สดช.

# คู่มือการตรวจสอบความมั่นคงปลอดภัย ของเทคโนโลยีสารสนเทศ

## ตามองค์ประกอบของมาตรฐานการควบคุมภายใน ด้านสารสนเทศและการสื่อสาร

URL : http://shorturl.at/bex05

**SCAN QR CODE**
**เพื่อดูคู่มือ ฯ**


กลุ่มตรวจสอบภายใน
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

# คู่มือการตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

## ตามองค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร

**กลุ่มตรวจสอบภายใน**

**สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ**

**กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม**

**สิงหาคม ๒๕๖๕**

# คำนำ

การตรวจสอบภายใน เป็นเครื่องมือของฝ่ายบริหารในกิจกรรมการให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานของหน่วยงานของรัฐให้ดีขึ้นการตรวจสอบภายในจะช่วยให้หน่วยงานของรัฐบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ การปฏิบัติงานโดยอิสระปราศจากการแทรกแซงในการทำหน้าที่ตรวจสอบและประเมินผลการดำเนินกิจกรรมต่าง ๆ ภายในองค์กร ด้วยการปฏิบัติงานเกี่ยวกับการวิเคราะห์ ประเมินให้คำปรึกษา ให้ข้อมูลและข้อเสนอแนะ เพื่อสนับสนุนผู้ปฏิบัติงานทุกระดับขององค์กรสามารถปฏิบัติหน้าที่และดำเนินงานเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องอย่างมีประสิทธิภาพยิ่งขึ้น จึงต้องได้รับการพัฒนาคุณภาพการบริหารจัดการของหน่วยงานและบุคลากรอยู่เสมอ

กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ จึงได้จัดทำคู่มือการตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ เพื่อสำหรับให้ผู้ตรวจสอบภายในใช้เป็นแนวทางในการปฏิบัติงานตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศให้สอดคล้องตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องให้เป็นไปอย่างถูกต้อง มีประสิทธิภาพและประสิทธิผล ตลอดจนเพื่อให้ข้อเสนอแนะในการปรับปรุงการปฏิบัติงานที่เป็นประโยชน์ และพัฒนาระบบงานของหน่วยงานให้ดียิ่งขึ้นต่อไป

กลุ่มตรวจสอบภายใน
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
สิงหาคม ๒๕๖๕

# สารบัญ

# บทที่ ๑
# บทนำ

## หลักการและเหตุผล

การปฏิบัติงานตรวจสอบภายใน คือ กิจกรรมการให้ความเชื่อมั่นและการให้คำปรึกษา อย่างเที่ยงธรรมและเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานของหน่วยงานของรัฐให้ดีขึ้น การตรวจสอบภายในจะช่วยให้หน่วยงานของรัฐบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ การปฏิบัติงานโดยอิสระปราศจากการแทรกแซงในการทำหน้าที่ตรวจสอบและประเมินผลการดำเนินกิจกรรมต่าง ๆ ภายในองค์กร ด้วยการปฏิบัติงานเกี่ยวกับการวิเคราะห์ ประเมิน ให้คำปรึกษา ให้ข้อมูลและข้อเสนอแนะเพื่อสนับสนุนผู้ปฏิบัติงานทุกระดับขององค์กรให้สามารถปฏิบัติหน้าที่และดำเนินงานเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องอย่างมีประสิทธิภาพยิ่งขึ้น จึงต้องได้รับการพัฒนาคุณภาพการบริหารจัดการของหน่วยงานและบุคลากรอยู่เสมอ

ในการดำเนินการพัฒนาคุณภาพการบริหารจัดการภาครัฐ (Public Sector Management Quality Award : PMQA ) ซึ่งสอดคล้องกับแผนยุทธศาสตร์การพัฒนาระบบราชการไทย มีการดำเนินงานในหมวดที่ ๖ การจัดการกระบวนการ ได้กำหนดให้ส่วนราชการมีการวิเคราะห์กระบวนการที่สำคัญที่ช่วยสร้างคุณค่าแก่ผู้รับบริการ ผู้มีส่วนได้ส่วนเสีย และการบรรลุพันธกิจของส่วนราชการ ตลอดจนกระบวนการสนับสนุนที่สำคัญต่าง ๆ ดังนั้น ในสภาวะแวดล้อมปัจจุบันที่มีการปรับเปลี่ยนอยู่ตลอดเวลา ทั้งนโยบายตลอดจนบุคลากรผู้รับผิดชอบงาน สิ่งหนึ่งที่จะทำให้คนเรียนรู้งานได้เร็วขึ้นและปฏิบัติงานทดแทนกันได้ในกรณีที่ผู้รับผิดชอบไม่สามารถปฏิบัติงานได้ หรือมีการโยกย้ายสับเปลี่ยน เครื่องมือนั้นก็คือ “คู่มือการปฏิบัติงาน” โดยจัดทำคู่มือการปฏิบัติงาน “การตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ตามองค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร” เพื่อแสดงขั้นตอนและวิธีการของกระบวนการปฏิบัติงานตรวจสอบ ตั้งแต่เริ่มต้นจนสิ้นสุดการดำเนินงาน แสดงขั้นตอนในแต่ละกระบวนการย่อยตามผังกระบวนการ วิธีการดำเนินงาน รายละเอียดของงาน มาตรฐานคุณภาพงาน ระบบติดตาม/ประเมินผล ตลอดจนผู้รับผิดชอบและเอกสารอ้างอิงต่าง ๆ ซึ่งจะทำให้ผู้ปฏิบัติงานมองเห็นภาพรวมและเส้นทางการปฏิบัติงานจากจุดเริ่มต้นถึงจุดสิ้นสุดของงานได้อย่างครอบคลุมและชัดเจน

## วัตถุประสงค์

๑. เป็นคู่มือสำหรับให้ผู้บริหาร ผู้ตรวจสอบภายใน และเจ้าหน้าที่ผู้ปฏิบัติงาน ในการตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศตามองค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร ให้เป็นไปอย่างถูกต้องตามกระบวนการและแผนการปฏิบัติงานตรวจสอบภายใน รวมถึงขอบเขต กฎระเบียบ หลักเกณฑ์และวิธีปฏิบัติที่เกี่ยวข้อง ส่งผลให้การตรวจสอบภายในมีประสิทธิภาพ ได้รับประสิทธิผลมากยิ่งขึ้น

๒. เพื่อให้ผู้ตรวจสอบภายในทราบและเข้าใจกระบวนงานต่าง ๆ ของการดำเนินงานในการตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศตามการควบคุมภายในด้านสารสนเทศและการสื่อสาร

