คู่มือ การตรวจสอบ
การรักษาความมั่นคงปลอดภัยไซเบอร์










กลุ่มตรวจสอบภายใน
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

คำนำ

การตรวจสอบภายในเป็นกระบวนการสำคัญที่ช่วยให้องค์กรมั่นใจว่าการดำเนินงานเป็นไปตามกฎหมาย ข้อบังคับ และนโยบายที่กำหนดไว้ การตรวจสอบนี้ไม่เพียงแต่ช่วยป้องกันความเสี่ยงและการทุจริต แต่ยังช่วยในการปรับปรุงกระบวนการทำงานและเพิ่มประสิทธิภาพในการบริหารจัดการทรัพยากร การตรวจสอบภายในยังมีบทบาทสำคัญในการสร้างความเชื่อมั่นให้กับผู้บริหาร และผู้มีส่วนได้ส่วนเสียอื่นๆ ว่าองค์กรมีการดำเนินงานที่โปร่งใสและมีระบบการควบคุมภายในที่เข้มแข็ง เพื่อให้องค์กรสามารถพัฒนาการดำเนินงานได้อย่างยั่งยืนและมีประสิทธิภาพสูงสุด

การตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นกระบวนการที่สำคัญในการประเมินความปลอดภัย ประสิทธิภาพ และความเป็นไปได้ของระบบเทคโนโลยีสารสนเทศในองค์กร การตรวจสอบนี้มีวัตถุประสงค์เพื่อให้มั่นใจได้ว่าระบบเทคโนโลยีสารสนเทศขององค์กรมีความปลอดภัย มีการจัดการความเสี่ยงอย่างเหมาะสม และสามารถรองรับการดำเนินงานขององค์กรได้อย่างมีประสิทธิภาพ

กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ จึงได้จัดทำคู่มือการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อสำหรับผู้ตรวจสอบภายในใช้เป็นแนวทางในการปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศให้สอดคล้องตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง ให้เป็นไปอย่างถูกต้อง มีประสิทธิภาพและประสิทธิผลตลอดจน เพื่อให้ข้อเสนอแนะในการปรับปรุงการปฏิบัติงานที่เป็นประโยชน์และพัฒนาระบบของหน่วยงานให้ดียิ่งขึ้นต่อไป

กลุ่มตรวจสอบภายใน
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

สารบัญ

บทที่ ๑
บทนำ
หลักการและเหตุผล

การตรวจสอบภายใน คือ กิจกรรมให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานของหน่วยงานของรัฐให้ดีขึ้น และจะช่วยให้หน่วยงานของรัฐบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบโดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่าองค์กรปฏิบัติตามกฎหมาย กฎระเบียบ และนโยบายที่เกี่ยวข้อง ตลอดจนการบริหารจัดการทรัพยากรอย่างมีประสิทธิภาพ การตรวจสอบภายในมีบทบาทสำคัญในการป้องกันความเสี่ยงและการทุจริต ช่วยให้องค์กรสามารถปรับปรุงกระบวนการปฏิบัติงาน และสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียว่าการดำเนินงานขององค์กรเป็นไปอย่างถูกต้องและโปร่งใส

การตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ มีความสำคัญอย่างยิ่งต่อการรักษาความปลอดภัยและประสิทธิภาพของระบบเทคโนโลยีสารสนเทศในองค์กร หลักการของการตรวจสอบประกอบด้วยความเป็นอิสระและเที่ยงตรงของผู้ตรวจสอบ ความเชี่ยวชาญและความรู้ในด้านเทคโนโลยี การประเมินความเสี่ยง การปฏิบัติตามมาตรฐาน และการรายงานผลอย่างชัดเจน เหตุผลหลักในการการรักษาความมั่นคงปลอดภัยไซเบอร์คือเพื่อป้องกันข้อมูลรั่วไหล ลดความเสี่ยงจากการโจมตีทางไซเบอร์ ปฏิบัติตามกฎหมายและข้อกำหนด เพิ่มประสิทธิภาพการทำงาน และสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสีย ทั้งหมดนี้ช่วยให้องค์กรดำเนินงานได้อย่างราบรื่นและมั่นคงในยุคดิจิทัล

วัตถุประสงค์

๑. เป็นคู่มือสำหรับให้ผู้บริหาร ผู้ตรวจสอบภายใน และเจ้าหน้าที่ผู้ปฏิบัติงาน ในการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างถูกต้อง

๒. เพื่อให้การปฏิบัติงานเป็นแนวทางเดียวกัน และมีคุณภาพตามมาตรฐานการตรวจสอบภายใน

๓. เพื่อตรวจประเมินความสอดคล้องของการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีต่อ

๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์

๓) นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ขอบเขตการตรวจสอบ

ศึกษา วิเคราะห์ กฎ ระเบียบ ข้อบังคับ แนวทางปฏิบัติที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมโดยพิจารณาความเสี่ยง และกำหนดแนวทางการตรวจสอบประกอบด้วย วัตถุประสงค์ ขอบเขต และวิธีการตรวจสอบ

ประโยชน์ที่คาดว่าจะได้รับ

๑. บุคลากรของกลุ่มตรวจสอบภายในใช้เป็นคู่มือสำหรับการปฏิบัติงานการตรวจสอบ

๒. สร้างความเชื่อมั่น รักษามาตรฐานคุณภาพงานตรวจสอบภายในภาครัฐของหน่วยงาน

๓. การปฏิบัติงานของหน่วยงาน เป็นไปตามกฎระเบียบ หลักเกณฑ์และวิธีปฏิบัติที่เกี่ยวข้อง

๔. กลุ่มตรวจสอบภายในมีกระบวนการควบคุมภายในที่ดี เป็นระบบ โปร่งใส มีประสิทธิภาพประสิทธิผลมากยิ่งขึ้น

๕. หน่วยรับตรวจหรือบุคลากรที่เกี่ยวข้องได้ทราบถึงแนวทาง วิธีการตรวจสอบที่ชัดเจน และสามารถจัดเตรียมเอกสารหลักฐานต่าง ๆ ให้ผู้ตรวจสอบภายในได้ครบถ้วนสมบูรณ์

คำจำกัดความ

“ผู้ตรวจสอบ” หมายถึง ผู้ตรวจสอบภายในของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)

“หน่วยรับตรวจ” หมายถึง หน่วยงานที่รับผิดชอบหรือเกี่ยวข้องกับกิจกรรมที่ดำเนินการตรวจสอบ

“กระดาษทำการ” หมายถึง เอกสารหลักฐานที่ได้มาจากการรวบรวมและจัดทำขึ้นในช่วงระยะเวลาที่ถือปฏิบัติงานตรวจสอบภายใน อาจอยู่ในรูปแบบตาราง การวิเคราะห์เอกสาร หรือแบบฟอร์มที่จัดทำขึ้น เพื่อใช้บันทึกสรุปข้อตรวจพบ ผลการตรวจสอบ ซึ่งเป็นส่วนหนึ่งของภารกิจการตรวจสอบภายใน

“หน่วยงานของรัฐ” หมายถึง ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)” หมายถึง หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล” หมายถึง หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“สกมช. (NCSA)” หมายถึง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“กกม.” หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“การตรวจสอบด้านเทคโนโลยีสารสนเทศ” หมายถึง กิจกรรมการสร้างความเชื่อมั่น (Assurance) ต่อระบบเทคโนโลยีสารสนเทศ และการให้ข้อเสนอแนะรวมถึงแนวทางการปรับปรุงระบบงานด้านเทคโนโลยีสารสนเทศของหน่วยงานให้มีความสอดคล้องกับกฎ ระเบียบ และความเสี่ยงรวมถึงการตรวจสอบเพื่อช่วยให้หน่วยงานบรรลุเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการควบคุมทั่วไปของระบบเทคโนโลยีสารสนเทศและการควบคุมเฉพาะระบบงาน

“การควบคุมภายในระบบเทคโนโลยีสารสนเทศ” หมายถึง กระบวนการหรือขั้นตอนการทำงานที่เป็นผลมาจากการออกแบบ โดย ผู้บริหาร หรือบุคลากรอื่นๆ ของหน่วยงาน เพื่อก่อให้เกิดความมั่นใจได้อย่างสมเหตุสมผลว่าหน่วยงานจะสามารถบรรลุวัตถุประสงค์ความมีประสิทธิผล และประสิทธิภาพของการดำเนินงานระบบเทคโนโลยีสารสนเทศ

