสาธารณะ ซึ่งต้องใช้ ความรู้ด้านเทคนิคในระดับกลาง	การโจมตี: • สามารถทำซ้ำได้ ตามเงื่อนไขเหตุการณ์ ที่คาดเดาได้บางอย่าง • สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย

๖ การกำหนดค่า หมายถึง การตั้งค่าในฮาร์ดแวร์ ซอฟต์แวร์ หรือเฟิร์มแวร์ที่สามารถเปลี่ยนแปลงได้ ซึ่งส่งผลต่อท่าทางการ รักษาความมั่นคงปลอดภัยและ/หรือการทำงานของระบบ ตัวอย่างเช่น การเปิดใช้งานบริการ Telnet

๗ เงื่อนไขของเหตุการณ์ หมายถึง สถานการณ์/สภาพแวดล้อมของคอมพิวเตอร์ที่ต้องมีอยู่เพื่อให้ได้ผลลัพธ์ที่ต้องการ ตัวอย่างเช่น งานแบทช์เฉพาะกิจ (ad-hoc batch job) จำเป็นต้องทำงานเพื่อให้การโจมตีดำเนินการได้

Likelihood Rating	Discoverability	Exploitability	Reproducibility
Low (๑)	ช่องโหว่ของเป้าหมาย: • สามารถค้นพบได้โดยการดำเนินการและโต้ตอบ กับการตั้งค่าปัจจุบันหรือ ที่คล้ายกันของเป้าหมาย • สามารถถูกค้นพบและ โจมตีด้วยการเข้าถึง แบบลอจิคัลโลคัล	การโจมตี: • สามารถดำเนินการได้ ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin/ SYSTEM / Root) • สามารถดำเนินการได้ ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะ ซึ่งต้องการความรู้ด้าน เทคนิคขั้นสูงอาจต้องการรวมกันของการ แสวงหาผลประโยชน์ หลายอย่างร่วมกัน	การโจมตี: • สามารถทำซ้ำได้ ตามเงื่อนไขเหตุการณ์ สุ่มบางอย่าง • สามารถทำซ้ำได้ในทาง ทฤษฎี หรือด้วยการพิสูจน์การใช้ประโยชน์ จากแนวคิดที่เผยแพร่

สิ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติ: ในรายงานการประเมินความเสี่ยง

-ความน่าจะเป็นของความเสี่ยงจะต้องให้คะแนนตามระดับ ๑ ถึง ๓ (เช่น ๑ เป็น “เป็นไปได้ยาก” และ ๓ คือ “มีแนวโน้มสูง” [๘]

- ความน่าจะเป็นของความเสี่ยงจะต้องพิจารณาจากภัยคุกคามและช่องโหว่

- แนะนำให้ใช้ปัจจัยความน่าจะเป็น (เช่น ความสามารถในการค้นพบ ความสามารถในการใช้ ประโยชน์ และความสามารถในการทำซ้ำ) เพื่อกำหนดความเป็นไปได้ของความเสี่ยง

งาน B: กำหนดผลกระทบ (Determine Impact) โดยทั่วไป การแสดงสถานการณ์ความเสี่ยงอาจส่งผลต่อการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และ/หรือความพร้อมใช้งาน (Availability) ของทรัพย์สิน (เช่น ข้อมูล อุปกรณ์ การ ดำเนินงาน) การโจมตีใด ๆ ของทรัพย์สินจะแปลเป็นผลกระทบในสาม (๓) ระดับต่อไปนี้:

- ระดับชาติ (National) – ในระดับประเทศ ผลกระทบอาจถูกมองว่าเป็นอันตรายต่อความมั่นคง และ เศรษฐกิจของประเทศ

- หน่วยงาน (Organisational) – ในระดับหน่วยงาน ผลกระทบอาจถูกมองว่าเป็นการหยุดชะงักในการดำเนินธุรกิจ ความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน

- บุคคล (Individual) - ในระดับบุคคล ผลกระทบสามารถมองได้ว่าเป็นการสูญเสียชีวิต และการบาดเจ็บ

ตารางด้าน ล่าง คือ ตารางประเมินสำหรับ การพิจารณาผลกระทบของความเสี่ยง ในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” และ ๑ คือ “เล็กน้อย”) คำอธิบายที่ระบุในตารางด้านล่างเป็นข้อมูลทั่วไป เมื่อใช้ตารางผลกระทบที่คล้ายกันควรตรวจสอบและปรับแต่งคำอธิบายสำหรับการจัดอันดับผลกระทบแต่ละรายการเพื่อให้แน่ใจว่า

- เกี่ยวข้องกับบทบาทภารกิจกรมพินิจและคุ้มครองเด็กและเยาวชน – เชื่อมโยงคำอธิบายกับวัตถุประสงค์ทางธุรกิจของหน่วยงานหรือวัดผลงาน

๘ ความสอดคล้อง (Consistency) ในการใช้มาตรวัดความเสี่ยงเป็นสิ่งที่จำเป็น เพื่อให้สามารถรวบรวมและดูความเสี่ยง ของ หน่วยงานในระดับประเทศได้

- ไม่กำกวม (Unambiguous) - ใช้คำอธิบายที่เป็นเลขฐานสองหรือที่มีช่วงเชิงปริมาณ (เช่น การรั่วไหลของข้อมูลที่ถูกจัดประเภทเป็น “ความลับ” หรือทำให้การบริการของลูกค้ามากกว่าร้อยละ ๕๐ หยุดชะงัก)

- มุมมองที่หลากหลาย (Multi-perspectives) - ระบุประเภทย่อยของผลกระทบจากแต่ละระดับจาก ๓ ระดับ (เช่น ระดับประเทศ หน่วยงาน และบุคคล)

ตารางคำอธิบายทั่วไปสำหรับการพิจารณาผลกระทบของความเสี่ยง

วัตถุประสงค์ด้านความ มั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์ แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต อาจส่งผลกระทบ อย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต อาจส่งผลกระทบ อย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหาก เปิดเผยทั้งหมดหรือเพียง บางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ แห่งรัฐ)	มีผลกระทบต่อข้อมูล ที่ลับมาก(ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมดหรือ เพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ แห่งรัฐอย่างร้ายแรง)	มีผลกระทบต่อข้อมูล ที่ลับที่สุด(ข้อมูลข่าวสาร ลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อ ให้เกิดความเสียหายแก่ ประโยชน์แห่งรัฐ อย่างร้ายแรงที่สุด)
ด้านการรักษาความถูกต้องครบถ้วน (Integrity)	การแก้ไขหรือทำลายข้อมูล โดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรือ อย่างจำกัด(Limited) และเกิดผลประโยชน์ แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูล โดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่าง ร้ายแรง (Serious)และเกิด ผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูล โดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่าง ร้ายแรงมาก (Severe or Catastrophic) และเกิด ผลประโยชน์แห่งชาติสำคัญ ยิ่ง (Extremely Important National Interests)

ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการ เข้าถึงหรือการใช้ข้อมูล ข่าวสารหรือระบบสารสนเทศอาจส่งผล กระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญ น้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูล ข่าวสารหรือระบบสารสนเทศอาจส่งผล กระทบอย่างร้ายแรง (Serious)และเกิดผลประโยชน์แห่งชาติ ที่สำคัญ (Important National Interests)	การหยุดชะงักของการ เข้าถึงหรือการใช้ข้อมูล ข่าวสารหรือระบบ สารสนเทศอาจส่งผล กระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์ แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ตารางเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	**ระดับผลกระทบ**		
	ต่ำ	**กลาง**	**สูง**
การเงินหรือทรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินหนึ่งร้อยล้านบาท	กินกว่าหนึ่งร้อยล้านบาทขึ้นไป
อันตรายต่อชีวิตร่างกายหรืออนามัย	ไม่มีผู้ใช้บริการ หรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ไม่เกินหนึ่งพันคน	ผู้ใช้บริการหรือผู้มีส่วนได้เสีย ได้รับผลกระทบต่อร่างกาย หรืออนามัยเกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน
ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับ ความเสียหายนอกจากอันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	ไม่มีผลกระทบ หรือมีผลกระทบต่อ การดำเนินการตามหน้าที่ ของหน่วยงาน เพียงเล็กน้อย	การดำเนินการตามหน้าที่หลักของหน่วยงานด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถ กู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	การดำเนินการตามหน้าที่หลัก ของหน่วยงานต้องหยุดชะงัก ไม่ต่อเนื่อง และไม่สามารถกู้คืน ระบบให้กลับมาดำเนินการ ตามปกติได้ ภายในระยะเวลา ตามแผนกู้คืนระบบของหน่วยงาน

ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อ ความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถ กู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศ ที่เกี่ยวข้องกับความมั่นคงของ รัฐต้องหยุดชะงัก ไม่ต่อเนื่องและไม่สามารถกู้คืนระบบให้ กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน เป็นผลให้ ไม่สามารถทำงานหรือให้บริการ ได้

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่ แตกต่างกันในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบสูงสุดควรถือ เป็นคะแนนสุดท้าย

สิ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติ:

ในรายงานการประเมินความเสี่ยงหน่วยงาน

- ผลกระทบต่อความเสี่ยงที่กำหนดในแนวทางฉบับนี้ ให้คะแนนตามระดับ ๑ ถึง ๓ (โดยระดับคะแนน ๑ คือ “ต่ำ” และระดับคะแนน ๓ คือ “สูง”) [๙]

ทั้งนี้ กรมพินิจและคุ้มครองเด็กและเยาวชนอาจพิจารณาใช้ระดับความน่าจะเป็น ผลกระทบที่เกิดขึ้นและความเสี่ยงที่ยอมรับได้ ที่แตกต่างกันไปตามที่เห็นสมควร

- คำอธิบายสำหรับการให้คะแนนผลกระทบแต่ละรายการต้องปรับให้เหมาะกับบริบทของหน่วยงานที่เกี่ยวข้อง

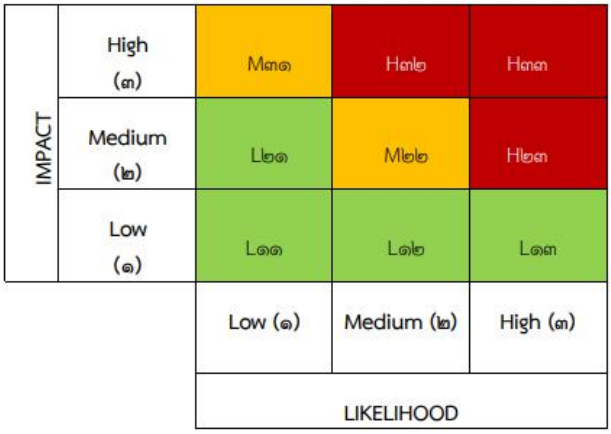
๒.๒.๔.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation) เป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้:

- กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)
- ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

งาน A: กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk) ดังที่กล่าวไว้ในหัวข้อที่ ๓ ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นแผนภาพโดยใช้เมทริกซ์ความเสี่ยง แสดงดังภาพด้านล่างเป็นตัวอย่างเมทริกซ์ความเสี่ยง ๓ ต่อ ๓ สำหรับกำหนดระดับความเสี่ยง

[๙] ความสอดคล้อง (Consistency) ในการใช้มาตรวัดผลกระทบต่อความเสี่ยงเป็นสิ่งที่จำเป็น เพื่อให้สามารถรวบรวมและดูความเสี่ยงของหน่วยงานในระดับประเทศได้