๓. เพื่อให้บุคลากรสามารถปฏิบัติงานทดแทนกันและปฏิบัติงานต่อเนื่องกันได้ ในกรณีจำเป็นเร่งด่วนไม่ก่อให้เกิดผลเสียทางราชการ

**ประโยชน์ที่คาดว่าจะได้รับ**

๑. บุคลากรของกลุ่มตรวจสอบภายในใช้เป็นคู่มือสำหรับการปฏิบัติงานการตรวจสอบ

๒. สร้างความเชื่อมั่น รักษามาตรฐานคุณภาพงานตรวจสอบภายในภาครัฐของหน่วยงาน

๓. การปฏิบัติงานของหน่วยงาน เป็นไปตามกฎระเบียบ หลักเกณฑ์และวิธีปฏิบัติที่เกี่ยวข้อง

๔. กลุ่มตรวจสอบภายในมีกระบวนการควบคุมภายในที่ดี เป็นระบบ โปร่งใส มีประสิทธิภาพประสิทธิผลมากยิ่งขึ้น

๕. หน่วยรับตรวจหรือบุคลากรที่เกี่ยวข้องได้ทราบถึงแนวทาง วิธีการตรวจสอบที่ชัดเจน และสามารถจัดเตรียมเอกสารหลักฐานต่าง ๆ ให้ผู้ตรวจสอบภายในได้ครบถ้วนสมบูรณ์

**ระเบียบและหลักเกณฑ์ที่เกี่ยวข้อง**

๑. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

๒. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๓. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ ๒) พ.ศ. ๒๕๔๘

๔. ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๕. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๖. กฎระเบียบ หลักเกณฑ์และวิธีปฏิบัติที่เกี่ยวข้อง

**คำจำกัดความ**

๑. ผู้ตรวจสอบ หมายถึง ผู้ตรวจสอบภายในของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)

๒. หน่วยรับตรวจ หมายถึง หน่วยงานที่รับผิดชอบหรือเกี่ยวข้องกับกิจกรรมที่ดำเนินการตรวจสอบ

๓. กระดาษทำการ หมายถึง เอกสารหลักฐานที่ได้มาจากการรวบรวมและจัดทำขึ้นในช่วงระยะเวลาที่ถือปฏิบัติงานตรวจสอบภายใน อาจอยู่ในรูปแบบตาราง การวิเคราะห์เอกสาร หรือแบบฟอร์มที่จัดทำขึ้นเพื่อใช้บันทึกสรุปข้อตรวจพบ ผลการตรวจสอบ ซึ่งเป็นส่วนหนึ่งของภารกิจการตรวจสอบภายใน

๔. การตรวจสอบด้านเทคโนโลยีสารสนเทศ หมายถึง กิจกรรมการสร้างความเชื่อมั่น (Assurance) ต่อระบบเทคโนโลยีสารสนเทศ และการให้ข้อเสนอแนะรวมถึงแนวทางการปรับปรุงระบบงานด้านเทคโนโลยีสารสนเทศของหน่วยงานให้มีความสอดคล้องกับกฎ ระเบียบ และความเสี่ยงรวมถึงการตรวจสอบเพื่อช่วยให้

หน่วยงานบรรลุเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการควบคุมทั่วไปของระบบเทคโนโลยีสารสนเทศและการควบคุมเฉพาะระบบงาน

๕. การควบคุมภายในระบบเทคโนโลยีสารสนเทศ หมายถึง กระบวนการหรือขั้นตอนการทำงานที่เป็นผลมาจากการออกแบบ โดย ผู้บริหาร หรือบุคลากรอื่นๆ ของหน่วยงาน เพื่อก่อให้เกิดความมั่นใจได้อย่างสมเหตุสมผลว่าหน่วยงานจะสามารถบรรลุวัตถุประสงค์ความมีประสิทธิผล และประสิทธิภาพของการดำเนินงานระบบเทคโนโลยีสารสนเทศ

# บทที่ ๒
# ความรู้ทั่วไปเกี่ยวกับสารสนเทศ

**หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑** มีองค์ประกอบของมาตรฐานการควบคุมภายใน ๕ องค์ประกอบ ๑๗ หลักการ ดังนี้

๑. สภาพแวดล้อมการควบคุม (Control Environment) ๕ หลักการ
๒. การประเมินความเสี่ยง (Risk Assessment) ๔ หลักการ
๓. กิจกรรมการควบคุม (Control Activities) ๓ หลักการ
๔. สารสนเทศและการสื่อสาร (Information and communication) ๓ หลักการ
๕. กิจกรรมการติดตามผล (Monitoring Activities) ๒ หลักการ

**องค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร**

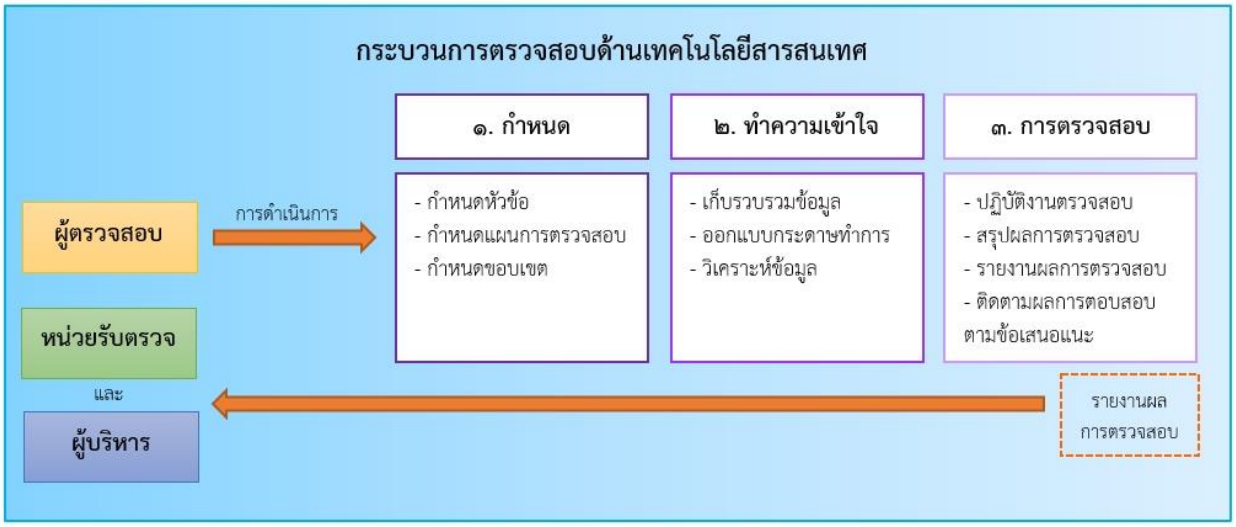
- สารสนเทศจะช่วยให้มีการดำเนินการตามการควบคุมภายในที่กำหนด เพื่อสนับสนุนให้บรรลุวัตถุประสงค์ของหน่วยงานของรัฐ
- การสื่อสารเกิดขึ้นได้ทั้งจากภายในและภายนอก เป็นช่องทางให้ทราบถึงสารสนเทศที่สำคัญในการควบคุมการดำเนินงานของหน่วยงานของรัฐ
- การสื่อสารจะช่วยให้บุคลากรในหน่วยงานมีความเข้าใจถึงความรับผิดชอบ และความสำคัญของการควบคุมภายในที่มีต่อการบรรลุวัตถุประสงค์