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอัน

กระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

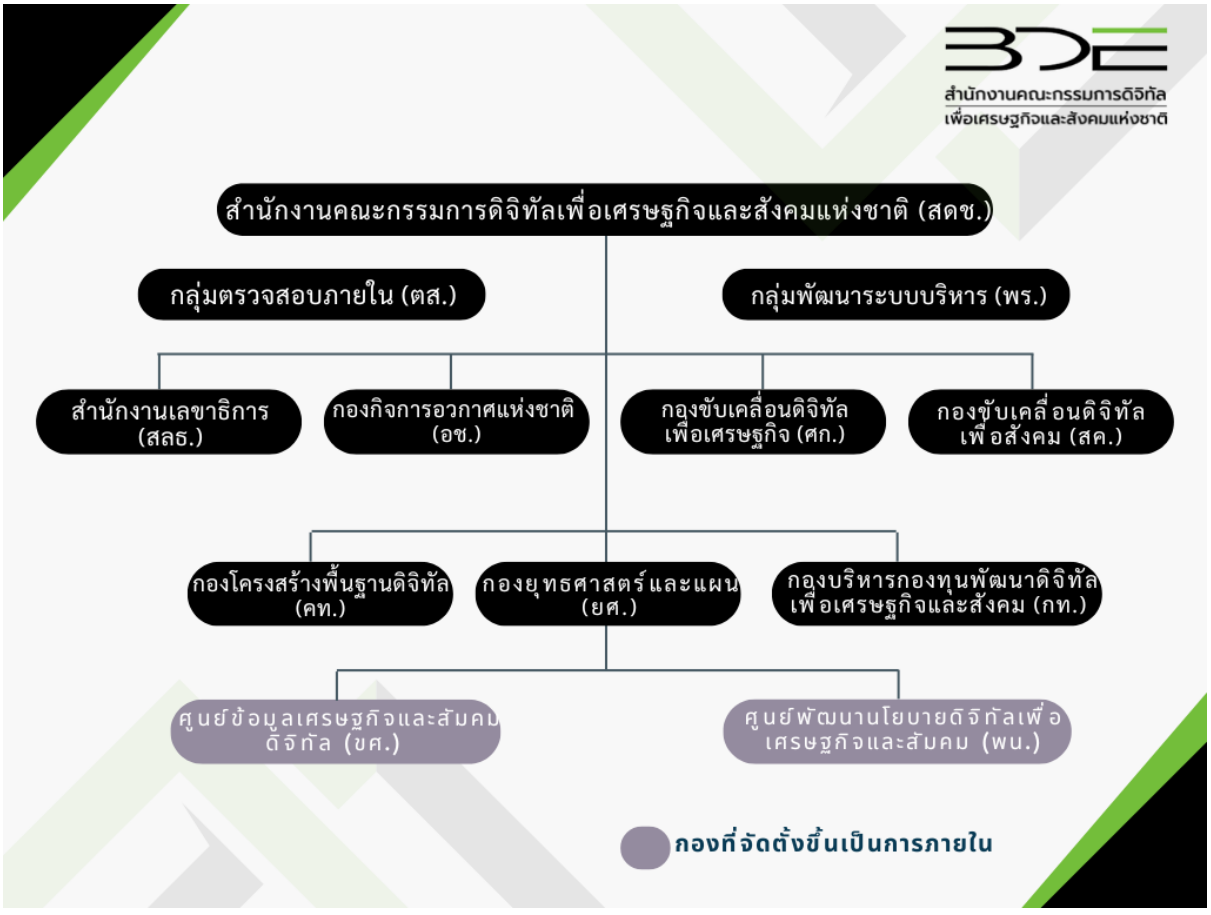
“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การแก้ไปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

บทที่ ๒
โครงสร้างและหน้าที่ความรับผิดชอบ

โครงสร้างการบริหารจัดการ

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติก่อตั้งขึ้นเมื่อวันที่ ๑๖ กันยายน พ.ศ. ๒๕๕๙ ตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ ๑๗) พ.ศ. ๒๕๕๙ พร้อมการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและต่อมาเมื่อวันที่ ๒๕ มกราคม พ.ศ. ๒๕๖๐ ได้มีการประกาศใช้ พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๐ ที่มีการกำหนดอำนาจหน้าที่ของสำนักงานในฐานะที่เป็นฝ่ายเลขานุการของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ โดยได้มีการแบ่งส่วนราชการมาเป็นกลุ่มตรวจสอบภายใน บทบาทหน้าที่เพื่อสนับสนุนการบริหารงานและการดำเนินงานด้านต่าง ๆ ของหน่วยงานของรัฐ โดยให้สอดคล้องกับนโยบายของหน่วยงานของรัฐ

โครงสร้างสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ



โครงสร้างกลุ่มตรวจสอบภายใน

ภาระหน้าที่งานของกลุ่มตรวจสอบภายใน

ตามระเบียบกระทรวงการคลังว่าด้วยการตรวจสอบภายในของส่วนราชการ พ.ศ. ๒๕๕๑ หลักเกณฑ์ กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายใน สำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๖ (ฉบับที่ ๔) กำหนดให้หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ มีหน้าที่และความรับผิดชอบ กำหนดเป้าหมาย ทิศทาง ภารกิจงานตรวจสอบภายใน เพื่อสนับสนุนการบริหารงานและการดำเนินงาน ด้านต่าง ๆ ของหน่วยงานของรัฐ โดยให้สอดคล้องกับนโยบายของหน่วยงานของรัฐ คณะกรรมการ และคณะกรรมการตรวจสอบหรือคณะกรรมการอื่นใดที่ปฏิบัติงานในลักษณะเดียวกัน โดยคำนึงถึงการกำกับ ดูแลที่ดี ความมีประสิทธิภาพของกิจกรรมการบริหารความเสี่ยงและความเพียงพอของการควบคุมภายในของ หน่วยงานของรัฐด้วย

๑. งานบริการให้ความเชื่อมั่น (Assurance Services) การตรวจสอบหลักฐานต่าง ๆ อย่างเที่ยงธรรม เพื่อให้ได้มาซึ่งการประเมินผลอย่างเป็นอิสระในกระบวนการกำกับดูแล การบริหารความเสี่ยงและการควบคุมของหน่วยรับตรวจ ว่าสามารถดำเนินการได้บรรลุผลตามเป้าหมาย มีประสิทธิภาพ

ประสิทธิผล และคุ้มค่า โดยกระทรวงการคลังได้กำหนดประเภทการตรวจสอบไว้ ๔ ด้าน (หนังสือ ที่ กค ๐๔๐๙.๒/ว๖๑๔ ลงวันที่ ๒๓ ธันวาคม ๒๕๖๓ เรื่อง การกำหนดประเภทของงานตรวจสอบภายใน) ดังนี้

๑.๑ การตรวจสอบการเงิน (Financial Audit) หมายถึง การตรวจสอบความถูกต้อง ความครบถ้วน และความเชื่อถือได้ของข้อมูลการเงิน และรายงานการเงิน การตรวจสอบการปฏิบัติตามมาตรฐานการบัญชี นโยบายการบัญชี กฎหมาย ระเบียบ ข้อบังคับ หลักเกณฑ์ ประกาศที่เกี่ยวข้อง รวมถึงการประเมินความเสี่ยง ระบบการควบคุมภายใน และความเป็นไปได้ที่จะเกิดข้อผิดพลาดและการทุจริตด้านการเงินการบัญชี

๑.๒ การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit) การตรวจสอบการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หลักเกณฑ์ ประกาศ มติคณะรัฐมนตรี รวมถึงมาตรฐาน แนวปฏิบัติ และนโยบายที่กำหนดไว้

๑.๓ การตรวจสอบการดำเนินงาน (Performance Audit) การตรวจสอบความประหยัด ความมีประสิทธิผล ความมีประสิทธิภาพ และความคุ้มค่าของกิจกรรมที่ตรวจสอบ

๑.๔ การตรวจสอบอื่น ๆ การตรวจสอบอื่นนอกเหนือจาก ข้อ ๑.๑ – ๑.๓ เช่น การตรวจสอบการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ โดยการประเมินความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ และการตรวจสอบพิเศษ (การตรวจสอบตามที่ได้รับมอบหมายเป็นกรณีพิเศษ) เป็นต้น