สำหรับแต่ละสถานการณ์ความเสี่ยง โดยที่ระดับความเสี่ยงเป็นการคูณของ “โอกาสเป็นไปได้” และ “ผลกระทบ” ซึ่งกำหนดจากขั้นตอนการวิเคราะห์ความเสี่ยง (หัวข้อ ๔.๒)



รูปที่ ๒ เมทริกซ์ความเสี่ยง ๓ คูณ ๓ สำหรับกำหนดระดับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนดโดยกรมพินิจและคุ้มครองเด็กและเยาวชน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับ การจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ เมื่อจัดลำดับ ความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

สิ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติ:

ในรายงานการประเมินความเสี่ยงหน่วยงาน จะต้องกำหนดระดับความเสี่ยงโดยใช้เมทริกซ์ ๓ คูณ ๓ ตามตัวอย่างนี้ หรือสามารถกำหนดระดับความเสี่ยงเองได้ตามความเหมาะสม [๑๐]

งาน B: ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk) การประเมินความเสี่ยงจะไม่สมบูรณ์หากไม่มีเอกสารประกอบ ผลลัพธ์จากขั้นตอนก่อนหน้าจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยงเพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย การลงทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงที่กำหนด การลงทะเบียนความเสี่ยงเป็นเอกสารที่มีชีวิตซึ่งได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (update) เป็นประจำ เพื่อให้แน่ใจว่าฝ่ายบริหารของกรมพินิจและคุ้มครองเด็กและเยาวชนมีภาพปัจจุบันเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชนเมื่อทำการตัดสินใจโดยแจ้งความเสี่ยง ควรมีอย่างน้อยดังต่อไปนี้

- สถานการณ์ความเสี่ยง (Risk Scenario) – สถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สินเพื่อสร้างผลกระทบในทางลบได้อย่างไร

๑๐ ความสอดคล้อง (Consistency) ในการใช้เมทริกซ์ความเสี่ยงเป็นสิ่งจำเป็น เพื่อให้สามารถรวบรวมและดูความเสี่ยง ของหน่วยงานในระดับประเทศได้

- วันที่ระบุความเสี่ยง (Identification Date) – วันที่ที่ระบุสถานการณ์ความเสี่ยง

- มาตรการที่มีอยู่ (Existing Measures) – มาตรการปัจจุบันที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง

- ความเสี่ยงในปัจจุบัน (Current Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่ (เช่น ความเสี่ยงโดยธรรมชาติ (Inherent Risk) [๑๑] โดยใช้มาตรการที่มีอยู่)

- แผนจัดการความเสี่ยง (Treatment Plan) – กิจกรรมที่วางแผนไว้ (เช่น การใช้มาตรการเพิ่มเติม) และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้ (เช่น ภายในระดับการยอมรับความเสี่ยงของหน่วยงาน)

- สถานะความคืบหน้า (Progress Status) – สถานะของการดำเนินการตามแผนจัดการความเสี่ยง

- ความเสี่ยงที่คงเหลืออยู่ (Residual Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากดำเนินการตามแผนจัดการความเสี่ยง (เช่น ความเสี่ยงปัจจุบันที่มีมาตรการเพิ่มเติม)

- เจ้าของความเสี่ยง (Risk Owner) – บุคคลหรือกลุ่มที่รับผิดชอบในการดูแลให้ความเสี่ยงที่เหลืออยู่อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

สิ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติ:

ในรายงานการประเมินความเสี่ยง ทะเบียนความเสี่ยงต้องมีองค์ประกอบอย่างน้อย ๘ ประการ ได้แก่ สถานการณ์ความเสี่ยง วันที่ระบุ มาตรการที่มีอยู่ ความเสี่ยงปัจจุบัน แผนจัดการความเสี่ยง สถานะความคืบหน้า ความเสี่ยงที่เหลืออยู่ เจ้าของความเสี่ยง