ประกอบด้วย ๓ หลักการ ดังนี้

๑. หน่วยงานจัดทำ/จัดหาและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้ปฏิบัติตามการควบคุมภายในที่กำหนด
๒. หน่วยงานมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบที่มีต่อการควบคุมภายใน ซึ่งจำเป็นในการสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด
๓. หน่วยงานสื่อสารกับบุคคลภายนอกเกี่ยวกับเรื่องที่มีผลกระทบต่อการปฏิบัติตามการควบคุมภายในที่กำหนด

**กระบวนการตรวจสอบระบบสารสนเทศ**

มีกระบวนการเช่นเดียวกับตรวจสอบภายในประเภทอื่น ๆ โดยเริ่มตั้งแต่ผู้ตรวจสอบภายในศึกษาทำความเข้าใจระบบงานสารสนเทศ จัดทำแผนการตรวจสอบ จัดทำกระดาษทำการ สรุปข้อเท็จจริง รายงานผลการตรวจสอบ และการติดตามผลการตรวจสอบ ทั้งนี้ ผู้ตรวจสอบระบบสารสนเทศต้องมีความรู้ ความเชี่ยวชาญเกี่ยวกับระบบเทคโนโลยีสารสนเทศ




**การควบคุมภายในด้านเทคโนโลยีสารสนเทศ**

ประกอบด้วยการควบคุมทั่วไป (General Control) และการควบคุมเฉพาะระบบงาน (Application Control)

**การควบคุมทั่วไป (General Control)**

หมายถึง การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุมนโยบายและวิธีการในการควบคุมระบบสารสนเทศ การควบคุมความปลอดภัย การควบคุมการพัฒนาและปรับปรุง และการป้องกัน/ลดความเสียหายของระบบ เป็นการควบคุมภายในสำหรับองค์กรในภาพรวม

๑. การกำหนดนโยบายในการใช้สารสนเทศ
   - มีนโยบายการรักษาความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศที่ชัดเจน ว่าใครต้องการเข้าถึงข้อมูลอะไร เมื่อไหร่ ในระบบงานใด
   - การให้สิทธิ์ในการเข้าถึงข้อมูลเฉพาะบุคคลที่มีสิทธิ์ในการเข้าถึงข้อมูลนั้น
๒. การแบ่งแยกหน้าที่งานในระบบสารสนเทศ มีการแบ่งแยกหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในระบบงานคอมพิวเตอร์ให้ชัดเจน เช่น แยกหน้าที่การพัฒนาระบบออกจากหน้าที่ผู้ปฏิบัติการคอมพิวเตอร์ ผู้บริหารฐานข้อมูล (Database Administrator) ต้องไม่ทำหน้าที่อื่น
๓. การควบคุมโครงการพัฒนาระบบสารสนเทศ โดยกำหนดแผนระยะยาว แผนงานพัฒนาระบบ กำหนดการประมวลผลข้อมูล มอบหมายหน้าที่และความรับผิดชอบการประเมินผลงานระหว่างการดำเนินโครงการ การสอบทานภายหลังการติดตั้งระบบ และนำระบบมาใช้งาน การวัดผลการดำเนินงานของระบบ
๔. การควบคุมการเปลี่ยนแปลงแก้ไขระบบ โดยการกำหนดระเบียบวิธีปฏิบัติในการแก้ไขระบบที่เป็นลายลักษณ์อักษร มีการศึกษาถึงผลกระทบต่าง ๆ มีการทดสอบระบบที่แก้ไขแล้วก่อนนำไปใช้ จัดทำเอกสารคู่มือประกอบการแก้ไข และประเมินผลและสอบทานระบบงานภายหลังเริ่มใช้
๕. การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์ การประมวลผลข้อมูลของระบบงานต่าง ๆ การกู้ระบบและการสำรองข้อมูล การทดสอบ และการจัดการกับปัญหาของระบบ จัดทำแผนสำรอง มีความถูกต้อง ครบถ้วน

๖. การควบคุมเข้าถึงอุปกรณ์คอมพิวเตอร์ มีสถานที่จัดเก็บอุปกรณ์คอมพิวเตอร์มิดชิด ไม่มีอากาศร้อนชื้น และแม่เหล็ก มีการรักษาความปลอดภัย กำหนดการเข้าออกได้เฉพาะผู้เกี่ยวข้อง กำหนดนโยบายรักษาความปลอดภัยที่ชัดเจน ติดระบบเตือนภัยกรณีมีผู้บุกรุก จำกัดให้ใช้โทรศัพท์เฉพาะเรื่องที่เกี่ยวกับงาน ติดอุปกรณ์ป้องกันเครื่องคอมพิวเตอร์

๗. การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ การกำหนดผู้ใช้ (User Views or Subschema) ตารางแสดงสิทธิ์ในการเข้าถึงฐานข้อมูล (Database Authorization Table) และการเข้ารหัสข้อมูล (Data Encryption)

๘. การควบคุมการเข้าถึงระบบงาน

- การพิสูจน์ตัวจริง (Authentication) โดยกำหนดรหัสผ่าน (Password) การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ (Physical Possession Identification)
- การกำหนดสิทธิ์ (Authorization)
- การบันทึกกิจกรรมต่าง ๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)

**การควบคุมเฉพาะระบบงาน (Application Control)**

หมายถึง การควบคุมรายการข้อมูลในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของข้อมูล เป็นแนวทางในการกำหนดขอบเขตการควบคุม ตัวอย่างเช่น ระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban)

๑. การควบคุมการเข้าถึงระบบสารบรรณอิเล็กทรอนิกส์ ต้องพิสูจน์ความถูกต้องของการเข้าใช้งานระบบ เช่น การแสดงตัวตนการเข้าถึงระบบโดยใช้ ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งาน