๒. งานให้คำปรึกษา (Consulting Services) หมายถึง การบริการให้คำปรึกษา แนะนำ และบริการอื่นๆ ที่เกี่ยวข้อง ซึ่งลักษณะงานและขอบเขตของงานจะเป็นไปตามข้อตกลงที่ทำขึ้นร่วมกับผู้รับบริการ โดยมีจุดประสงค์เพื่อเพิ่มคุณค่าให้กับหน่วยงานของรัฐ และปรับปรุงกระบวนการการกำกับดูแล การบริหารความเสี่ยง และการควบคุมของหน่วยงานของรัฐให้ดีขึ้น

๓. ทำการสอบทานระบบการควบคุมภายในของหน่วยงานในสำนักงานฯ ตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

๔. งานบริหารสำนักงาน

๑) จัดทำแผนปฏิบัติราชการประจำปีและแผนงบประมาณประจำปี

๒) งานบริหารงานบุคคล และแผนพัฒนาบุคคล

๓) งานพัฒนาขีดสมรรถนะ

๔) งานประกันคุณภาพการตรวจสอบภายในภาครัฐ ทบทวนกฎบัตร

๕) งานบริหารการเงินและงบประมาณ

๖) งานบริหารสินทรัพย์และวัสดุสำนักงาน

๗) งานบริหารทั่วไป อาทิงานสารบรรณ งานเอกสารการพิมพ์ งานประชุม งานรายงานและประเมินผล การประสานงานกับหน่วยงานภายในและภายนอก เป็นต้น

๘) งานประชาสัมพันธ์ อาทิ จัดทำข้อมูลองค์ความรู้ จัดทำเอกสาร วารสารเผยแพร่ข้อมูลองค์ความรู้ ข่าวสารทั้งภายในและภายนอก ผ่านทาง Website สำนักงาน

๕. งานอื่นๆ ที่ได้รับมอบหมาย

บทบาทหน้าที่ความรับผิดชอบ

ด้านการปฏิบัติการ

ศึกษากฎ ระเบียบ หลักเกณฑ์ข้อบังคับที่เกี่ยวข้อง ทำหนังสือแจ้งหน่วยรับตรวจถึงกำหนดการเข้าตรวจสอบ และขอเอกสาร/หลักฐานประกอบการตรวจสอบ จัดทำแผนการตรวจสอบ จัดประชุมเปิดการตรวจสอบ ดำเนินการปฏิบัติงานตรวจสอบ จัดทำแบบสรุปข้อตรวจพบ จัดทำรายงานสรุปผลปฏิบัติการตรวจสอบ จัดประชุมปิดการตรวจสอบ รายงานผลการตรวจสอบต่อหัวหน้าส่วนราชการ รายงานผลการตรวจสอบต่อหน่วยรับตรวจ การติดตามผลการตรวจสอบ

ด้านการวางแผน

วางแผนการดำเนินงานตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพ และเป็นไปตามกฎ ระเบียบ หลักเกณฑ์ข้อบังคับที่เกี่ยวข้อง

ด้านการประสานงาน

๑) ประสานการทำงานร่วมกันระหว่างหน่วยงาน ทั้งภายในและภายนอก เพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้

๒) ชี้แจงและให้รายละเอียดเกี่ยวกับข้อมูล ข้อเท็จจริง แก่บุคคลหรือหน่วยงานที่เกี่ยวข้องเพื่อสร้างความเข้าใจหรือความร่วมมือในการดำเนินงานตามที่ได้รับมอบหมาย

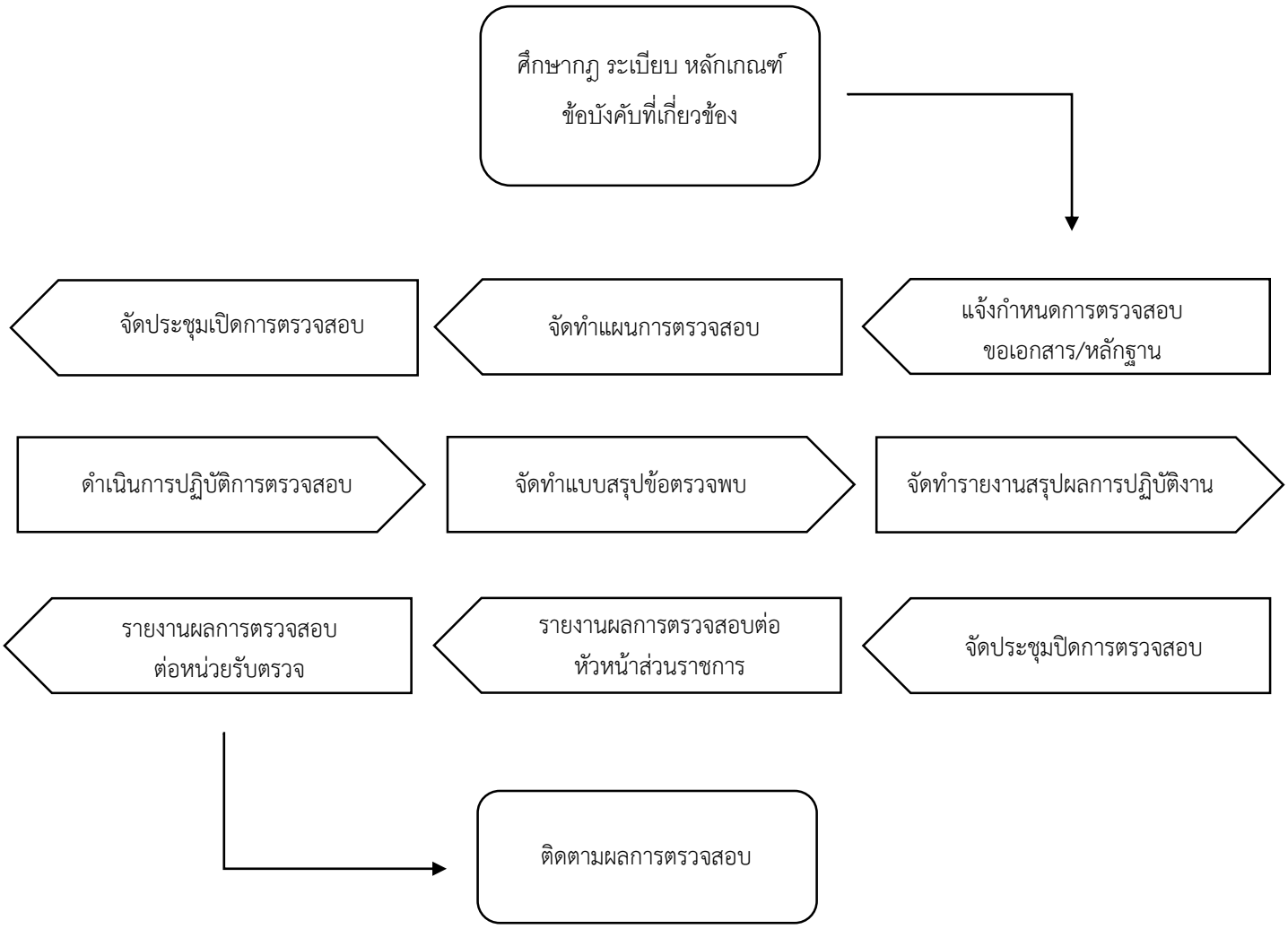
ด้านการบริการ

๑) คำปรึกษา แนะนำเบื้องต้น เผยแพร่ ถ่ายทอดความรู้ ด้านการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งตอบปัญหาและชี้แจงเรื่องต่างๆ เกี่ยวกับงานในหน้าที่ เพื่อให้ผู้รับบริการได้รับทราบข้อมูลความรู้ต่างๆ ที่เป็นประโยชน์

๒) จัดเก็บข้อมูลการตรวจสอบเบื้องต้น และให้บริการข้อมูลทางวิชาการเกี่ยวกับด้านการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้บุคลากรทั้งภายในและภายนอกหน่วยงานได้ทราบข้อมูลและความรู้

ขั้นตอนการปฏิบัติงาน (Flow Chart)

ขั้นตอนการปฏิบัติงานตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ มีดังนี้



๑) ศึกษากฎ ระเบียบ หลักเกณฑ์ข้อบังคับที่เกี่ยวข้อง

๑.๑ หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

๑.๒ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑.๔ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๑.๕ พระราชกฤษฎีกาการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๑.๖ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖

๑.๗ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ ๔) พ.ศ. ๒๕๖๔

๑.๘ ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑.๙ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

๑.๑๐ ประกาศสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พ.ศ. ๒๕๖๔

๑.๑๑ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๒) แจ้งกำหนดการเข้าตรวจสอบให้หน่วยรับตรวจทราบ/ขอเอกสารหลักฐานประกอบการตรวจสอบ

๒.๑ จัดทำหนังสือแจ้งกำหนดการตรวจสอบให้หน่วยรับตรวจทราบ

๒.๒ แจ้งรายการเอกสาร/หลักฐาน ที่ต้องใช้ในการตรวจสอบ ตามหลักเกณฑ์การตรวจสอบ

๓) จัดทำแผนการตรวจสอบ

๓.๑ ศึกษาระเบียบที่เกี่ยวข้องเพื่อกำหนดวัตถุประสงค์ หลักเกณฑ์การตรวจสอบ ตั้งแต่เริ่มต้นจนจบสิ้นสุดกระบวนการของการตรวจสอบว่าเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องหรือไม่

๓.๒ จัดทำแผนการปฏิบัติงานตรวจสอบ

๓.๓ เสนอแผนปฏิบัติงานตรวจสอบต่อหัวหน้าหน่วยตรวจสอบเพื่อพิจารณาอนุมัติ

๔) ประชุมเปิดการตรวจสอบ

๔.๑ จัดทำบันทึกหนังสือเชิญประชุมเปิดตรวจ

๔.๒ จัดทำแบบตอบรับการเข้าร่วมประชุม

๔.๓ จัดเตรียมเอกสารประกอบการประชุม ได้แก่

๔.๓.๑ แผนการปฏิบัติงานตรวจสอบ

๔.๓.๒ แบบรายชื่อผู้เข้าร่วมการเปิดตรวจ

๔.๔ จดบันทึกการประชุม

๔.๕ จัดทำรายงานการประชุม

๔.๖ นำส่งรายงานการประชุมแก่หน่วยรับตรวจ พร้อมแบบตอบรับรายงานการประชุม

๕) ดำเนินการปฏิบัติงานตรวจสอบ เป็นการลงมือปฏิบัติงานตรวจสอบ โดยการสอบทานข้อมูล ความครบถ้วน ถูกต้อง ของข้อมูลรวมถึงการดำเนินการ โดยการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ยึดหลักเกณฑ์ในการตรวจสอบ ดังนี้

๕.๑ สอบทานตามหลักเกณฑ์ของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๕.๒ สอบทานตามหลักเกณฑ์ของ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

๕.๓ สอบทานตามหลักเกณฑ์ของ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๕.๔ สอบทานการดำเนินงานจากเอกสารหลักฐานต่าง ๆ ที่เกี่ยวข้อง

๕.๕ การสัมภาษณ์ผู้ปฏิบัติงาน

๕.๖ การสังเกตการณ์

๕.๗ การจดบันทึกข้อมูล

๕.๘ จัดทำกระดาษทำการ

๖) จัดทำแบบสรุปข้อตรวจพบ สรุปประเด็นข้อเท็จจริงที่พบทั้งด้านดีและปัญหาข้อบกพร่องที่มีค่าแก่การตรวจสอบและรายงานให้ผู้เกี่ยวข้องทราบ โดยใช้ข้อมูลที่ได้จากการรวบรวมข้อมูลข้อเท็จจริงและหลักฐานต่าง ๆ ที่ได้ระหว่างการตรวจสอบ

๗) จัดทำรายงานสรุปผลปฏิบัติการตรวจสอบ เป็นการดำเนินการสรุปข้อมูลการตรวจสอบทั้งหมด โดยใช้ข้อมูลที่ได้จากการรวบรวมข้อมูลข้อเท็จจริง และหลักฐานต่าง ๆ ที่ได้ระหว่างการตรวจสอบเพื่อรายงานให้หน่วยรับตรวจและผู้บริหารทราบ

๘) ประชุมปิดการตรวจสอบ

๘.๑ จัดทำบันทึกหนังสือเชิญประชุมปิดตรวจ

๘.๒ จัดทำแบบตอบรับการเข้าร่วมประชุม

๘.๓ จัดเตรียมเอกสารประกอบการประชุม ได้แก่

๘.๓.๑ รายงานสรุปข้อตรวจพบ (Audit Finding)

๘.๓.๒ แบบรายชื่อผู้เข้าร่วมการปิดตรวจ

๘.๓.๓ แบบสอบถามความพึงพอใจหน่วยรับตรวจที่มีต่อกลุ่มตรวจสอบภายใน

๙) รายงานผลการตรวจสอบต่อหัวหน้าส่วนราชการ เป็นการรายงานผลการปฏิบัติงานให้ผู้บริหารทราบถึงวัตถุประสงค์ ขอบเขต วิธีปฏิบัติงานและผลการตรวจสอบข้อมูลทั้งหมด ทุกขั้นตอน สรุปข้อบกพร่องที่ตรวจพบประเด็นความเสี่ยงที่สำคัญและการควบคุม รวมทั้งเรื่องอื่น ๆ ที่ผู้บริหารควรทราบ พร้อมเสนอแนะในการแก้ไข ปรับปรุงเพื่อเสนอผู้บริหารหรือผู้ที่เกี่ยวข้องพิจารณาสั่งการแก้ไขปรับปรุงต่อไป

๑๐) รายงานผลการตรวจสอบต่อหน่วยรับตรวจ เมื่อผู้บริหารได้มีการรับทราบและสั่งการเรียบร้อยแล้ว จากนั้นรายงานผลการตรวจสอบให้หน่วยรับตรวจทราบและแก้ไข ปรับปรุง ตามข้อเสนอแนะของกลุ่มตรวจสอบภายใน

๑๑) การติดตามผลการตรวจสอบ เป็นหน้าที่ของผู้ตรวจสอบภายในที่จะต้องดำเนินการเพื่อให้มั่นใจว่าข้อเสนอแนะ/แนวทางแก้ไขในการปฏิบัติงานนั้น หน่วยรับตรวจสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ ประสิทธิผลหรือไม่ หรือหัวหน้าส่วนราชการพิจารณาจะยอมรับความเสี่ยงจากการไม่ปฏิบัติตามข้อเสนอแนะนั้น

บทที่ ๓
หลักเกณฑ์การปฏิบัติงาน

ระเบียบและหลักเกณฑ์ที่เกี่ยวข้อง

หลักเกณฑ์ที่ใช้ในการปฏิบัติงานตรวจสอบ ที่ครอบคลุมองค์ประกอบของระเบียบและหลักเกณฑ์ที่เกี่ยวข้องทั้งหมด มีดังนี้

๑. พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒. นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

๓. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่อาจดำเนินการหรือปฏิบัติตามวรรคหนึ่งได้ สำนักงานอาจให้ความช่วยเหลือด้านบุคลากรหรือเทคโนโลยีแก่หน่วยงานนั้นตามที่ร้องขอได้

มาตรา ๔๖ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้หน่วยงานของรัฐหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

ในกรณีที่มีการเปลี่ยนแปลงเจ้าหน้าที่ตามวรรคหนึ่ง ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งให้สำนักงานทราบโดยเร็ว

มาตรา ๕๒ เพื่อประโยชน์ในการติดต่อประสานงาน ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์และผู้ดูแลระบบ

คอมพิวเตอร์ไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลของตน และหน่วยงาน ตามมาตรา ๕๐ ภายในสามสิบวันนับแต่วันที่คณะกรรมการประกาศตามมาตรา ๔๙ วรรคสอง และมาตรา ๕๐ วรรคสอง หรือนับแต่วันที่คณะกรรมการมีคำวินิจฉัยตามมาตรา ๕๑ แล้วแต่กรณี โดยอย่างน้อยเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ต้องเป็นบุคคลซึ่งรับผิดชอบในการบริหารงานของหน่วยงานโครงสร้างพื้นฐานสาคัญทางสารสนเทศนั้น

ในกรณีที่มีการเปลี่ยนแปลงเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่ง ให้แจ้งการเปลี่ยนแปลงไปยังหน่วยงานที่เกี่ยวข้องตามวรรคหนึ่งก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่าเจ็ดวัน เว้นแต่มีเหตุจำเป็นอันไม่อาจก้าวล่วงได้ให้แจ้งโดยเร็ว