๒.๒.๕ ตอบสนองต่อความเสี่ยง หลังจากประเมินความเสี่ยงที่ระบุแล้ว (เช่น ความเสี่ยงในปัจจุบัน) ขั้นตอนต่อไปคือการระบุและกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

๒.๒.๕.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options) มีตัวเลือกการตอบสนองความเสี่ยง จำนวน ๔ ตัวเลือก ที่ต้องพิจารณา

(๑) ยอมรับ (Accept) การยอมรับความเสี่ยงหมายถึงการรับความเสี่ยงตามที่เป็นอยู่ โดยไม่ต้องดำเนินการเพิ่มเติม เพื่อลดความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของหน่วยงานเท่านั้น

(๒) หลีกเลี่ยง (Avoid) การหลีกเลี่ยงความเสี่ยงหมายถึงการยุติการกระทำหรือกิจกรรมที่ทำให้หน่วยงานมีความเสี่ยงที่ระบุ สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

(๓) โอนย้าย (Transfer) การโอนความเสี่ยงหมายถึงการแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือหน่วยงานอื่น เช่น โดยทั่วไปตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

(๔) การลดความเสี่ยง (Mitigate) การลดความเสี่ยงหมายถึงการวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

๑๑ ความเสี่ยงโดยธรรมชาติ (Inherent risk) หมายถึง ระดับความเสี่ยงที่มีอยู่โดยพิจารณาถึงมาตรการควบคุมในปัจจุบัน แต่ไม่ คำนึงถึงมาตรการใด ๆ ที่จะดำเนินการเพิ่มเติม

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในกรมพินิจและคุ้มครองเด็กและเยาวชนจะต้องอนุมัติการตอบสนองความเสี่ยง ที่เลือกอย่างเป็นทางการ และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

๒.๒.๕.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุมความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตาม กรมพินิจและคุ้มครองเด็กและเยาวชนควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่า

เมื่อกรมพินิจและคุ้มครองเด็กและเยาวชนเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยง ที่กำลังจัดการ ทั้งนี้ ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยง หรือการลดผลกระทบจากความเสี่ยง

สิ่งที่กรมพินิจและคุ้มครองเด็กและเยาวชนพึงปฏิบัติ:

ในรายงานการประเมินความเสี่ยง

- ผู้บริหารระดับสูงต้องอนุมัติแผนจัดการความเสี่ยงทั้งหมดอย่างเป็นทางการ
- ผู้บริหารระดับสูงต้องยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมดอย่างเป็นทางการ

๒.๓ แผนการรับมือภัยคุกคามทางไซเบอร์

๒.๓.๑ หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชน ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไป ตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ(๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ.๒๕๖๖ ด้วย

๒.๓.๒ วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในกรมพินิจและคุ้มครองเด็กและเยาวชน โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานในสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชน การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของกรมพินิจและคุ้มครองเด็กและเยาวชน

๒.๓.๓ ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศและข้อมูลดิจิทัลของกรมพินิจและคุ้มครองเด็กและเยาวชน รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศและข้อมูลดิจิทัลดังกล่าว

๒.๓.๔ หน้าที่การทบทวนแผน

ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึงผู้บริหารสูงสุดระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) หรือผู้ที่รับมอบอำนาจหน่วยงานของกรมพินิจและคุ้มครองเด็กและเยาวชน

๒.๓.๕ หน้าที่ในการดำเนินการตามแผน

ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการ ตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย กอง (ทุกกอง) งานตรวจราชการ (ทุกงาน) กลุ่ม (ทุกกลุ่ม) ศูนย์ (ทุกศูนย์) สำนักเลขานุการกรม ศูนย์ฝึกและอบรมเด็กและเยาวชน (ทุกศูนย์ฝึกฯ) สถานพินิจและคุ้มครองเด็กและเยาวชน (ทุกสถานพินิจฯ) รวมถึงหน่วยงานเฉพาะกิจที่กรมพินิจและคุ้มครองเด็กและเยาวชนจัดตั้ง