- การควบคุมการใช้งานระบบสารบรรณโดยผู้ดูแลระบบ มีการบันทึกข้อมูลหน่วยงาน ทำการระบุรหัสเป็นตัวเลขที่ไม่ซ้ำกันภายในต้นสังกัดเดียวกัน เพื่อระบุชื่อหน่วยงานที่ต้องการ และมีการกำหนดบทบาทการเข้าใช้งาน ทำการบันทึกข้อมูลบุคลากร โดยอ้างอิงเลขรหัสหน่วยงานที่สังกัดอยู่

๒. การควบคุมการนำเข้าข้อมูลระบบสารบรรณอิเล็กทรอนิกส์ โดยข้อมูลที่นำเข้านั้นจะเป็นข้อมูลเอกสารหนังสือราชการที่ได้มีการเสนอให้ผู้บังคับบัญชา/ผู้บริหาร/ผู้อำนวยการ ทำการตรวจสอบรับทราบ และเห็นชอบเป็นที่เรียบร้อยแล้ว

๓. การควบคุมการจัดเก็บข้อมูลไว้ในระบบ มีการกำหนดสิทธิ์ในการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การสำรองข้อมูล และการกำหนดอายุการจัดเก็บแฟ้มข้อมูล

**ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

๑. ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ (IT Management Risk)

๑.๑ การควบคุมดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยผู้บริหารของหน่วยงาน (Oversight of Technology Risks)

๑.๒ การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risk Management)

๒. ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (Operation Risk)

๒.๑ ความเสี่ยงที่เกี่ยวกับการรักษาความปลอดภัย (Security)

- การรักษาความปลอดภัยให้กับโครงสร้างพื้นฐานของระบบปฏิบัติการ (Operational Infrastructure Security Management) และการควบคุมการเข้าถึง (Access Control)
- การควบคุมและป้องกันศูนย์ข้อมูล (Data Centers Protection and Controls)
- การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (Management of IT Outsourcing Risks)

๒.๒ ความเสี่ยงที่เกี่ยวกับความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)

- การสร้างและพัฒนาระบบข้อมูล (Acquisition and Development of Information Systems)

๒.๓ ความเสี่ยงที่เกี่ยวกับความพร้อมใช้งาน (Availability)

- การบริหารจัดการบริการทางด้านเทคโนโลยีสารสนเทศ (IT Service Management)
- การทำให้ระบบเทคโนโลยีสารสนเทศมีความน่าเชื่อถือ พร้อมใช้งาน และสามารถนำกลับมาใช้งานใหม่ได้หากเกิดกรณีฉุกเฉิน (Systems Reliability, Availability and Recoverability)

๒.๔ ความเสี่ยงด้านชื่อเสียงและการปฏิบัติตามกฎหมาย (Reputation and Regulation)

# บทที่ ๓
# การตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

การตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ตามองค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร มีรายละเอียดดังต่อไปนี้ การบริหารจัดการเป็นไปตามหลักเกณฑ์การปฏิบัติการควบคุมภายในของหน่วยงานรัฐ พ.ศ. ๒๕๖๑ องค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร ประกอบด้วย ๓ หลักการ ดังนี้

๑. หน่วยงานของรัฐจัดทำหรือจัดหาและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด

๒. หน่วยงานของรัฐมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบที่มีต่อการควบคุมภายในซึ่งมีความจำเป็นในการสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด

๓. หน่วยงานของรัฐมีการสื่อสารกับบุคคลภายนอกเกี่ยวกับเรื่องที่มีผลกระทบต่อการปฏิบัติตามการควบคุมภายในที่กำหนด

**แผนผังขั้นตอนการปฏิบัติงานตรวจสอบภายใน**

| | |
|---|---|
| ๑ | ศึกษากฎ ระเบียบ หลักเกณฑ์ข้อบังคับที่เกี่ยวข้อง |
| ๒ | แจ้งหน่วยรับตรวจถึงกำหนดการตรวจสอบและขอเอกสารประกอบการตรวจสอบ |
| ๓ | จัดทำแผนการปฏิบัติงานตรวจสอบ |
| ๔ | ประชุมเปิดตรวจ |
| ๕ | ปฏิบัติงานตรวจสอบ |
| ๖ | จัดทำรายงานสรุปข้อตรวจพบ |
| ๗ | ประชุมปิดตรวจ |
| ๘ | จัดทำรายงานสรุปผลการปฏิบัติงานตรวจสอบ |
| ๙ | รายงานผลการตรวจสอบต่อหัวหน้าส่วนราชการ |
| ๑๐ | รายงานผลการตรวจสอบแก่หน่วยรับตรวจ |
| ๑๑ | การติดตามผลการตรวจสอบ |

**รายละเอียดขั้นตอนการปฏิบัติงานตรวจสอบภายใน**

๑. ศึกษากฎ ระเบียบ หลักเกณฑ์ข้อบังคับที่เกี่ยวข้อง ดังนี้

๑.๑ หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

๑.๒ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑.๓ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ ๒) พ.ศ. ๒๕๔๘

๑.๔ ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑.๕ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑.๖ กฎระเบียบ หลักเกณฑ์และวิธีปฏิบัติที่เกี่ยวข้อง

๒. แจ้งหน่วยรับตรวจถึงกำหนดการเข้าตรวจสอบ และขอเอกสาร/หลักฐานประกอบการตรวจสอบเบื้องต้น ดังนี้

๒.๑ คำสั่งแต่งตั้งคณะกรรมการ/คณะทำงานที่เกี่ยวข้อง

๒.๒ คำสั่งมอบหมายการทำงาน/การกำหนดบุคลากร กำหนดบทบาทหน้าที่การดูแลบำรุงรักษาและการพัฒนาระบบสารสนเทศ

๒.๓ แผนงานการใช้งานระบบสารสนเทศ

๒.๔ หลักเกณฑ์ วิธีการ คู่มือ นโยบายและแนวปฏิบัติในการใช้งานระบบสารสนเทศ

๒.๕ ข้อมูลสัญญา และขอบเขตของงาน (TOR) ที่เกี่ยวข้อง

๒.๖ แผนการบริหารความมั่นคงปลอดภัยสำหรับการดำเนินงานด้านสารสนเทศ

๒.๗ รายงานการสำรองข้อมูลในกรณีฉุกเฉิน

๒.๘ ข้อมูลการเผยแพร่แผนฉุกเฉินด้านสารสนเทศให้บุคคลที่เกี่ยวข้องรับทราบ

ทั้งนี้ ผู้ตรวจสอบภายในสามารถปรับเปลี่ยนรายการเอกสารหลักฐานต่างๆ ข้างต้นได้ตามความเหมาะสม เพื่อให้ได้มาซึ่งข้อมูลที่ครบถ้วนและเพียงพอต่อการตรวจสอบ