มาตรา ๕๔ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

มาตรา ๕๖ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแลและตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการหรือ กกม. กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

มาตรา ๕๘ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนการปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

ข้อ ๑.๑ มีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กร พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)

ข้อ ๑.๒ เฉพาะหน่วยงานของรัฐ, หน่วยงานของรัฐ มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงาน

(๑) เฉพาะหน่วยงานของรัฐ, โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์

(๒) เฉพาะหน่วยงานของรัฐ, ควรมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งควรมีบทบาทหน้าที่และความรับผิดชอบให้หน่วยงานดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อ ๑.๓ เฉพาะหน่วยงาน CII, หน่วยงาน CII มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน

(๑) เฉพาะหน่วยงาน CII, ควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล

ข้อ ๒.๑ มีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร

(ก) เกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และระดับความเสี่ยงที่ยอมรับได้ (Risk appetite)

(ข) วิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(ค) การเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๒.๒ มีการเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk register) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงาน CII

ข้อ ๒.๓ มีการติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอเพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้

ข้อ ๓.๑ มีการกำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงาน CII จากภัยคุกคามทางไซเบอร์

(ก) นโยบาย มาตรฐาน และแนวปฏิบัติมีความสอดคล้องกับหลักประมวลแนวทางปฏิบัติที่คณะกรรมการกำหนด ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วน และนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือระดับประเทศ

(ข) นโยบาย มาตรฐาน และแนวปฏิบัติมีการเผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงาน CII

ข้อ ๓.๒ มีการทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของหน่วยงานหน่วยงานของรัฐ และหน่วยงาน CII และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ข้อ ๑๗.๑ มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงาน CII เป็นเจ้าของและใช้บริการ

(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่ กมช. ประกาศกำหนด

ข้อ ๑๗.๒ หน่วยงาน CII มีการจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแล (รูปแบบตามคำแนะนำ เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยง และการตรวจสอบฯ)

ข้อ ๑๗.๓ ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑๗.๑ เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงาน CII ส่งแผนการดำเนินการแก้ไขไปยัง สกมช. ภายในกำหนด ๓๐ (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงาน CII จะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๑๗.๓ (ก)

ข้อ ๑๗.๔ ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงาน CII ดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยัง สกมช. ภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

ข้อ ๑๗.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงาน CII จะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.

ข้อ ๑๘ มีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) มีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

ข้อ ๑๘.๑ การประเมินความเสี่ยง (Risk Assessment)

(ก) มีการระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ

(ข) มีความเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(ค) มีการประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

ข้อ ๑๘.๒ การจัดการความเสี่ยง (Risk treatment)

(๑) มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

(๒) มีการกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน

ข้อ ๑๘.๓ การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)

มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๑๘.๔ การรายงานความเสี่ยง (Risk reporting)

(๑) มีการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ

(๒) การทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ข้อ ๑๙.๑ มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ข้อ ๑๙.๒ มีการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมดอย่างมีประสิทธิผล

ข้อ ๑๙.๓ มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

ข้อ ๑๙.๔ มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ข้อ ๒๑.๑.๑ มีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

ข้อ ๒๑.๑.๒ มีการระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

ข้อ ๒๑.๑.๓ มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

ข้อ ๒๑.๑.๔ มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญตามรายการที่ระบุไว้ในทะเบียนทรัพย์สินในข้อ ๒๑.๑.๑ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒๑.๒.๑ มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด

ข้อ ๒๑.๒.๒ มีการปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๒๑.๓.๑ มีการประเมินช่องโหว่ของบริการที่สำคัญ อ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน โดยครอบคลุมบริการที่สำคัญซึ่งเป็นระบบเทคโนโลยีสารสนเทศ (Information Technology system) และระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

ข้อ ๒๑.๓.๒ ขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญครอบคลุมการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม

ข้อ ๒๑.๓.๓ มีการประเมินช่องโหว่ของบริการที่สำคัญก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ

ข้อ ๒๑.๓.๔ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

ข้อ ๒๑.๓.๕ มีการตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) ได้รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ

ข้อ ๒๑.๓.๖ ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ตามความจำเป็น

ข้อ ๒๑.๓.๗ มีการตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระ

ข้อ ๒๑.๓.๘ มีการตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

ข้อ ๒๑.๓.๙ มีกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

ข้อ ๒๑.๓.๑๐ มีการส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบให้ กกม. หรือ สกมช. ทราบภายใน ๓๐ วันนับจากที่ได้รับการร้องขอ

ข้อ ๒๑.๔.๑ ผู้ให้บริการภายนอกต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ แม้ว่าจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญ

ข้อ ๒๑.๔.๒ มีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก

ข้อ ๒๑.๔.๓ ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา

ข้อ ๒๑.๔.๔ ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

ข้อ ๒๒.๑.๑ มีการจำกัดการเข้าถึงบริการที่สำคัญเฉพาะบุคลากร กิจกรรม อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตเท่านั้น

ข้อ ๒๒.๑.๒ มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

ข้อ ๒๒.๑.๓ มีการเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ

ข้อ ๒๒.๑.๔ มีการตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญและการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยหน่วยงาน และดำเนินการในสถานที่ หากเป็นไปได้

ข้อ ๒๒.๒.๑ มีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)

ข้อ ๒๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ตามข้อ ๒๒.๒.๒ (ก) – ๒๒.๒.๒ (ซ)

ข้อ ๒๒.๒.๓ มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ

ข้อ ๒๒.๒.๔ มีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

ข้อ ๒๒.๒.๕ มีกระบวนการจัดการเปลี่ยนแปลง (Change Management Process)

ข้อ ๒๒.๓.๑ มีการตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ

ข้อ ๒๒.๓.๒ มีการปฏิบัติตามแนวทางปฏิบัติในข้อ ๒๒.๓.๒ (ก) – (จ)

ข้อ ๒๒.๔.๑ มีการควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา กับบริการที่สำคัญ

ข้อ ๒๒.๔.๒ มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

ข้อ ๒๒.๕.๑ แผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้

ข้อ ๒๒.๕.๒ มีการทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒๒.๖.๑ กำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าว

ข้อ ๒๓.๑.๑ มีการสร้างกลไกและกระบวนเพื่อ ตรวจจับ จัดประเภท วิเคราะห์ และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ

ข้อ ๒๓.๑.๒ มีการทบทวนกลไกและกระบวนการภายในข้อ ๒๓.๑.๑ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

ข้อ ๒๔.๑.๑ มีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

ข้อ ๒๔.๒.๑ มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ข้อ ๒๔.๒.๒ มีแผนการสื่อสารในภาวะวิกฤต ซึ่งกำหนดรายละเอียดตามข้อ ๒๔.๒.๒ (ก) – (จ)

ข้อ ๒๔.๒.๓ มีการตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ

ข้อ ๒๔.๒.๔ มีการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

ข้อ ๒๔.๓.๑ มีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งในระดับชาติหรือระดับภาคส่วน

ข้อ ๒๔.๓.๒ มีการตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

ข้อ ๒๔.๓.๓ มีการปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์

ข้อ ๒๕.๑.๑ มีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)

ข้อ ๒๕.๑.๒ มีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

ข้อควรระวังในการปฏิบัติงาน

๑. ผู้ตรวจสอบภายในต้องมีความรู้ความเข้าใจ ทั้งในระบบเทคโนโลยีที่ตรวจสอบ และกฎ ระเบียบ หลักเกณฑ์ที่เกี่ยวข้อง หากไม่มีความรู้อาจทำให้การตรวจสอบไม่ครอบคลุมหรือพลาดประเด็นสำคัญ

๒. การกำหนดระยะเวลาในการตรวจสอบที่เหมาะสม หากกำหนดระยะเวลาในการตรวจสอบสั้นเกินไปอาจทำให้เกิดความกดดัน ทำให้การตรวจสอบล่าช้าได้ และประสิทธิภาพลดลงได้

๓. การจัดการกับข้อมูลที่เป็นความลับและความปลอดภัยของข้อมูลต้องระมัดระวังเป็นพิเศษเพื่อไม่ให้ข้อมูลรั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

๔. ความเข้าใจไม่ตรงกันจากการสื่อสารอาจทำให้งานไม่สามารถทำได้อย่างมีประสิทธิภาพ ส่งผลให้เกิดความล่าช้าและลดประสิทธิภาพการทำงาน