๒.๓.๖ เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๓.๖.๑ ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖

๓.๖.๒ ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน เรื่อง แผนรองรับสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของกรมพินิจและคุ้มครองเด็กและเยาวชน

๓.๖.๓ ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคลของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๕

๒.๓.๗ นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (observable occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึง ประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่น

ที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยไม่ชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒.๓.๘ บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

<u>๓.๘.๑ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)</u>

กรมพินิจและคุ้มครองเด็กและเยาวชน ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบ แบบรวมศูนย์ (Centralize) ประกอบด้วย

ลำดับ	ชื่อ - นามสกุล ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	**รองอธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน ที่กำกับดูแลศูนย์เทคโนโลยีสารสนเทศ** เบอร์โทรศัพท์ภายใน : ๐ ๒๑๔๑ ๓๕๕๘ Email : komol.p@djop.mail.go.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	**ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ** เบอร์โทรศัพท์ภายใน : ๐ ๒๑๔๑ ๖๔๘๖ Email:it_information@djop.mail.go.th	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	- **หัวหน้าฝ่ายเทคโนโลยีเครือข่ายและคอมพิวเตอร์** - **หัวหน้าฝ่ายฝ่ายบริหารฐานข้อมูลสารสนเทศ** เบอร์โทรศัพท์ภายใน : ๐ ๒๑๔๑ ๖๔๘๖ Email:it_information@djop.mail.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือหน่วยงานของกรมให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้

ลำดับ	ชื่อ - นามสกุล ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๔	**นักวิชาการคอมพิวเตอร์** เบอร์โทรศัพท์ภายใน : ๐ ๒๑๔๑ ๖๔๘๖ Email:it_information@djop.mail.go.th	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๕	**เจ้าหน้าที่ Outsource ประจำโครงการของกรมพินิจและคุ้มครองเด็กและเยาวชน**	เจ้าหน้าที่ดูแลระบบงานสารสนเทศของกรม	ทำหน้าที่ดูแลระบบให้สามารถใช้งานได้

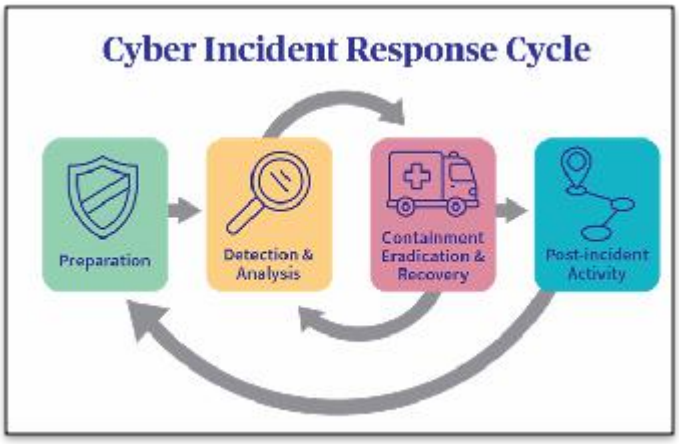
ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	หัวหน้าหน่วยงานในสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชน	เจ้าหน้าที่บริหารจัดการสั่งการ ควบคุม ผลกระทบจากภัยคุกคามทางไซเบอร์	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
๒	หัวหน้ากลุ่มกฎหมาย	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่เป็นที่ปรึกษากฎหมายที่เกี่ยวข้อง
๓	เลขานุการกรม	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ด้านการสื่อสารองค์กรและประชาสัมพันธ์ข่าวสาร
๔	หัวหน้ากลุ่มตรวจสอบภายใน	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามที่ได้รับมอบหมายตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ.๒๕๖๖

ลำดับ	ชื่อ - นามสกุล ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๕	เจ้าหน้าที่ Outsource ประจำโครงการของกรมพินิจและคุ้มครองเด็กและเยาวชน	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามที่ได้รับมอบหมายตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ.๒๕๖๖