๓. จัดทำแผนการปฏิบัติงานตรวจสอบ

๓.๑ ศึกษาข้อมูลที่ได้รับจากหน่วยรับตรวจ

๓.๒ วิเคราะห์ข้อมูล กำหนดวัตถุประสงค์ หลักเกณฑ์ เพื่อตรวจสอบการดำเนินการตรวจสอบ ตั้งแต่เริ่มต้นจบสิ้นสุดกระบวนการของการตรวจสอบว่าเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องหรือไม่

๓.๓ จัดทำแผนการปฏิบัติงานตรวจสอบ

๓.๔ เสนอแผนปฏิบัติงานตรวจสอบต่อหัวหน้าหน่วยตรวจสอบเพื่อพิจารณาอนุมัติ

๔. ประชุมเปิดตรวจ มีกระบวนการดังนี้

๔.๑ จัดทำบันทึกหนังสือเชิญประชุมเปิดตรวจ

๔.๒ จัดทำแบบตอบรับการเข้าร่วมประชุม

๔.๓ จัดเตรียมเอกสารประกอบการประชุม ได้แก่

(๑) แผนการปฏิบัติงานตรวจสอบ

(๒) แบบรายชื่อผู้เข้าร่วมการเปิดตรวจ

๔.๔ จดบันทึกการประชุม

๔.๕ จัดทำรายงานการประชุม

๔.๖ นำส่งรายงานการประชุมแก่หน่วยรับตรวจ พร้อมแบบตอบรับรายงานการประชุม

๕. ปฏิบัติงานตรวจสอบ เป็นการลงมือปฏิบัติงานตรวจสอบ โดยการสอบทานข้อมูล ความครบถ้วน ถูกต้องของข้อมูลรวมถึงการดำเนินการ ดังนี้

๕.๑ สอบทานการดำเนินงานจากเอกสารหลักฐาน คำสั่งแต่งตั้ง คำสั่งมอบหมายงานต่าง ๆ

๕.๒ สอบทานผลการดำเนินงานว่าเป็นไปตามสัญญาและขอบเขตของงาน (TOR) หรือไม่

๕.๓ สอบทานจากแผนการบริหารความมั่นคงปลอดภัยสำหรับการดำเนินงานด้านสารสนเทศ

๕.๔ สอบทานจากผลการตรวจสอบระบบควบคุมภายในประจำปีงบประมาณ

๕.๕ สอบทานจากหลักเกณฑ์ วิธีการ คู่มือ นโยบายและแนวปฏิบัติในการใช้งานระบบสารสนเทศ

๕.๖ สอบทานการดำเนินงานจากเอกสารหลักฐานต่าง ๆ ที่เกี่ยวข้อง

๕.๗ การสัมภาษณ์ผู้ปฏิบัติงาน

๕.๘ การสังเกตการณ์

๕.๙ การจดบันทึกข้อมูล

๕.๑๐ จัดทำกระดาษทำการ

๖. จัดทำรายงานสรุปข้อตรวจพบ เป็นการสรุปประเด็นข้อเท็จจริงที่พบทั้งด้านดีและปัญหา ข้อบกพร่องที่คิดว่ามีค่าควรแก่การตรวจสอบและรายงานให้ผู้เกี่ยวข้องทราบ โดยใช้ข้อมูลที่ได้จากการรวบรวมข้อมูล ข้อเท็จจริง และหลักฐานต่าง ๆ ที่ได้ระหว่างการตรวจสอบ

๗. ประชุมปิดตรวจ มีกระบวนการดังนี้

๗.๑ จัดทำบันทึกหนังสือเชิญประชุมปิดตรวจ

๗.๒ จัดทำแบบตอบรับการเข้าร่วมประชุม

๗.๓ จัดเตรียมเอกสารประกอบการประชุม ได้แก่

(๑) รายงานสรุปข้อตรวจพบ (Audit Finding)

(๒) แบบรายชื่อผู้เข้าร่วมการปิดตรวจ

(๓) แบบสอบถามความพึงพอใจหน่วยรับตรวจที่มีต่อกลุ่มตรวจสอบภายใน

๘. จัดทำรายงานสรุปผลการปฏิบัติงานตรวจสอบ

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

๑๐. รายงานผลการตรวจสอบแก่หน่วยรับตรวจ เมื่อผู้บริหารได้มีการรับทราบและสั่งการเรียบร้อยแล้ว จากนั้นรายงานผลการตรวจสอบให้หน่วยรับตรวจทราบและแก้ไข ปรับปรุง ตามข้อเสนอแนะของกลุ่มตรวจสอบภายใน

๑๑. การติดตามผลการตรวจสอบ เป็นหน้าที่ของผู้ตรวจสอบภายในที่จะต้องดำเนินการ เพื่อให้มั่นใจว่าข้อเสนอแนะ/แนวทางแก้ไขในการปฏิบัติงานนั้น หน่วยรับตรวจสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพประสิทธิผลหรือไม่ หรือหัวหน้าส่วนราชการพิจารณาจะยอมรับความเสี่ยงจากการไม่ปฏิบัติตามข้อเสนอแนะนั้น ๆ กำหนดให้ดำเนินการภายใน ๖ เดือน หลังการตรวจสอบแล้วเสร็จ (หรือโครงการแล้วเสร็จ)

**แนวทางในการตรวจสอบ**

ผู้ตรวจสอบภายในอาศัยข้อมูลจากเอกสาร/หลักฐานที่ได้รับจากหน่วยรับตรวจ ข้อมูลความเสี่ยงที่เป็นปัจจุบัน และประเด็นที่อาจก่อให้เกิดความผิดพลาดมีผลกระทบต่อองค์กร ผู้ตรวจสอบภายในจะทำการสอบทาน วิเคราะห์ข้อมูลที่ได้รับมาตรวจสอบเปรียบเทียบกับหลักเกณฑ์ มาตรฐาน หรือสิ่งที่ควรจะเป็น ซึ่งมีประเด็นที่สำคัญดังต่อไปนี้

๑. หน่วยงานของรัฐระบุจัดทำหรือจัดหาและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด

- หน่วยงานมีการพิจารณาจัดทำหรือจัดหาสารสนเทศที่มีคุณภาพ ที่ใช้ในการจัดเก็บข้อมูลที่สำคัญเพื่อสนับสนุนให้มีการปฏิบัติตามการควบคุมภายใน

๒. หน่วยงานของรัฐมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบที่มีต่อการควบคุมภายในซึ่งมีความจำเป็นในการสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด

- หน่วยงานมีกระบวนการสื่อสารข้อมูลภายในอย่างมีประสิทธิภาพ และมีช่องทางการสื่อสารที่เหมาะสม เพื่อสนับสนุนการควบคุมภายใน
- หน่วยงานมีช่องทางการสื่อสาร เพื่อแจ้งข้อมูล แจ้งปัญหาการใช้งานหรือเบาะแสเกี่ยวกับการฉ้อฉลหรือทุจริตแก่หน่วยงานได้อย่างปลอดภัย

๓. หน่วยงานของรัฐมีการสื่อสารกับบุคคลภายนอกเกี่ยวกับเรื่องที่มีผลกระทบต่อการปฏิบัติตามการควบคุมภายในที่กำหนด

- หน่วยงานมีช่องทางการแจ้งปัญหากับผู้รับจ้างในกรณีที่ระบบงานเกิดเหตุขัดข้อง
- หน่วยงานมีกระบวนการติดตามผลการดำเนินการจ้างบำรุงโครงการฯ ที่เหมาะสม

๔. หน่วยงานมีการกำหนดนโยบาย/แนวทางในการควบคุมการใช้งานระบบ

- มีการกำหนดนโยบายที่ชัดเจน สอดคล้องกับการทำงานขององค์กร
- มีการลงนามอนุมัติ เห็นชอบจากผู้บริหาร
- มีการประกาศใช้งานให้ผู้ที่เกี่ยวข้องทราบ

๕. หน่วยงานมีการปฏิบัติงานที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ

- หน่วยงานต้องมีการวิเคราะห์กระบวนการปฏิบัติที่เสี่ยงต่อการละเมิดกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง

๖. หน่วยงานมีการบริหารจัดการโครงสร้างความมั่นคงปลอดภัยสารสนเทศ

- มีการวางแผนความต้องการใช้ทรัพยากรสารสนเทศที่มีประสิทธิภาพ
- มีการจัดสรร กำหนดบุคลากร กำหนดบทบาทหน้าที่การดูแลบำรุงรักษาและการพัฒนาระบบ

๗. หน่วยงานมีการควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ
- มีตารางแสดงสิทธิ์การเข้าถึงฐานข้อมูล
- มีการกำหนดสิทธิ์ผู้ดูแลระบบ และการเก็บรักษารหัสผ่าน
- มีการเข้ารหัสข้อมูลที่สำคัญ

๘. หน่วยงานมีการควบคุมการเข้าถึงระบบงาน
- มีการพิสูจน์ตัวตน
- การกำหนดสิทธิ์ของผู้ใช้งาน มีการกำหนดระดับสิทธิ์ของการเข้าใช้งานด้านระบบคอมพิวเตอร์, ระบบเครือข่าย ให้เหมาะสมกับผู้ใช้งานและผู้ดูแลระบบให้เหมาะสมตามการกำหนด ระดับชั้นความลับสารสนเทศ
- มีการบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ

๙. หน่วยงานมีการควบคุมการปฏิบัติงานระบบเครือข่าย
- การสำรองข้อมูลของระบบงาน
- การทดสอบกู้คืนข้อมูล
- การตรวจสอบทางกายภาพของอุปกรณ์เครือข่ายหลัก

๑๐. การจัดเตรียมอุปกรณ์ประมวลผลสำรอง
- มีการจัดลำดับความสำคัญของระบบงาน/กระบวนงานความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือการประเมินผลกระทบของกระบวนงานหลัก
- การกำหนดเจ้าหน้าที่รับผิดชอบและผู้มีอำนาจในการตัดสินใจ
- การทบทวนหรือปรับปรุงแผนฉุกเฉิน
- การสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับ

๑๑. หน่วยงานมีการจัดการความมั่นคงปลอดภัยสำหรับการดำเนินงาน
- มีการจัดทำคู่มือ/ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร
- มีการทบทวนปรับปรุงให้ทันสมัยอยู่เสมอ มีการจัดเก็บคู่มือ/ขั้นตอนการปฏิบัติงานไว้ในสถานที่ที่ผู้จำเป็นต้องใช้งานสามารถเข้าถึงได้

๑๒. หน่วยงานมีการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย
- ออกมาตรการการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส
- สร้างระบบจัดเก็บ log ไฟล์ในการเข้าถึงเครือข่าย
- ถ้าไม่มีการใช้งานในระยะเวลาหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเทอร์เน็ต (Session timeout) เพื่อนำสัญญาณไปเข้าสู่ระบบใหม่อีกครั้ง

๑๓. หน่วยงานมีการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
- มีการกำหนดผู้รับผิดชอบในการ แก้ไขปัญหา/แก้ไขเหตุการณ์ที่ไม่มั่นคงปลอดภัย
- มีการสื่อสารประชาสัมพันธ์กระบวนการให้บริการ ผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

๑๔. การป้องกันโปรแกรมไม่ประสงค์ดี
- มีการติดตั้งระบบป้องกันโปรแกรมที่ไม่ประสงค์ดีรวมทั้งตรวจสอบประสิทธิภาพให้สามารถป้องกันได้อย่างมีประสิทธิภาพ

- มีการจัดอบรมเจ้าหน้าที่ให้ทราบถึงพฤติกรรมที่พึงประสงค์ต่อการใช้งานที่ถูกต้อง ปลอดภัย และไม่มีความเสี่ยง
- ต้องมีการตรวจสอบประเมินผลมาตรการที่กำหนดไว้อย่างสม่ำเสมอ เพื่อนำมาสู่การปรับปรุงความมั่นคงปลอดภัย

# บทที่ ๔
# ตัวอย่างรูปแบบเอกสารที่ใช้ในการปฏิบัติงานตรวจสอบ

## ๑. รูปแบบการจัดทำแผนการปฏิบัติงาน

การจัดทำแผนการปฏิบัติงานตรวจสอบควรมีรูปแบบซึ่งมีสาระสำคัญ ดังนี้

**๑) หัวกระดาษ**

**แผนปฏิบัติงานตรวจสอบ**

**ด้าน.....**

**ประจำปีงบประมาณ .....**

**กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ**

.....