บทที่ ๔
เทคนิคการปฏิบัติงาน

วิธีการและขั้นตอนการปฏิบัติงาน

๑. ศึกษากฎ ระเบียบ หลักเกณฑ์ที่เกี่ยวข้อง

๑.๑ หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

๑.๒ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑.๔ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๑.๕ พระราชกฤษฎีกาการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๑.๖ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖

๑.๗ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ ๔) พ.ศ. ๒๕๖๔

๑.๘ ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑.๙ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

๑.๑๐ ประกาศสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พ.ศ. ๒๕๖๔

๑.๑๑ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๒. แจ้งกำหนดการเข้าตรวจสอบให้หน่วยรับตรวจทราบ/ขอเอกสารหลักฐานประกอบการตรวจสอบ

จัดทำหนังสือแจ้งกำหนดการตรวจสอบให้หน่วยรับตรวจทราบ และใส่รายการเอกสารหลักฐานที่ต้องการใช้ประกอบการตรวจสอบในหนังสือแจ้งกำหนดการตรวจสอบ โดยการร่างหนังสือใน microsoft word และสร้างหนังสือที่ระบบ e-office ตรวจสอบความถูกต้อง เสนอลงนามต่อหัวหน้าผู้ตรวจสอบ และดำเนินการส่งหนังสือแจ้งหน่วยรับตรวจ

๓. จัดทำแผนการตรวจสอบ

๓.๑ กำหนดชื่อแผนงาน/งาน/เรื่องที่จะตรวจสอบ แสดงรายละเอียดว่าเป็นเอกสารแผนปฏิบัติงานตรวจสอบ ชื่อเรื่องที่ตรวจสอบ ประจำปีงบประมาณใด หน่วยงานผู้รับผิดชอบ

๓.๒ กำหนดหน่วยงานเป้าหมายที่เข้ารับการตรวจสอบ

๓.๓ กำหนดประเภทการตรวจสอบ เรื่องที่ตรวจสอบอยู่ในประเภทการตรวจสอบแบบใด ซึ่งการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ จัดอยู่ในประเภทการตรวจสอบอื่นๆ

๓.๔ กำหนดประเด็นการตรวจสอบ ประเด็นหลักที่ควรดำเนินการตรวจสอบในเรื่องการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ การตรวจสอบภาพรวมของการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามนโยบาย กฎ ระเบียบ หลักเกณฑ์ที่เกี่ยวข้อง

ทั้งนี้ ในการกำหนดประเด็นการตรวจสอบ ผู้ตรวจสอบควรอาศัยข้อมูลความเสี่ยงที่เป็นปัจจุบัน และประเด็นที่อาจก่อให้ให้ความผิดพลาดมีผลกระทบต่อองค์กร

๒.๕ กำหนดวัตถุประสงค์ในการปฏิบัติงาน ด้านการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการกำหนดวัตถุประสงค์ปฏิบัฏิบติงานไว้ ดังนี้

เพื่อตรวจประเมินความสอดคล้องของการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีต่อ

๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์

๓) นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔) ตรวจสอบความพร้อมของเอกสารหลักฐานที่เกี่ยวข้อง

ทั้งนี้ ผู้ตรวจสอบควรกำหนดวัตถุประสงค์ให้ชัดเจน และสามารถปรับปรุงเปลี่ยนแปลงให้เหมาะสมกับสถานการณ์และข้อมูลที่ได้รับ

๒.๖ กำหนดขอบเขตการปฏิบัติงาน ควรกำหนดขอบเขตให้เหมาะสม ครบถ้วน เพียงพอต่อการปฏิบัติงานที่กำหนดไว้ในรื่องการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์มีการกำหนดขอบเขตการปฏิบัติงานเบื้องต้น ดังนี้

๑) การตรวจสอบกระบวนการและบริการที่สำคัญ

๒) การตรวจสอบการปฏิบัติตามกฎหมาย พรบ. ไซเบอร์ และมาตรฐานอื่นๆ ที่เกี่ยวข้อง

๒.๗ กำหนดแนวทางการปฏิบัติงาน กำหนดขั้นตอนหรือวิธีการปฏิบัติงานตรวจสอบให้ชัดเจนและเพียงพอ รวมถึงกำหนดเทคนิคการตรวจสอบที่เหมาะสม ดังนี้

- ประเด็นการตรวจสอบ
- เกณฑ์การตรวจสอบ/สิ่งที่ควรจะเป็น
- วิธีการตรวจสอบ
- แหล่งที่มาของข้อมูล/เอกสาร/หลักฐาน

๒.๘ ระยะเวลาที่ตรวจสอบ ระบุระยะเวลาที่ใช้ในการปฏิบัติงานตรวจสอบให้ชัดเจน ควรมีระยะเวลาการตรวจสอบอย่างน้อย ๓๐ วัน และสามารถเพิ่มระยะเวลาการตรวจสอบได้ตามความเหมาะสม

๒.๙ หลักเกณฑ์และวิธีการที่ใช้ในการตรวจสอบ

ผู้ตรวจสอบจะต้องศึกษาระเบียบและหลักเกณฑ์ที่เกี่ยวข้อง กำหนดหลักเกณฑ์และวิธีการตรวจสอบตามระเบียบหรือหลักเกณฑ์ที่เกี่ยวข้อง ดังนี้

๑) การกำกับดูและการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) การบริหารความเสี่ยง

๓) นโยบาย และแนวปฏิบัติ

๔) แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

๕) การประเมินความเสี่ยงด้านการรักษาความปลอดภัยไซเบอร์

๖) แผนการรับมือภัยคุกคามทางไซเบอร์

๗) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. จัดการประชุมเปิดการตรวจสอบ

การจัดการประชุมเปิดการตรวจสอบมีขั้นตอนดังนี้

๑. จัดทำหนังสือเชิญประชุมเปิดการตวจสอบ โดยการร่างหนังสือใน microsoft word และสร้างหนังสือที่ระบบ e-office แนบไฟล์เอกสารประกอบการประชุม ได้แก่ แผนการตรวจสอบ และแบบฟอร์มลงทะเบียนเข้าร่วมประชุม ตรวจสอบความถูกต้อง เสนอลงนามต่อหัวหน้าผู้ตรวจสอบ ออกเลขหนังสือ และส่งแจ้งหน่วยรับตรวจ

๒. จัดเตรียมห้องประชุม โดยการจองห้องประชุมที่ระบบ intranet ขอยืม ipad เพื่อใช้ในการประชุม จัดเตรียมข้อมูลการประชุมลง ipad (แผนการตรวจสอบ) จัดเตรียมความพร้อมห้องประชุม

๓. จดบันทึกการประชุม

๔. นำประเด็นสาระสำคัญในการประชุมมาจัดทำรายงานการประชุม โดยการร่างรายงานการประชุมใน microsoft word เสนอตรวจสอบและลงนามต่อหัวหน้าผู้ตรวจสอบ

๕. นำส่งรายงานการประชุมต่อหน่วยรับตรวจ โดยการร่างหนังสือใน microsoft word และสร้างหนังสือที่ระบบ e-office แนบไฟล์เอกสาร ได้แก่ รายงานการประชุม และแบบฟอร์มรับรองการประชุม ตรวจสอบความถูกต้อง เสนอลงนามต่อหัวหน้าผู้ตรวจสอบ ออกเลขหนังสือ และส่งหนังสือแจ้งหน่วยรับตรวจ

๕. ดำเนินการปฏิบัติงานตรวจสอบ

๑. ดำเนินการสอบทานเอกสารหลักฐานการดำเนินงานว่าเป็นไปตามกฎ ระเบียบ หลักเกณฑ์ที่กำหนดหรือไม่

๒. สอบทานโดยการสัมภาษณ์ผู้ปฏิบัติงาน สอบทานข้อมูลการปฏิบัติงานต่างๆ เพิ่มเติมของหน่วยรับตรวจ

๓. บันทึกข้อมูลการตรวจสอบลงกระดาษทำการ โดยการกรอกข้อมูลการสอบทานว่ามีการดำเนินการตามกฎ ระเบียบ หลักเกณฑ์หรือไม่ มีเอกสารประกอบหรือไม่ การดำเนินการดังกล่าวเพียงพอต่อการควบคุมภายในหรือไม่ หากเห็นว่าไม่เพียงพอให้เขียนข้อเสนอแนะเพื่อให้หน่วยรับตรวจดำเนินการแก้ไขหรือเพิ่มมาตรการเพื่อให้การควบคุมภายในมีประสิทธิภาพและเป็นไปตามกฎ ระเบียบ หลักเกณฑ์ต่อไป

๖. จัดทำแบบสรุปข้อตรวจพบ

เป็นการสรุปประเด็นข้อเท็จจริงที่พบทั้งด้านดีและปัญหา ข้อบกพร่องที่คิดว่ามีค่าควรแก่การตรวจสอบและรายงานให้ผู้เกี่ยวข้องทราบ โดยใช้ข้อมูลที่ได้จากการรวบรวมข้อมูลข้อเท็จจริง และหลักฐานต่าง ๆ ที่ได้ระหว่างการตรวจสอบ มาวิเคราะห์ถึงสาเหตุ ผลกระทบ และข้อเสนอแนะของผู้ตรวจสอบภายในให้หน่วยรับตรวจดำเนินการแก้ไขหรือเพิ่มมาตรการควบคุม

๗. จัดทำรายงานการตรวจสอบ

นำข้อมูลที่ได้จากการสรุปข้อตรวจพบมาจัดทำสรุปรายงานผลการปฏิบติงาน เพื่อรายงานต่อหน่วยรับตรวจ ผู้บริหาร และหน่วยงานที่เกี่ยวข้อง

๘. จัดการประชุมปิดการตรวจสอบ

การจัดการประชุมปิดการตรวจสอบมีขั้นตอนดังนี้

๑. จัดทำหนังสือเชิญประชุมปิดการตวจสอบ โดยการร่างหนังสือใน microsoft word และสร้างหนังสือที่ระบบ e-office แนบไฟล์เอกสารประกอบการประชุม ตรวจสอบความถูกต้อง เสนอลงนามต่อหัวหน้าผู้ตรวจสอบ ออกเลขหนังสือ และส่งหนังสือแจ้งหน่วยรับตรวจ

๒. จัดเตรียมห้องประชุม โดยการจองห้องประชุมที่ระบบ intranet ขอยืม ipad เพื่อใช้ในการประชุม จัดเตรียมข้อมูลการประชุมลง ipad (แบบสรุปข้อตรวจพบ) จัดเตรียมความพร้อมห้องประชุม

๓. จดบันทึกการประชุม

๔. นำประเด็นสาระสำคัญในการประชุมมาจัดทำรายงานการประชุม โดยการร่างรายงานการประชุมใน microsoft word เสนอตรวจสอบและลงนามต่อหัวหน้าผู้ตรวจสอบ

๕. นำส่งรายงานการประชุมต่อหน่วยรับตรวจ โดยการร่างหนังสือใน microsoft word และสร้างหนังสือที่ระบบ e-office แนบไฟล์เอกสาร ได้แก่ รายงานการประชุม และแบบฟอร์มรับรองการประชุม ตรวจสอบความถูกต้อง เสนอลงนามต่อหัวหน้าผู้ตรวจสอบ ออกเลขหนังสือ และส่งหนังสือแจ้งหน่วยรับตรวจ

๙. รายงานผลการตรวจสอบต่อหัวหน้าส่วนราชการและหน่วยงานที่เกี่ยวข้อง

เป็นการรายงานผลการปฏิบัติงานตรวจสอบ สรุปข้อเท็จจริงและข้อบกพร่องที่ตรวจพบประเด็นความเสี่ยงที่สำคัญและการควบคุม รวมทั้งเรื่องอื่น ๆ ที่ผู้บริหารควรทราบ พร้อมเสนอแนะในการแก้ไขปรับปรุงเพื่อเสนอผู้บริหารหรือผู้ที่เกี่ยวข้องพิจารณาสั่งการแก้ไขปรับปรุง การจัดทำหนังสือเรียนหัวหน้าส่วนราชการ โดยร่างหนังสือใน microsoft word และสร้างหนังสือที่ระบบ e-office แนบไฟล์เอกสาร ได้แก่ แบบสรุปข้อตรวจพบ แบบรายงานผลการปฏิบัติงาน และรายงานการประชุม ตรวจสอบความถูกต้อง เสนอลงนามต่อหัวหน้าผู้ตรวจสอบ ออกเลขหนังสือ และส่งเสนอรายงานต่อหัวหน้าส่วนราชการและหน่วยงานที่เกี่ยวข้อง

๑๐. รายงานผลการตรวจสอบต่อหน่วยรับตรวจ

เมื่อหัวหน้าส่วนราชการได้มีการรับทราบและสั่งการเรียบร้อยแล้ว จากนั้นรายงานผลการตรวจสอบให้หน่วยรับตรวจทราบและแก้ไข ปรับปรุง ตามข้อเสนอแนะของผู้ตรวจสอบภายใน

๑๑. การติดตามผลการตรวจสอบ

เป็นการติดตามผลการดำเนินการตามข้อเสนอแนะที่ให้ไว้ว่าที่การดำเนินการถูกต้องและครบถ้วน โดยการจัดทำหนังสือแจ้งหน่วยรับตรวจ ให้รายงานผลการดำเนินการตามข้อเสนอแนะที่หน่วยงานตรวจสอบให้ไว้ว่าได้ดำเนินการอย่างไร พร้อมรายงานผลให้หัวหน้าส่วนราชการทราบและพิจารณาสั่งการหรือยอมรับความเสี่ยงนั้น

บทที่ ๕
ปัญหา อุปสรรคและข้อเสนอแนะ

การดำเนินงานในองค์กร มักเผชิญกับปัญหาและอุปสรรคที่หลากหลาย ซึ่งอาจเกิดขึ้นจากปัจจัยภายในและภายนอกองค์กร การวิเคราะห์ปัญหาและอุปสรรคเป็นขั้นตอนสำคัญที่ช่วยให้องค์กรสามารถปรับตัวและพัฒนากระบวนการทำงานได้อย่างมีประสิทธิภาพ ทั้งนี้ การนำเสนอข้อเสนอแนะที่สร้างสรรค์และเป็นไปได้ถือเป็นส่วนสำคัญที่จะช่วยแก้ไขปัญหา ลดอุปสรรค และส่งเสริมการดำเนินงานให้เป็นไปตามเป้าหมาย

ส่วนของปัญหา อุปสรรคและข้อเสนอแนะนี้ เพื่อรวบรวมข้อมูลเกี่ยวกับปัญหา อุปสรรคที่พบในกระบวนการทำงาน รวมถึงข้อเสนอแนะที่สามารถนำไปปรับใช้เพื่อพัฒนาและปรับปรุงกระบวนการดำเนินงานขององค์กรให้ดียิ่งขึ้น หวังเป็นอย่างยิ่งว่าข้อมูลในส่วนนี้จะเป็นประโยชน์ต่อการวางแผนและการตัดสินใจเพื่อพัฒนาศักยภาพขององค์กรในระยะยาว

ปัญหา อุปสรรคและแนวทางการแก้ไข

ขั้นตอนการดำเนินงาน	ปัญหาและอุปสรรค	แนวทางแก้ไข
๑. การศึกษากฎ ระเบียบ หลักเกณฑ์ที่เกี่ยวข้อง	การต้องศึกษาและปฏิบัติตามระเบียบจำนวนมากอาจเพิ่มภาระงานให้กับผู้ปฏิบัติงาน โดยเฉพาะหากต้องใช้เวลาในการทำความเข้าใจและตรวจสอบความถูกต้อง	จัดระบบระเบียบให้เป็นหมวดหมู่และจัดลำดับความสำคัญ เพื่อลดเวลาการศึกษาและปฏิบัติตาม
๒. แจ้งกำหนดการเข้าตรวจสอบให้หน่วยรับตรวจทราบ ขอเอกสาร/หลักฐานประกอบการตรวจสอบ	หน่วยรับตรวจใช้เวลานานในการรวบรวมเอกสาร/หลักฐาน ที่จะจัดส่งให้ผู้ตรวจสอบ	๑. แจ้งหน่วยรับตรวจให้รวบรวมข้อมูลล่วงหน้าอย่างไม่เป็นทางการ ๒. กำหนดระยะเวลาในการจัดส่งเอกสาร/หลักฐาน ให้ชัดเจน
๓. จัดทำแผนการตรวจสอบ	การขาดข้อมูลที่จำเป็นหรือข้อมูลไม่ครบถ้วนอาจทำให้การตรวจสอบไม่สมบูรณ์ และส่งผลให้ข้อสรุปหรือรายงานการตรวจสอบไม่ถูกต้อง	๑. แจ้งหน่วยรับตรวจให้รวบรวมข้อมูลให้ครบถ้วนตามหลักเกณฑ์การตรวจสอบ ๒. อัพเดตการรวบรวมข้อมูลจากหน่วยรับตรวจเป็นระยะ
๔. การจัดประชุมเปิด/ปิดการตรวจสอบ	ห้องประชุมเต็ม	ดำเนินการจองห้องประชุมก่อนล่วงหน้า
๕. การดำเนินการตรวจสอบ	การพบข้อมูลหรือหลักฐานที่ไม่สอดคล้องกันอาจทำให้การตรวจสอบซับซ้อนขึ้น และต้องใช้เวลาในการตรวจสอบเพิ่มเติมเพื่อหาข้อเท็จจริง	๑. ตรวจสอบข้อมูลจากหลายแหล่งเพื่อยืนยันความถูกต้อง ๒. สอบถามผู้เกี่ยวข้องเพื่อหาข้อเท็จจริงเพิ่มเติมและบันทึกเหตุผลของความไม่สอดคล้องนั้น