๒.๓.๙ ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ , ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ รวมถึง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ.๒๕๖๖ ดังนี้



๒.๓.๙.๑ ขั้นการเตรียมการ (preparation)

เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ ๘

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใดๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าวตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๒.๓.๙.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๒.๓.๙.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

หน่วยงานจะต้องดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่ง การดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่ อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

(๖) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๒.๓.๙.๔. ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

เป็นการดำเนินการที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) นั้น หน่วยงานควรกำหนดขั้นตอนวิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าวจะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมาและสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่นๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

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

(๒) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๔ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ตารางแสดงความสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนรับมือฯ ฉบับนี้
๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	
(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	ข้อที่ ๘

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนรับมือฯ ฉบับนี้
(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ข้อที่ ๙.๑ (๒)
(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT	ข้อที่ ๙.๑ (๓)
(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	ข้อที่ ๙.๓ (๑)
(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	ข้อที่ ๙.๓ (๒)
(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	ข้อที่ ๙.๓ (๓)
(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	ข้อที่ ๙.๓ (๔)
(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ	ข้อที่ ๙.๓ (๕)
(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อที่ ๙.๔ (๑)

ส่วนที่ ๓
กรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify) หน่วยงานต้องทำการระบุว่า กระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้าง ที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อ บริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูลของ หน่วยงานได้อย่างเหมาะสม

๓.๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) หน่วยงานต้องมีมาตรการป้องกันที่เหมาะสมเพื่อจากัดผลกระทบของเหตุการณ์ภัยคุกคาม ไซเบอร์ ซึ่งครอบคลุมถึง เรื่องการควบคุมการเข้าถึง การฝึกอบรมและการสร้างความตระหนัก ให้แก่เจ้าหน้าที่และผู้ที่เกี่ยวข้องความปลอดภัยของข้อมูล และมาตรการด้านความมั่นคง ปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี นอกจากนี้ หน่วยงานต้องทำการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบอิเล็กทรอนิกส์อย่างสม่ำเสมอ เพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง รวมทั้งการเปลี่ยนแปลงแก้ไข Patch หรือ update software

๓.๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) หน่วยงานต้องมีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์ อย่างต่อเนื่อง และแจ้งเตือนถึงสิ่งที่ผิดปกติต่าง ๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคาม ทางไซเบอร์ที่เกิดขึ้นจากทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคาม ที่เกิดขึ้น เพื่อเป็นข้อมูลประกอบในการพิจารณาทบทวนแนวทางการป้องกันความเสี่ยงและ ผลกระทบที่จะเกิดขึ้นกับหน่วยงานในอนาคต

๓.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)

๓.๔.๑ มีการกำหนดมาตรการและกระบวนการรับมือภัยคุกคามไซเบอร์ที่ทันท่วงที

๓.๔.๒ มีความร่วมมือกับหน่วยงานที่เกี่ยวข้องเกี่ยวกับแผนรับมือภัยคุกคามไซเบอร์

๓.๔.๓ มีการวิเคราะห์สาเหตุภัยคุกคามหรือตรวจพิสูจน์พยานหลักฐานดิจิทัล

๓.๔.๔ มีมาตรการป้องกันการลุกลามของภัยคุกคาม ๔.๕ มีการทดสอบ ปรับปรุงกลยุทธ์และแผนรับมือภัยคุกคามไซเบอร์อย่างสม่ำเสมอ

๓.๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

๓.๕.๑ มีแผนการกู้คืนระบบทั้งระหว่างเกิดเหตุและหลังเกิดเหตุภัยคุกคาม

๓.๕.๒ มีการปรับปรุงกลยุทธ์และแผนการกู้คืนอย่างสม่ำเสมอ

๓.๕.๓ มีการสื่อสารให้ผู้บริหารและ ผู้ที่เกี่ยวข้องทราบภายในองค์กรให้ทราบถึงกระบวนการกู้คืนข้อมูลหลังเกิดเหตุภัยคุกคามไซเบอร์