**๒) หน่วยรับตรวจ** .....

**๓) เรื่องที่ตรวจสอบ** .....

**๔) ประเด็นการตรวจสอบ** .....

**๕) วัตถุประสงค์การปฏิบัติงาน** .....

**๖) ขอบเขตการปฏิบัติงาน** .....

**๗) ระยะเวลาที่ตรวจสอบ** ระหว่างวันที่ .....

**แนวทางการปฏิบัติงานตรวจสอบ**

| วัตถุประสงค์/ประเด็นการตรวจสอบ | เกณฑ์การตรวจสอบ | วิธีการตรวจสอบ | แหล่งข้อมูล/เอกสาร/หลักฐาน/กระดาษทำการ |
|---|---|---|---|
| | | | |

**ผู้รับผิดชอบการตรวจสอบ** (รายชื่อผู้ที่ปฏิบัติงานตรวจสอบในเรื่องนั้นๆ อาจระบุทุกคน หรือตามที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ตรวจสอบในเรื่องนั้นๆ)

**ผู้ควบคุมการตรวจสอบ** ผู้อำนวยการกลุ่มตรวจสอบภายใน

**ลงลายมือชื่อรับทราบแผนการปฏิบัติงาน/วันที่** (ผู้ปฏิบัติงานตรวจสอบ/ผู้จัดทำ)

**ลงลายมือชื่อรับทราบแผนการปฏิบัติงานและผู้อนุมัติแผน/วันที่** (ผู้อำนวยการกลุ่มตรวจสอบภายใน)

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

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

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

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

**๒. รูปแบบการจัดทำกระดาษทำการ**

การจัดทำกระดาษทำการควรมีรูปแบบซึ่งมีสาระสำคัญ ดังนี้

| IT๑_xx/xx |
|---|

รหัสกระดาษทำการ

**กระดาษทำการ**

**กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ**

**การตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ**

**ตามองค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร**

**ประจำปีงบประมาณ** .....

**หน่วยรับตรวจ** ..... **ระยะเวลา** .....

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

**ประเด็นการตรวจสอบ** การควบคุมภายในด้านสารสนเทศและการสื่อสาร ให้มีความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

| ลำดับ | รายการ | ผลการตรวจสอบ | | เอกสาร/หลักฐานประกอบ | | คำอธิบายเพิ่มเติม |
|---|---|---|---|---|---|---|
| | | มี/ใช่/สมบูรณ์ | ไม่มี/ไม่ใช่/ไม่สมบูรณ์ | มี/ครบถ้วน | ไม่มี/ไม่ครบถ้วน | |
| **๑. หน่วยงานของรัฐระบุจัดทำหรือจัดหาและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด** | | | | | | |
| ๑) | หน่วยงานมีการพิจารณาจัดทำหรือจัดหาสารสนเทศที่มีคุณภาพ ที่ใช้ในการจัดเก็บข้อมูลที่สำคัญเพื่อสนับสนุนให้มีการปฏิบัติตามการควบคุมภายใน | | | | | |
| **๒. หน่วยงานของรัฐมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบที่มีต่อการควบคุมภายในซึ่งมีความจำเป็นในการสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด** | | | | | | |
| ๑) | หน่วยงานมีกระบวนการสื่อสารข้อมูลภายในอย่างมีประสิทธิภาพและมีช่องทางการสื่อสารที่เหมาะสม เพื่อสนับสนุนการควบคุมภายใน | | | | | |
| ๒) | หน่วยงานมีช่องทางการสื่อสารเพื่อแจ้งข้อมูล แจ้งปัญหาการใช้งานหรือเบาะแสเกี่ยวกับ | | | | | |

| ลำดับ | รายการ | ผลการตรวจสอบ | | เอกสาร/หลักฐานประกอบ | | คำอธิบายเพิ่มเติม |
|---|---|---|---|---|---|---|
| | | มี/ใช่/สมบูรณ์ | ไม่มี/ไม่ใช่/ไม่สมบูรณ์ | มี/ครบถ้วน | ไม่มี/ไม่ครบถ้วน | |
| | การฉ้อฉลหรือทุจริตแก่หน่วยงานได้อย่างปลอดภัย | | | | | |
| **๓. หน่วยงานของรัฐมีการสื่อสารกับบุคคลภายนอกเกี่ยวกับเรื่องที่มีผลกระทบต่อการปฏิบัติตามการควบคุมภายในที่กำหนด** | | | | | | |
| ๑) | หน่วยงานมีช่องทางการแจ้งปัญหากับผู้รับจ้างในกรณีที่ระบบงานเกิดเหตุขัดข้อง | | | | | |
| ๒) | หน่วยงานมีกระบวนการติดตามผลการดำเนินการจ้างบำรุงโครงการฯ ที่เหมาะสม | | | | | |
| **๔. หน่วยงานมีการกำหนดนโยบาย/แนวทางในการควบคุมการใช้งานระบบ** | | | | | | |
| ๑) | มีการกำหนดนโยบายที่ชัดเจนสอดคล้องกับการทำงานขององค์กร | | | | | |
| ๒) | มีการลงนามอนุมัติ เห็นชอบจากผู้บริหาร | | | | | |
| ๓) | มีการประกาศใช้งานให้ผู้ที่เกี่ยวข้องทราบ | | | | | |
| **๕. หน่วยงานมีการปฏิบัติงานที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ** | | | | | | |
| ๑) | หน่วยงานต้องมีการวิเคราะห์กระบวนการปฏิบัติที่เสี่ยงต่อการละเมิดกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง | | | | | |
| **๖. หน่วยงานมีการบริหารจัดการโครงสร้างความมั่นคงปลอดภัยสารสนเทศ** | | | | | | |
| ๑) | มีการวางแผนความต้องการใช้ทรัพยากรสารสนเทศที่มีประสิทธิภาพ | | | | | |
| ๒) | มีการจัดสรร กำหนดบุคลากรกำหนดบทบาทหน้าที่การดูแลบำรุงรักษาและการพัฒนาระบบ | | | | | |
| **๗. หน่วยงานมีการควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ** | | | | | | |
| ๑) | มีตารางแสดงสิทธิ์การเข้าถึงฐานข้อมูล | | | | | |
| ๒) | มีการกำหนดสิทธิ์ผู้ดูแลระบบและการเก็บรักษารหัสผ่าน | | | | | |

| ลำดับ | รายการ | ผลการตรวจสอบ | | เอกสาร/หลักฐานประกอบ | | คำอธิบายเพิ่มเติม |
|---|---|---|---|---|---|---|
| | | มี/ใช่/สมบูรณ์ | ไม่มี/ไม่ใช่/ไม่สมบูรณ์ | มี/ครบถ้วน | ไม่มี/ไม่ครบถ้วน | |
| ๓) | มีการเข้ารหัสข้อมูลที่สำคัญ | | | | | |
| **๘. หน่วยงานมีการควบคุมการเข้าถึงระบบงาน** | | | | | | |
| ๑) | มีการพิสูจน์ตัวตน | | | | | |
| ๒) | การกำหนดสิทธิ์ของผู้ใช้งาน มีการกำหนดระดับสิทธิ์ของการเข้าใช้งานด้านระบบคอมพิวเตอร์, ระบบเครือข่าย ให้เหมาะสมกับผู้ใช้งานและผู้ดูแลระบบให้เหมาะสมตามการกำหนด ระดับชั้นความลับสารสนเทศ | | | | | |
| ๓) | มีการบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ | | | | | |
| **๙. หน่วยงานมีการควบคุมการปฏิบัติงานระบบเครือข่าย** | | | | | | |
| ๑) | การสำรองข้อมูลของระบบงาน | | | | | |
| ๒) | การทดสอบกู้คืนข้อมูล | | | | | |
| ๓) | การตรวจสอบทางกายภาพของอุปกรณ์เครือข่ายหลัก | | | | | |
| **๑๐. การจัดเตรียมอุปกรณ์ประมวลผลสำรอง** | | | | | | |
| ๑) | มีการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือการประเมินผลกระทบของกระบวนงานหลัก | | | | | |
| ๒) | การกำหนดเจ้าหน้าที่รับผิดชอบและผู้มีอำนาจในการตัดสินใจ | | | | | |
| ๓) | การทบทวนหรือปรับปรุงแผนฉุกเฉิน | | | | | |
| ๔) | การสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับ | | | | | |
| **๑๑. หน่วยงานมีการจัดการความมั่นคงปลอดภัยสำหรับการดำเนินงาน** | | | | | | |