๖. การจัดทำแบบสรุปข้อตรวจพบ/รายงานสรุปผลการตรวจสอบ	การนำเสนอข้อมูลในรายงานที่ไม่ชัดเจน หรือใช้ภาษาที่ซับซ้อน อาจทำให้ผู้รับรายงานเข้าใจผิด	๑. ใช้ภาษาที่กระชับและเข้าใจง่าย ๒. เพิ่มส่วนสรุปหรือไฮไลต์ประเด็นสำคัญเพื่อให้ผู้รับรายงานเข้าใจได้เร็วขึ้น
๗. การรายงานผลการตรวจสอบต่อหัวหน้าส่วนราชการ/หน่วยงานที่เกี่ยวข้อง	ข้อผิดพลาดเล็กน้อย เช่น คำผิด การเว้นวรรค การรายงานผิดหน่วยงานหรืออื่นๆ	๑. ตรวจสอบอย่างรอบคอบอีก ๑-๒ ครั้ง ๒. เพิ่มผู้ตรวจสอบเพื่อช่วยลดข้อผิดพลาด
๘. การติดตามผลการตรวจสอบ	หน่วยรับตรวจอาจไม่ให้ความร่วมมือหรือไม่ดำเนินการตามข้อเสนอแนะ ทำให้การติดตามผลไม่บรรลุวัตถุประสงค์	สื่อสารถึงความสำคัญและประโยชน์ของการติดตามผลให้หน่วยงานที่ถูกตรวจสอบเข้าใจ

ข้อเสนอแนะเพื่อการพัฒนา

๑. ให้บุคลากรเข้าร่วมการอบรมและพัฒนาทักษะอย่างสม่ำเสมอ เพื่อให้มีความรู้และความเชี่ยวชาญทั้งด้านการตรวจสอบภายใน และด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. จัดทำคู่มือการตรวจสอบ เพื่อให้ผู้ตรวจสอบมีแนวทางปฏิบัติที่ชัดเจนและลดความคลาดเคลื่อนในการดำเนินงาน

๓. มีการหารือร่วมกับหน่วยรับตรวจในเรื่องต่างๆที่เกี่ยวกับการตรวจสอบ และประเมินความพึงพอใจในการตรวจสอบเพื่อปรับปรุงกระบวนการตรวจสอบ

๔. มีการประสานงานหรือการขอความร่วมมือจากหน่วยงานที่เกี่ยวข้อง ที่มีความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ภาคผนวก

แผนปฏิบัติงานตรวจสอบ

ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประจำปีงบประมาณ .....

กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

.....

หน่วยรับตรวจ .....

เรื่องที่ตรวจสอบ .....

ประเด็นการตรวจสอบ .....

.....

วัตถุประสงค์ .....

การปฏิบัติงาน .....

ขอบเขตการปฏิบัติงาน .....

.....

ระยะเวลาที่ตรวจสอบ .....

ผู้รับผิดชอบการตรวจสอบ .....

.....

.....

แนวทางการปฏิบัติงาน

ประเด็นการตรวจสอบ	เกณฑ์/สิ่งที่ควรจะเป็น	วิธีการตรวจสอบ	เอกสาร/หลักฐาน สำหรับตรวจสอบ

ผู้รับผิดชอบ.....
.....
.....

ผู้รับผิดชอบ.....
.....
.....

ผู้รับผิดชอบ.....
.....
.....

ผู้รับผิดชอบ.....
.....
.....

ผู้รับผิดชอบ.....
.....
.....

ผู้รับผิดชอบ/ผู้สอบทาน.....
.....
.....

บันทึกสรุปข้อตรวจพบ Audit Finding
กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
เรื่อง การตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์
ตามองค์ประกอบของมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์
ประจำปีงบประมาณ .....

.....

หน่วยรับตรวจ .....

ประเด็นการตรวจสอบ .....

.....

วัตถุประสงค์การตรวจสอบ .....

.....

หลักเกณฑ์ (Criteria) .....

.....

ข้อเท็จจริง (Condition) .....

.....

ผลกระทบ (Effect) .....

สาเหตุ (Cause) .....

ข้อเสนอแนะ .....

(Recommendation) .....

ข้อตอบกลับ

.....

.....

.....

ลงนาม.....

ตำแหน่ง.....

รายงานผลการปฏิบัติงาน

กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

เรื่อง การตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามองค์ประกอบของมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

ประจำปีงบประมาณ .....

.....

หน่วยรับตรวจ .....

ประเด็นการตรวจสอบ .....

.....

วัตถุประสงค์การตรวจสอบ .....

.....

ขอบเขตการตรวจสอบ .....

.....

ระยะเวลาที่ตรวจสอบ .....

วิธีการตรวจสอบ .....

.....

สรุปผลการตรวจสอบ .....

.....

ผลกระทบ (Effect) .....

.....

สาเหตุ (Cause) .....

.....

ข้อเสนอแนะ .....

(Recommendation) .....

ลงลายมือชื่อผู้ปฏิบัติงานตรวจสอบ

ลงลายมือชื่อผู้ตรวจสอบ/สอบทาน

ผู้รับผิดชอบ.....
(ชื่อ – นามสกุล)
ตำแหน่ง .....

ผู้รับผิดชอบ.....
(ชื่อ – นามสกุล)
ตำแหน่ง .....

ผู้รับผิดชอบ.....
(ชื่อ – นามสกุล)
ตำแหน่ง .....

ผู้รับผิดชอบ/ผู้สอบทาน.....
(ชื่อ – นามสกุล)
ตำแหน่ง ผู้อำนวยการกลุ่มตรวจสอบภายใน
วันที่ .....

IT๑_xx/xx

รหัสกระดาษทำการ

กระดาษทำการ

กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

การตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามองค์ประกอบของมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

ประจำปีงบประมาณ .....

หน่วยรับตรวจ ..... **ระยะเวลา** .....

แบบสอบทาน ..... **วันที่เข้าตรวจ** .....

ประเด็นการตรวจสอบ การตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	รายการ	ผลการตรวจสอบ		เอกสาร/หลักฐานประกอบ		คำอธิบายเพิ่มเติม
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	มี/ครบถ้วน	ไม่มี/ไม่ครบถ้วน	

สรุปผลการตรวจสอบ

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

ผู้รับผิดชอบ.....
(ชื่อ – นามสกุล)
ตำแหน่ง .....
วันที่ .....

ผู้รับผิดชอบ.....
(ชื่อ – นามสกุล)
ตำแหน่ง .....
วันที่ .....

ผู้รับผิดชอบ.....
(ชื่อ – นามสกุล)
ตำแหน่ง .....
วันที่ .....

ผู้รับผิดชอบ/ผู้สอบทาน.....
(ชื่อ – นามสกุล)
ตำแหน่ง ผู้อำนวยการกลุ่มตรวจสอบภายใน
วันที่ .....

เอกสารอ้างอิง

๑. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

๒. พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๔. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๕. พระราชกฤษฎีกาการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๖. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖

๗. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ ๔) พ.ศ. ๒๕๖๔

๘. ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๙. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

๑๐. ประกาศสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พ.ศ. ๒๕๖๔

๑๑. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

กลุ่มตรวจสอบภายใน
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