| ลำดับ | รายการ | ผลการตรวจสอบ | | เอกสาร/หลักฐานประกอบ | | คำอธิบายเพิ่มเติม |
|---|---|---|---|---|---|---|
| | | มี/ใช่/สมบูรณ์ | ไม่มี/ไม่ใช่/ไม่สมบูรณ์ | มี/ครบถ้วน | ไม่มี/ไม่ครบถ้วน | |
| ๑) | มีการจัดทำคู่มือ/ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร | | | | | |
| ๒) | มีการทบทวนปรับปรุงให้ทันสมัยอยู่เสมอ มีการจัดเก็บคู่มือ/ขั้นตอนการปฏิบัติงานไว้ในสถานที่ที่ผู้จำเป็นต้องใช้งานสามารถเข้าถึงได้ | | | | | |
| **๑๒. หน่วยงานมีการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย** | | | | | | |
| ๑) | ออกมาตรการการเข้าถึงระบบเครือข่ายโดยใช้ ไอพีแอดเดรส | | | | | |
| ๒) | สร้างระบบจัดเก็บ log ไฟล์ในการเข้าถึงเครือข่าย | | | | | |
| ๓) | ถ้าไม่มีการใช้งานในระยะเวลาหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเทอร์เน็ต (Session timeout) เพื่อนำสัญญาณไปเข้าสู่ระบบใหม่อีกครั้ง | | | | | |
| **๑๓. หน่วยงานมีการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ** | | | | | | |
| ๑) | มีการกำหนดผู้รับผิดชอบในการ แก้ไขปัญหา/แก้ไขเหตุการณ์ที่ไม่มั่นคงปลอดภัย | | | | | |
| ๒) | มีการสื่อสารประชาสัมพันธ์กระบวนการให้บริการ ผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้ | | | | | |
| **๑๔. การป้องกันโปรแกรมไม่ประสงค์ดี** | | | | | | |
| ๑) | มีการติดตั้งระบบป้องกันโปรแกรมที่ไม่ประสงค์ดีรวมทั้งตรวจสอบประสิทธิภาพให้สามารถป้องกันได้อย่างมีประสิทธิภาพ | | | | | |
| ๒) | มีการจัดอบรมเจ้าหน้าที่ให้ทราบถึงพฤติกรรมที่พึง | | | | | |

| ลำดับ | รายการ | ผลการตรวจสอบ | | เอกสาร/หลักฐานประกอบ | | คำอธิบายเพิ่มเติม |
|---|---|---|---|---|---|---|
| | | มี/ใช่/สมบูรณ์ | ไม่มี/ไม่ใช่/ไม่สมบูรณ์ | มี/ครบถ้วน | ไม่มี/ไม่ครบถ้วน | |
| | ประสงค์ต่อการใช้งานที่ถูกต้อง ปลอดภัย และไม่มีความเสี่ยง | | | | | |
| ๓) | ต้องมีการตรวจสอบประเมินผลมาตรการที่กำหนดไว้อย่างสม่ำเสมอ เพื่อนำมาสู่การปรับปรุงความมั่นคงปลอดภัย | | | | | |

**<u>สรุปผลการตรวจสอบ</u>**

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

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

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

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

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

**๓. รูปแบบการจัดทำบันทึกสรุปข้อตรวจพบ**

การจัดทำบันทึกสรุปข้อตรวจพบควรมีรูปแบบซึ่งมีสาระสำคัญ ดังนี้

**บันทึกสรุปข้อตรวจพบ Audit Finding**

**กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ**

**เรื่อง การตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ**

**ตามองค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร**

**ประจำปีงบประมาณ** .....

.....

**หน่วยรับตรวจ** .....

**ประเด็นการตรวจสอบ** .....

.....

**วัตถุประสงค์การตรวจสอบ** .....

..... .....

**หลักเกณฑ์ (Criteria)** .....

..... .....

**ข้อเท็จจริง (Condition)** .....

.....

**ผลกระทบ (Effect)** .....

**สาเหตุ (Cause)** .....

**ข้อเสนอแนะ** .....

**(Recommendation)** .....

**ข้อตอบกลับ**

.....

.....

.....

ลงนาม.....

ตำแหน่ง.....

**๔. รูปแบบการจัดทำรายงานผลการปฏิบัติงาน**

การจัดทำรายงานผลการปฏิบัติงานควรมีรูปแบบซึ่งมีสาระสำคัญ ดังนี้

**รายงานผลการปฏิบัติงาน**

**กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ**

**เรื่อง การตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ**

**ตามองค์ประกอบของมาตรฐานการควบคุมภายในด้านสารสนเทศและการสื่อสาร**

**ประจำปีงบประมาณ** .....

**.....**

**หน่วยรับตรวจ** .....

**ประเด็นการตรวจสอบ** .....

.....

**วัตถุประสงค์การตรวจสอบ** .....

.....

**ขอบเขตการตรวจสอบ** .....

.....

**ระยะเวลาที่ตรวจสอบ** .....

**วิธีการตรวจสอบ** .....

.....

**สรุปผลการตรวจสอบ** .....

.....

**ผลกระทบ (Effect)** .....

.....

**สาเหตุ (Cause)** .....

.....

**ข้อเสนอแนะ** .....

**(Recommendation)** .....

**ลงลายมือชื่อผู้ปฏิบัติงานตรวจสอบ**

**ลงลายมือชื่อผู้ตรวจสอบ/สอบทาน**

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

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

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

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

# เอกสารอ้างอิง

หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ ๒) พ.ศ. ๒๕๔๘

ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

สดช.

กลุ่มตรวจสอบภายใน
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม