คู่มือปฏิบัติงาน
การตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ
(Information Technology Auditing)

ธิดารัตน์ อุปชัย
นักตรวจสอบภายในปฏิบัติการ

หน่วยตรวจสอบภายใน มหาวิทยาลัยราชภัฏสกลนคร

คำนำ

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ได้กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยให้ผู้ตรวจสอบภายในภาครัฐ (Internal Audit) ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของสารสนเทศของหน่วยงาน ประกอบกับมาตรฐานการตรวจสอบภายใน และแนวทางการประกันคุณภาพงานตรวจสอบภายในภาครัฐ กำหนดมาตรฐานด้านคุณสมบัติ รหัส ๑๒๑๐.A๓ ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ ได้แก่ การควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแล โดยจัดให้มีระบบควบคุมในส่วนโครงสร้างพื้นฐานด้านสารสนเทศ เช่น ระบบงานข้อมูล ระบบเครือข่าย ซึ่งประกอบด้วย การควบคุมทั่วไปและแบบเฉพาะทาง รวมถึงเทคนิควิธีการตรวจสอบด้านเทคโนโลยีสารสนเทศ และประเด็นที่ใช้พิจารณา : การวางแผนการตรวจสอบ การเสนอ และการอนุมัติแผนการตรวจสอบ กำหนดให้การวางแผนการตรวจสอบครอบคลุมประเภทงานให้ความเชื่อมั่นควรครอบคลุมการตรวจสอบด้านสารสนเทศ

ดังนั้น ผู้จัดทำจึงเล็งเห็นความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศดังกล่าว จึงได้จัดทำคู่มือปฏิบัติงานดังกล่าวเพื่อใช้เป็นแนวทางปฏิบัติให้กับผู้ตรวจสอบภายใน บุคลากร หรือเจ้าหน้าที่ที่มีความสนใจในการเรียนรู้เพิ่มเติมเกี่ยวกับการตรวจสอบด้านสารสนเทศ ทั้งนี้ ผู้จัดทำได้ดำเนินการจัดทำคู่มือดังกล่าวเสร็จสิ้นแล้ว และหวังเป็นอย่างยิ่งว่าคู่มือการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศนี้จะเป็นประโยชน์ต่อหน่วยงานหรือองค์กรของท่านอย่างแท้จริง

ธิดารัตน์ อุปชัย
นักตรวจสอบภายในปฏิบัติการ

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

บทที่ ๑
บทนำ

๑. ความเป็นมาและความสำคัญ

ด้วยพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ มีผลบังคับใช้เมื่อวันที่ ๒๐ เมษายน ๒๕๖๑ โดยในมาตรา ๗๙ ระบุ บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายใน และการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

กระทรวงการคลังจึงได้กำหนดหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ ให้หน่วยงานของรัฐถือปฏิบัติ หากหน่วยงานของรัฐมีเจตนาปล่อยปละละเลยในการปฏิบัติตามมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐที่กระทรวงการคลังกำหนดโดยไม่มีเหตุอันควร ให้กระทรวงการคลังพิจารณาความเหมาะสมในการเสนอความเห็นเกี่ยวกับพฤติการณ์ของหน่วยงานของรัฐดังกล่าวให้ผู้ที่เกี่ยวข้องดำเนินการตามอำนาจและหน้าที่ต่อไป และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ ได้กำหนดมาตรฐานการตรวจสอบภายใน ประกอบด้วย ๒ ส่วน คือ มาตรฐานด้านคุณสมบัติ (Attribute Standards) และมาตรฐานการปฏิบัติงาน (Performance Standards) รายละเอียด ดังนี้

๑. มาตรฐานด้านคุณสมบัติ (Attribute Standards) เป็นมาตรฐานที่กล่าวถึงลักษณะของหน่วยงานและบุคลากรที่ปฏิบัติงานด้านการตรวจสอบภายใน โดยเริ่มตั้งแต่รหัสมาตรฐานที่ ๑๐๐๐ เป็นต้นไป ประกอบด้วย

รหัส ๑๐๐๐ วัตถุประสงค์อำนาจหน้าที่และความรับผิดชอบ
รหัส ๑๑๐๐ ความเป็นอิสระและ ความเที่ยงธรรม
รหัส ๑๒๐๐ ความเชี่ยวชาญ และความระมัดระวัง รอบคอบเยี่ยง ผู้ประกอบวิชาชีพ
รหัส ๑๓๐๐ การประกัน และการปรับปรุง คุณภาพงาน

๒. มาตรฐานด้านการปฏิบัติงาน (Performance Standards) เป็นมาตรฐานที่กล่าวถึงลักษณะของงานและกระบวนการปฏิบัติงานด้านการตรวจสอบภายใน โดยเริ่มตั้งแต่รหัสมาตรฐานที่ ๒๐๐๐ เป็นต้นไป ประกอบด้วย

รหัส ๒๐๐๐ การบริหารงานตรวจสอบภายใน
รหัส ๒๑๐๐ ลักษณะของงานตรวจสอบภายใน
รหัส ๒๒๐๐ การวางแผนการปฏิบัติงาน
รหัส ๒๓๐๐ การปฏิบัติงาน
รหัส ๒๔๐๐ การรายงานผลการตรวจสอบ
รหัส ๒๕๐๐ การติดตามผล
รหัส ๒๖๐๐ การยอมรับสภาพความเสี่ยงของฝ่ายบริหาร

ในการปฏิบัติงานของหน่วยงานตามมาตรฐานการตรวจสอบภายในนั้น มีความเกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศร่วมด้วยเสมอ กล่าวคือ ระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐนั้นจะต้องมีส่วนสนับสนุนวัตถุประสงค์และกลยุทธ์ของหน่วยงานของรัฐ และหน่วยงานของรัฐมีการควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแล โดยหน่วยงานของรัฐจำเป็นต้องจัดให้มีระบบการควบคุมในส่วนโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เช่น ระบบงานข้อมูล ระบบเครือข่าย และบุคลากรซึ่ง

ประกอบด้วยการควบคุมแบบทั่วไป (General Controls) และแบบเฉพาะทาง (Technical Controls) ทั้งนี้การควบคุมระบบเทคโนโลยีสารสนเทศนั้น มีความสอดคล้องกับมาตรฐานด้านคุณสมบัติและมาตรฐานด้านการปฏิบัติงานของผู้ตรวจสอบภายใน เช่น

มาตรฐานด้านคุณสมบัติ

รหัส ๑๒๐๐ ความเชี่ยวชาญและความระมัดระวัง รอบคอบเยี่ยง ผู้ประกอบวิชาชีพ

๑๒๑๐ : ความเชี่ยวชาญ

ผู้ตรวจสอบภายในต้องมีความรู้ทักษะและความสามารถอื่น ๆ ที่จำเป็นต่อการปฏิบัติงานที่รับผิดชอบและต้องสะสมความรู้ทักษะ และความสามารถอื่น ๆ จากการปฏิบัติงานตรวจสอบ ทั้งนี้การปฏิบัติงานตรวจสอบต้องดำเนินการ โดยผู้ที่มีความรู้ทักษะ และความสามารถอื่น ๆ ที่จำเป็นต่อการปฏิบัติงาน ตามที่ได้รับมอบหมาย

<u>การตีความ</u> : ความเชี่ยวชาญ หมายถึง ความรู้ทักษะ และความสามารถอื่น ๆ ที่จำเป็นต่อการปฏิบัติงานตามที่ได้รับมอบหมายของผู้ตรวจสอบภายในได้อย่างมีประสิทธิผล ซึ่งความเชี่ยวชาญจะครอบคลุมถึงกิจกรรมต่าง ๆ ในปัจจุบัน แนวโน้ม และประเด็น ที่เกิดขึ้นใหม่ๆ เพื่อสามารถให้คำแนะนำและข้อเสนอแนะที่ตรงประเด็นได้ ดังนั้น ผู้ตรวจสอบภายในควรเข้ารับการฝึกอบรมและแสวงหาความรู้จากองค์กร ในทางวิชาชีพ เพื่อให้ได้รับวุฒิบัตรที่เกี่ยวข้องกับการปฏิบัติงานตรวจสอบภายใน ที่แสดงให้เห็นถึงความเชี่ยวชาญ

๑๒๑๐.A๓ : ผู้ตรวจสอบภายในต้องเป็นผู้ที่มีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ รวมทั้งเทคนิค วิธีการ ตรวจสอบด้านเทคโนโลยีสารสนเทศเพื่อให้การปฏิบัติงานตรวจสอบ ภายในสามารถดำเนินไปได้อย่างมีประสิทธิผล แต่อย่างไรก็ตามผู้ตรวจสอบภายในทั้งหมดไม่จำเป็นต้องมีความเชี่ยวชาญเทียบเท่ากับ ผู้ตรวจสอบภายในที่มีหน้าที่รับผิดชอบในการปฏิบัติงานตรวจสอบ ด้านเทคโนโลยีสารสนเทศโดยตรง

๑๒๒๐ : ความระมัดระวังรอบคอบเยี่ยงผู้ประกอบวิชาชีพ

ผู้ตรวจสอบภายในต้องปฏิบัติงานด้วยความระมัดระวังรอบคอบเยี่ยงผู้ประกอบวิชาชีพและมีทักษะการปฏิบัติงานอย่างสมเหตุสมผลในอันที่จะทำให้การปฏิบัติงาน เป็นที่ยอมรับและน่าเชื่อถือ ทั้งนี้การปฏิบัติงานด้วยความระมัดระวังรอบคอบ เยี่ยงผู้ประกอบวิชาชีพไม่ได้หมายความว่าจะไม่มีข้อผิดพลาดใด ๆ เกิดขึ้น

๑๒๒๐.A๒ : ผู้ตรวจสอบภายในต้องพิจารณาใช้เทคโนโลยีสารสนเทศและเทคนิคการวิเคราะห์ข้อมูลอื่น ๆ มาเป็นเครื่องมือช่วยสนับสนุนการปฏิบัติงาน ตรวจสอบภายใน เพื่อให้การปฏิบัติงานเป็นไปด้วยความระมัดระวัง รอบคอบเยี่ยงผู้ประกอบวิชาชีพ

มาตรฐานด้านการปฏิบัติงาน

รหัส ๒๑๒๐ : การบริหารความเสี่ยง

การปฏิบัติงานตรวจสอบภายในต้องสามารถประเมินความมีประสิทธิผล และสนับสนุนให้เกิดการปรับปรุงกระบวนการบริหารความเสี่ยง

<u>การตีความ</u> : การพิจารณาว่ากระบวนการบริหารความเสี่ยงมีประสิทธิผลหรือไม่ เป็นดุลยพินิจ ของผู้ตรวจสอบภายในจากผลการประเมินว่า

- วัตถุประสงค์ของหน่วยงานมีส่วนสนับสนุนและเป็นไปในทิศทางเดียวกับพันธกิจ
- การระบุและประเมินความเสี่ยงที่มีนัยสำคัญ
- การเลือกใช้แนวทางในการตอบสนองความเสี่ยงที่เหมาะสม โดยเป็นไปในทิศทางเดียวกับระดับความเสี่ยงที่หน่วยงานยอมรับได้และการสื่อสารข้อมูลสารสนเทศที่เกี่ยวข้องกับความเสี่ยง

ที่ถูกตรวจพบทั่วทั้งหน่วยงานอย่างทันเวลา เพื่อช่วยให้เจ้าหน้าที่ผู้ปฏิบัติงานฝ่ายบริหารและคณะกรรมการตรวจสอบหรือหัวหน้าหน่วยงานของรัฐ นำมาปรับปรุงการดำเนินงานภายในหน่วยงาน

๒๑๒๐.A๑ : การปฏิบัติงานตรวจสอบภายในต้องประเมินความเสี่ยงที่เกี่ยวกับการกำกับดูแล การดำเนินงานและระบบข้อมูลสารสนเทศในเรื่องต่าง ๆ ดังนี้

- การบรรลุวัตถุประสงค์เชิงยุทธศาสตร์ของหน่วยงานของรัฐ
- ความถูกต้องครบถ้วน และความน่าเชื่อถือของข้อมูลสารสนเทศ ด้านการเงินและการดำเนินงาน
- ความมีประสิทธิผลและประสิทธิภาพของการดำเนินงาน
- การดูแลทรัพย์สิน และการปฏิบัติตามกฎ ระเบียบ หลักเกณฑ์ข้อบังคับ นโยบาย วิธีการ ปฏิบัติงาน และข้อสัญญาต่าง ๆ

รหัส ๒๑๓๐ : การควบคุม

การปฏิบัติงานตรวจสอบภายในต้องมีส่วนสนับสนุนและส่งเสริมให้มีการควบคุมในเรื่องต่าง ๆ ที่เหมาะสมและเพียงพอ โดยการประเมินประสิทธิผลและประสิทธิภาพของการควบคุม รวมทั้งสนับสนุนให้มีการปรับปรุงอย่างต่อเนื่อง

๒๑๓๐.A๑ : การปฏิบัติงานตรวจสอบภายในต้องประเมินถึงความเพียงพอและประสิทธิผลของการควบคุม เพื่อให้การควบคุมที่มีอยู่สามารถ ตอบสนองความเสี่ยงภายใต้การกำกับดูแล การดำเนินงานและระบบข้อมูลสารสนเทศในเรื่องต่าง ๆ ดังนี้

- การบรรลุวัตถุประสงค์เชิงยุทธศาสตร์ของหน่วยงานของรัฐ
- ความถูกต้อง ครบถ้วน และความน่าเชื่อถือของข้อมูลสารสนเทศ ด้านการเงินและการดำเนินงาน
- ความมีประสิทธิผลและประสิทธิภาพของการดำเนินงาน
- การดูแลและรักษาทรัพย์สิน และการปฏิบัติตามกฎ ระเบียบ หลักเกณฑ์ข้อบังคับ นโยบาย วิธีการ ปฏิบัติงาน และข้อสัญญาต่าง ๆ

การติดตามและประเมินผลการบริหารความเสี่ยงจากฝ่ายบริหารอย่างต่อเนื่อง โดยสามารถดำเนินการประเมินผลแยกต่างหากหรือรวมทั้งสองแบบ

ดังนั้น จะเห็นได้ว่าการจัดทำคู่มือการปฏิบัติงาน เรื่อง ตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศดังกล่าวสะท้อนให้เห็นถึงความสำคัญในการใช้ข้อมูลสารสนเทศที่มีความหลากหลาย ดังนั้นผู้จัดทำจึงเล็งเห็นถึงความสำคัญและจำเป็นต้องควบคุมข้อมูลด้านสารสนเทศดังกล่าว และในการจัดทำคู่มือการปฏิบัติงานในครั้งนี้เป็นการจัดทำเพื่อให้บุคคลภายนอก หรือเจ้าหน้าที่ปฏิบัติงานในด้านต่าง ๆ ได้ทราบถึงแนวทางวิธีการปฏิบัติงานที่มีความเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างชัดเจน

๒. วัตถุประสงค์

๒.๑ เพื่อให้การปฏิบัติงานเป็นมาตรฐานเดียวกัน
๒.๒ เพื่อให้ผู้ปฏิบัติงานมีความเข้าใจในการปฏิบัติ
๒.๓ เพื่อใช้เป็นเอกสารอ้างอิงในการปฏิบัติงาน

๓. ประโยชน์ที่คาดว่าจะได้รับ

๓.๑ หน่วยงานมีการปฏิบัติงานที่เป็นมาตรฐานเดียวกัน
๓.๒ ผู้ปฏิบัติงานมีความเข้าใจในการปฏิบัติ
๓.๓ หน่วยงานสามารถนำคู่มือปฏิบัติงานไปเป็นเอกสารอ้างอิงได้

๔. ขอบเขตของคู่มือ

การจัดทำคู่มือการปฏิบัติงาน เรื่อง การตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม มีเนื้อหาครอบคลุมถึงขั้นตอนรายละเอียดต่าง ๆ ตั้งแต่การวางแผนการตรวจสอบ การดำเนินการตรวจสอบ การจัดทำรายงานผลการตรวจสอบ การนำเสนอรายงานผลของผู้ตรวจสอบภายใน รวมถึงการติดตามผลการตรวจสอบของหน่วยรับตรวจ ซึ่งเป็นไปตามพันธกิจและเป้าประสงค์ของหน่วยงาน

ทั้งนี้ คู่มือการปฏิบัติงานฉบับนี้จัดทำขึ้นเพื่อใช้เป็นแนวทางในการตรวจสอบให้กับผู้ตรวจสอบภายใน ได้ดำเนินการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ

๕. คำจำกัดความเบื้องต้น

หน่วยตรวจสอบภายใน	หมายถึง	หน่วยงานที่ได้รับมอบหมายให้ดำเนินการตรวจสอบภายในของส่วนราชการ
หน่วยรับตรวจ	หมายถึง	หน่วยงานภายในส่วนราชการของมหาวิทยาลัยราชภัฏสกลนคร
ผู้ตรวจสอบภายใน	หมายถึง	นักตรวจสอบภายใน หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ตรวจสอบภายใน
กระดาษทำการ	หมายถึง	กระดาษทำงานที่ผู้ตรวจสอบภายในใช้บันทึกข้อมูลและหลักฐานที่ตรวจพบ ตั้งแต่เริ่มต้นจนสิ้นสุดการปฏิบัติงาน
การรายงานผล	หมายถึง	การรายงานผลการตรวจสอบตามข้อเท็จจริงที่ตรวจพบ และการรายงานผลการตรวจสอบอยู่ในองค์ประกอบตามกระดาษทำการ

บทที่ ๒
โครงสร้างและหน้าที่ความรับผิดชอบ

๑. โครงสร้างมหาวิทยาลัยราชภัฏสกลนคร

ด้วยพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. ๒๕๔๗ บัญญัติให้มีการจัดตั้ง การรวม และการยุบเลิกสำนักงานวิทยาเขต บัณฑิตวิทยาลัย คณะ สถาบัน สำนัก วิทยาลัย ศูนย์ ส่วนราชการหรือหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าคณะให้ทำเป็นกฎกระทรวง และอาศัยอำนาจตามความในมาตรา ๖ และมาตรา ๑๑ วรรคหนึ่ง แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. ๒๕๔๗ รัฐมนตรีว่าการกระทรวงศึกษาธิการจึงให้จัดตั้งส่วนราชการในมหาวิทยาลัยราชภัฏสกลนคร ดังนี้

(๑) สำนักงานอธิการบดี

(๒) คณะครุศาสตร์

(๓) คณะเทคโนโลยีการเกษตร

(๔) คณะเทคโนโลยีอุตสาหกรรม

(๕) คณะมนุษยศาสตร์และสังคมศาสตร์

(๖) คณะวิทยาการจัดการ

(๗) คณะวิทยาศาสตร์และเทคโนโลยี

(๘) สถาบันภาษา ศิลปะและวัฒนธรรม

(๙) สถาบันวิจัยและพัฒนา

(๑๐) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๑๑) สำนักส่งเสริมวิชาการและงานทะเบียน

และอาศัยอำนาจตามความในมาตรา ๖ มาตรา ๑๐ วรรคสาม วรรคสี่ วรรคห้า และมาตรา ๑๑ วรรคสอง แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. ๒๕๔๗ รัฐมนตรีว่าการกระทรวงศึกษาธิการ ออกประกาศไว้ ดังนี้

ข้อ ๑ ให้แบ่งส่วนราชการในสำนักงานอธิการบดี ดังนี้

(๑) กองกลาง

(๒) กองนโยบายและแผน

(๓) กองพัฒนานักศึกษา

ข้อ ๒ ให้แบ่งส่วนราชการในคณะครุศาสตร์ คณะเทคโนโลยีการเกษตร คณะเทคโนโลยีอุตสาหกรรม คณะมนุษยศาสตร์และสังคมศาสตร์ คณะวิทยาการจัดการ และคณะวิทยาศาสตร์และเทคโนโลยี เป็นสำนักงานคณบดี

ข้อ ๓ ให้แบ่งส่วนราชการในสถาบันภาษา ศิลปะและวัฒนธรรม สถาบันวิจัยและพัฒนา สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และสำนักส่งเสริมวิชาการและงานทะเบียน เป็นสำนักงานผู้อำนวยการ และประกาศมหาวิทยาลัยราชภัฏสกลนคร เรื่อง การแบ่งส่วนราชการภายในมหาวิทยาลัยราชภัฏสกลนคร เป็นระดับงานหรือเทียบเท่างาน พ.ศ. ๒๕๒๗ เพื่อให้การแบ่งส่วนราชการภายในของมหาวิทยาลัยราชภัฏสกลนครเป็นไปด้วยความเรียบร้อย ตามที่ประชุมคณะกรรมการบริหารบุคคลในมหาวิทยาลัยราชภัฏสกลนคร (ก.บ.ม.) และคณะกรรมการบริหาร มหาวิทยาลัยราชภัฏสกลนคร (ก.บ.) ในคราวประชุมครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๑๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗ ประกอบกับมติที่ประชุมสภามหาวิทยาลัยราชภัฏสกลนคร ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๒๓ กุมภาพันธ์ พ.ศ. ๒๕๐๗ อาศัยอำนาจตาม

ความในมาตรา ๑๑ มาตรา ๑๘ (๕) มาตรา ๒๒ (๔) และมาตรา ๓ (๑) (๒) แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. ๒๕๔๗ กฎกระทรวงจัดตั้งส่วนราชการในมหาวิทยาลัยราชภัฏสกลนคร กระทรวง ศึกษาธิการ พ.ศ. ๒๕๔๘ ประกาศกระทรวงศึกษาธิการ เรื่อง การแบ่งส่วนราชการในมหาวิทยาลัยราชภัฏสกลนคร พ.ศ. ๒๕๕๙ จึงแบ่งส่วนราชการภายในมหาวิทยาลัยราชภัฏสกลนคร เป็นระดับงานหรือเทียบเท่างาน ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่าประกาศมหาวิทยาลัยราชภัฏสกลนคร เรื่อง การแบ่งส่วนราชการภายในมหาวิทยาลัยราชภัฏสกลนคร เป็นระดับงานหรือเทียบเท่างาน พ.ศ. ๒๕๖๗

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศมหาวิทยาลัยราชภัฏสกลนคร เรื่อง การแบ่งส่วนราชการภายในมหาวิทยาลัยราชภัฏสกลนคร เป็นระดับงานหรือเทียบเท่างาน พ.ศ. ๒๕๖๑

ข้อ ๔ สำนักงานอธิการบดี

๔.๑ กองกลาง ให้แบ่งส่วนราชการเป็นระดับงานหรือเทียบเท่างาน ดังนี้

(๑) งานบริหารทั่วไป

(๒) งานบริหารบุคคลและนิติการ

(๓) งานพัสดุ

(๔) งานอาคารสถานที่และยานพาหนะ

(๕) งานประชาสัมพันธ์และโสตทัศนูปกรณ์

(๖) งานทรัพย์สินและรายได้

(๗) งานประกันคุณภาพการศึกษา

(๘) หน่วยตรวจสอบภายใน

(๙) โรงเรียนวิถีธรรมแห่งมหาวิทยาลัยราชภัฏสกลนคร

๔.๒ กองนโยบายและแผน ให้แบ่งส่วนราชการเป็นระดับงานหรือเทียบเท่างาน ดังนี้

(๑) งานบริหารทั่วไป

(๒) งานสารสนเทศและการเผยแพร่

(๓) งานวิเคราะห์และงบประมาณ

(๔) งานยุทธศาสตร์และติดตามประเมินผล

(๕) งานพันธกิจสากลและจัดอันดับมหาวิทยาลัย

๔.๓ กองพัฒนานักศึกษา ให้แบ่งส่วนราชการเป็นระดับงานหรือเทียบเท่างาน ดังนี้

(๑) งานบริหารทั่วไป

(๒) งานส่งเสริมและพัฒนากิจกรรมนักศึกษา

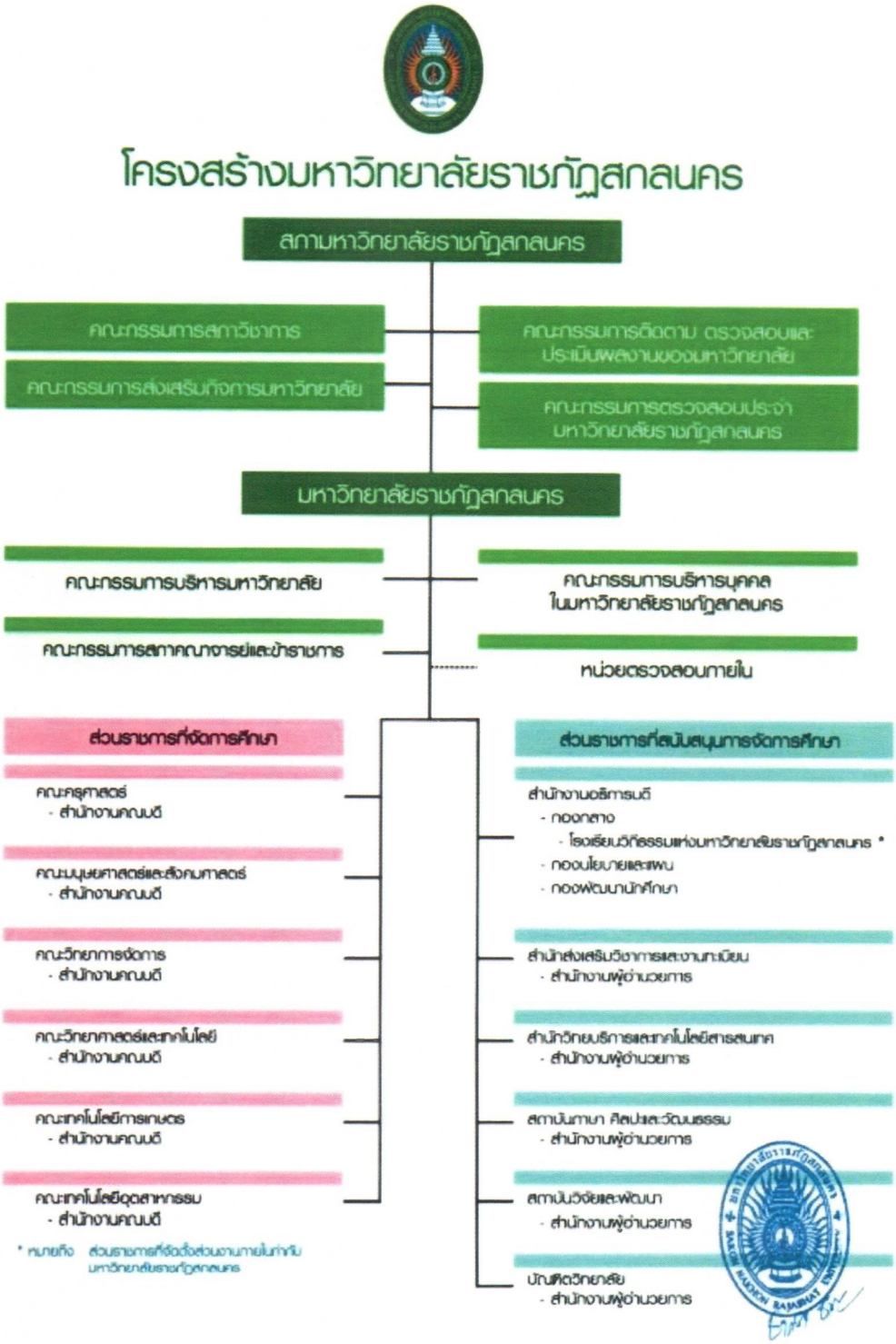
(๓) งานสวัสดิการนักศึกษาและกองทุนให้กู้ยืมเพื่อการศึกษา

(๔) งานแนะแนวและศิษย์เก่าสัมพันธ์

(๕) งานอนามัยและสุขาภิบาล

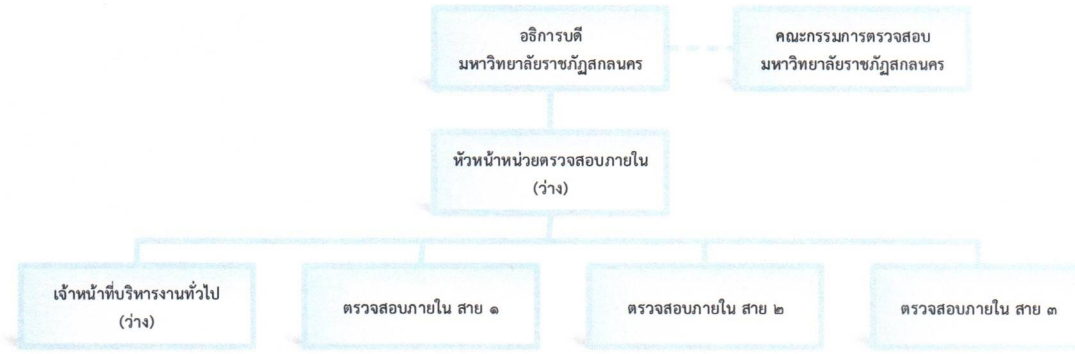
(๖) งานพัฒนาและส่งเสริมการศึกษานักศึกษาพิการ (DSS)

๑.๑ ผังโครงสร้างมหาวิทยาลัยราชภัฏสกลนคร



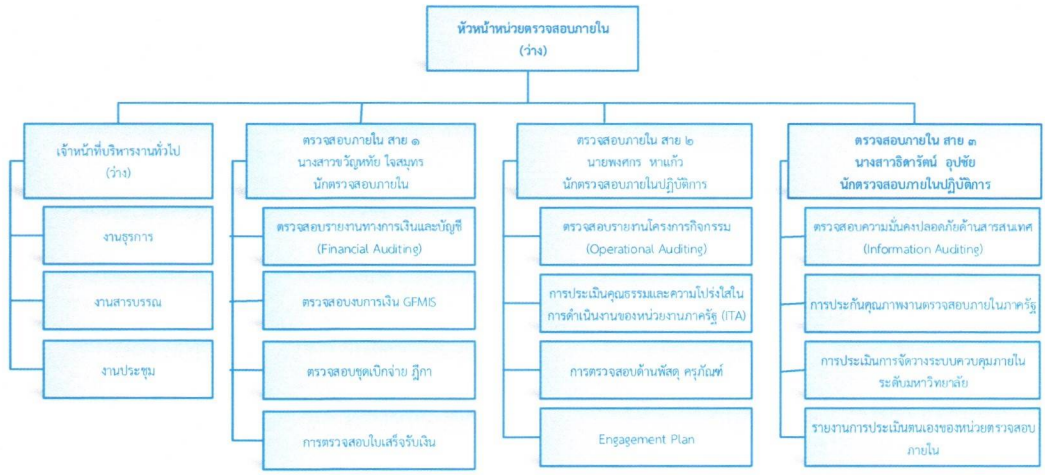
ภาพที่ ๑ แสดงโครงสร้างมหาวิทยาลัยราชภัฏสกลนคร

๑.๒ โครงสร้างการบริหารหน่วยงาน



ภาพที่ ๒ แสดงโครงสร้างการบริหารหน่วยงาน

๑.๓ โครงสร้างหน่วยงาน



ภาพที่ ๓ แสดงโครงสร้างหน่วยงาน

๒. ภาระหน้าที่ของหน่วยงาน

ภาระหน้าที่ของหน่วยงานตรวจสอบภายใน คือ การตรวจสอบการดำเนินงานภายในมหาวิทยาลัย และสนับสนุนการปฏิบัติงานของมหาวิทยาลัย โดยความรับผิดชอบในการตรวจสอบด้านต่าง ๆ จะต้องขึ้นตรงต่อหัวหน้าส่วนราชการโดยตรง โดยภาระหน้าที่หลักในการปฏิบัติงานของหน่วยงาน ประกอบด้วย

๒.๑ งานบริการให้ความเชื่อมั่น (Assurance Services) เป็นการตรวจสอบหลักฐานต่าง ๆ อย่างเที่ยงธรรม เพื่อให้ได้มาซึ่งการประเมินผลอย่างอิสระในกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลของส่วนราชการ เช่น การให้ความเชื่อมั่นทางด้านการเงิน การปฏิบัติงาน การปฏิบัติตามกฎ ระเบียบ ความมั่นคงปลอดภัยของระบบต่าง ๆ

๒.๒ งานบริการให้คำปรึกษา (Consulting Services) เป็นการบริการให้คำปรึกษาแนะนำและบริการอื่น ๆ ที่เกี่ยวข้องแก่ผู้รับบริการ โดยลักษณะและขอบเขตของงานจะเป็นไปตามความต้องการของผู้รับบริการ และมีจุดประสงค์เพื่อเพิ่มพูนคุณค่าและปรับปรุงกระบวนการกำกับดูแล การบริหารความเสี่ยงและการควบคุมของมหาวิทยาลัยให้ดีขึ้น

ทั้งนี้ หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐได้ปฏิบัติตามหลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์การปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ ดังนี้

ข้อ ๑ ในหลักเกณฑ์นี้

"การตรวจสอบภายใน" หมายความว่า กิจกรรมให้ความเชื่อมั่นและการให้คำปรึกษา อย่างเที่ยงธรรมและเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานของหน่วยงานของรัฐ ให้ดีขึ้น และจะช่วยให้หน่วยงานของรัฐบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ด้วยการประเมิน และปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ

"หน่วยงานของรัฐ" หมายความว่า

(๑) ส่วนราชการ

(๒) รัฐวิสาหกิจ

(๓) หน่วยงานของรัฐสภา ศาลยุติธรรม ศาลปกครอง ศาลรัฐธรรมนูญ องค์กรอิสระตามรัฐธรรมนูญ และองค์กรอัยการ

(๔) องค์การมหาชน

(๕) ทุนหมุนเวียนที่มีฐานะเป็นนิติบุคคล

(๖) องค์กรปกครองส่วนท้องถิ่น

(๗) หน่วยงานอื่นของรัฐตามที่กฎหมายกำหนด

"คณะกรรมการ" หมายความว่า คณะกรรมการที่กำกับดูแลหรือผู้กำกับดูแลหน่วยงานของรัฐตามกฎหมายของหน่วยงานของรัฐนั้น

"หัวหน้าหน่วยงานของรัฐ" หมายความว่า ผู้บริหารสูงสุดของหน่วยงานของรัฐ

"ฝ่ายบริหาร" หมายความว่า ผู้ทำหน้าที่บริหารซึ่งดำรงตำแหน่งรองจากหัวหน้าหน่วยงานของรัฐไม่เกินสามลำดับ

"คณะกรรมการตรวจสอบ" หมายความว่า คณะกรรมการตรวจสอบ ตามข้อ ๑๐ – ๑๕ ของหลักเกณฑ์นี้

"หน่วยงานตรวจสอบภายใน" หมายความว่า หน่วยงานที่รับผิดชอบงานตรวจสอบภายในของหน่วยงานของรัฐ

"หัวหน้าหน่วยงานตรวจสอบภายใน" หมายความว่า ผู้ดำรงตำแหน่งสูงสุดในหน่วยงาน ตรวจสอบภายใน

"ผู้ตรวจสอบภายใน" หมายความว่า ผู้ดำรงตำแหน่งผู้ตรวจสอบภายในของหน่วยงานของรัฐ หรือดำรงตำแหน่งอื่นที่ทำหน้าที่เช่นเดียวกับผู้ตรวจสอบภายในของหน่วยงานของรัฐ

"หน่วยรับตรวจ" หมายความว่า หน่วยงานที่รับผิดชอบในการปฏิบัติงานของหน่วยงานของรัฐ

ข้อ ๒ กรมบัญชีกลางเป็นผู้กำหนดคู่มือหรือแนวปฏิบัติเกี่ยวกับการตรวจสอบภายใน ให้หน่วยงานของรัฐ ตามข้อ (๑) และ (๓) –(๗) ถือปฏิบัติและสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ เป็นผู้กำหนดคู่มือหรือแนวปฏิบัติให้หน่วยงานของรัฐ ตามข้อ (๒) ถือปฏิบัติ

ความทั่วไป

ข้อ ๓ ในการปฏิบัติงานตรวจสอบภายใน ให้หน่วยงานของรัฐจัดให้มีหน่วยงานตรวจสอบภายในขึ้นตรงต่อคณะกรรมการตรวจสอบ

ข้อ ๔ การบริหารงานทั่วไปของหน่วยงานตรวจสอบภายใน ให้หน่วยงานตรวจสอบภายในขึ้นตรงต่อหัวหน้าหน่วยงานของรัฐเว้นแต่ การแต่งตั้ง โยกย้าย ถอดถอน เลื่อนขั้น เลื่อนตำแหน่ง และประเมินผล

งานของหัวหน้าหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐที่มีคณะกรรมการตรวจสอบ ให้เป็นไปตามอำนาจ หน้าที่ของคณะกรรมการตรวจสอบ ตามข้อ ๑๓

หัวหน้าหน่วยงานของรัฐต้องจัดสรรบุคลากรและทรัพยากร เพื่อให้การปฏิบัติงานของหน่วยงานตรวจสอบภายในเป็นไปอย่างเหมาะสมและสอดคล้องกับปริมาณงานและความซับซ้อนของภารกิจของหน่วยงานของรัฐ

ข้อ ๕ หัวหน้าหน่วยงานตรวจสอบภายในและผู้ตรวจสอบภายในต้องมีคุณสมบัติดังต่อไปนี้

(๑) มีความรู้ ทักษะ และความสามารถที่จำเป็นต่อการปฏิบัติหน้าที่ที่ได้รับมอบหมาย

(๒) มีความรู้เกี่ยวกับกฎหมาย ระเบียบ ข้อบังคับ มติคณะรัฐมนตรี ประกาศ และคำสั่งที่เกี่ยวข้องกับการดำเนินงานของหน่วยงานของรัฐ

(๓) มีความรู้เกี่ยวกับการปฏิบัติงาน การกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายในของหน่วยงานของรัฐ

ข้อ ๖ หัวหน้าหน่วยงานของรัฐจะแต่งตั้งให้ผู้ตรวจสอบภายในรักษาการตำแหน่งอื่นในขณะเดียวกัน ไม่ได้ หัวหน้าหน่วยงานของรัฐและหรือคณะกรรมการตรวจสอบจะพิจารณาสั่งการให้ผู้ตรวจสอบภายใน ปฏิบัติงานอื่นได้ตามควรแก่กรณี ทั้งนี้ งานดังกล่าวต้องไม่ทำให้ผู้ตรวจสอบภายในขาดความเป็นอิสระ และความเที่ยงธรรมในกิจกรรมที่ตรวจสอบ

ข้อ ๗ ให้ผู้ตรวจสอบภายในดำรงไว้ซึ่งความเป็นอิสระและไม่มีความขัดแย้งทางผลประโยชน์ในกิจกรรมที่ตรวจสอบและปราศจากการแทรกแซงในการปฏิบัติงานและการเสนอความเห็นในการตรวจสอบ ของฝ่ายบริหารหรือบุคคลหนึ่งบุคคลใด รวมทั้งต้องไม่ตรวจสอบงานที่ตนเคยทำหน้าที่บริหารหรือปฏิบัติงาน ภายในระยะเวลาหนึ่งปีก่อนการตรวจสอบ ผู้ตรวจสอบภายในไม่ควรเป็นกรรมการในคณะกรรมการใด ๆ ของหน่วยงานของรัฐหรือหน่วยงาน ในสังกัดอันมีผลกระทบต่อความเป็นอิสระในการปฏิบัติงานและการเสนอความเห็นในการตรวจสอบ

ข้อ ๘ ให้ผู้ตรวจสอบภายในมีสิทธิในการเข้าถึงข้อมูล บุคคล เอกสารหลักฐาน และทรัพย์สินต่าง ๆ เพื่อรับทราบข้อมูลที่จะเป็นประโยชน์ต่อการปฏิบัติงานตรวจสอบภายใน

ข้อ ๙ กรณีหน่วยงานของรัฐไม่สามารถปฏิบัติตามหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐที่กระทรวงการคลังกำหนดได้ ให้ขอทำความตกลงกับกระทรวงการคลัง

คณะกรรมการตรวจสอบ

ข้อ ๑๐ ให้คณะกรรมการเป็นผู้แต่งตั้งคณะกรรมการตรวจสอบ ประกอบด้วย ประธานกรรมการตรวจสอบหนึ่งคน กรรมการตรวจสอบผู้ทรงคุณวุฒิไม่น้อยกว่าสองคนแต่ไม่เกินสี่คน และให้หัวหน้าหน่วยงาน ตรวจสอบภายในเป็นเลขานุการ กรรมการตรวจสอบผู้ทรงคุณวุฒิอย่างน้อยหนึ่งคนต้องเป็นกรรมการในคณะกรรมการหรือ ผู้ที่ได้รับมอบหมายจากคณะกรรมการ

ข้อ ๑๑ คุณสมบัติของคณะกรรมการตรวจสอบ ประกอบด้วย

(๑) เป็นผู้มีความรู้ความเข้าใจและมีประสบการณ์เพียงพอที่จะทำหน้าที่ในฐานะกรรมการตรวจสอบ ตามภารกิจที่ได้รับมอบหมาย โดยอย่างน้อยหนึ่งคนต้องมีความรู้ความเข้าใจและมีประสบการณ์ด้านการเงินการบัญชีหรือด้านการตรวจสอบภายใน

(๒) เป็นผู้มีความเข้าใจในภารกิจของหน่วยงานของรัฐ

(๓) เป็นผู้สามารถอุทิศเวลาในการปฏิบัติหน้าที่ และแสดงความเห็นและรายงานผลการดำเนินงานตามหน้าที่ที่ได้รับมอบหมายด้วยความเป็นอิสระและเที่ยงธรรม

ข้อ ๑๒ คณะกรรมการตรวจสอบต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) ไม่เป็นข้าราชการประจำที่ดำรงตำแหน่งในกระทรวงเจ้าสังกัดของหน่วยงานของรัฐนั้น

(๒) ไม่เป็นกรรมการที่ได้รับมอบหมายให้เป็นผู้กำหนดนโยบายหรือระเบียบปฏิบัติหรือ มีอำนาจในการตัดสินใจด้านการบริหารรวมทั้งไม่เป็นข้าราชการ พนักงาน ลูกจ้าง หรือที่ปรึกษาได้รับเงินเดือนหรือค่าตอบแทนประจำจากหน่วยงานของรัฐ ผู้ที่เกี่ยวข้องกับหน่วยงานของรัฐนั้น ทั้งนี้ ไม่ว่าในขณะดำรงตำแหน่ง หรือภายในระยะเวลาสองปีก่อนวันที่ได้รับการแต่งตั้งเป็นคณะกรรมการตรวจสอบ

(๓) ไม่เป็นผู้มีความขัดแย้งทางผลประโยชน์กับหน่วยงานของรัฐนั้น ทั้งนี้ ไม่ว่าในขณะดำรงตำแหน่ง หรือภายในระยะเวลาหนึ่งปีก่อนวันที่ได้รับแต่งตั้งเป็นคณะกรรมการตรวจสอบ

(๔) ไม่เป็นบุพการี ผู้สืบสันดาน หรือคู่สมรส ของคณะกรรมการ หัวหน้าหน่วยงานของรัฐ หัวหน้าหน่วยงานตรวจสอบภายใน หรือผู้ตรวจสอบภายในของหน่วยงานของรัฐนั้น

ข้อ ๑๓ คณะกรรมการตรวจสอบมีหน้าที่และความรับผิดชอบ ดังนี้

(๑) จัดทำกฎบัตรของคณะกรรมการตรวจสอบให้ สอดคล้องกับขอบเขตความรับผิดชอบ ในการดำเนินงานของหน่วยงานของรัฐ โดยต้องได้รับความเห็นชอบจากคณะกรรมการ และมีการสอบทานความเหมาะสมของกฎบัตรดังกล่าวอย่างน้อยปีละหนึ่งครั้ง

(๒) สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายใน กระบวนการบริหารความเสี่ยงและกระบวนการกำกับดูแลที่ดี

(๓) สอบทานให้หน่วยงานของรัฐมีการรายงานการเงินอย่างถูกต้องและน่าเชื่อถือ

(๔) สอบทานการดำเนินงานของหน่วยงานของรัฐให้ถูกต้องตามกฎหมาย ระเบียบ และข้อบังคับหรือมติคณะรัฐมนตรีที่เกี่ยวข้องกับการดำเนินงาน รวมทั้งข้อกำหนดอื่นของหน่วยงานของรัฐ

(๕) กำกับดูแลระบบงานตรวจสอบภายในของหน่วยงานของรัฐ ให้มีความเป็นอิสระเพื่อพัฒนาการปฏิบัติงานในหน้าที่

(๖) พิจารณารายการที่เกี่ยวโยงกันหรือรายการที่อาจมีความขัดแย้งทางผลประโยชน์ หรือมีโอกาสเกิดการทุจริตที่อาจมีผลกระทบต่อการปฏิบัติงานของหน่วยงานของรัฐ

(๗) ให้ข้อเสนอแนะการพิจารณาแต่งตั้ง โยกย้าย เลื่อนขั้น เลื่อนตำแหน่ง และประเมินผลงาน ของหัวหน้าหน่วยงานตรวจสอบภายในต่อคณะกรรมการ

(๘) ประชุมหารือร่วมกับสำนักงานการตรวจเงินแผ่นดิน หรือผู้สอบบัญชีที่สำนักงาน การตรวจเงินแผ่นดินเห็นชอบเกี่ยวกับผลการตรวจสอบและเรื่องอื่น ๆ และอาจเสนอแนะให้สอบทาน หรือตรวจสอบรายการใดที่เห็นว่าจำเป็น รวมถึงเสนอค่าตอบแทนของผู้สอบบัญชีต่อคณะกรรมการ

(๙) รายงานผลการดำเนินงานของคณะกรรมการตรวจสอบอย่างน้อยปีละหนึ่งครั้งต่อคณะกรรมการ

(๑๐) ประเมินผลการดำเนินงาน ปัญหาและอุปสรรคของหน่วยงานตรวจสอบภายใน รวมทั้งเสนอแนะแนวทางการพัฒนาระบบการตรวจสอบภายในและศักยภาพของผู้ตรวจสอบภายในของหน่วยงานตรวจสอบภายในอย่างน้อยปีละหนึ่งครั้งต่อคณะกรรมการ

(๑๑) ปฏิบัติงานอื่นใดตามที่กฎหมายกำหนดหรือคณะกรรมการมอบหมายหน่วยงานของรัฐสามารถกำหนดหน้าที่และความรับผิดชอบของคณะกรรมการตรวจสอบ เพิ่มเติมจากวรรคหนึ่งได้

ข้อ ๑๔ วาระการดำรงตำแหน่ง วาระการประชุม และอื่น ๆ ของคณะกรรมการตรวจสอบให้เป็นไปตามที่หน่วยงานของรัฐกำหนด

ข้อ ๑๕ ค่าตอบแทนของคณะกรรมการตรวจสอบให้เป็นไปตามอัตราที่กฎหมายกำหนด

ข้อ ๑๖ ให้หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐรับผิดชอบตรวจสอบหน่วยรับตรวจดังนี้

(๑) หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ ตามข้อ (๑) ให้รับผิดชอบตรวจสอบ ดังนี้

(๑.๑) หน่วยงานตรวจสอบภายในระดับกระทรวง รับผิดชอบตรวจสอบการปฏิบัติงานของส่วนราชการในสังกัดกระทรวง ในกรณีที่ตรวจสอบงาน/โครงการของส่วนราชการในสังกัดของกระทรวง นอกเหนือจากงานของสำนักงานปลัดกระทรวง จะต้องเป็นการตรวจสอบและประเมินผลการดำเนินงานตามแผนงาน งาน/โครงการที่มีความสำคัญต่อผลสำเร็จของนโยบายกระทรวง และเป็นงาน/โครงการที่ได้รับนโยบาย ให้ติดตามกำกับดูแลเป็นกรณีพิเศษ โดยให้ประสานแผนการตรวจสอบกับส่วนราชการนั้น ๆ ด้วย

(๑.๒) หน่วยงานตรวจสอบภายในระดับกรม รับผิดชอบตรวจสอบราชการบริหารส่วนกลาง ที่มีสำนักงานตั้งอยู่ในส่วนกลาง ส่วนภูมิภาคหรือต่างประเทศ ในกรณีที่มีความจำเป็นหรือสมควร หัวหน้าส่วนราชการ อาจมอบหมายให้หน่วยงาน ตรวจสอบภายในระดับกรม ตรวจสอบส่วนราชการในสังกัดราชการบริหารส่วนภูมิภาคได้

(๑.๓) หน่วยงานตรวจสอบภายในระดับจังหวัด รับผิดชอบ ตรวจสอบราชการบริหารส่วนภูมิภาค ในกรณีที่ส่วนราชการในส่วนกลาง มีหน่วยงานตั้งอยู่ในส่วนภูมิภาค หัวหน้าส่วนราชการ ในส่วนกลาง อาจมอบอำนาจให้ผู้ว่าราชการจังหวัดดำเนินการแทนตามระเบียบว่าด้วยการบริหารงบประมาณ ระเบียบว่าด้วยการบริหารราชการแผ่นดิน กฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กฎหมายว่าด้วยการเงินหรือระเบียบอื่น ๆ ของทางราชการ โดยให้ผู้ตรวจสอบภายใน ตามข้อ (๑.๓) เป็นผู้รับผิดชอบตรวจสอบเฉพาะในส่วนที่ผู้ว่าราชการจังหวัดได้รับมอบอำนาจให้ดำเนินการแทน

(๒) หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ ตามข้อ (๒) – (๗) ให้รับผิดชอบตรวจสอบการปฏิบัติงานของหน่วยงานของรัฐนั้น

ข้อ ๑๗ ให้หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ มีหน้าที่และความรับผิดชอบดังนี้

(๑) กำหนดเป้าหมาย ทิศทาง ภารกิจงานตรวจสอบภายใน เพื่อสนับสนุนการบริหารงาน และการดำเนินงานด้านต่าง ๆ ของหน่วยงานของรัฐ โดยให้สอดคล้องกับนโยบายของหน่วยงานของรัฐ คณะกรรมการ และคณะกรรมการตรวจสอบหรือคณะกรรมการอื่นใดที่ปฏิบัติงานในลักษณะเดียวกัน โดยคำนึงถึงการกำกับดูแลที่ดี ความมีประสิทธิภาพของกิจกรรมการบริหารความเสี่ยงและความเพียงพอ ของการควบคุมภายในของหน่วยงานของรัฐด้วย

(๒) กำหนดกฎบัตรไว้เป็นลายลักษณ์อักษรและเสนอหัวหน้าหน่วยงานของรัฐก่อนเสนอคณะกรรมการตรวจสอบ เพื่อพิจารณาให้ความเห็นชอบและเผยแพร่หน่วยรับตรวจทราบ รวมทั้งมีการสอบทาน ความเหมาะสมของกฎบัตรอย่างน้อยปีละหนึ่งครั้ง

(๓) จัดให้มีการประกันคุณภาพงานตรวจสอบภายในทั้งภายในและภายนอก และเสนอรายงานผลประเมิน ปัญหาและอุปสรรค รวมทั้งแผนปรับปรุงการ ดำเนินงานเสนอหัวหน้าหน่วยงานของรัฐและคณะกรรมการตรวจสอบ

(๔) จัดทำและเสนอแผนการตรวจสอบประจำปีต่อหัวหน้าหน่วยงานของรัฐก่อนเสนอคณะกรรมการตรวจสอบ เพื่อพิจารณาอนุมัติภายในเดือนสุดท้ายของปีงบประมาณหรือปีปฏิทินแล้วแต่กรณี ในกรณีที่หน่วยงานตรวจสอบภายในวางแผนการตรวจสอบที่มีระยะเวลาตั้งแต่หนึ่งปีขึ้นไป ให้นำมาใช้ประกอบการพิจารณาอนุมัติแผนการตรวจสอบประจำปีด้วย

(๔.๑) กรณีหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ ตามข้อ (๑) หน่วยงานตรวจสอบภายในระดับกระทรวง ตรวจสอบส่วนราชการในสังกัดกระทรวงที่นอกเหนือจากงานใน สำนักงานปลัดกระทรวงให้สำเนาแผนการตรวจสอบให้หัวหน้าส่วนราชการในสังกัดกระทรวงทราบด้วย

(๔.๒) กรณีหน่วยตรวจสอบภายในของหน่วยงานของรัฐตาม ข้อ (๑) หน่วยงานตรวจสอบภายใน ระดับกรม ตรวจสอบส่วนราชการในสังกัดราชการบริหารส่วนภูมิภาค ให้สำเนาแผนการตรวจสอบให้ผู้ว่าราชการจังหวัดทราบด้วย

(๕) ให้ปฏิบัติงานตรวจสอบให้เป็นไปตามแผนการตรวจสอบประจำปีที่ได้รับอนุมัติตามข้อ (๔)

(๖) จัดทำและเสนอรายงานผลการตรวจสอบต่อหัวหน้าหน่วยงานของรัฐและคณะกรรมการตรวจสอบ ภายในเวลาอันสมควรหรืออย่างน้อยทุกสองเดือนนับจากวันที่ดำเนินการตรวจสอบแล้วเสร็จตามแผน กรณีเรื่องที่ตรวจพบเป็นเรื่องที่จะมีผลเสียหายต่อทางราชการให้รายงานผลการตรวจสอบทันที

(๖.๑) กรณีหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐตามข้อ (๑) หน่วยงานตรวจสอบภายใน ระดับกระทรวง ตรวจสอบส่วนราชการระดับกรมในสังกัดกระทรวง ให้ส่งสำเนารายงานผลการตรวจสอบ ให้หัวหน้าส่วนราชการนั้น ๆ ทราบด้วย

(๖.๒) กรณีหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ ตามข้อ (๑) หน่วยงานตรวจสอบภายในระดับกรม ตรวจสอบหน่วยงานของรัฐในส่วนภูมิภาค ให้ส่งสำเนารายงานผลการตรวจสอบ ให้ผู้ว่าราชการจังหวัดทราบด้วย

(๖.๓) กรณีหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ ตามข้อ (๑) หน่วยงานตรวจสอบภายในระดับจังหวัด ตรวจสอบส่วนราชการส่วนภูมิภาค ให้ส่งสำเนารายงานผลการตรวจสอบให้หัวหน้าส่วนราชการเจ้าสังกัดของหน่วยรับตรวจนั้นทราบด้วย

(๗) ติดตามผลการตรวจสอบ เสนอแนะและให้คำปรึกษาแก่หน่วยรับตรวจเพื่อให้การปรับปรุงแก้ไขของหน่วยรับตรวจเป็นไปตามข้อเสนอแนะในรายงานผลการตรวจสอบ

(๘) ในกรณีมีความจำเป็นต้องอาศัยผู้เชี่ยวชาญมาร่วมปฏิบัติงานตรวจสอบ ให้เสนอขอบเขตและรายละเอียดของงาน คุณสมบัติของผู้รับจ้าง ระยะเวลาดำเนินการ และผลงานที่คาดหวังจากผู้รับจ้าง รวมทั้งข้อเสนอโครงการของผู้รับจ้างให้หัวหน้าหน่วยงานของรัฐพิจารณาอนุมัติให้ว่าจ้างผู้เชี่ยวชาญต่อไป

(๙) ปฏิบัติงานในการให้คำปรึกษาแก่หัวหน้าหน่วยงานของรัฐ หน่วยรับตรวจและผู้ที่เกี่ยวข้อง

(๑๐) ประสานงานกับผู้สอบบัญชี คณะกรรมการตรวจสอบหรือคณะกรรมการอื่นที่ปฏิบัติงานเช่นเดียวกัน และหน่วยงานต่าง ๆ ที่เกี่ยวข้อง เพื่อให้เกิดความมั่นใจว่าขอบเขตของงานตรวจสอบครอบคลุม เรื่องที่สำคัญอย่างเหมาะสมและลดการปฏิบัติงานที่ซ้ำซ้อนกัน

(๑๑) ปฏิบัติงานอื่นที่เกี่ยวข้องกับการตรวจสอบภายใน ตามที่ได้รับมอบหมายจากคณะกรรมการตรวจสอบและหัวหน้าหน่วยงานของรัฐ

ข้อ ๑๘ ขอบเขตงานของการตรวจสอบภายในให้ครอบคลุมถึง การตรวจสอบ วิเคราะห์ รวมทั้งการประเมินความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน และการบริหารความเสี่ยงของหน่วยงานของรัฐ ซึ่งรวมถึง

(๑) ประเมินความมีประสิทธิภาพและประสิทธิผลของการดำเนินงานในหน้าที่ของหน่วยรับตรวจ เสนอแนะการปรับปรุงการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างต่อเนื่อง

(๒) สอบทานระบบการปฏิบัติงานตามกฎหมาย ระเบียบ และข้อบังคับหรือมติคณะรัฐมนตรีที่เกี่ยวข้องกับการดำเนินงาน รวมทั้งข้อกำหนดอื่นของหน่วยงานของรัฐ

(๓) สอบทานความถูกต้องและเชื่อถือได้ของข้อมูลการดำเนินงานและการเงินการคลัง

(๔) ตรวจสอบระบบการดูแลรักษา และความปลอดภัยของทรัพย์สินของหน่วยรับตรวจ ให้มีความเหมาะสมกับประเภทของทรัพย์สินนั้น

(๕) วิเคราะห์และประเมินความมีประสิทธิภาพ ประหยัดและคุ้มค่าในการใช้ทรัพยากร

ข้อ ๑๙ ให้ผู้ตรวจสอบภายในปฏิบัติงานตรวจสอบให้เป็นไปตามมาตรฐานการตรวจสอบภายในสำหรับหน่วยงานของรัฐ กรณีที่ไม่ได้กำหนดไว้ให้ถือปฏิบัติตามมาตรฐานสากล

ข้อ ๒๐ ให้ผู้ตรวจสอบภายในปฏิบัติตนให้เป็นไปตามจรรยาบรรณการตรวจสอบภายในสำหรับหน่วยงาน ของรัฐตามที่แนบท้ายหลักเกณฑ์ปฏิบัตินี้

หน่วยรับตรวจ

ข้อ ๒๑ ให้หน่วยรับตรวจ มีหน้าที่และความรับผิดชอบ ดังนี้

(๑) อำนวยความสะดวกและให้ความร่วมมือแก่ผู้ตรวจสอบภายใน

(๒) จัดเตรียมเอกสารหลักฐานที่เกี่ยวกับการดำเนินงาน รวมถึงข้อมูลที่เกี่ยวข้องให้ครบถ้วนสมบูรณ์ พร้อมที่จะตรวจสอบได้

(๓) จัดทำบัญชีและจัดเก็บเอกสารประกอบรายการบัญชีพร้อมที่จะให้ผู้ตรวจสอบภายในตรวจสอบได้

(๔) จัดให้มีระบบการเก็บเอกสารในการปฏิบัติงานที่เหมาะสมและครบถ้วน

(๕) ชี้แจงและตอบข้อซักถามต่าง ๆ พร้อมทั้งหาข้อมูลเพิ่มเติมให้แก่ผู้ตรวจสอบภายใน

(๖) ปฏิบัติตามข้อทักท้วง และข้อเสนอแนะของผู้ตรวจสอบภายในในเรื่องต่าง ๆ ที่หัวหน้าหน่วยงานของรัฐสั่งให้ปฏิบัติ กรณีที่เจ้าหน้าที่ของหน่วยรับตรวจกระทำการโดยจงใจไม่ปฏิบัติ หรือละเลยต่อการปฏิบัติหน้าที่ ตามวรรคหนึ่งให้ผู้ตรวจสอบภายในรายงานหัวหน้าหน่วยงานของรัฐพิจารณาสั่งการตามควรแก่กรณี

ข้อ ๒๒ กรณีหน่วยงานของรัฐไม่มีคณะกรรมการตรวจสอบให้ขึ้นตรงต่อหัวหน้าหน่วยงานของรัฐไปพลางก่อน และจัดให้มีคณะกรรมการตรวจสอบภายในระยะเวลาสามปีนับแต่วันที่หลักเกณฑ์ปฏิบัตินี้ ใช้บังคับตามรูปแบบที่กระทรวงการคลังกำหนด

ข้อ ๒๓ บรรดาการตรวจสอบภายในที่อยู่ระหว่างการดำเนินการก่อนวันที่หลักเกณฑ์ปฏิบัตินี้ ใช้บังคับ ให้ดำเนินการต่อไปตามระเบียบกระทรวงมหาดไทยว่าด้วยการตรวจสอบภายในขององค์กรปกครองส่วนท้องถิ่น พ.ศ. ๒๕๔๕ ระเบียบกระทรวงการคลังว่าด้วยการตรวจสอบภายในของส่วนราชการ พ.ศ. ๒๕๕๑ ระเบียบกระทรวงกลาโหมว่าด้วยการตรวจสอบภายใน พ.ศ. ๒๕๕๓ และระเบียบกระทรวงการคลังว่าด้วย คณะกรรมการตรวจสอบและหน่วยตรวจสอบภายในของรัฐวิสาหกิจ พ.ศ. ๒๕๕๕ จนกว่าจะแล้วเสร็จภายใน หนึ่งปีนับแต่วันที่หลักเกณฑ์ปฏิบัตินี้ใช้บังคับ

แนบท้ายหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ

วัตถุประสงค์ เพื่อเป็นการยกฐานะและศักดิ์ศรีของวิชาชีพตรวจสอบภายในให้ได้รับการยกย่อง และยอมรับจากบุคคลทั่วไป รวมทั้งให้การปฏิบัติหน้าที่ตรวจสอบภายในเป็นไปอย่างมีประสิทธิภาพ ผู้ตรวจสอบภายในจึงต้องพึงประพฤติปฏิบัติตนภายใต้กรอบความประพฤติที่ดีงาม ในอันที่จะนำมาซึ่งความเชื่อมั่นและให้คำปรึกษา อย่างเที่ยงธรรม เป็นอิสระ และเปี่ยมด้วยคุณภาพ

แนวปฏิบัติ

๑. หลักปฏิบัติที่กำหนดในจรรยาบรรณการตรวจสอบภายใน เป็นหลักการพื้นฐานในการปฏิบัติหน้าที่ ที่ผู้ตรวจสอบภายในพึงปฏิบัติ โดยใช้สามัญสำนึกและวิจารณญาณอันเหมาะสม

๒. ผู้ตรวจสอบภายในควรประพฤติปฏิบัติตนตามกรอบจรรยาบรรณนี้ นอกเหนือจากการปฏิบัติตามจรรยาบรรณของเจ้าหน้าที่ของหน่วยงานของรัฐ และกฎหมายหรือหลักเกณฑ์อื่นที่เกี่ยวข้อง

๓. ผู้ตรวจสอบภายในพึงยึดถือและดำรงไว้ซึ่งหลักปฏิบัติ ดังต่อไปนี้

๓.๑ ความซื่อสัตย์ (Integrity) ความซื่อสัตย์ของผู้ตรวจสอบภายในจะสร้างให้เกิดความไว้วางใจและทำให้ดุลยพินิจของผู้ตรวจสอบภายในมีความน่าเชื่อถือและยอมรับจากบุคคลทั่วไป

๓.๒ ความเที่ยงธรรม (Objectivity) ผู้ตรวจสอบภายในจะแสดงความเที่ยงธรรมเยี่ยงผู้ประกอบวิชาชีพในการรวบรวมข้อมูล ประเมินผล และรายงานด้วยความไม่ลำเอียง ผู้ตรวจสอบภายใน ต้องทำหน้าที่อย่างเป็นธรรมในทุก ๆ สถานการณ์ และไม่ปล่อยให้ความรู้สึกส่วนตัวหรือความรู้สึกนึกคิด ของบุคคลอื่นเข้ามามีอิทธิพลเหนือการปฏิบัติงาน

๓.๓ การปกปิดความลับ (Confidentiality) ผู้ตรวจสอบภายในจะเคารพในคุณค่าและสิทธิของผู้เป็นเจ้าของข้อมูลที่ได้รับทราบจากการปฏิบัติงาน และไม่เปิดเผยข้อมูลดังกล่าว โดยไม่ได้รับอนุญาตจากผู้ที่มีอำนาจหน้าที่โดยตรงเสียก่อน ยกเว้นในกรณีที่มีพันธะในแง่ของงานอาชีพและเกี่ยวข้องกับกฎหมายเท่านั้น

๓.๔ ความสามารถในหน้าที่ (Competency) ผู้ตรวจสอบภายในจะนำความรู้ ทักษะ และประสบการณ์มาใช้ในการปฏิบัติงานอย่างเต็มที่

หลักปฏิบัติ

๑. ความซื่อสัตย์ (Integrity)

๑.๑ ผู้ตรวจสอบภายในต้องปฏิบัติหน้าที่ของตนด้วยความซื่อสัตย์ ขยันหมั่นเพียร และมีความรับผิดชอบ

๑.๒ ผู้ตรวจสอบภายในต้องปฏิบัติตามกฎหมาย หลักเกณฑ์ ข้อบังคับ และเปิดเผยข้อมูลตามวิชาชีพที่กำหนด

๑.๓ ผู้ตรวจสอบภายในต้องไม่เข้าไปเกี่ยวข้องในการกระทำใด ๆ ที่ขัดต่อกฎหมาย หรือไม่เข้าไปมีส่วนร่วมในการกระทำที่อาจนำความเสื่อมเสียมาสู่วิชาชีพการตรวจสอบภายใน หรือสร้างความเสียหายต่อหน่วยงานของรัฐ

๑.๔ ผู้ตรวจสอบภายในต้องให้ความเคารพและสนับสนุนการปฏิบัติตามกฎหมาย หลักเกณฑ์ข้อบังคับและจรรยาบรรณของหน่วยงานของรัฐ

๒. ความเป็นอิสระและเที่ยงธรรม (Objectivity)

๒.๑ ผู้ตรวจสอบภายในต้องไม่มีส่วนเกี่ยวข้องหรือสร้างความสัมพันธ์ใด ๆ ที่จะนำไปสู่ความขัดแย้งกับผลประโยชน์ของหน่วยงานของรัฐ รวมทั้งกระทำการใด ๆ ที่จะทำให้เกิดอคติ ลำเอียงจนเป็นเหตุให้ไม่สามารถปฏิบัติงานตามหน้าที่ความรับผิดชอบได้อย่างเที่ยงธรรม

๒.๒ ผู้ตรวจสอบภายในไม่พึงรับสิ่งของใด ๆ ที่จะทำให้เกิดหรือก่อให้เกิดความไม่เที่ยงธรรมในการใช้วิจารณญาณเยี่ยงผู้ประกอบวิชาชีพพึงปฏิบัติ

๒.๓ ผู้ตรวจสอบภายในต้องเปิดเผยหรือรายงานข้อเท็จจริงอันเป็นสาระสำคัญทั้งหมดที่ตรวจพบซึ่งหากละเว้นไม่เปิดเผยหรือไม่รายงานข้อเท็จจริงดังกล่าวแล้ว อาจจะทำให้รายงานบิดเบือนไปจากข้อเท็จจริง หรือเป็นการปิดบังการกระทำผิดกฎหมาย

๓. การปกปิดความลับ (Confidentiality)

๓.๑ ผู้ตรวจสอบภายในต้องมีความรอบคอบในการใช้และรักษาข้อมูลต่าง ๆ ที่ได้รับจากการปฏิบัติงาน

๓.๒ ผู้ตรวจสอบภายในต้องไม่นำข้อมูลต่าง ๆ ที่ได้รับจากการปฏิบัติงานไปใช้แสวงหาผลประโยชน์เพื่อตนเอง และจะไม่กระทำการใด ๆ ที่ขัดต่อกฎหมายและประโยชน์ของหน่วยงานของรัฐ

๔. ความสามารถในหน้าที่ (Competency)

๔.๑ ผู้ตรวจสอบภายในต้องปฏิบัติหน้าที่เฉพาะในส่วนที่ตนมีความรู้ ความสามารถ ทักษะ และประสบการณ์ที่จำเป็นสำหรับการปฏิบัติงานเท่านั้น

๔.๒ ผู้ตรวจสอบภายในจะต้องปฏิบัติหน้าที่โดยยึดหลักมาตรฐานการตรวจสอบภายในสำหรับหน่วยงานของรัฐ

๔.๓ ผู้ตรวจสอบภายในต้องพัฒนาศักยภาพของตนเอง รวมทั้งพัฒนาประสิทธิผล และคุณภาพของการให้บริการอย่างสม่ำเสมอและต่อเนื่อง และในการดูแลเรื่องของสัญญาว่าจ้าง และคุณภาพความน่าเชื่อถือของผลงาน รวมทั้งรายงานให้หัวหน้าหน่วยงานของรัฐและคณะกรรมการตรวจสอบได้รับทราบและติดตามผลของการปฏิบัติงานตรวจสอบภายใน

๓. บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง

ตามมาตรฐานกำหนดตำแหน่งที่กำหนดโดย ก.พ.อ. เมื่อวันที่ ๒๑ กันยายน พ.ศ.๒๕๕๓ ได้ระบุหน้าที่ความรับผิดชอบของตำแหน่งนักตรวจสอบภายในปฏิบัติการ ดังนี้

หน้าที่และความรับผิดชอบหลัก

ปฏิบัติงานในฐานะผู้ปฏิบัติงานระดับต้นที่ต้องใช้ความรู้ความสามารถทางวิชาการในการทำงานปฏิบัติงานด้านการตรวจสอบภายใน ภายใต้การกำกับ แนะนำ ตรวจสอบ และปฏิบัติงานอื่นที่ได้รับมอบหมายโดยมีลักษณะงานที่ปฏิบัติในด้านต่าง ๆ ดังนี้

๓.๑ ด้านการปฏิบัติการ

๑. ตรวจสอบการปฏิบัติงานของหน่วยงานต่าง ๆ ในด้านงบประมาณ บัญชี ตรวจสอบยอดเงินทดรองราชการคงเหลือให้ตรงตามบัญชี ตรวจสอบหลักฐานเอกสารทางบัญชี ควบคุมเอกสารทางด้านการเงิน การตรวจสอบปฏิบัติงานพร้อมทั้งหลักฐานการทำสัญญา การจัดซื้อพัสดุ การเบิกจ่าย การลงบัญชี การจัดเก็บรักษาพัสดุในคลังพัสดุ การใช้และการเก็บรักษายานพาหนะให้ประหยัดและถูกต้องตามระเบียบของทางราชการ ตรวจสอบรายละเอียดงบประมาณรายได้ รายจ่าย และการก่อหนี้ผูกพันงบประมาณรายจ่าย รวมทั้งเงินยืมทดรองจ่าย เงินทดรองราชการ และเงินนอกงบประมาณทุกประเภท เพื่อดูแลให้การใช้งบประมาณและทรัพยากรเป็นไปอย่างประหยัด มีประสิทธิภาพ และตรงตามวัตถุประสงค์ที่กำหนด

๒. จัดทำรายงานการตรวจสอบรายเดือน เพื่อเสนอข้อตรวจพบและข้อเสนอแนะให้ผู้บังคับบัญชาหรือหน่วยงานต้นสังกัดรับทราบผลการดำเนินงาน

๓. ศึกษา ค้นคว้า รวบรวม และตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลตัวเลข หลักฐานการทำสัญญา และเอกสารต่าง ๆ ทางด้านการเงิน การบัญชี เพื่อให้การตรวจสอบดำเนินไปอย่างถูกต้องได้ผลตรงกับหลักฐานที่เกิดขึ้นจริง

๔. ให้บริการวิชาการด้านต่าง ๆ เช่น ให้คำปรึกษา แนะนำ ในการปฏิบัติงานแก่เจ้าหน้าที่ระดับรองลงมา และแก่นักศึกษาที่มาฝึกปฏิบัติงาน ตอบปัญหาและชี้แจงเรื่องต่าง ๆ เกี่ยวกับงานในหน้าที่เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง มีประสิทธิภาพ และปฏิบัติหน้าที่อื่นที่เกี่ยวข้อง

๓.๒ ด้านการวางแผน

วางแผนการทำงานที่รับผิดชอบ ร่วมวางแผนการทำงานของหน่วยงานหรือโครงการเพื่อให้การดำเนินงานบรรลุตามเป้าหมายและผลสัมฤทธิ์ที่กำหนด

๓.๓ ด้านการประสานงาน

๑. ประสานการทำงานร่วมกันระหว่างทีมงานหรือหน่วยงานทั้งภายในและภายนอก เพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้

๒. ชี้แจงและให้รายละเอียดเกี่ยวกับข้อมูล ข้อเท็จจริง แก่บุคคลหรือหน่วยงานที่เกี่ยวข้อง เพื่อสร้างความเข้าใจหรือความร่วมมือในการดำเนินงานตามที่ได้รับมอบหมาย

๓.๔ ด้านการบริการ

๑. ให้คำปรึกษา แนะนำเบื้องต้น เผยแพร่ ถ่ายทอดความรู้ทางด้านการตรวจสอบภายใน รวมทั้งตอบปัญหาและชี้แจงเรื่องต่าง ๆ เกี่ยวกับงานในหน้าที่ เพื่อให้ผู้รับบริการได้รับทราบข้อมูลความรู้ต่าง ๆ ที่เป็นประโยชน์

๒. จัดเก็บข้อมูลเบื้องต้น และให้บริการข้อมูลทางวิชาการเกี่ยวกับด้านการตรวจสอบภายใน เพื่อให้บุคลากรทั้งภายในภายนอกหน่วยงาน นักศึกษา ตลอดจนผู้รับบริการได้ทราบข้อมูลและความรู้ต่าง ๆ ที่เป็นประโยชน์ สอดคล้องและสนับสนุนภารกิจของหน่วยงาน และใช้ประกอบพิจารณากำหนดนโยบาย แผนงาน หลักเกณฑ์ มาตรการต่าง ๆ

๔. หน้าที่ความรับผิดชอบของตำแหน่งตามที่ได้รับมอบหมาย

บทบาทหน้าที่ความรับผิดชอบของตำแหน่งตามที่ได้รับมอบหมาย ของนางสาวธิดารัตน์ อุปชัย ตำแหน่ง นักตรวจสอบภายใน ระดับปฏิบัติการ มีดังนี้

๔.๑ ด้านการปฏิบัติการ

๔.๑.๑ งานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ การตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Auditing)

๔.๑.๒ งานการประกันคุณภาพงานตรวจสอบภายในภาครัฐ

๔.๑.๓ การประเมินผลการควบคุมภายในระดับหน่วยงานย่อย และรายงานผลการตรวจสอบให้กับกลุ่มตรวจสอบภายในระดับกระทรวง

๔.๑.๔ การจัดทำรายงานประจำปี

๔.๑.๕ จัดทำรายงานผลการตรวจสอบภายใน เพื่อเสนอข้อตรวจพบและข้อเสนอแนะให้ผู้บังคับบัญชาหรือหน่วยงานต้นสังกัดรับทราบผลการดำเนินงาน

๔.๑.๖ ศึกษาค้นคว้า รวบรวมข้อมูลและเอกสารต่าง ๆ เพื่อจัดทำแนวปฏิบัติและคู่มือการปฏิบัติงาน

๔.๑.๗ ให้บริการวิชาการด้านต่าง ๆ เช่น ให้คำปรึกษาแนะนำในการปฏิบัติงานแก่เจ้าหน้าที่ระดับรองลงมาและตอบปัญหาและชี้แจงเรื่องต่าง ๆ เกี่ยวกับงานในหน้าที่ เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง มีประสิทธิภาพและปฏิบัติหน้าที่อื่นที่เกี่ยวข้อง

๔.๑.๘ การประเมินตนเองของหน่วยตรวจสอบภายใน (Self - Assessment)

๔.๑.๙ งานประชาสัมพันธ์ข้อมูลข่าวสารเว็บไซต์

๔.๒ ด้านการวางแผน

วางแผนการทำงานที่รับผิดชอบ ร่วมวางแผนการทำงานของหน่วยงานหรือโครงการเพื่อให้การดำเนินงานบรรลุตามเป้าหมายและผลสัมฤทธิ์ที่กำหนด

๔.๓ ด้านการประสานงาน

๔.๓.๑ ประสานการทำงานร่วมกันระหว่างทีมงาน หรือหน่วยงานทั้งภายในและภายนอก เพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้

๔.๓.๒ ชี้แจงและให้รายละเอียดเกี่ยวกับข้อมูล ข้อเท็จจริง แก่บุคคลหรือหน่วยงานที่เกี่ยวข้อง เพื่อสร้างความเข้าใจหรือความร่วมมือในการดำเนินงานตามที่ได้รับมอบหมาย

๔.๔ ด้านการบริการ

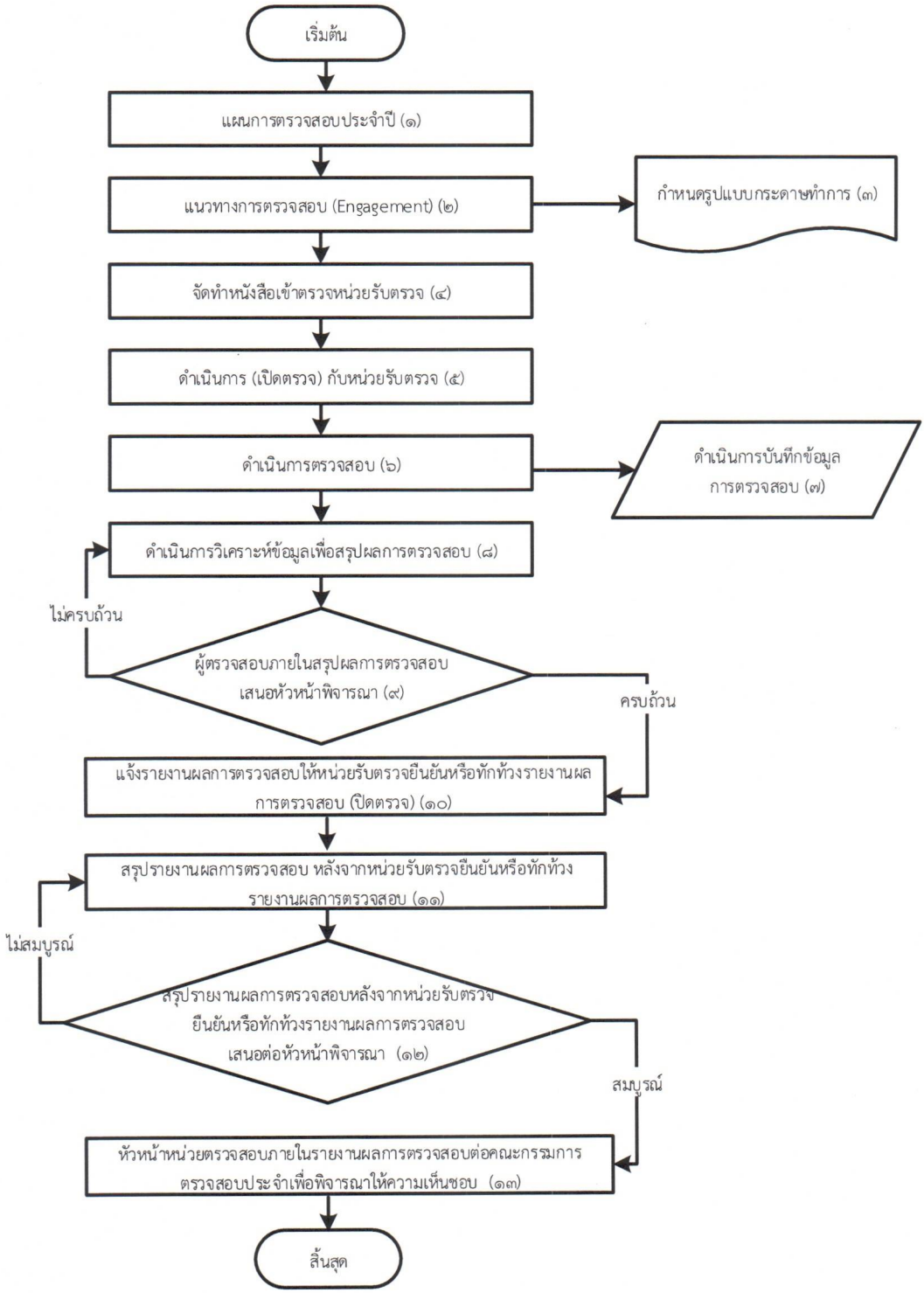
๔.๔.๑ ให้คำปรึกษา แนะนำเบื้องต้น เผยแพร่ ถ่ายทอดความรู้ ทางด้านการตรวจสอบภายใน รวมทั้งตอบปัญหาและชี้แจงเรื่องต่าง ๆ เกี่ยวกับงานในหน้าที่ เพื่อให้ผู้รับบริการได้รับทราบข้อมูลความรู้ต่าง ๆ ที่เป็นประโยชน์

๔.๔.๒ จัดเก็บข้อมูลเบื้องต้น และให้บริการข้อมูลทางวิชาการ เกี่ยวกับด้านการตรวจสอบภายใน เพื่อให้บุคลากรทั้งภายในและภายนอกหน่วยงาน นักศึกษา ตลอดจนผู้รับบริการ ได้ทราบข้อมูลและความรู้ต่าง ๆ ที่เป็นประโยชน์ สอดคล้อง และสนับสนุนภารกิจของหน่วยงาน และใช้ประกอบการพิจารณา กำหนดนโยบาย แผนงาน หลักเกณฑ์ มาตรการต่าง ๆ

๔.๕ งานอื่น ๆ ตามที่ได้รับมอบหมาย

จากภาระหน้าที่ที่ได้รับมอบหมายผู้เขียนได้เลือกงานในการจัดทำคู่มือการปฏิบัติงาน เรื่อง การตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ มาเขียนเป็นคู่มือการปฏิบัติงาน โดยมีขั้นตอนการปฏิบัติงาน (Flow Chart) ดังภาพที่ ๔ ดังนี้

ขั้นตอนปฏิบัติงานตรวจสอบ เรื่อง การตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ



ภาพที่ ๔ แสดงขั้นตอนการปฏิบัติงานตรวจสอบ เรื่อง การตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ

บทที่ ๓
หลักเกณฑ์และวิธีการปฏิบัติ

๑. หลักเกณฑ์ที่เกี่ยวข้อง

๑.๑ พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ (มาตรา ๗๙)

ด้วยพระราชบัญญัติ วินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ ได้กำหนดให้รัฐต้องรักษาวินัยการเงินการคลังอย่างเคร่งครัดเพื่อให้ฐานะทางการเงินการคลังของรัฐมีเสถียรภาพ และมั่นคงอย่างยั่งยืน ตามกฎหมายว่าด้วยวินัยการเงินการคลังของรัฐ ซึ่งกฎหมายดังกล่าวอย่างน้อยต้องมีบทบัญญัติเกี่ยวกับกรอบการดำเนินการทางการคลังและงบประมาณของรัฐ การกำหนดวินัยทางการคลัง ด้านรายได้และรายจ่ายทั้งเงินงบประมาณและเงินนอกงบประมาณ การบริหารทรัพย์สินของรัฐและเงินคงคลัง และการบริหารหนี้สาธารณะ จึงตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ทำหน้าที่รัฐสภา ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป

มาตรา ๓ การปฏิบัติการเกี่ยวกับการเงินการคลังของรัฐตามกฎหมายต่าง ๆ ถ้าเป็นกรณี ที่บัญญัติไว้แล้วตามพระราชบัญญัตินี้ ให้เป็นไปตามที่กำหนดในพระราชบัญญัตินี้

มาตรา ๔ ในพระราชบัญญัตินี้ “หน่วยงานของรัฐ” หมายความว่า

(๑) ส่วนราชการ

(๒) รัฐวิสาหกิจ

(๓) หน่วยงานของรัฐสภา ศาลยุติธรรม ศาลปกครอง ศาลรัฐธรรมนูญ องค์กรอิสระตามรัฐธรรมนูญ และองค์กรอัยการ

(๔) องค์การมหาชน

(๕) ทุนหมุนเวียนที่มีฐานะเป็นนิติบุคคล

(๖) องค์กรปกครองส่วนท้องถิ่น

(๗) หน่วยงานอื่นของรัฐตามที่กฎหมายกำหนด

“ส่วนราชการ” หมายความว่า กระทรวง ทบวง กรม หรือส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม และให้หมายความรวมถึงจังหวัดและกลุ่มจังหวัดตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดินด้วย

“รัฐวิสาหกิจ” หมายความว่า

(๑) องค์การของรัฐบาลตามกฎหมายว่าด้วยการจัดตั้งองค์การของรัฐบาล กิจการของรัฐซึ่งมีกฎหมายจัดตั้งขึ้น หรือหน่วยงานธุรกิจที่รัฐบาลเป็นเจ้าของ

(๒) บริษัทจำกัดหรือบริษัทมหาชนจำกัดที่ส่วนราชการหรือรัฐวิสาหกิจตาม (๑) มีทุนรวมอยู่ด้วย เกินร้อยละห้าสิบ

(๓) บริษัทจำกัดหรือบริษัทมหาชนจำกัดที่ส่วนราชการและรัฐวิสาหกิจตาม (๑) หรือ (๒) หรือ ที่รัฐวิสาหกิจตาม (๑) และ (๒) หรือที่รัฐวิสาหกิจตาม (๒) มีทุนรวมอยู่ด้วยเกินร้อยละห้าสิบ

“ทุนหมุนเวียน” หมายความว่า กองทุน กองทุนหมุนเวียน เงินทุน เงินทุนหมุนเวียน ทุน หรือ ทุนหมุนเวียน ที่ตั้งขึ้นเพื่อกิจการที่อนุญาตให้นำรายรับสมทบทุนไว้ใช้จ่ายได้โดยไม่ต้องนำส่งคลัง

"องค์กรปกครองส่วนท้องถิ่น" หมายความว่า องค์การบริหารส่วนจังหวัด เทศบาล องค์การบริหารส่วนตำบล กรุงเทพมหานคร เมืองพัทยา และองค์กรปกครองส่วนท้องถิ่นอื่นที่มีกฎหมายจัดตั้ง

"เงินนอกงบประมาณ" หมายความว่า บรรดาเงินทั้งปวงที่หน่วยงานของรัฐจัดเก็บ หรือได้รับ ไว้เป็นกรรมสิทธิ์ตามกฎหมาย ระเบียบ ข้อบังคับ หรือจากนิติกรรมหรือนิติเหตุ หรือกรณีอื่นใด ที่ต้องนำส่งคลัง แต่มีกฎหมายอนุญาตให้สามารถเก็บไว้ใช้จ่ายได้โดยไม่ต้องนำส่งคลัง

"หนี้สาธารณะ" หมายความว่า หนี้สาธารณะตามกฎหมายว่าด้วยการบริหารหนี้สาธารณะ

"คลัง" หมายความว่า ที่เก็บรักษาเงินแผ่นดินของกระทรวงการคลัง และให้หมายความรวมถึง บัญชีเงินฝากที่ธนาคารแห่งประเทศไทยเพื่อการนี้ด้วย

"คณะกรรมการ" หมายความว่า คณะกรรมการนโยบายการเงินการคลังของรัฐ

"กรรมการ" หมายความว่า กรรมการนโยบายการเงินการคลังของรัฐ

"รัฐมนตรี" หมายความว่า รัฐมนตรีว่าการกระทรวงการคลัง

มาตรา ๕ ให้นายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงการคลังรักษาการตาม พระราชบัญญัตินี้ และให้มีอำนาจออกระเบียบและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้ ระเบียบและประกาศเมื่อประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

มาตรา ๗๙ ให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

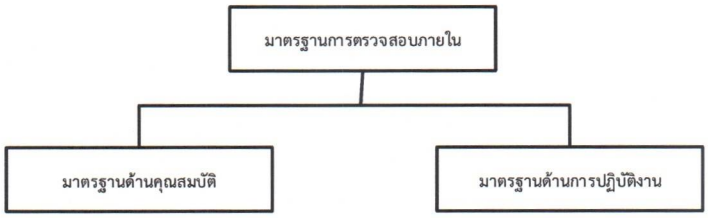
๑.๒ หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒ (ฉบับที่ ๓) พ.ศ. ๒๕๖๔ (ฉบับที่ ๔) พ.ศ. ๒๕๖๖

ด้วยกระทรวงการคลังได้กำหนดมาตรฐานการตรวจสอบภายในสำหรับหน่วยงานของรัฐ เพื่อให้ผู้ตรวจสอบภายในของหน่วยงานของรัฐ ใช้เป็นแนวทางการปฏิบัติงานตรวจสอบภายในให้มีประสิทธิภาพและประสิทธิผล เนื่องจากการตรวจสอบภายในนับว่าเป็นเครื่องมือหรือผู้ช่วยที่สำคัญของผู้บริหารหน่วยงานในการติดตามและประเมินการปฏิบัติงานของส่วนงานต่าง ๆ ภายในหน่วยงาน รวมทั้งการให้ข้อเสนอแนะแนวทางหรือมาตรการที่จะทำให้ผลการดำเนินงานสามารถบรรลุผลตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้ โดยการปฏิบัติงานของหน่วยงานเป็นไปตามโครงสร้างมาตรฐานการตรวจสอบภายใน ซึ่งประกอบด้วย ๒ ส่วน คือ มาตรฐานด้านคุณสมบัติ (Attribute Standards) และมาตรฐานการปฏิบัติงาน (Performance Standards)

มาตรฐานคุณสมบัติ เป็นมาตรฐานที่กล่าวถึงลักษณะของหน่วยงานและบุคลากรที่ต้องปฏิบัติงานด้านการตรวจสอบภายใน โดยใช้รหัสมาตรฐานที่ ๑๐๐๐ เป็นต้นไป

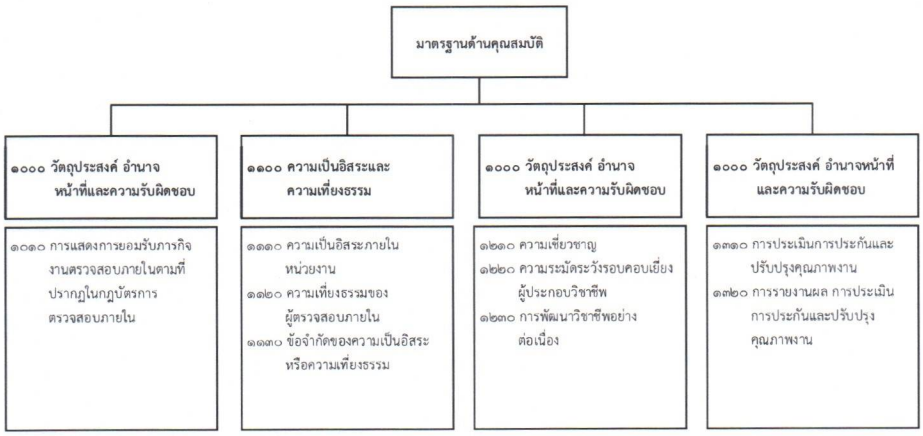
มาตรฐานด้านการปฏิบัติงาน เป็นมาตรฐานที่กล่าวถึงลักษณะของงานและกระบวนการตรวจสอบภายใน โดยเริ่มรหัสมาตรฐานที่ ๒๐๐๐ เป็นต้นไป

ผังโครงสร้างมาตรฐานการตรวจสอบภายใน



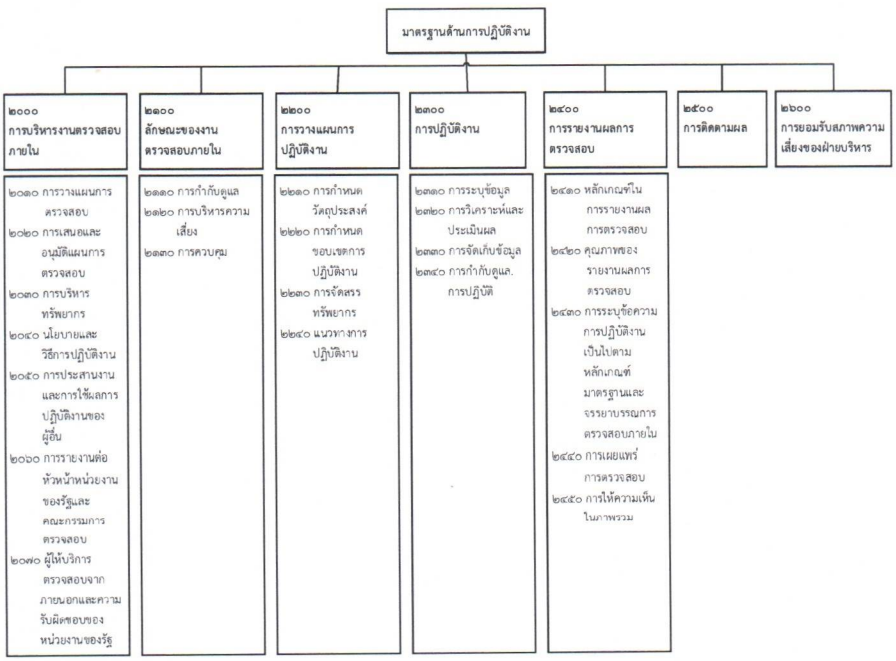
ภาพที่ ๕ แสดงผังโครงสร้างมาตรฐานการตรวจสอบภายใน

ผังมาตรฐานด้านคุณสมบัติ



ภาพที่ ๖ แสดงผังมาตรฐานด้านคุณสมบัติ

ผังมาตรฐานด้านการปฏิบัติงาน



ภาพที่ ๗ แสดงผังมาตรฐานด้านการปฏิบัติงาน

การนำมาตรฐานไปใช้ในงานบริการให้ความเชื่อมั่นและงานบริการให้คำปรึกษา จะมีตัวอักษร A (Assurance Service) และ C (Consulting Service) ต่อท้ายเลขมาตรฐาน ดังนี้

๑. งานบริการด้านให้ความเชื่อมั่นจะแทนด้วยอักษร A ต่อท้ายจากเลขรหัสมาตรฐาน เช่น ๑๐๐๐.A๑ เป็นการอธิบายถึงลักษณะงานบริการให้ความเชื่อมั่นแก่หน่วยงานของรัฐที่ต้องกำหนดไว้ในกฎบัตร และ ๑๑๓๐.A๓ เป็นการอธิบายถึงการให้ความเชื่อมั่นต่องานที่เคยให้คำปรึกษามาก่อน เป็นต้น

๒. งานบริการด้านให้คำปรึกษาจะแทนด้วยอักษร C ต่อท้ายจากเลขรหัสมาตรฐาน เช่น ๑๐๐๐.C๑ เป็นการอธิบายถึงลักษณะงานบริการให้คำปรึกษาที่ต้องกำหนดไว้ในกฎบัตร และ ๑๒๒๐.C๑ เป็นการอธิบายถึงการปฏิบัติงานบริการให้คำปรึกษาด้วยความระมัดระวังอย่างรอบคอบ เป็นต้น

ทั้งนี้ หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒ (ฉบับที่ ๓) พ.ศ. ๒๕๖๔ (ฉบับที่ ๔) พ.ศ. ๒๕๖๖ ได้กำหนดแนวทางการปฏิบัติสำหรับผู้ตรวจสอบภายใน ดังนี้

ข้อ ๑ ในหลักเกณฑ์นี้

“การตรวจสอบภายใน” หมายความว่า กิจกรรมให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานของหน่วยงานของรัฐให้ดีขึ้น และจะช่วยให้หน่วยงานของรัฐบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ

“หน่วยงานของรัฐ” หมายความว่า

(๑) ส่วนราชการ

(๒) รัฐวิสาหกิจ

(๓) หน่วยงานของรัฐสภา ศาลยุติธรรม ศาลปกครอง ศาลรัฐธรรมนูญ องค์กรอิสระตามรัฐธรรมนูญ และองค์กรอัยการ

(๔) องค์การมหาชน

(๕) ทุนหมุนเวียนที่มีฐานะเป็นนิติบุคคล

(๖) องค์กรปกครองส่วนท้องถิ่น

(๗) หน่วยงานอื่นของรัฐตามที่กฎหมายกำหนด

“คณะกรรมการ” หมายความว่า คณะกรรมการของหน่วยงานของรัฐตามโครงสร้างองค์กรของหน่วยงานของรัฐ ซึ่งมีหน้าที่กำหนดนโยบายการดำเนินงานของหน่วยงาน กำกับดูแลและควบคุมหน่วยงานของรัฐตามกฎหมายของหน่วยงานของรัฐนั้น

“หัวหน้าหน่วยงานของรัฐ” หมายความว่า ผู้บริหารสูงสุดของหน่วยงานของรัฐ

“ฝ่ายบริหาร” หมายความว่า ผู้ทำหน้าที่บริหารซึ่งดำรงตำแหน่งรองจากหัวหน้าหน่วยงานของรัฐ ไม่เกินสามลำดับ

“คณะกรรมการตรวจสอบ” หมายความว่า คณะกรรมการตรวจสอบตามข้อ ๑๐ โดยอาจใช้ชื่อเรียกอื่นที่ทำหน้าที่เช่นเดียวกับคณะกรรมการตรวจสอบ

“หน่วยงานตรวจสอบภายใน” หมายความว่า หน่วยงานที่รับผิดชอบงานตรวจสอบภายในของหน่วยงานของรัฐ

“หัวหน้าหน่วยงานตรวจสอบภายใน” หมายความว่า ผู้ดำรงตำแหน่งสูงสุดในหน่วยงานตรวจสอบภายใน

“ผู้ตรวจสอบภายใน” หมายความว่า ผู้ดำรงตำแหน่งผู้ตรวจสอบภายในของหน่วยงานของรัฐหรือดำรงตำแหน่งอื่นที่ทำหน้าที่เช่นเดียวกับผู้ตรวจสอบภายในของหน่วยงานของรัฐ

"หน่วยรับตรวจ" หมายความว่า หน่วยงานที่รับผิดชอบในการปฏิบัติงานของหน่วยงานของรัฐ

ข้อ ๒ คู่มือหรือแนวปฏิบัติเกี่ยวกับการตรวจสอบภายในและคณะกรรมการตรวจสอบสำหรับหน่วยงานของรัฐตามข้อ ๑(๑) และข้อ ๑(๓) - (๗) ให้เป็นไปตามที่กรมบัญชีกลางกำหนด สำหรับหน่วยงานของรัฐ ตามข้อ ๑ (๒) ให้เป็นไปตามที่สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจกำหนด

ข้อ ๓ ในการปฏิบัติงานตรวจสอบภายในให้หน่วยงานของรัฐจัดให้มีหน่วยงานตรวจสอบภายใน กรณีหน่วยงานของรัฐมีคณะกรรมการ ให้คณะกรรมการเป็นผู้แต่งตั้งคณะกรรมการตรวจสอบ และให้หน่วยงานตรวจสอบภายในขึ้นตรงต่อคณะกรรมการตรวจสอบ กรณีหน่วยงานของรัฐไม่มีคณะกรรมการให้หน่วยงานตรวจสอบภายในขึ้นตรงต่อหัวหน้าหน่วยงานของรัฐ

ข้อ ๔ การบริหารงานทั่วไปของหน่วยงานตรวจสอบภายใน ให้หน่วยงานตรวจสอบภายในขึ้นตรงต่อหัวหน้าหน่วยงานของรัฐ สำหรับการพิจารณาแต่งตั้ง โยกย้าย ถอดถอน เลื่อนขั้น เลื่อนตำแหน่ง และประเมินผลงานของหัวหน้าหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐที่มีคณะกรรมการตรวจสอบ ให้เป็นไปตาม ข้อ ๑๓ (๗)

ข้อ ๕ หัวหน้าหน่วยงานตรวจสอบภายในและผู้ตรวจสอบภายในต้องมีคุณสมบัติดังต่อไปนี้

(๑) มีความรู้ ทักษะ และความสามารถที่จำเป็นต่อการปฏิบัติหน้าที่ที่ได้รับมอบหมาย

(๒) มีความรู้เกี่ยวกับกฎหมาย ระเบียบ ข้อบังคับ มติคณะรัฐมนตรี ประกาศ และคำสั่งที่เกี่ยวข้องกับการดำเนินงานของหน่วยงานของรัฐ

(๓) มีความรู้เกี่ยวกับการปฏิบัติงาน การกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายในของหน่วยงานของรัฐ

หัวหน้าหน่วยงานของรัฐต้องจัดสรรบุคลากรและทรัพยากร เพื่อให้การปฏิบัติงานของหน่วยงานตรวจสอบภายในเป็นไปอย่างเหมาะสมและสอดคล้องกับปริมาณงานและความซับซ้อนของภารกิจของหน่วยงานของรัฐ

ข้อ ๖ หัวหน้าหน่วยงานของรัฐจะแต่งตั้งให้ผู้ตรวจสอบภายในรักษาการในตำแหน่งอื่นหรือแต่งตั้งให้ผู้ดำรงตำแหน่งอื่นมารักษาการในตำแหน่งผู้ตรวจสอบภายในได้เฉพาะกรณีที่การปฏิบัติงานของบุคลากรดังกล่าวได้ขาดจากการปฏิบัติงานในหน้าที่เดิม

ในกรณีที่หน่วยงานของรัฐอยู่ระหว่างการสรรหาบุคลากรมาดำรงตำแหน่งเป็นผู้ตรวจสอบภายในของหน่วยงานของรัฐ หน่วยงานของรัฐอาจพิจารณามอบหมายให้บุคลากรภายในหน่วยงานของรัฐมาปฏิบัติงานด้านการตรวจสอบภายในเป็นการชั่วคราวและยังคงปฏิบัติงานในตำแหน่งหน้าที่เดิมได้ ทั้งนี้ บุคลากรดังกล่าวควรมีความรู้ทักษะและความสามารถที่จำเป็นต่อการปฏิบัติงานด้านการตรวจสอบภายใน และต้องไม่เป็นผู้ที่รับผิดชอบด้านการเงิน การบัญชี การพัสดุ หรือปฏิบัติงานในภารกิจหลักของหน่วยงานของรัฐ

หัวหน้าหน่วยงานของรัฐและหรือคณะกรรมการตรวจสอบจะพิจารณาสั่งการให้ผู้ตรวจสอบภายในปฏิบัติงานอื่นได้ตามควรแก่กรณี ทั้งนี้ ให้พิจารณาถึงประโยชน์ที่หน่วยงานของรัฐจะได้รับ และผลกระทบต่อความเป็นอิสระและเที่ยงธรรมในการปฏิบัติงานตรวจสอบ

ข้อ ๗ ให้ผู้ตรวจสอบภายในดำรงไว้ซึ่งความเป็นอิสระและไม่มีความขัดแย้งทางผลประโยชน์ในกิจกรรมที่ตรวจสอบ และปราศจากการแทรกแซงในการปฏิบัติงานและการเสนอความเห็นในการตรวจสอบ ของฝ่ายบริหารหรือบุคคลหนึ่งบุคคลใด รวมทั้งต้องไม่ตรวจสอบงานที่ตนเคยทำหน้าที่บริหารหรือปฏิบัติงาน ภายในระยะเวลาหนึ่งปีก่อนการตรวจสอบ ผู้ตรวจสอบภายในไม่ควรเป็นกรรมการ

ในคณะกรรมการใด ๆ ของหน่วยงานของรัฐหรือหน่วยงาน ในสังกัดอันมีผลกระทบต่อความเป็นอิสระในการปฏิบัติงานและการเสนอความเห็นในการตรวจสอบ

ข้อ ๘ ให้ผู้ตรวจสอบภายในมีสิทธิในการเข้าถึงข้อมูล บุคคล เอกสารหลักฐาน และทรัพย์สินต่าง ๆ เพื่อรับทราบข้อมูลที่จะเป็นประโยชน์ต่อการปฏิบัติงานตรวจสอบภายใน

ข้อ ๙ กรณีหน่วยงานของรัฐไม่สามารถปฏิบัติตามหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับ หน่วยงานของรัฐที่กระทรวงการคลังกำหนดได้ ให้ขอทำความตกลงกับกระทรวงการคลัง

คณะกรรมการตรวจสอบ

ข้อ ๑๐ ให้คณะกรรมการเป็นผู้แต่งตั้งคณะกรรมการตรวจสอบ ประกอบด้วย ประธานกรรมการตรวจสอบหนึ่งคน กรรมการตรวจสอบไม่น้อยกว่าสองคนแต่ไม่เกินสี่คน และให้หัวหน้าหน่วยงานตรวจสอบภายในเป็นเลขานุการ

กรรมการตรวจสอบอย่างน้อยหนึ่งคนต้องเป็นกรรมการในคณะกรรมการหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการ

ให้คณะกรรมการกำหนดวาระการดำรงตำแหน่งของกรรมการตรวจสอบ โดยการแต่งตั้งกรรมการตรวจสอบควรกำหนดวาระการดำรงตำแหน่งให้เหมาะสมกับบริบทของหน่วยงานของรัฐ ทั้งนี้ ไม่ควรเกินคราวละสี่ปี ในการพิจารณาต่ออายุการดำรงตำแหน่งของกรรมการตรวจสอบให้คณะกรรมการพิจารณา ความเหมาะสมเป็นรายคราว ทั้งนี้ ควรพิจารณาจำกัดจำนวนวาระการดำรงตำแหน่งของกรรมการตรวจสอบให้เหมาะสมตามหลักสากล

ข้อ ๑๑ คุณสมบัติของคณะกรรมการตรวจสอบ กรรมการตรวจสอบต้องเป็นผู้มีความรู้ความเข้าใจและมีประสบการณ์เพียงพอที่จะทำหน้าที่ในฐานะกรรมการตรวจสอบด้วยความเป็นอิสระและเที่ยงธรรม และสามารถอุทิศเวลาในการปฏิบัติหน้าที่ โดยคณะกรรมการตรวจสอบ ต้องประกอบด้วย

(๑) กรรมการตรวจสอบซึ่งมีความรู้ความสามารถที่จำเป็นต่อการปฏิบัติงานของคณะกรรมการตรวจสอบ โดยคณะกรรมการควรพิจารณาและกำหนดความรู้ความสามารถที่จำเป็นของคณะกรรมการตรวจสอบ (List of Competencies) เพื่อให้คณะกรรมการตรวจสอบที่ได้รับการแต่งตั้งสามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ ทั้งนี้ คณะกรรมการตรวจสอบองค์รวมควรมีความรู้ที่เพียงพอเกี่ยวกับ

- ลักษณะการดำเนินงานของหน่วยงานของรัฐ
- การเงินและการบัญชี
- การบริหารจัดการความเสี่ยง และการควบคุมภายใน
- การตรวจสอบภายใน
- กฎหมาย ระเบียบ หลักเกณฑ์ ข้อบังคับ ที่เกี่ยวของกับหน่วยงานของรัฐ

(๒) กรรมการตรวจสอบอย่างน้อยหนึ่งคนต้องมีความรู้ความเชี่ยวชาญ และมีประสบการณ์ด้านการเงินการบัญชีหรือด้านการตรวจสอบภายใน

(๓) กรรมการตรวจสอบต้องสามารถอุทิศเวลาในการปฏิบัติหน้าที่ โดยคณะกรรมการอาจพิจารณาความเหมาะสมของจำนวนคณะกรรมการตรวจสอบที่กรรมการตรวจสอบสามารถดำรงตำแหน่งในคณะกรรมการตรวจสอบของหน่วยงานอื่นได้เพื่อให้การปฏิบัติหน้าที่กรรมการตรวจสอบเป็นไปอย่างมีประสิทธิภาพ

ข้อ ๑๒ คณะกรรมการตรวจสอบต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) ไม่เป็นข้าราชการ พนักงาน ลูกจ้าง ที่ปรึกษา ผู้ที่ได้รับเงินเดือน ค่าจ้างหรือค่าตอบแทนประจำ และไม่เป็นผู้มีส่วนร่วมในการบริหารงานของหน่วยงานของรัฐนั้น โดยให้รวมถึงผู้ที่

โอนย้าย ลาออก เกษียณอายุ หรือพ้นสภาพจากหน่วยงานของรัฐที่เคยสังกัด ภายในระยะเวลาสองปีก่อนวันที่ได้รับการแต่งตั้งเป็นคณะกรรมการตรวจสอบ

(๒) ไม่เป็นผู้มีความขัดแย้งทางผลประโยชน์กับหน่วยงานของรัฐนั้น ทั้งนี้ ไม่ว่าในขณะดำรงตำแหน่งหรือภายในระยะเวลาหนึ่งปีก่อนวันที่ได้รับแต่งตั้งเป็นคณะกรรมการตรวจสอบ

(๓) ไม่เป็นบุพการี ผู้สืบสันดาน หรือคู่สมรสของคณะกรรมการ หัวหน้าหน่วยงานของรัฐ หัวหน้าหน่วยงานตรวจสอบภายใน หรือผู้ตรวจสอบภายในของหน่วยงานของรัฐนั้น

ข้อ ๑๓ คณะกรรมการตรวจสอบมีหน้าที่และความรับผิดชอบ ดังนี้

(๑) จัดทำกฎบัตรของคณะกรรมการตรวจสอบให้สอดคล้องกับขอบเขตความรับผิดชอบในการดำเนินงานของหน่วยงานของรัฐ โดยต้องได้รับความเห็นชอบจากคณะกรรมการ และมีการสอบทานความเหมาะสมของกฎบัตรดังกล่าวอย่างน้อยปีละหนึ่งครั้ง

(๒) สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายใน กระบวนการบริหารจัดการความเสี่ยงและกระบวนการกำกับดูแลที่ดี รวมถึงระบบบริหารจัดการความเสี่ยง ด้านการทุจริตของหน่วยงานของรัฐและระบบการรับแจ้งเบาะแส

(๓) สอบทานให้หน่วยงานของรัฐมีการรายงานการเงินอย่างถูกต้องและน่าเชื่อถือ

(๔) สอบทานการดำเนินงานของหน่วยงานของรัฐให้ถูกต้องตามกฎหมาย ระเบียบและข้อบังคับ หรือมติคณะรัฐมนตรีที่เกี่ยวของกับการดำเนินงาน รวมทั้งข้อกำหนดอื่นของหน่วยงานของรัฐ

(๕) กำกับดูแลระบบงานตรวจสอบภายในของหน่วยงานของรัฐ ให้มีความเป็นอิสระเพื่อพัฒนาการปฏิบัติงานในหน้าที่

(๖) พิจารณารายการที่เกี่ยวโยงกันหรือรายการที่อาจมีความขัดแย้งทางผลประโยชน์หรือมีโอกาสเกิดการทุจริตที่อาจมีผลกระทบต่อการปฏิบัติงานของหน่วยงานของรัฐ

(๗) ให้ข้อเสนอแนะการพิจารณาแต่งตั้ง โยกย้าย ถอดถอน เลื่อนขั้น เลื่อนตำแหน่ง และประเมินผลงานของหัวหน้าหน่วยงานตรวจสอบภายในต่อคณะกรรมการ ทั้งนี้ หน่วยงานของรัฐอาจกำหนดให้หัวหน้าหน่วยงานของรัฐมีส่วนร่วมในการพิจารณาด้วยก็ได้

(๘) ประชุมหารือร่วมกับสำนักงานการตรวจเงินแผ่นดินหรือผู้สอบบัญชีที่สำนักงานการตรวจเงินแผ่นดินเห็นชอบเกี่ยวกับผลการตรวจสอบและเรื่องอื่น ๆ และอาจเสนอแนะให้สอบทาน หรือตรวจสอบรายการใดที่เห็นว่าจำเป็น รวมถึงเสนอค่าตอบแทนของผู้สอบบัญชีต่อคณะกรรมการ

(๙) รายงานผลการดำเนินงานของคณะกรรมการตรวจสอบอย่างน้อยปีละหนึ่งครั้ง ประกอบด้วย การรายงานต่อคณะกรรมการและการรายงานต่อบุคคลภายนอก ทั้งนี้ การรายงานต่อบุคคลภายนอกให้รายงานในรายงานประจำปีของหน่วยงานของรัฐหรือเผยแพร่ทางเว็บไซต์ของหน่วยงานของรัฐ โดยประธานกรรมการ ตรวจสอบเป็นผู้ลงนามในรายงานดังกล่าว และต้องมีเนื้อหาอย่างน้อย ดังนี้

ก. ความเห็นของคณะกรรมการตรวจสอบเกี่ยวกับการบริหารจัดการความเสี่ยงและการบริหารจัดการความเสี่ยงด้านการทุจริตของหน่วยงานของรัฐ

ข. ความเห็นของคณะกรรมการตรวจสอบเกี่ยวกับการควบคุมภายในด้านการเงิน

ค. จำนวนครั้งในการจัดประชุมของคณะกรรมการตรวจสอบ และการเขาร่วมประชุมของกรรมการตรวจสอบแต่ละราย

(๑๐) ประเมินผลการดำเนินงาน ปัญหาและอุปสรรคของหน่วยงานตรวจสอบภายใน รวมทั้งเสนอแนะแนวทางการพัฒนาระบบการตรวจสอบภายในและศักยภาพของผู้ตรวจสอบภายในของหน่วยงาน ตรวจสอบภายในอย่างน้อยปีละ ๑ ครั้งต่อคณะกรรมการ

(๑๑) ปฏิบัติงานอื่นใดตามที่กฎหมายกำหนดหรือคณะกรรมการมอบหมายหน่วยงานของรัฐสามารถกำหนดหน้าที่และความรับผิดชอบของคณะกรรมการตรวจสอบเพิ่มเติมจากวรรคหนึ่งได้

ข้อ ๑๔ คณะกรรมการตรวจสอบควรมีการประชุมและการประเมินผล ดังนี้

(๑) การประชุมของคณะกรรมการตรวจสอบควรกำหนดไม่น้อยกว่า ๔ ครั้งต่อปี โดยองค์ประชุมและการลงมติที่ประชุมให้เป็นไปตามที่ให้ไว้ในกฎบัตรของคณะกรรมการตรวจสอบที่ผ่านความเห็นชอบจากคณะกรรมการของหน่วยงานของรัฐ และคณะกรรมการตรวจสอบควรมีการประชุมร่วมกับผู้บริหารของหน่วยงานของรัฐ ผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกอย่างน้อยปีละหนึ่งครั้ง

(๒) การประเมินผลการปฏิบัติงานของคณะกรรมการตรวจสอบต้องดำเนินการอย่างน้อยปีละหนึ่งครั้ง ประกอบด้วย การประเมินผลการปฏิบัติงานของคณะกรรมการตรวจสอบในภาพรวม และการประเมินผลการปฏิบัติงานกรรมการตรวจสอบรายบุคคล

ข้อ ๑๕ ค่าตอบแทนของคณะกรรมการตรวจสอบให้เป็นไปตามอัตราที่ระเบียบหรือข้อบังคับหรือคำสั่งหรือประกาศที่หน่วยงานของรัฐกำหนดไว้หรือตามมติคณะรัฐมนตรีหรือมติคณะกรรมการหรือมติที่ประชุมถือหุ้นกำหนด การจ่ายค่าตอบแทนตามวรรคหนึ่งที่หน่วยงานของรัฐได้ดำเนินการอยู่ในวันก่อนวันที่หลักเกณฑ์นี้ใช้บังคับให้ถือว่าเป็นการจ่ายค่าตอบแทนตามหลักเกณฑ์นี้

ข้อ ๑๖ ให้หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐรับผิดชอบตรวจสอบหน่วยรับตรวจดังนี้

(๑) หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ ตามข้อ (๑) ให้รับผิดชอบตรวจสอบ ดังนี้

(๑.๑) หน่วยงานตรวจสอบภายในระดับกระทรวง รับผิดชอบตรวจสอบการปฏิบัติงานของส่วนราชการในสังกัดกระทรวง ในกรณีที่ตรวจสอบงาน/โครงการของส่วนราชการในสังกัดของกระทรวงนอกเหนือจากงานของสำนักงานปลัดกระทรวงจะต้องเป็นการตรวจสอบและประเมินผลการดำเนินงานตามแผนงาน งาน/โครงการที่มีความสำคัญต่อผลสำเร็จของนโยบายกระทรวง และเป็นงาน/โครงการที่ได้รับนโยบาย ให้ติดตามกำกับดูแลเป็นกรณีพิเศษ โดยให้ประสานแผนการตรวจสอบกับส่วนราชการนั้น ๆ ด้วย

(๑.๒) หน่วยงานตรวจสอบภายในระดับกรม รับผิดชอบตรวจสอบราชการบริหารส่วนกลาง ที่มีสำนักงานตั้งอยู่ในส่วนกลาง ส่วนภูมิภาคหรือต่างประเทศ ในกรณีที่มีความจำเป็นหรือสมควร หัวหน้าส่วนราชการ อาจมอบหมายให้หน่วยงาน ตรวจสอบภายในระดับกรม ตรวจสอบส่วนราชการในสังกัดราชการบริหารส่วนภูมิภาคได้

(๑.๓) หน่วยงานตรวจสอบภายในระดับจังหวัด รับผิดชอบตรวจสอบราชการบริหารส่วนภูมิภาค ในกรณีที่ส่วนราชการในส่วนกลาง มีหน่วยงานตั้งอยู่ในส่วนภูมิภาค หัวหน้าส่วนราชการ ในส่วนกลาง อาจมอบอำนาจให้ผู้ว่าราชการจังหวัดดำเนินการแทนตามระเบียบว่าด้วยการบริหารงบประมาณ ระเบียบว่าด้วยการบริหารราชการแผ่นดิน กฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กฎหมายว่าด้วยการเงินหรือระเบียบอื่น ๆ ของทางราชการ โดยให้ผู้ตรวจสอบภายในตามข้อ (๑.๓) เป็นผู้รับผิดชอบตรวจสอบเฉพาะในส่วนที่ผู้ว่าราชการจังหวัดได้รับมอบอำนาจให้ดำเนินการแทน

(๒) หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ ตามข้อ (๒) – (๗) ให้รับผิดชอบตรวจสอบ การปฏิบัติงานของหน่วยงานของรัฐนั้น

ข้อ ๑๗ ให้หน่วยงานตรวจสอบภายในของหน่วยงานของรัฐมีหน้าที่และความรับผิดชอบดังนี้

(๑) กำหนดเป้าหมาย ทิศทาง ภารกิจงานตรวจสอบภายใน เพื่อสนับสนุนการบริหารงานและการดำเนินงานด้านต่าง ๆ ของหน่วยงานขององค์กร โดยให้สอดคล้องกับนโยบายของหน่วยงาน หัวหน้าส่วนราชการ และคณะกรรมการตรวจสอบ หรือคณะกรรมการอื่นใดที่ปฏิบัติงานในลักษณะเดียวกัน โดยคำนึงถึงการกำกับดูแลที่ดี ความมีประสิทธิภาพของกิจกรรมการบริหารความเสี่ยงและความเพียงพอของการควบคุมภายในของหน่วยงานของรัฐด้วย

(๒) กำหนดกฎบัตรไว้เป็นลายลักษณ์อักษรและเสนอหัวหน้าหน่วยงานของรัฐก่อนเสนอคณะกรรมการตรวจสอบ เพื่อพิจารณาให้ความเห็นชอบและเผยแพร่หน่วยรับตรวจทราบ รวมทั้งมีการสอบทานความเหมาะสมของกฎบัตรอย่างน้อยปีละหนึ่งครั้ง

(๓) จัดให้มีการประกันและปรับปรุงคุณภาพงานตรวจสอบภายในทั้งภายในและภายนอกตามรูปแบบและวิธีการที่กรมบัญชีกลางกำหนด

(๔) จัดทำและเสนอแผนการตรวจสอบประจำปีต่อหัวหน้าหน่วยงานของรัฐก่อนเสนอคณะกรรมการตรวจสอบ เพื่อพิจารณาอนุมัติภายในเดือนสุดท้ายของปีงบประมาณหรือปีปฏิทินแล้วแต่กรณี ในกรณีที่หน่วยงานตรวจสอบภายในวางแผนการตรวจสอบที่มีระยะเวลาตั้งแต่หนึ่งปีขึ้นไป ให้นำมาใช้ประกอบการพิจารณาอนุมัติแผนการตรวจสอบประจำปีด้วย

(๔.๑) กรณีหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐ ตามข้อ (๑) หน่วยงาน ตรวจสอบภายในระดับกระทรวง ตรวจสอบส่วนราชการในสังกัดกระทรวงที่นอกเหนือจากงานใน สำนักงาน ปลัดกระทรวงให้สำเนาแผนการตรวจสอบให้หัวหน้าส่วนราชการในสังกัดกระทรวงทราบด้วย

(๔.๒) กรณีหน่วยตรวจสอบภายในของหน่วยงานของรัฐตามข้อ (๑) หน่วยงานตรวจสอบภายใน ระดับกรม ตรวจสอบส่วนราชการในสังกัดราชการบริหารส่วนภูมิภาค ให้สำเนาแผนการตรวจสอบ ให้ผู้ว่าราชการจังหวัดทราบด้วย

(๕) ให้ปฏิบัติงานตรวจสอบให้เป็นไปตามแผนการตรวจสอบประจำปีที่ได้รับอนุมัติตามข้อ (๔)

(๖) รายงานผลการตรวจสอบต่อหัวหน้าหน่วยงานของรัฐและคณะกรรมการตรวจสอบดังต่อไปนี้

(๖.๑) รายงานผลการตรวจสอบตามแผนการตรวจสอบ ภายในเวลาอันสมควรและไม่เกินสองเดือนนับจากวันที่ดำเนินการตรวจสอบแล้วเสร็จ กรณีเรื่องที่ตรวจพบเป็นเรื่องที่จะมีผลเสียหายต่อทางราชการให้รายงานผลการตรวจสอบทันที

(๖.๑.๑) กรณีหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐตามข้อ (๑) หน่วยงานตรวจสอบภายในระดับกระทรวง ตรวจสอบส่วนราชการระดับกรมในสังกัดกระทรวง ให้ส่งสำเนารายงานผลการตรวจสอบให้หัวหน้าส่วนราชการนั้น ๆ ทราบด้วย

(๖.๑.๒) กรณีหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐตามข้อ (๑) หน่วยงานตรวจสอบภายในระดับกรม ตรวจสอบหน่วยงานของรัฐในส่วนภูมิภาค ให้ส่งสำเนารายงานผลการตรวจสอบให้ผู้ว่าราชการจังหวัดทราบด้วย

(๖.๑.๓) กรณีหน่วยงานตรวจสอบภายในของหน่วยงานของรัฐตามข้อ (๑) หน่วยงานตรวจสอบภายในระดับจังหวัด ตรวจสอบส่วนราชการส่วนภูมิภาคให้ส่งสำเนารายงานผลการตรวจสอบให้หัวหน้าส่วนราชการเจ้าสังกัดของหน่วยรับตรวจนั้นทราบด้วย

(๖.๒) รายงานเกี่ยวกับการบริหารจัดการความเสี่ยง และการควบคุมภายในอย่างน้อยปีละหนึ่งครั้ง ประกอบด้วย

(๖.๒.๑) ความเสี่ยงที่สำคัญเกี่ยวกับการดำเนินงานของหน่วยงานของรัฐ

(๖.๒.๒) ความเห็นเกี่ยวกับประสิทธิผลของการบริหารจัดการความเสี่ยง และการบริหารจัดการความเสี่ยงด้านการทุจริต รวมถึงระบบการร้องเรียน (Whistleblowing) ของหน่วยงานของรัฐ

(๖.๒.๓) ความเห็นเกี่ยวกับความเพียงพอและเหมาะสมของการควบคุมภายใน ด้านการเงิน และกระบวนการอื่นที่พิจารณาว่ามีความเสี่ยงสูงต่อการเกิดการทุจริต

(๖.๒.๔) สรุปภาพรวมของการฟ้องร้องต่อหน่วยงานของรัฐ คดีความต่าง ๆ และความรับผิดทางละเมิดของเจ้าหน้าที่ในทางแพ่ง โดยวิเคราะห์สาเหตุที่แท้จริง (Root cause analysis) และเสนอแนะแนวทาง การแก้ไขปัญหาในระยะยาว

(๗) ติดตามผลการตรวจสอบ เสนอแนะและให้คำปรึกษาแก่หน่วยรับตรวจเพื่อให้การปรับปรุง แก้ไขของหน่วยรับตรวจเป็นไปตามข้อเสนอแนะในรายงานผลการตรวจสอบ

(๘) ในกรณีมีความจำเป็นต้องอาศัยผู้เชี่ยวชาญมาร่วมปฏิบัติงานตรวจสอบให้เสนอขอบเขต และรายละเอียดของงาน คุณสมบัติของผู้รับจ้าง ระยะเวลาดำเนินการ และผลงานที่คาดหวังจากผู้รับจ้าง รวมทั้งขอเสนอโครงการของผู้รับจ้าง ให้หัวหน้าหน่วยงานของรัฐพิจารณาอนุมัติให้ว่าจ้างผู้เชี่ยวชาญต่อไป

(๙) ปฏิบัติงานในการให้คำปรึกษาแก่หัวหน้าหน่วยงานของรัฐ หน่วยรับตรวจและผู้ที่เกี่ยวข้อง

(๑๐) ประสานงานกับผู้สอบบัญชี คณะกรรมการตรวจสอบหรือคณะกรรมการอื่นที่ปฏิบัติงาน เช่นเดียวกันและหน่วยงานต่าง ๆ ที่เกี่ยวข้อง เพื่อให้เกิดความมั่นใจว่าขอบเขตของงานตรวจสอบครอบคลุม เรื่องที่สำคัญอย่างเหมาะสมและลดการปฏิบัติงานที่ซ้ำซ้อนกัน

(๑๑) ปฏิบัติงานอื่นที่เกี่ยวของกับการตรวจสอบภายใน ตามที่ได้รับมอบหมายจากคณะกรรมการตรวจสอบและหัวหน้าหน่วยงานของรัฐ

ข้อ ๑๘ ขอบเขตงานของการตรวจสอบภายในให้ครอบคลุมถึง การตรวจสอบ วิเคราะห์ รวมทั้งการประเมินความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน และการบริหารความเสี่ยงของหน่วยงานของรัฐ ซึ่งรวมถึง

(๑) ประเมินความมีประสิทธิภาพและประสิทธิผลของการดำเนินงานในหน้าที่ของหน่วยรับตรวจ เสนอแนะการปรับปรุงการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างต่อเนื่อง

(๒) สอบทานระบบการปฏิบัติงานตามกฎหมาย ระเบียบ และข้อบังคับหรือมติคณะรัฐมนตรีที่เกี่ยวข้องกับการดำเนินงาน รวมทั้งข้อกำหนดอื่นของหน่วยงานของรัฐ

(๓) สอบทานความถูกต้องและเชื่อถือได้ของข้อมูลการดำเนินงานและการเงินการคลัง

(๔) ตรวจสอบระบบการดูแลรักษา และความปลอดภัยของทรัพย์สินของหน่วยรับตรวจให้มีความเหมาะสมกับประเภทของทรัพย์สินนั้น

(๕) วิเคราะห์และประเมินความมีประสิทธิภาพ ประหยัดและคุ้มค่าในการใช้ทรัพยากร

ข้อ ๑๙ ให้ผู้ตรวจสอบภายในปฏิบัติงานตรวจสอบให้เป็นไปตามมาตรฐานการตรวจสอบภายใน สำหรับหน่วยงานของรัฐ กรณีที่ไม่ได้กำหนดไว้ให้ถือปฏิบัติตามมาตรฐานสากล

ข้อ ๒๐ ให้ผู้ตรวจสอบภายในปฏิบัติตนให้เป็นไปตามจรรยาบรรณการตรวจสอบภายในสำหรับหน่วยงาน ของรัฐตามที่แนบท้ายหลักเกณฑ์ปฏิบัตินี้

หน่วยรับตรวจ

ข้อ ๒๑ ให้หน่วยรับตรวจ มีหน้าที่และความรับผิดชอบ ดังนี้

(๑) อำนวยความสะดวกและให้ความร่วมมือแก่ผู้ตรวจสอบภายใน

(๒) จัดเตรียมเอกสารหลักฐานที่เกี่ยวกับการดำเนินงาน รวมถึงข้อมูลที่เกี่ยวข้องให้ครบถ้วน สมบูรณ์ พร้อมที่จะตรวจสอบได้

(๓) จัดทำบัญชีและจัดเก็บเอกสารประกอบรายการบัญชีพร้อมที่จะให้ผู้ตรวจสอบภายในตรวจสอบได้

(๔) จัดให้มีระบบการเก็บเอกสารในการปฏิบัติงานที่เหมาะสมและครบถ้วน

(๕) ชี้แจงและตอบข้อซักถามต่าง ๆ พร้อมทั้งหาข้อมูลเพิ่มเติมให้แก่ผู้ตรวจสอบภายใน

(๖) ปฏิบัติตามข้อทักท้วง และข้อเสนอแนะของผู้ตรวจสอบภายในในเรื่องต่าง ๆ ที่หัวหน้าหน่วยงานของรัฐสั่งให้ปฏิบัติ กรณีที่เจ้าหน้าที่ของหน่วยรับตรวจกระทำการโดยจงใจไม่ปฏิบัติ หรือละเลยต่อการปฏิบัติหน้าที่ตามวรรคหนึ่งให้ผู้ตรวจสอบภายในรายงานหัวหน้าหน่วยงานของรัฐพิจารณาสั่งการตามควรแก่กรณี

บทเฉพาะกาล

ข้อ ๒๒ หน่วยงานของรัฐที่มีโครงสร้างองค์กรในรูปแบบของคณะกรรมการและยังไม่มีคณะกรรมการตรวจสอบ ให้ขึ้นตรงต่อหัวหน้าหน่วยงานของรัฐไปพลางก่อน และให้จัดให้มีคณะกรรมการตรวจสอบ ภายในระยะเวลาสามปีนับแต่วันที่หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์การปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ ใช้บังคับตามรูปแบบที่กระทรวงการคลังกำหนด

ข้อ ๒๓ บรรดาการตรวจสอบภายในที่อยู่ระหว่างการดำเนินการก่อนวันที่หลักเกณฑ์ปฏิบัตินี้ ใช้บังคับ ให้ดำเนินการต่อไปตามระเบียบกระทรวงมหาดไทยว่าด้วยการตรวจสอบภายในขององค์กรปกครองส่วนท้องถิ่น พ.ศ. ๒๕๔๕ ระเบียบกระทรวงการคลังว่าด้วยการตรวจสอบภายในของส่วนราชการ พ.ศ. ๒๕๕๑ ระเบียบกระทรวงกลาโหมว่าด้วยการตรวจสอบภายใน พ.ศ. ๒๕๕๓ และระเบียบกระทรวงการคลังว่าด้วย คณะกรรมการตรวจสอบและหน่วยตรวจสอบภายในของรัฐวิสาหกิจ พ.ศ. ๒๕๕๕ จนกว่าจะแล้วเสร็จภายใน หนึ่งปีนับแต่วันที่หลักเกณฑ์ปฏิบัตินี้ใช้บังคับ

ข้อ ๒๔ หน่วยงานของรัฐตามข้อ (๖) องค์กรปกครองส่วนท้องถิ่นที่ยังไม่มีการตรวจสอบภายใน ให้จัดให้มีการตรวจสอบภายใน ภายในระยะเวลาสามปีนับแต่วันที่หลักเกณฑ์นี้ใช้บังคับ

๑.๓ การกำหนดประเภทของงานตรวจสอบ

หนังสือกระทรวงการคลังได้กำหนดหลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒ เพื่อให้หน่วยงานของรัฐถือปฏิบัติและจัดให้มีการตรวจสอบภายในให้เป็นไปตามบทบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ โดยหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ ข้อ ๒ กำหนดให้กรมบัญชีกลางเป็นผู้กำหนดคู่มือหรือแนวทางปฏิบัติเกี่ยวกับการตรวจสอบภายในให้หน่วยงานของรัฐถือปฏิบัติ เพื่อให้การปฏิบัติงานของผู้ตรวจสอบภายในของหน่วยงานของรัฐเป็นไปตามนิยามของการตรวจสอบภายในจึงได้กำหนดประเภทของงานตรวจสอบภายใน ดังนี้

๑. งานบริการให้ความเชื่อมั่น (Assurance Services) หมายถึง การตรวจสอบหลักฐานต่าง ๆ อย่างเที่ยงธรรม เพื่อให้ได้มาซึ่งการประเมินผลอย่างอิสระในกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุมของหน่วยงานของรัฐ โดยตัวอย่างของงานบริการให้ความเชื่อมั่น เช่น

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) หมายถึง การตรวจสอบ การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หลักเกณฑ์ ประกาศ มติคณะรัฐมนตรี รวมถึงมาตรฐาน แนวปฏิบัติ และนโยบายที่กำหนดไว้

๑.๓ การตรวจสอบการดำเนินงาน (Performance Audit) หมายถึง การตรวจสอบความประหยัด ความมีประสิทธิผล ความมีประสิทธิภาพ และความคุ้มค่าของกิจกรรมที่ตรวจสอบ

๑.๔ การตรวจสอบอื่น ๆ หมายถึง การตรวจสอบอื่นนอกเหนือจากข้อ ๑.๑ – ๑.๓ เช่น การตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ โดยการประเมินความเสี่ยงและการควบคุม ภายในด้านเทคโนโลยีสารสนเทศ และการตรวจสอบพิเศษ (การตรวจสอบตามที่ได้รับมอบหมายเป็นกรณีพิเศษ) เป็นต้น

๒. งานบริการให้คำปรึกษา (Consulting Services) หมายถึง การบริการให้คำปรึกษาแนะนำและบริการอื่น ๆ ที่เกี่ยวข้อง ซึ่งลักษณะงานและขอบเขตของงานจะเป็นไปตามข้อตกลงที่ทำขึ้นร่วมกับผู้รับบริการ โดยมีจุดประสงค์เพื่อเพิ่มคุณค่าให้กับหน่วยงานของรัฐ และปรับปรุงกระบวนการการกำกับดูแล การบริหารความเสี่ยง และการควบคุมของหน่วยงานของรัฐให้ดีขึ้น โดยหน่วยงานตรวจสอบภายในจะต้องประเมินความเสี่ยงของหัวข้อของงานตรวจสอบทั้งหมด

๑.๔ พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูลหรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคลไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา ๘ ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้น

สำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

๑.๕ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และฉบับที่ ๒ (พ.ศ. ๒๕๕๖)

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอย่างน้อยต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

ข้อ ๒ หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๔ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕-๑๕

ข้อ ๕ ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗ ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘ ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙ ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐ ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึง

สารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๒ หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๓ หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๕ หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่าหรือเทียบเท่า

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

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๒ ให้ยกเลิกความในข้อ ๑๔ ของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และให้ใช้ความต่อไปนี้แทน

"ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น"

๒. วิธีการปฏิบัติงาน

ในการปฏิบัติงานของคู่มือการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ มีวิธีการปฏิบัติ ดังนี้

๒.๑ ผู้ตรวจสอบภายในใช้แผนการตรวจสอบภายในประจำปี

ผู้ตรวจสอบภายในใช้แผนการตรวจสอบภายในประจำปีงบประมาณตามที่ได้กำหนดขอบเขตการตรวจสอบไว้ในแผนการตรวจสอบภายในประจำปี

๒.๒ ผู้ตรวจสอบภายในเตรียมแนวทางการตรวจสอบ (Engagement Plan)

ผู้ตรวจสอบภายในเตรียมแนวทางการตรวจสอบ (Engagement Plan) เพื่อจัดทำกระดาษทำการในการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ โดยจัดทำเป็นแนวปฏิบัติเพื่อการตรวจสอบได้ ดังนี้

แนวทางการตรวจสอบ (Engagement Plan)

ตารางที่ ๑ แนวทางการตรวจสอบ (Engagement Plan)

ประเด็นการตรวจสอบ	วัตถุประสงค์
๑. การรักษาความมั่นคงปลอดภัยทางกายภาพ	เพื่อให้มั่นใจว่าการจัดทำนโยบายการรักษาความมั่นคงลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ
๒. แบบสำรวจภัยคุกคาม	เพื่อให้มั่นใจได้ว่าหน่วยงานมีแบบสำรวจภัยคุกคามเป็นการป้องกันเหตุการณ์ล่วงหน้าก่อนเกิดความเสียหายต่อหน่วยงาน
๓. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ.คอมพิวเตอร์	เพื่อให้มั่นใจว่าหน่วยงานได้ดำเนินการเพื่อเป็นการป้องกัน มิให้ผู้ใช้งานเข้าไปกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงาน
๔. การควบคุมการเข้าถึงระบบสารสนเทศ	เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.๓ แนวทางการตรวจสอบ (Engagement Plan)

ผู้ตรวจสอบภายในกำหนดรูปแบบกระดาษทำการในการตรวจสอบจากแนวทางการตรวจสอบ (Engagement Plan)

๒.๔ จัดทำหนังสือเข้าตรวจหน่วยรับตรวจ

ผู้ตรวจสอบภายในประสานงานกับหน่วยรับตรวจเพื่อกำหนดวัน เวลา ในการเข้าตรวจสอบ และจัดทำหนังสือเข้าตรวจหน่วยรับตรวจอย่างเป็นทางการ

๒.๕ ดำเนินการ (เปิดตรวจ) กับหน่วยรับตรวจ

ผู้ตรวจสอบภายในดำเนินการเปิดประชุมกับหน่วยรับตรวจ โดยการเปิดตรวจกับหน่วยรับตรวจนั้น เป็นการแจ้งถึงการเปิดตรวจอย่างเป็นทางการ ผู้ตรวจสอบภายในต้องชี้แจงถึงวัตถุประสงค์ในการเข้าตรวจสอบ ขอบเขตการตรวจสอบ ระยะเวลาที่จะดำเนินการตรวจสอบให้กับหน่วยรับตรวจได้รับทราบ

๒.๖ ดำเนินการตรวจสอบ

ผู้ตรวจสอบภายในดำเนินการตรวจสอบตามวัตถุประสงค์ ขอบเขต ระยะเวลา และประเด็นการตรวจสอบตามขอบเขตที่กำหนด

๒.๗ ดำเนินการบันทึกข้อมูลการตรวจสอบ

ผู้ตรวจสอบภายในดำเนินการบันทึกข้อมูลการตรวจสอบลงกระดาษทำการตามรูปแบบที่กำหนด

๒.๘ ดำเนินการวิเคราะห์ข้อมูลเพื่อสรุปผลการตรวจสอบ

ผู้ตรวจสอบภายในดำเนินการวิเคราะห์ข้อมูลจากการตรวจสอบ และจัดทำ (ร่าง) รายงานสรุปผลการตรวจสอบเสนอหัวหน้าหน่วยตรวจสอบภายในพิจารณา

๒.๙ รายงานสรุปผลการตรวจสอบเสนอหัวหน้าหน่วยตรวจสอบภายในพิจารณา

เมื่อผู้ตรวจสอบภายในดำเนินการตรวจสอบแล้วเสร็จสิ้น ผู้ตรวจสอบภายในต้องดำเนินการรวบรวมกระดาษทำการทั้งหมดมาวิเคราะห์ว่าสิ่งที่ตรวจสอบนั้นครอบคลุมในบริบทของขอบเขตการตรวจสอบ และนำไปวิเคราะห์ในแต่ละด้านว่า หน่วยรับตรวจควรปรับปรุงหรือพัฒนาตรงจุดใด และจัดทำบันทึก (ร่าง) รายงานสรุปผลการตรวจสอบเสนอหัวหน้าหน่วยตรวจสอบภายในพิจารณา

๒.๑๐ แจ้งรายงานผลการตรวจสอบให้หน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบ (ปิดตรวจ)

เมื่อผู้ตรวจสอบภายในรายงานสรุปผลการตรวจสอบเสนอหัวหน้าหน่วยตรวจสอบภายในพิจารณา แล้วพบว่ารายงานสรุปผลดังกล่าวมีความครบถ้วน สมบูรณ์ดีแล้ว ผู้ตรวจสอบภายในต้องดำเนินการแจ้งรายงานผลต่อหน่วยรับตรวจ เพื่อให้หน่วยรับตรวจยืนยันหรือทักท้วงในการรายงานผลของผู้ตรวจสอบภายใน

๒.๑๑ สรุปรายงานผลการตรวจสอบหลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบ

ผู้ตรวจสอบภายในดำเนินการแจ้งรายงานผลการตรวจสอบภายในเพื่อให้หน่วยรับตรวจยืนยันหรือทักท้วงการตรวจสอบ (ปิดตรวจ)

๒.๑๒ สรุปรายงานผลการตรวจสอบหลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบเสนอต่อหัวหน้าตรวจสอบภายในพิจารณา

เมื่อมีการยืนยันหรือทักท้วงจากหน่วยรับตรวจ ผู้ตรวจสอบภายในจะต้องพิจารณาการทักท้วงของหน่วยรับตรวจว่าเป็นความจริงหรือไม่ และหากการแสดงข้อมูลในการทักท้วงไม่แน่ชัด

ผู้ตรวจสอบภายในต้องลงพื้นที่เพื่อยืนยันหรือทักท้วงในการตรวจสอบอีกครั้ง เป็นการพิสูจน์ตัวตนที่แท้จริงของบันทึกข้อมูล

๒.๑๓ หัวหน้าหน่วยตรวจสอบภายในรายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบประจำเพื่อพิจารณาให้ความเห็นชอบ และให้หัวหน้าส่วนราชการพิจารณาสั่งการ

หากรายงานผลการตรวจสอบได้ข้อสรุปที่ได้รับการยืนยันถูกต้องกับหน่วยรับตรวจแล้วนั้น ผู้ตรวจสอบภายในต้องจัดทำรายงานผลการตรวจสอบฉบับสมบูรณ์เพื่อรายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบประจำเพื่อพิจารณาให้ความเห็นชอบ และให้หัวหน้าส่วนราชการพิจารณาสั่งการ โดยการรายงานผลการตรวจสอบดังกล่าวจะสรุปข้อเท็จจริงจากการตรวจสอบ ทั้งนี้ผู้ตรวจสอบภายในจะต้องให้ข้อเสนอแนะจากการตรวจสอบด้วย

๓. ข้อควรระวังในการปฏิบัติงาน

๓.๑ การดำเนินการตรวจสอบ

ผู้ตรวจสอบภายในจะต้องประเมินความพร้อมของทีมงาน และต้องสำรวจสภาพแวดล้อมของหน่วยรับตรวจในเบื้องต้น ผู้ตรวจสอบภายในต้องชี้แจงวัตถุประสงค์ ขอบเขต และระยะเวลาในการตรวจสอบให้กับหน่วยรับตรวจให้ชัดเจน เตรียมความพร้อมในเรื่องของกระดาษทำการจะต้องครอบคลุมกับวัตถุประสงค์และขอบเขตการเข้าตรวจสอบ และในขณะดำเนินการตรวจสอบไม่ควรเปิดเผยข้อมูลในการตรวจสอบให้กับหน่วยรับตรวจ เนื่องจากการเปิดเผยข้อมูลขณะดำเนินการตรวจนั้นผู้ตรวจสอบภายในอาจไม่ได้รับข้อมูลที่แท้จริงได้

๓.๒ ระยะเวลาในการตรวจสอบ

ผู้ตรวจสอบภายในพึงระวังเรื่องของระยะเวลาในการตรวจสอบ ซึ่งการตรวจสอบในแต่ละประเด็นมีความยากง่ายแตกต่างกัน หากประเด็นใดที่ผู้ตรวจสอบภายในเข้าถึงข้อมูลได้ยาก หรือต้องใช้ระยะเวลาในการตรวจสอบค่อนข้างนาน ผู้ตรวจสอบภายในต้องพิจารณาว่าประเด็นที่ตรวจสอบอยู่นั้นมีความเสี่ยงสูงหรือไม่เพียงใด หากมีความเสี่ยงสูงผู้ตรวจสอบภายในจะต้องจัดทำบันทึกข้อความขอเพิ่มระยะเวลาในการเข้าตรวจเฉพาะประเด็นได้และสามารถดำเนินการปรับแผนการตรวจสอบใหม่ตามความเหมาะสม

๓.๓ การรายงานผลการตรวจสอบ

ในการรายงานผลการตรวจสอบภายใน ผู้ตรวจสอบภายในจะต้องรายงานผลการตรวจสอบตามข้อเท็จจริงที่ตรวจพบ โดยอ้างอิงหลักการ แนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ผู้ตรวจสอบภายในไม่ควรรายงานผลการตรวจสอบที่นอกเหนือจากประเด็นที่ชี้แจงในเบื้องต้น แต่หากตรวจพบประเด็นที่นอกเหนือจากที่กำหนดไว้ในขอบเขตของการตรวจสอบหรือผู้ตรวจสอบภายในพิจารณาแล้วเห็นว่าเหตุการณ์หรือพฤติการณ์ดังกล่าวอาจส่งผลให้หน่วยรับตรวจหรือองค์กรได้รับความเสียหาย และจำเป็นต้องแก้ไขอย่างเร่งด่วน ให้ผู้ตรวจสอบภายในดำเนินการรายงานผลการตรวจสอบต่อหัวหน้าส่วนราชการทันทีโดยให้รายงานผลการตรวจสอบนอกเหนือจากการแผนการตรวจสอบ

๓.๔ การยืนยันหรือทักท้วงจากหน่วยรับตรวจ

หากมีการยืนยันหรือทักท้วงในการรายงานผลการตรวจสอบของผู้ตรวจสอบภายในผู้ตรวจสอบภายในจะต้องพิจารณาโดยละเอียดและรอบคอบ รวมไปถึงต้องลงพื้นที่เพื่อยืนยันสิ่งที่หน่วยรับตรวจทักท้วงในการตรวจสอบอีกครั้งเป็นการพิสูจน์ตัวตนที่แท้จริงของบันทึกข้อมูล หากข้อมูลของหน่วยรับตรวจเป็นจริงตามกล่าวอ้างให้ผู้ตรวจสอบภายในหักล้างข้อมูลในรายงานผลดังกล่าวด้วย

บทที่ ๔
เทคนิคการปฏิบัติงาน

๑. กิจกรรม/แผนการปฏิบัติงาน

การดำเนินงานเกี่ยวกับการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศนั้น ผู้ตรวจสอบภายในมีแนวทางการปฏิบัติงานอย่างชัดเจน ซึ่งการตรวจสอบในเรื่องดังกล่าวได้ถูกกำหนดไว้ในผังการปฏิบัติงาน (Flow Chart) หน่วยงานหรือผู้ตรวจสอบภายในสามารถนำผังการปฏิบัติงานดังกล่าวไปปฏิบัติงานด้านการตรวจสอบได้จริง โดยมีรายละเอียดในการปฏิบัติงาน ดังนี้

ตารางที่ ๒ กิจกรรม/แผนการปฏิบัติงาน

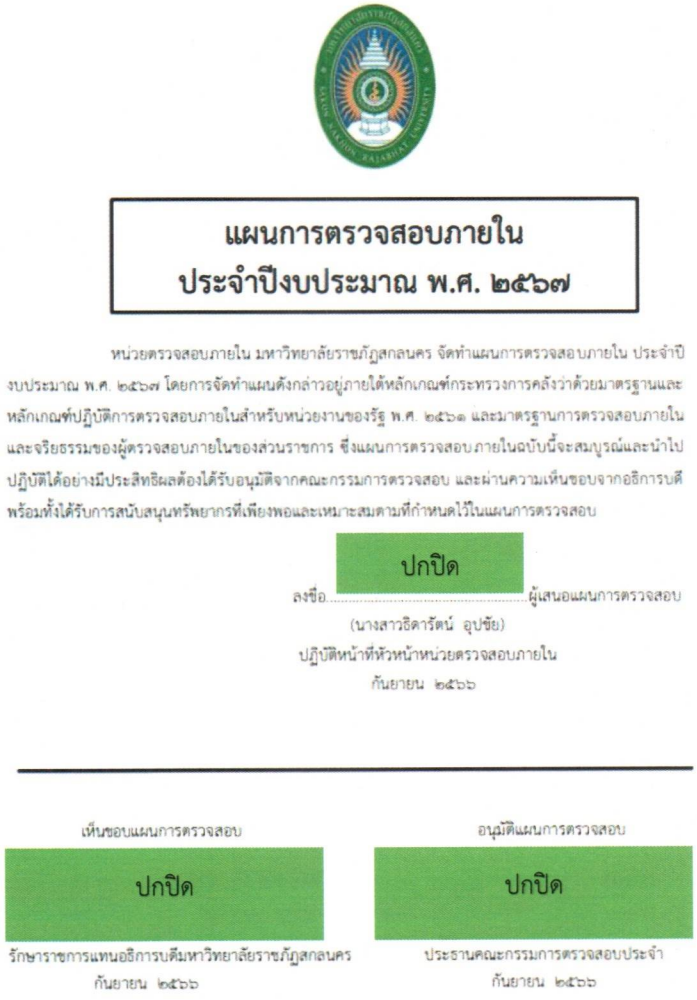
กิจกรรม	แผนการปฏิบัติงาน	ระยะเวลาในการตรวจสอบ							
		สัปดาห์ที่/เดือน.....				สัปดาห์ที่/เดือน.....			
		๑	๒	๓	๔	๑	๒	๓	๔
๑	แผนการตรวจสอบภายในประจำปี	ระบุในแผนการตรวจสอบภายในประจำปีงบประมาณ							
๒	แนวทางการตรวจสอบ (Engagement Plan)	←	→						
๓	ผู้ตรวจสอบภายในดำเนินการกำหนดรูปแบบกระดาษทำการ	←	→						
๔	ผู้ตรวจสอบภายในจัดทำหนังสือเข้าตรวจหน่วยรับตรวจ	←	→						
๕	ผู้ตรวจสอบภายในดำเนินการ (เปิดตรวจ) กับหน่วยรับตรวจ	←	→						
๖	ผู้ตรวจสอบภายในดำเนินการตรวจสอบ		←	→					
๗	ผู้ตรวจสอบภายในดำเนินการบันทึกข้อมูลการตรวจสอบ		←	→					
๘	ผู้ตรวจสอบภายในดำเนินการวิเคราะห์ข้อมูลเพื่อสรุปผลการตรวจสอบ			←	→				
๙	ผู้ตรวจสอบภายในรายงานสรุปผลการตรวจสอบเสนอหัวหน้าพิจารณา			←	→				
๑๐	ผู้ตรวจสอบภายในแจ้งรายงานผลการตรวจสอบให้หน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบ (ปิดตรวจ)					←	→		
๑๑	ผู้ตรวจสอบภายในสรุปรายงานผลการตรวจสอบ หลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบ					←	→		
๑๒	ผู้ตรวจสอบภายในสรุปรายงานผลการตรวจสอบหลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบ เสนอต่อหัวหน้าตรวจสอบภายในพิจารณา						←	→	
๑๓	หัวหน้าหน่วยตรวจสอบภายในรายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบประจำและให้หัวหน้าส่วนราชการพิจารณาสั่งการ								← →

๒. เทคนิคการปฏิบัติงาน

เทคนิคการปฏิบัติงานการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย ๑๓ ขั้นตอนหลัก โดยมีรายละเอียด ดังนี้

ขั้นตอนที่ ๑ แผนการตรวจสอบภายในประจำปี

หน่วยตรวจสอบภายใน มหาวิทยาลัยราชภัฏสกลนคร จะต้องจัดทำแผนการตรวจสอบภายในประจำปีงบประมาณ โดยการจัดทำแผนการตรวจสอบนั้นอยู่ภายใต้หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ มาตรฐานการตรวจสอบภายในและจริยธรรมของผู้ตรวจสอบภายในของส่วนราชการ แผนการตรวจสอบภายในประจำปีจะสมบูรณ์และนำไปปฏิบัติได้อย่างมีประสิทธิภาพ ประสิทธิผล จะต้องได้รับอนุมัติจากคณะกรรมการตรวจสอบประจำ และผ่านความเห็นชอบจากหัวหน้าส่วนราชการ เพื่อให้หน่วยรับตรวจเกิดความเชื่อมั่นในแผนการตรวจสอบภายในประจำปีดังกล่าว



แผนการตรวจสอบภายใน
ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

หน่วยตรวจสอบภายใน มหาวิทยาลัยราชภัฏสกลนคร จัดทำแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ โดยการจัดทำแผนดังกล่าวอยู่ภายใต้หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ และมาตรฐานการตรวจสอบภายในและจริยธรรมของผู้ตรวจสอบภายในของส่วนราชการ ซึ่งแผนการตรวจสอบภายในฉบับนี้จะสมบูรณ์และนำไปปฏิบัติได้อย่างมีประสิทธิผลต้องได้รับอนุมัติจากคณะกรรมการตรวจสอบ และผ่านความเห็นชอบจากอธิการบดี พร้อมทั้งได้รับการสนับสนุนทรัพยากรที่เพียงพอและเหมาะสมตามที่กำหนดไว้ในแผนการตรวจสอบ

ปกปิด

ลงชื่อ.....ผู้เสนอแผนการตรวจสอบ
(นางสาวธิดารัตน์ อุปชัย)
ปฏิบัติหน้าที่หัวหน้าหน่วยตรวจสอบภายใน
กันยายน ๒๕๖๖

เห็นชอบแผนการตรวจสอบ

ปกปิด

รักษาราชการแทนอธิการบดีมหาวิทยาลัยราชภัฏสกลนคร
กันยายน ๒๕๖๖

อนุมัติแผนการตรวจสอบ

ปกปิด

ประธานคณะกรรมการตรวจสอบประจำ
กันยายน ๒๕๖๖

ภาพที่ ๘ แสดงแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ขั้นตอนที่ ๒ แนวทางการตรวจสอบ (Engagement Plan)

ผู้ตรวจสอบภายในจะมีการจัดทำแผนการปฏิบัติงาน (Engagement Plan) และตรวจสอบในกิจกรรมที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน เพื่อเป็นกรอบในการปฏิบัติงานของหน่วยตรวจสอบภายใน ซึ่งแผนปฏิบัติงานต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานก่อนนำไปปฏิบัติงานจริง โดยมีรายละเอียด ดังนี้

๑. หน่วยรับตรวจ .....

๒. กิจกรรมที่ตรวจสอบ งานบริการให้ความเชื่อมั่น

๓. ประเด็นการตรวจสอบ การควบคุม การปฏิบัติตามการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔. วัตถุประสงค์ของการตรวจสอบ

เพื่อให้มั่นใจว่าหน่วยงานได้กำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีการประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และการควบคุมการปฏิบัติที่เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยการตรวจสอบดังกล่าวเป็นไปตามมาตรฐาน COBIT (Control Objectives for Information and related Technology) ทั้งนี้ รวมถึงการตรวจสอบการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ขอบเขตการตรวจสอบ

๑. ตรวจสอบตามกระดาษทำการ IT.A ๑ – IT.A ๘ (ตามเอกสารแนบท้าย)

๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย

แนวทางการปฏิบัติการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ (Engagement Plan)

ผู้ตรวจสอบภายในจะต้องออกแบบแนวทางการปฏิบัติงานหรือกระดาษทำการเพื่อเข้าตรวจสอบการปฏิบัติงานของหน่วยงานที่มีความเกี่ยวข้องกับการใช้ข้อมูลระบบสารสนเทศ โดยระบุแนวทางการปฏิบัติ ชื่อผู้ตรวจสอบรวมไปถึงการกำหนดแนวทางการปฏิบัติการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมระบุประเด็นการตรวจสอบ/วัตถุประสงค์ย่อย เกณฑ์การตรวจสอบ และวิธีการตรวจสอบ โดยสรุปเป็นรายละเอียดได้ดังนี้

ตารางที่ ๓ แนวทางการปฏิบัติการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ

แนวทางการปฏิบัติ	ชื่อผู้ตรวจสอบ
๑. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (นโยบาย/แนวปฏิบัติ)	๑. นางสาว..... ๒. นาย..... ๓. XX.....

แนวทางการปฏิบัติ	ชื่อผู้ตรวจสอบ
๒. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (การจัดแบ่งพื้นที่)	๑. นางสาว..... ๒. นาย..... ๓. XX.....
๓. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (การสำรองข้อมูล)	๑. นางสาว..... ๒. นาย..... ๓. XX.....
๔. แบบสำรวจภัยคุกคาม	๑. นางสาว..... ๒. นาย..... ๓. XX.....
๕. แบบการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ. คอมพิวเตอร์	๑. นางสาว..... ๒. นาย..... ๓. XX.....
๖. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบปฏิบัติการ)	๑. นางสาว..... ๒. นาย..... ๓. XX.....
๗. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบเครือข่าย)	๑. นางสาว..... ๒. นาย..... ๓. XX.....
๘. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบอินเทอร์เน็ต)	๑. นางสาว..... ๒. นาย..... ๓. XX.....

ตารางที่ ๔ การกำหนดแนวทางการปฏิบัติการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ

ประเด็นการตรวจสอบ/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
๑. การรักษาความมั่นคงปลอดภัยทางกายภาพ (นโยบาย/แนวปฏิบัติ) **วัตถุประสงค์** เพื่อให้มั่นใจว่าการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	๑. การควบคุมการเข้าถึงระบบ ๒. การใช้รหัสผ่าน (Password) ๓. การป้องกันไวรัสคอมพิวเตอร์ ๔. การจัดทำสำรองข้อมูลและการกู้คืนข้อมูล ๕. การจัดทำการป้องกันระบบไฟฟ้าขัดข้อง ๖. การตรวจสอบระบบเครือข่าย (Network) ๗. การบันทึกเพื่อตรวจสอบ (Audit Logs)	๑. ตรวจสอบหลักฐานที่แสดงว่ามีการควบคุมการเข้าถึงข้อมูลอุปกรณ์ในการประมวลผลข้อมูลทางกายภาพของหน่วยงานหรือไม่อย่างไร ๒. ตรวจสอบทานสิทธิการอนุญาต และการมอบอำนาจให้เป็นไปตามคำสั่งหรือการมอบหมายสั่งการในการใช้รหัสผ่าน ๓. ตรวจสอบการติดตั้งและการใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันไวรัส การ Update	กระดาษทำการ (IT ๑)

ประเด็นการตรวจสอบ/วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
		ระบบปฏิบัติการ ๔. ตรวจสอบขั้นตอนการจัดระบบซอฟต์แวร์ ข้อมูลต่าง ๆ ในระบบ ระยะเวลาการกู้คืนข้อมูลของระบบ ๕. ตรวจสอบอัตราความคงที่ของกระแสไฟ ระบบสำรองไฟ เพื่อป้องกันระบบไฟฟ้าขัดข้อง ๖. ตรวจสอบการแบ่งแยกระบบเครือข่าย Firewall ข้อมูลการบุกรุกผ่านระบบเครือข่าย Network ๗. ตรวจสอบข้อกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย	
๒. การรักษาความมั่นคงปลอดภัยทางกายภาพ (การจัดแบ่งพื้นที่) **วัตถุประสงค์** เพื่อให้มั่นใจว่าการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	๑. มีการจัดแบ่งพื้นที่ ๒. มีข้อกำหนดของห้องควบคุมระบบ (Computer Room) ๓. ข้อกำหนดการเข้าไปในพื้นที่ควบคุม ๔. ข้อกำหนดการเข้าไปในพื้นที่จำกัดการเข้าถึง	๑. ตรวจสอบการจัดแบ่งพื้นที่ห้องควบคุมระบบ ๒. ตรวจสอบการแยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป ๓. ตรวจสอบข้อกำหนดการเข้าไปในพื้นที่ควบคุม ๔. ตรวจสอบข้อกำหนดการเข้าไปในพื้นที่จำกัดการเข้าถึง	กระดาษทำการ (IT ๒)
๓. การรักษาความมั่นคงปลอดภัยทางกายภาพ (การสำรองข้อมูล) **วัตถุประสงค์** เพื่อให้มั่นใจว่าการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	๑. แนวปฏิบัติการสำรองข้อมูล ๒. แผนเตรียมความพร้อมกรณีฉุกเฉิน	๑. ตรวจสอบการจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย ๒. ตรวจสอบขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง	กระดาษทำการ (IT ๓)

ประเด็นการตรวจสอบ/วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
๔. แบบสำรวจภัยคุกคาม **วัตถุประสงค์** เพื่อให้มั่นใจได้ว่าหน่วยงานมีแบบสำรวจภัยคุกคามเป็นการป้องกันเหตุการณ์ล่วงหน้าก่อนเกิดความเสียหายต่อหน่วยงาน	๑. เหตุการณ์/ปัจจัยการคุกคาม ๒. ผลกระทบ ๓. ความถี่ ๔. ผลการประเมิน	ตรวจสอบการประเมินภัยคุกคามด้านสารสนเทศของหน่วยงาน	กระดาษทำการ (IT ๔)
๕. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ. คอมพิวเตอร์ **วัตถุประสงค์** เพื่อให้มั่นใจว่าหน่วยงานได้ดำเนินการเพื่อเป็นการป้องกันมิให้ผู้ใช้งานเข้าไปกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงาน	๑. การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน ๒. การเปิดเผยวิธีการที่จะเข้าไปยังระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน ๓. การเข้าข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน ๔. การดักข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่งของระบบคอมพิวเตอร์ ๕. การทำลาย แก้ไข เปลี่ยนแปลงเพิ่มเติมข้อมูลผู้อื่น ๖. การระงับ ชะลอ ขัดขวาง หรือรบกวนระบบคอมพิวเตอร์ ของผู้อื่น ๗. การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ที่มีการปกปิดหรือปลอมแปลงแหล่งที่มาของข้อมูลเพื่อรบกวนข้อมูลการทำงานของผู้อื่น ๘. ก่อให้เกิดความเสียหายแก่ประชาชน เศรษฐกิจความมั่นคงของประเทศชาติ ๙. การจำหน่ายหรือเผยแพร่ชุดคำสั่ง ๑๐. การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบ	มีการประกาศแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ. คอมพิวเตอร์ เช่น - มีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน - มีการประกาศไม่ให้ผู้ใช้บริการมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น - มีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งข้อมูล คอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน - ฝ่าย IT มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ ๙๐ วัน	กระดาษทำการ (IT ๕)

ประเด็นการตรวจสอบ/วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
	คอมพิวเตอร์ ๑๑. การเผยแพร่ข้อมูลความผิดที่เกี่ยวกับการก่อการร้ายเข้าสู่ระบบคอมพิวเตอร์ ๑๒. การนำเข้าหรือเผยแพร่เนื้อหาอันไม่เหมาะสม ๑๓. การเผยแพร่ภาพตัดต่อที่เป็นการหมิ่นประมาทเข้าสู่ระบบคอมพิวเตอร์ ๑๔. ผู้ให้บริการการเข้าถึงอินเทอร์เน็ตไม่มีการเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ ๙๐ วัน		
๖. การควบคุมการเข้าถึงระบบสารสนเทศ (ระบบปฏิบัติการ) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. การควบคุมการเข้าถึงระบบปฏิบัติการ ๒. การใช้รหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์	๑. ตรวจสอบการควบคุมการเข้าถึงระบบปฏิบัติการ ๒. ตรวจสอบการใช้รหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์ การเปลี่ยนรหัสผ่าน (Password) ของหน่วยงานทุก ๓-๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล	กระดาษทำการ (IT ๖)
๗. การควบคุมการเข้าถึงระบบสารสนเทศ (ระบบเครือข่าย) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	การป้องกันจากโปรแกรมประสงค์ร้าย	๑. ตรวจสอบการป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งตรวจสอบการปรับปรุงการป้องกันให้ทันสมัยอยู่เสมอ ๒. ตรวจสอบแนวปฏิบัติการป้องกันการทำการปิดหรือยกเลิกโปรแกรมประสงค์ร้าย	กระดาษทำการ (IT ๗)

ประเด็นการตรวจสอบ/วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
๘. การควบคุมการเข้าถึงระบบสารสนเทศ (ระบบอินเทอร์เน็ต) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	การใช้งานระบบอินเทอร์เน็ต	๑. ตรวจสอบการเชื่อมต่อระบบคอมพิวเตอร์ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้ ๒. ตรวจสอบการเข้าถึงข้อมูลตามสิทธิ์ที่ได้รับ ๓. ตรวจสอบการปกปิดความลับของข้อมูลที่ยังไม่ได้รับอนุญาตอย่างเป็นทางการ ๔. ตรวจสอบแนวปฏิบัติการละเมิดลิขสิทธิ์ด้านสารสนเทศหรือทรัพย์สินทางปัญญา ๕. ตรวจสอบการให้บริการเมื่อผู้ใช้งานใช้งานเสร็จสิ้นแล้ว	กระดาษทำการ (IT ๘)

ขั้นตอนที่ ๓ การกำหนดรูปแบบกระดาษทำการ

ผู้ตรวจสอบภายในมีการกำหนดรูปแบบกระดาษทำการตามขอบเขตการตรวจสอบเพื่อใช้ในการดำเนินการตรวจสอบให้เป็นไปตามวัตถุประสงค์และขอบเขตการตรวจสอบ โดยผู้ตรวจสอบภายในจัดทำแผนการปฏิบัติงานมีรายละเอียด ดังนี้

๑. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (นโยบาย/แนวปฏิบัติ) รหัสกระดาษทำการ (IT ๑)

๒. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (การจัดแบ่งพื้นที่) รหัสกระดาษทำการ (IT ๒)

๓. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (การสำรองข้อมูล) รหัสกระดาษทำการ (IT ๓)

๔. แบบสำรวจภัยคุกคาม รหัสกระดาษทำการ (IT ๔)

๕. แบบการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ. คอมพิวเตอร์ รหัสกระดาษทำการ (IT ๕)

๖. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบปฏิบัติการ) รหัสกระดาษทำการ (IT ๖)

๗. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบเครือข่าย) รหัสกระดาษทำการ (IT ๗)

๘. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบอินเทอร์เน็ต) รหัสกระดาษทำการ (IT ๘)

๑. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (นโยบาย/แนวปฏิบัติ) (IT ๑)

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
๑	แนวปฏิบัติการควบคุมการเข้าถึงระบบ					
	๑.๑ หน่วยงานมีข้อกำหนดในการให้ผู้ใช้งานได้เข้าถึงระบบ โดยกำหนด (Username) และ (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงานในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์หรือไม่					
	๑.๒ หน่วยงานได้มีข้อกำหนดให้ผู้ใช้บริการไม่ควรอนุญาตให้ผู้ใช้บริการอื่นใช้ชื่อผู้ใช้ (Username) และ (Password) ของตนเองเพื่อเข้าถึงการใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน					
	๑.๓ หน่วยงานมีการกำหนดระยะเวลาเมื่อไม่มีการใช้งานโดยการต้องทำการล็อคหน้าจอภาพหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานใหม่					
	๑.๔ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการจะต้องลงบันทึกเข้าใช้ (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว					
๒	แนวปฏิบัติการใช้รหัสผ่าน (Password)					
	๒.๑ รหัสผ่าน (Password) หน่วยงานมีข้อกำหนดให้ผู้รับบริการกำหนดรหัสผ่านที่มีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษสัญลักษณ์ต่าง ๆ					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๒.๒ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการ ไม่ควรกำหนดรหัสผ่าน (Password) จากชื่อหรือชื่อสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์					
	๒.๓ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการทำการเปลี่ยนรหัสผ่านเพื่อใช้งานเครื่องคอมพิวเตอร์ทุก ๓ - ๖ เดือน หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล					
	๒.๔ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการต้องเก็บรักษารหัสผ่านสำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา					
๓	แนวปฏิบัติการป้องกันไวรัสคอมพิวเตอร์					
	๓.๑ หน่วยงานมีข้อกำหนดในการติดตั้งเครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงาน โดยต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันไวรัส รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ					
	๓.๒ หน่วยงานมีข้อกำหนดให้ผู้ใช้งานควรทำการ (Update) ระบบปฏิบัติการเว็บบราวเซอร์และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ					
	๓.๓ ห้ามมิให้ผู้ใช้งาน ทำการปิดหรือเปลี่ยนระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๓.๔ หน่วยงานมีข้อกำหนดให้ผู้ใช้งานตรวจสอบเครื่องคอมพิวเตอร์ว่า หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์ ห้ามมิให้ผู้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของไวรัสไปยังเครื่องคอมพิวเตอร์อื่น ๆ					
๔	แนวการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูล					
	๔.๑ หน่วยงานมีการขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบ					
	๔.๒ หน่วยงานมีการขั้นตอนการปฏิบัติเพื่อตรวจสอบความถูกต้องหลังจากทำการสำรองข้อมูล					
	๔.๓ หน่วยงานมีการขั้นตอนการปฏิบัติการจัดการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบ					
	๔.๔ หน่วยงานมีการขั้นตอนการปฏิบัติเพื่อทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอและมีการตรวจสอบความถูกต้องหลังจากทำการกู้คืนข้อมูล					
	๔.๕ หน่วยงานมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม					
๕	แนวการปฏิบัติการจัดทำการป้องกันระบบไฟฟ้าขัดข้อง					
	๕.๑ หน่วยงานมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ					
	๕.๒ หน่วยงานมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์เพื่อให้การดำเนินงานมีความต่อเนื่อง					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
๖	การตรวจสอบระบบเครือข่าย (Network)					
	๖.๑ หน่วยงานมีการแบ่งแยกระบบเครือข่ายของระบบให้ออกจากระบบเครือข่ายของโรงงาน					
	๖.๒ หน่วยงานมีระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น ระหว่างเครือข่ายภายนอกในกับเครือข่ายภายนอก					
	๖.๓ หน่วยงานมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ					
	๖.๓.๑ หน่วยงานมีระบบหรือจุดสังเกตตรวจสอบ เมื่อเกิดเหตุการณ์ผิดปกติในการพยายามในการบุกรุกผ่านระบบเครือข่าย					
	๖.๓.๒ หน่วยงานมีจุดสังเกต หากพบการใช้งานในลักษณะที่ผิดปกติ					
	๖.๓.๓ หน่วยงานมีวิธีการกำจัดการใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง					
	๖.๔ หน่วยงานมีแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ					
	๖.๕ หน่วยงานมีการตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่าความคงที่ต่าง ๆ เกี่ยวกับการรักษาความปลอดภัยเป็นต้นและต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical Disconnect) และจุดเชื่อมต่อ (Disable Port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่ายออกจากระบบเครือข่ายโดยสิ้นเชิง					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๖.๖ ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ Remote Access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้ Modem หน่วยงานมีข้อกำหนดในการได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด เช่น การใช้ระบบ Call Back การควบคุมการเปิดปิด Modem หรือการตรวจสอบตัวตนจริง และสิทธิของผู้ใช้งานการบันทึกรายละเอียดการใช้งาน และในกรณี Dial Out ก็ควรตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อออกจากระบบเครือข่ายภายใน เป็นต้น รวมทั้งต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว					
	๖.๗ หน่วยงานมีการกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าความคงที่ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่าความคงที่ และแจ้งให้บุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง					
	๖.๘ หน่วยงานมีการกำหนดใช้เครื่องมือต่าง ๆ เพื่อตรวจเช็คระบบเครือข่าย และควรได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น					
๗	การบันทึกเพื่อตรวจสอบ (Audit Logs)					
	๗.๑ หน่วยงานมีการกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องการบุกรุก เช่น บันทึกการเข้าออกระบบบันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้ และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๗.๒ หน่วยงานมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ					
	๗.๓ หน่วยงานมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกต่าง ๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น					
	๗.๔ หน่วยงานมีการกำหนดให้มีการบันทึกรายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่าง ๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้					
	๗.๔.๑. ผู้ปฏิบัติงาน					
	๗.๔.๒. เวลาปฏิบัติงาน					
	๗.๔.๓. รายละเอียดการปฏิบัติงาน					
	๗.๔.๔. ปัญหาที่เกิดขึ้นและการแก้ไข					
	๗.๔.๕. สถานะของระบบ					
	๗.๔.๖. ผู้ตรวจทานการปฏิบัติงาน					

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

.....

.....

.....

.....

..... ผู้ตรวจสอบ ..... ผู้สอบทาน

(.....) (.....)

๒. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (การจัดแบ่งพื้นที่) (IT ๒)

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
๑	การจัดแบ่งพื้นที่					
	๑.๑ หน่วยงานมีการแบ่งพื้นที่ห้องควบคุมระบบ แบ่งเป็น ๒ พื้นที่ ได้แก่ ๑. พื้นที่ควบคุม คือ พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ ๒. พื้นที่จำกัดการเข้าถึง คือ พื้นที่จำกัดการเข้าถึงเป็นห้องที่มีระบบ คอมพิวเตอร์และเครือข่ายติดตั้งอยู่					
๒	ข้อกำหนดของห้องควบคุมระบบ (Computer Room)					
	๒.๑ หน่วยงานมีการแยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้ เช่น Router, Switch และ Server ต่าง ๆ					
	๒.๒ หน่วยงานมีการจัดเก็บอุปกรณ์ต่าง ๆ ในตู้ Rack ที่เหมาะสม เพื่อสะดวกในการบำรุงรักษา					
	๒.๓ หน่วยงานมีการกำหนดจุดพื้นที่ไม่ควรวางอุปกรณ์ต่าง ๆ ในตำแหน่งใกล้ประตูหน้าต่าง เพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น					
	๒.๔ หน่วยงานมีการจัดวางสายสัญญาณและสายไฟฟ้า และมีการจัดเก็บสายให้เรียบร้อยเพื่อป้องกันการเดินสะดุด					
	๒.๕ หน่วยงานมีการติดประกาศการบำรุงรักษาอุปกรณ์ เช่น ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด					
	๒.๖ หน่วยงานมีการติดตั้งระบบรักษาความปลอดภัยในห้อง เช่น กล้อง CCTV เป็นต้น					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๒.๗ หน่วยงานมีมาตรการหรือแนวปฏิบัติระบบป้องกันอัคคีภัย					
	๒.๘ หน่วยงานมีระบบไฟฟ้าสำรองเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้าสำรอง					
	๒.๙ หน่วยงานมีระบบป้องกันไฟฟ้าจากฟ้าผ่า					
	๒.๑๐ หน่วยงานมีระบบปรับอากาศแบบควบคุมอุณหภูมิ (๕๐-๘๐°F) และความชื้น (๒๐- ๘๐%)					
	๒.๑๑ หน่วยงานมีการติดตั้งฉนวนกันไฟไหม้ ที่ฝ้าเพดานและผนังกำแพง					
๓	ข้อกำหนดการเข้าไปในพื้นที่ควบคุม					
	๓.๑ หน่วยงานมีข้อกำหนดไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้น เจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงานหรือบุคคลที่ผู้บริหารหน่วยงานนำเข้าเยี่ยมชม					
	๓.๒ หน่วยงานมีข้อกำหนดให้บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงาน หรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากหัวหน้างาน IT และจะต้องมีเจ้าหน้าที่นำเยี่ยมชมอยู่ด้วยตลอดเวลา					
	๓.๓ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากฝ่าย IT					
	๓.๔ หน่วยงานมีข้อกำหนดให้เจ้าหน้าที่หรือบุคคลภายนอกไม่นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
๔	ข้อกำหนดการเข้าไปในพื้นที่จำกัดการเข้าถึง					
	๔.๑ หน่วยงานมีข้อกำหนดไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ					
	๔.๒ หรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้บริหารฝ่าย IT และต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย ๑ คนเข้าไปร่วมปฏิบัติงาน และประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง					
	๔.๓ หรือบุคคลที่ได้รับคำสั่งจากผู้บริหารให้เข้าปฏิบัติหน้าที่ในพื้นที่ควบคุมซึ่งต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย ๑ คนเข้าไปร่วม ปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง					
	๔.๔ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้น ที่					
	๔.๕ ไม่อนุญาตให้มีการเข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง					
	๔.๖ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อ ทรัพย์สินจะอนุญาตให้เข้าไปในพื้นที่จำกัด การเข้าถึงได้โดยได้รับความเห็นชอบจากผู้บริหารฝ่าย IT					

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

..... ผู้ตรวจสอบ ..... ผู้สอบทาน

(.....) (.....)

๓. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (การสำรองข้อมูล) (IT ๓)

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
๑	แนวปฏิบัติการสำรองข้อมูล					
	๑.๑ หน่วยงานมีการจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับ ความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย					
	๑.๒ หน่วยงานมีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศโดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ					
	๑.๓ หน่วยงานมีการจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลโดยมีการพิมพ์ชื่อบนสื่อ เก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่ สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอRouter, Switch และ Server ต่าง ๆ					
	๑.๔ หน่วยงานมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม					
๒	แผนเตรียมความพร้อมกรณีฉุกเฉิน					
	๒.๑ หน่วยงานมีการประเมินสถานการณ์ความเสี่ยง					
	๒.๒ หน่วยงานมีแผนการสำรองข้อมูลและระบบงาน (Back Up)					
	๒.๓ หน่วยงานมีแผนการป้องกันไวรัสคอมพิวเตอร์					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๒.๔ หน่วยงานมีแผนการป้องกันและแก้ไขปัญหาที่เกิดจากไฟฟ้าดับ					
	๒.๕ หน่วยงานมีแผนการป้องกันความเสี่ยงจากไฟไหม้					
	๒.๖ หน่วยงานมีแผนการป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ (Hacker)					
	๒.๗ หน่วยงานมีแผนการป้องกันอุปกรณ์เครื่องแม่ข่ายชำรุด					
	๒.๘ หน่วยงานมีแผนการป้องกันความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่					

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

.....

.....

.....

.....

..... ผู้ตรวจสอบ ..... ผู้สอบทาน

(.....) (.....)

กระดาษทำการ (IT๔)

๔. แบบสำรวจภัยคุกคาม (IT ๔)

สาเหตุ/ปัจจัย	ความเสี่ยง	ระดับผลกระทบ	ระดับความถี่	ประเมินสถานการณ์			คะแนน	ผลการประเมิน
				ทันที	เฝ้าระวัง	ปลอดภัย		

ผลกระทบ

ระดับ ๕ ผลกระทบทั้งองค์กร และแก้ไขยาก
ระดับ ๔ ผลกระทบทั้งองค์กร แต่สามารถแก้ไขได้
ระดับ ๓ ผลกระทบเฉพาะส่วนงานแต่แก้ไขยาก
ระดับ ๒ ผลกระทบเฉพาะส่วนงานแต่แก้ไขได้
ระดับ ๑ ผลกระทบเล็กน้อยเฉพาะเครื่องหรือบุคคล
ระดับ ๐ ไม่คิด

ความถี่

ระดับ ๕ เกิดขึ้นทุกเดือน
ระดับ ๔ ๑-๖ เดือน
ระดับ ๓ ๖-๒ ปี
ระดับ ๒ ๒-๑๐ ปี
ระดับ ๑ ๑๐ ปีขึ้นไป
ระดับ ๐ ไม่คิดว่าจะเกิด

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

.....

.....

.....

.....

..... ผู้ตรวจสอบ
(.....)

..... ผู้สอบทาน
(.....)

๕. แบบการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ. คอมพิวเตอร์ (IT ๕)

ข้อ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง	เหตุการณ์ที่เคยเกิดขึ้น
			มี	ไม่มี			
๑	การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการ เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน					
๒	การเปิดเผยวิธีการที่จะเข้าไปยังระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกันของผู้อื่นที่มีการป้องกัน	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบ โดยมีมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น					
๓	การเข้าข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน					
๔	การดักข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่งของระบบคอมพิวเตอร์	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์					

ข้อ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง	เหตุการณ์ที่เคยเกิดขึ้น
			มี	ไม่มี			
๕	การทำลาย แก้ไข เปลี่ยนแปลงเพิ่มเติม ข้อมูลผู้อื่น	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูล คอมพิวเตอร์ของผู้อื่นโดยมิชอบ					
๖	การระงับ ชะลอ ขัดขวาง หรือรบกวน ระบบคอมพิวเตอร์ของผู้อื่น	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้					
๗	การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ที่มีการปกปิดหรือปลอมแปลงแหล่งที่มาของข้อมูลเพื่อรบกวนข้อมูลการทำงานของผู้อื่น	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข					
๘	ก่อให้เกิดความเสียหายแก่ประชาชน เศรษฐกิจความมั่นคงของประเทศชาติ	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศชาติ ความปลอดภัยสาธารณะความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ					

ข้อ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง	เหตุการณ์ที่เคยเกิดขึ้น
			มี	ไม่มี			
๙	การจำหน่ายหรือเผยแพร่ชุดคำสั่ง	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการจำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม พ.ร.บ. คอมพิวเตอร์					
๑๐	การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบคอมพิวเตอร์	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรหรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน					
๑๑	การเผยแพร่ข้อมูลความผิดที่เกี่ยวกับการก่อการร้ายเข้าสู่ระบบคอมพิวเตอร์	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น					
๑๒	การนำเข้าหรือเผยแพร่เนื้อหาอันไม่เหมาะสม	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน					
๑๓	การเผยแพร่ข้อมูลความผิดที่เกี่ยวกับการก่อการร้ายเข้าสู่ระบบคอมพิวเตอร์	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการ					

ข้อ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง	เหตุการณ์ที่เคยเกิดขึ้น
			มี	ไม่มี			
		ก่อการร้ายตามประมวลกฎหมายอาญา					
๑๔	การเผยแพร่ภาพตัดต่อที่เป็นการหมิ่นประมาทเข้าสู่ระบบคอมพิวเตอร์	หน่วยงานมีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการใด ๆ ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง					
๑๕	ผู้ให้บริการการเข้าถึงอินเทอร์เน็ต ไม่มีการเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ ๙๐ วัน	หน่วยงานมีฝ่าย IT ในการปฏิบัติหน้าที่จัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ ๙๐ วัน					

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

.....

.....

.....

..... ผู้ตรวจสอบ

(.....)

..... ผู้สอบทาน

(.....)

๖. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบปฏิบัติการ) (IT ๖)

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
๑	แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ (Windows, UNIX)					
	๑.๑ หน่วยงานมีการกำหนดชื่อผู้ใช้บริการ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ (Windows, UNIX) ของเครื่องคอมพิวเตอร์ของหน่วยงาน					
	๑.๒ ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เข้าสู่ระบบ (Windows, UNIX) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน					
	๑.๓ เมื่อไม่มีการในงานต้องทำการล็อกหน้าจอภาพ หลังจากนั้นเมื่อต้องการใช้งานผู้รับบริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานใหม่					
	๑.๔ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการ (Windows, UNIX) จะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว					
๒	แนวปฏิบัติการใช้รหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์					
	๒.๑ หน่วยงานมีการกำหนดรหัสผ่าน (Password) ควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือ ตัวพิมพ์ใหญ่ตัวอักขระพิเศษและสัญลักษณ์ต่าง ๆ ด้วย					
	๒.๒ หน่วยงานมีข้อกำหนดในการกำหนดรหัสผ่าน โดยไม่ให้ผู้รับบริการกำหนดรหัสผ่านจากชื่อหรือชื่อสกุลของผู้ใช้บริการชื่อบุคคลในครอบครัวบุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๒.๓ หน่วยงานมีข้อกำหนดให้ผู้รับบริการทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ ของหน่วยงานทุก ๓ - ๖ เดือนหรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล					
	๒.๔ หน่วยงานมีข้อกำหนดผู้ใช้บริการจะต้องเก็บรักษารหัสผ่าน สำหรับการใช้งาน เครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคลและจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบ โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา					

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

.....

.....

.....

.....

..... ผู้ตรวจสอบ

(.....)

..... ผู้สอบทาน

(.....)

กระดาษทำการ (IT๗)

๗. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบเครือข่าย) (IT ๗)

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
๑	แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)					
	๑.๑ หน่วยงานมีข้อกำหนดให้เครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ					
	๑.๒ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการควรทำการอัพเดทระบบปฏิบัติการเว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ					
	๑.๓ หน่วยงานมีข้อกำหนดห้ามมิให้ผู้ใช้บริการทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)					
	๑.๔ หากผู้ใช้บริการพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware) หน่วยงานมีข้อกำหนดห้ามมิให้ผู้ใช้บริการเชื่อต่อเครื่องคอมพิวเตอร์ เข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้ายไปยังเครื่องคอมพิวเตอร์อื่น ๆ					
	๑.๕ ก่อนการใช้งานสื่อบันทึกพกพาหน่วยงานมีการตรวจสอบเพื่อป้องกันและกำจัด (Malware)					
	๑.๖ ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ (Information) ผ่านทางระบบเครือข่ายหน่วยงานมีการกำหนดให้ผู้ใช้บริการต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๑.๗ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการควรทำการตรวจสอบไฟล์ก่อนทำการเปิด โดยใช้โปรแกรมป้องกัน (Malware) เป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น					

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

.....

..... ผู้ตรวจสอบ ..... ผู้สอบทาน

(.....) (.....)

๘. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบอินเทอร์เน็ต) (IT ๘)

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
๑	แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)					
	๑.๑ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้ เท่านั้น และห้ามผู้ใช้บริการทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้น แต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการ IT เป็นลายลักษณ์อักษร					
	๑.๒ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคง ต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงานเป็นต้น					
	๑.๓ หน่วยงานมีข้อกำหนดห้ามผู้ใช้บริการเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต					
	๑.๔ หน่วยงานมีข้อกำหนดให้ผู้ใช้บริการต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการอัพเดทโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา					

ข้อ	แนวนโยบาย/แนวปฏิบัติ	ผลการตรวจสอบ		ผู้รับผิดชอบ	ระบบควบคุมในปัจจุบัน	เอกสารที่เกี่ยวข้อง
		มี	ไม่มี			
	๑.๕ หน่วยงานมีข้อกำหนดในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน					
	๑.๖ หน่วยงานมีการมีข้อกำหนดโดยในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ					
	๑.๗ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว หน่วยงานได้กำหนดให้ผู้ใช้บริการทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ					

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

..... ผู้ตรวจสอบ ..... ผู้สอบทาน

(.....) (.....)

ขั้นตอนที่ ๔ จัดทำหนังสือเข้าตรวจหน่วยรับตรวจ

ผู้ตรวจสอบภายในจะต้องสรุปสาระสำคัญในการเข้าตรวจสอบร่วมกับทีมงาน เพื่อให้เข้าใจในแนวทางการตรวจสอบ แนวปฏิบัติ และการสรุปผลการตรวจสอบร่วมกัน ผู้ตรวจสอบภายในต้องดำเนินการจัดทำหนังสือบันทึกข้อความเข้าตรวจกับหน่วยรับตรวจ โดยหัวหน้าส่วนราชการเป็นผู้ลงนามในการอนุมัติเข้าตรวจสอบหน่วยรับตรวจ ผู้ตรวจสอบภายในจะต้องประสานงานกับหน่วยรับตรวจเพื่อกำหนดวัน เวลา สถานที่รับรอง รายชื่อผู้บริหาร และเจ้าหน้าที่ ที่จะเข้าร่วมรับตรวจสอบให้ชัดเจน

ในกรณีที่ผู้ตรวจสอบภายในและหน่วยรับตรวจได้ดำเนินการนัดหมายวันเวลาเสร็จสิ้นแล้ว แต่เกิดเหตุในกรณีที่ไม่สามารถดำเนินตามการนัดหมายได้นั้น ให้หน่วยงานที่ไม่สามารถร่วมดำเนินการจัดทำหนังสือบันทึกข้อความถึงหัวหน้าส่วนราชการเพื่อชี้แจงถึงเหตุการณ์ดังกล่าว ทั้งนี้ให้ระบุระยะเวลาในครั้งถัดไปให้ชัดเจน

บันทึกข้อความ

ส่วนราชการ XXX

ที่ XXX / XXX **วันที่** XXX

เรื่อง การเข้าตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕XX

เรียน .....**หน่วยรับตรวจ**.....

เพื่อให้เป็นไปตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕XX หน่วยตรวจสอบภายในจะดำเนินการตรวจสอบ.....**หน่วยรับตรวจ**..... (ด้าน Information Technology Audit) โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าหน่วยงานได้กำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์และการควบคุมการปฏิบัติที่เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยการตรวจสอบดังกล่าวเป็นไปตามมาตรฐาน COBIT (Control Objectives for Information and related Technology) ทั้งนี้รวมถึงการตรวจสอบการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล โดยมีกำหนดการเข้าตรวจสอบ ดังนี้

วันที่ ..... เปิดตรวจ.....**หน่วยรับตรวจ**.....และพบผู้บริหารบุคลากร เจ้าหน้าที่
วันที่ ..... ดำเนินการตรวจสอบเอกสารหลักฐานด้านสารสนเทศ
วันที่ ..... ปิดตรวจ.....**หน่วยรับตรวจ**.....

ขอบเขตการตรวจสอบ และการขอเอกสารหลักฐานในการตรวจสอบด้านสารสนเทศ มีรายละเอียดดังนี้

๑. ตรวจสอบตามกระดาษทำการ IT๑ – IT๘ (ตามเอกสารแนบท้าย)
๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ.....**หน่วยรับตรวจ**.....
๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ.....**หน่วยรับตรวจ**.....
๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย

โดยมีบุคลากรหน่วยตรวจสอบภายใน ที่ดำเนินการตรวจสอบ ดังนี้

๑. ..... ตำแหน่ง หัวหน้าหน่วยตรวจสอบภายใน
๒. ..... ตำแหน่ง นักตรวจสอบภายในปฏิบัติการ
๓. ..... ตำแหน่ง นักตรวจสอบภายใน

ดังนั้น เพื่อให้การตรวจสอบเป็นไปด้วยความเรียบร้อย บรรลุวัตถุประสงค์ตามแผน จึงขอให้ท่านแจ้งผู้บริหาร เจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งมอบหมายเจ้าหน้าที่ผู้รับผิดชอบอำนวยความสะดวก ในการให้ข้อมูลการดำเนินงาน จนกว่าการดำเนินการในเรื่องดังกล่าวจะแล้วเสร็จ

จึงเรียนมาเพื่อโปรดทราบและดำเนินการ

(.....**หัวหน้าส่วนราชการนาม**.....)
ตำแหน่ง.....

ภาพที่ ๙ แสดงการจัดทำบันทึกข้อความการเข้าตรวจสอบภายใน

บันทึกข้อความ

ส่วนราชการ หน่วยตรวจสอบภายใน มหาวิทยาลัยราชภัฏสกลนคร IP Phone. ๑๖๕

ที่ อว ๐๖๒๑ / ๔๐๗ **วันที่** ๑ พฤษภาคม ๒๕๖๖

เรื่อง การเข้าตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

เรียน ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

เพื่อให้เป็นไปตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ หน่วยตรวจสอบภายในจะดำเนินการตรวจสอบสำนักวิทยบริการและเทคโนโลยีสารสนเทศ (ด้าน Information Technology Audit) โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าหน่วยงานได้กำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์และการควบคุมการปฏิบัติที่เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยการตรวจสอบดังกล่าวเป็นไปตามมาตรฐาน COBIT (Control Objectives for Information and related Technology) ทั้งนี้รวมถึงการตรวจสอบการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล โดยมีกำหนดการเข้าตรวจสอบ ดังนี้

วันที่ ๑๕ พ.ค. ๖๖ เปิดตรวจสำนักวิทยบริการฯ และพบผู้บริหารบุคลากร เจ้าหน้าที่
วันที่ ๑๕ – ๓๑ พ.ค. ๖๖ ดำเนินการตรวจสอบเอกสารหลักฐานด้านเทคโนโลยีสารสนเทศ
วันที่ ๙ มิ.ย. ๖๖ ปิดตรวจสำนักวิทยบริการฯ

ขอบเขตการตรวจสอบ และการขอเอกสารหลักฐานในการตรวจสอบด้านเทคโนโลยีสารสนเทศ รายละเอียดดังนี้

๑. ตรวจสอบตามกระดาษทำการ IT.A ๑ – IT.A ๘ (ตามเอกสารแนบท้าย)
๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย
๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย
๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย

โดยมีบุคลากรหน่วยตรวจสอบภายใน ที่ดำเนินการตรวจสอบ ดังนี้

๑. นางสาวธิดารัตน์ อุปชัย ตำแหน่ง ปฏิบัติหน้าที่หัวหน้าหน่วยตรวจสอบภายใน
๒. นายพงศกร หาแก้ว ตำแหน่ง นักตรวจสอบภายในปฏิบัติการ
๓. นางสาวขวัญหทัย ใจสมุทร ตำแหน่ง นักตรวจสอบภายใน

ดังนั้น เพื่อให้การตรวจสอบเป็นไปด้วยความเรียบร้อย บรรลุวัตถุประสงค์ตามแผน จึงขอให้ท่านแจ้งผู้บริหาร เจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งมอบหมายเจ้าหน้าที่ผู้รับผิดชอบอำนวยความสะดวก ในการให้ข้อมูลการดำเนินงาน จนกว่าการดำเนินการในเรื่องดังกล่าวจะแล้วเสร็จ

จึงเรียนมาเพื่อโปรดทราบและดำเนินการ

ปกปิด

(ผู้ช่วยศาสตราจารย์ชาคริต ชาญชิตปริชา)
รักษาราชการแทนอธิการบดีมหาวิทยาลัยราชภัฏสกลนคร

ภาพที่ ๑๐ แสดงตัวอย่างการจัดทำบันทึกข้อความการเข้าตรวจสอบภายใน

ขั้นตอนที่ ๕ ดำเนินการ (เปิดตรวจ) กับหน่วยรับตรวจ

ผู้ตรวจสอบภายในดำเนินการ (เปิดตรวจ) กับหน่วยรับตรวจ โดยผู้ตรวจสอบภายในจะต้องชี้แจงถึงวัตถุประสงค์ในการตรวจสอบ ขอบเขตการตรวจสอบ แนวปฏิบัติในการตรวจสอบ (Engagement Plan) ระยะเวลาการตรวจสอบ กระดาษทำการ เอกสารหลักฐานที่ใช้ประกอบการตรวจสอบ รวมไปถึงแนวทางการรายงานผลการตรวจสอบ

บันทึกการประชุมเปิดตรวจ

.....ชื่อหน่วยรับตรวจ..... ประจำปีงบประมาณ พ.ศ. ๒๕XX

หน่วยรับตรวจ .....XXXX.....

วันที่ .....XXXX..... **เวลา** .....XXXX.....

ณ ห้อง.....XXXX.....

ผู้รับตรวจ

๑. ..... ตำแหน่ง ผู้อำนวยการ .....หน่วยรับตรวจ.....

๒. ..... ตำแหน่ง รองผู้อำนวยการ.....หน่วยรับตรวจ.....

๓. ..... ตำแหน่ง รองผู้อำนวยการ.....หน่วยรับตรวจ.....

๔. ..... ตำแหน่ง หัวหน้าสำนักงาน.....หน่วยรับตรวจ.....

ผู้ตรวจสอบ

๑. ..... ตำแหน่ง หัวหน้าหน่วยตรวจสอบภายใน

๒. ..... ตำแหน่ง นักตรวจสอบภายในปฏิบัติการ

๓. ..... ตำแหน่ง นักตรวจสอบภายใน

วัตถุประสงค์ของการตรวจสอบ

เพื่อให้มั่นใจว่าหน่วยงานได้กำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีการประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และการควบคุมการปฏิบัติที่เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยการตรวจสอบดังกล่าวเป็นไปตามมาตรฐาน COBIT (Control Objectives for Information and related Technology) ทั้งนี้ รวมถึงการตรวจสอบการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ขอบเขตการตรวจสอบ

๑. ตรวจสอบตามกระดาษทำการ IT๑ – IT๘ (ตามเอกสารแนบท้าย)

๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ.....**หน่วยรับตรวจ**.....

๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ.....**หน่วยรับตรวจ**.....

๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของ.....**หน่วยรับตรวจ**.....

หน่วยตรวจสอบภายในจึงมีความจำเป็นเข้าตรวจสอบตามแผนการตรวจสอบประจำปี ซึ่งการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Technology Audit) นั้น เป็นไปตามพระราช บัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ (ฉบับที่ ๒) พ.ศ ๒๕๕๑ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ ๒๕๕๐ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติ ลิขสิทธิ์ พ.ศ. ๒๕๓๗ (ฉบับที่ ๒) พ.ศ. ๒๕๕๘ (ฉบับที่ ๓) พ.ศ.๒๕๕๘ (ฉบับที่ ๔) พ.ศ. ๒๕๖๑ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ ให้ บริการ พ.ศ. ๒๕๕๐ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ และแนวทางการใช้บริการคลาวด์ พ.ศ. ๒๕๖๒ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ทั้งนี้ หน่วยตรวจสอบภายใน จึงขอความร่วมมือ ผู้บริหาร เจ้าหน้าผู้รับผิดชอบดังกล่าวจัดเตรียมเอกสาร ข้อมูล และตอบข้อซักถามที่เกี่ยวข้องกับในการตรวจสอบ และขอขอบคุณท่านที่ให้ความร่วมมือกับการตรวจสอบภายในในครั้งนี้เป็นอย่างสูง

ลงชื่อ..... ลงชื่อ.....

( ) ( )

นักตรวจสอบภายใน นักตรวจสอบภายในปฏิบัติการ

ลงชื่อ.....

( )

หัวหน้าหน่วยตรวจสอบภายใน

ภาพที่ ๑๑ แสดงการดำเนินการบันทึกการประชุมเปิดตรวจกับหน่วยรับตรวจ

บันทึกการประชุมเปิดตรวจ
มหาวิทยาลัยราชภัฏสกลนคร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

หน่วยรับตรวจ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

วันที่ ๑ มิถุนายน พ.ศ. ๒๕๖๖ **เวลา** ๑๓.๓๐ – ๑๖.๐๐ น.

ณ ห้องประชุมสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ผู้รับตรวจ

๑. อาจารย์กรกช มาตะรัตน์	ตำแหน่ง	ผู้อำนวยการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
๓. ผู้ช่วยศาสตราจารย์วัชระ อักขระ	ตำแหน่ง	รองผู้อำนวยการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
๔. อาจารย์ ดร.ชายแดน มิ่งเมือง	ตำแหน่ง	รองผู้อำนวยการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
๕. อาจารย์นวรัตน์ เมืองเล็น	ตำแหน่ง	รองผู้อำนวยการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
๖. นางสาวอังคณา ศิริกุล	ตำแหน่ง	หัวหน้าสำนักงานผู้อำนวยการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ผู้ตรวจสอบ

๑. นางสาวธิดารัตน์ อุปชัย	ตำแหน่ง	ปฏิบัติหน้าที่หัวหน้าหน่วยตรวจสอบภายใน
๒. นายพงศกร หาแก้ว	ตำแหน่ง	นักตรวจสอบภายในปฏิบัติการ
๓. นางสาวขวัญหทัย ใจสมุทร	ตำแหน่ง	นักตรวจสอบภายใน

วัตถุประสงค์ของการตรวจสอบ

เพื่อให้มั่นใจว่าหน่วยงานได้กำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีการประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และการควบคุมการปฏิบัติที่เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยการตรวจสอบดังกล่าวเป็นไปตามมาตรฐาน COBIT (Control Objectives for Information and related Technology) ทั้งนี้ รวมถึงการตรวจสอบการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ขอบเขตการตรวจสอบ

๑. ตรวจสอบตามกระดาษทำการ IT.A ๑ – IT.A ๘ (ตามเอกสารแนบท้าย)
๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย
๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย
๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย

หน่วยตรวจสอบภายในจึงมีความจำเป็นเข้าตรวจสอบตามแผนการตรวจสอบประจำปี ซึ่งการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Technology Audit) นั้น เป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ (ฉบับที่ ๒) พ.ศ ๒๕๕๑ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ ๒๕๕๐ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติ ลิขสิทธิ์ พ.ศ. ๒๕๓๗ (ฉบับที่ ๒) พ.ศ. ๒๕๕๘ (ฉบับที่ ๓) พ.ศ.๒๕๕๘ (ฉบับที่ ๔) พ.ศ. ๒๕๖๑ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ และแนวทางการใช้บริการคลาวด์ พ.ศ. ๒๕๖๒ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ทั้งนี้ หน่วยตรวจสอบภายใน จึงขอความร่วมมือ ผู้บริหาร เจ้าหน้าผู้รับผิดชอบดังกล่าวจัดเตรียมเอกสารข้อมูลและตอบข้อซักถามที่เกี่ยวข้องกับในการตรวจสอบ และขอขอบคุณท่านที่ให้ความร่วมมือกับการตรวจสอบภายในในครั้งนี้เป็นอย่างสูง

ลงชื่อ..... ปกปิด
(นางสาวขวัญหทัย ใจสมุทร)
นักตรวจสอบภายใน

ลงชื่อ..... ปกปิด
(นายพงศกร หาแก้ว)
นักตรวจสอบภายในปฏิบัติการ

ลงชื่อ..... ปกปิด
(นางสาวธิดารัตน์ อุปชัย)
ปฏิบัติหน้าที่หัวหน้าหน่วยตรวจสอบภายใน

ภาพที่ ๑๒ แสดงตัวอย่างการดำเนินการบันทึกการประชุมเปิดตรวจกับหน่วยรับตรวจ

ขั้นตอนที่ ๖ ดำเนินการตรวจสอบ

ผู้ตรวจสอบภายในดำเนินการตรวจสอบตามแผนการปฏิบัติงาน (Engagement Plan) กับหน่วยรับตรวจหลังจากดำเนินการเปิดตรวจกับหน่วยรับตรวจเสร็จสิ้นแล้ว โดยผู้ตรวจสอบภายในใช้กระดาษทำการที่ได้กำหนดไว้ในแนวทางการปฏิบัติ (Engagement Plan) หากช่วงระหว่างผู้ตรวจสอบภายในดำเนินการตรวจสอบ ผู้ตรวจสอบภายในพบเหตุที่อาจก่อให้เกิดความเสียหายต่อหน่วยรับตรวจหรือองค์กร ผู้ตรวจสอบภายจะต้องบันทึกเหตุการณ์ที่ตรวจพบดังกล่าวลงกระดาษทำการทันที ทั้งนี้ ให้ระบุเหตุที่พบ สิ่งที่พบ ช่วงระยะเวลา บุคคลหรือเจ้าหน้าที่ตามสภาพแวดล้อม ณ ขณะนั้นที่อยู่ในช่วงเวลาดังกล่าว และให้ผู้ตรวจสอบภายในรีบรายงานผลการตรวจสอบต่อหัวหน้าส่วนราชการอย่างเร่งด่วน

ประเด็นการตรวจสอบ/วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
๑. การรักษาความมั่นคงปลอดภัยทางกายภาพ (นโยบาย/แนวปฏิบัติ) **วัตถุประสงค์** เพื่อให้มั่นใจว่าการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	๑. การควบคุมการเข้าถึงระบบ ๒. การใช้รหัสผ่าน (Password) ๓. การป้องกันไวรัสคอมพิวเตอร์ ๔. การจัดทำสำรองข้อมูลและการกู้คืนข้อมูล ๕. การจัดทำการป้องกันระบบไฟฟ้าขัดข้อง ๖. การตรวจสอบระบบเครือข่าย (Network) ๗. การบันทึกเพื่อตรวจสอบ (Audit Logs)	๑. ตรวจสอบหลักฐานที่แสดงว่ามีการควบคุมการเข้าถึงข้อมูลอุปกรณ์ในการประมวลผลข้อมูลทางกายภาพของหน่วยงานหรือไม่อย่างไร ๒. ตรวจสอบทานสิทธิการอนุญาต และการมอบอำนาจให้เป็นไปตามคำสั่งหรือการมอบหมายสั่งการในการใช้รหัสผ่าน ๓. ตรวจสอบการติดตั้งและการใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันไวรัส การ Update ระบบปฏิบัติการ ๔. ตรวจสอบขั้นตอนการจัดระบบซอฟต์แวร์ ข้อมูลต่าง ๆ ในระบบ ระยะเวลาการกู้คืนข้อมูลของระบบ ๕. ตรวจสอบอัตราความคงที่ของกระแสไฟ ระบบสำรองไฟ เพื่อป้องกันระบบไฟฟ้าขัดข้อง ๖. ตรวจสอบการแบ่งแยกระบบเครือข่าย Firewall ข้อมูลการบุกรุกผ่านระบบเครือข่าย Network ๗. ตรวจสอบข้อกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย	กระดาษทำการ (IT ๑)

ประเด็นการตรวจสอบ/วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
๒. การรักษาความมั่นคงปลอดภัยทางกายภาพ (การจัดแบ่งพื้นที่) **วัตถุประสงค์** เพื่อให้มั่นใจว่าการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	๑. มีการจัดแบ่งพื้นที่ ๒. มีข้อกำหนดของห้องควบคุมระบบ (Computer Room) ๓. ข้อกำหนดการเข้าไปในพื้นที่ควบคุม ๔. ข้อกำหนดการเข้าไปในพื้นที่จำกัดการเข้าถึง	๑. ตรวจสอบการจัดแบ่งพื้นที่ห้องควบคุมระบบ ๒. ตรวจสอบการแยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป ๓. ตรวจสอบข้อกำหนดการเข้าไปในพื้นที่ควบคุม ๔. ตรวจสอบข้อกำหนดการเข้าไปในพื้นที่จำกัดการเข้าถึง	กระดาษทำการ (IT ๒)
๓. การรักษาความมั่นคงปลอดภัยทางกายภาพ (การสำรองข้อมูล) **วัตถุประสงค์** เพื่อให้มั่นใจว่าการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	๑. แนวปฏิบัติการสำรองข้อมูล ๒. แผนเตรียมความพร้อมกรณีฉุกเฉิน	๑. ตรวจสอบการจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย ๒. ตรวจสอบขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง	กระดาษทำการ (IT ๓)
๔. แบบสำรวจภัยคุกคาม **วัตถุประสงค์** เพื่อให้มั่นใจได้ว่าหน่วยงานมีแบบสำรวจภัยคุกคามเป็นการป้องกันเหตุการณ์ล่วงหน้าก่อนเกิดความเสียหายต่อหน่วยงาน	๑. เหตุการณ์/ปัจจัยการคุกคาม ๒. ผลกระทบ ๓. ความถี่ ๔. ผลการประเมิน	ตรวจสอบการประเมินภัยคุกคามด้านสารสนเทศของหน่วยงาน	กระดาษทำการ (IT ๔)
๕. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ. คอมพิวเตอร์ **วัตถุประสงค์** เพื่อให้มั่นใจว่าหน่วยงานได้ดำเนินการเพื่อเป็นการป้องกันมิให้ผู้ใช้งานเข้าไปกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงาน	๑. การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน ๒. การเปิดเผยวิธีการที่จะเข้าไปยังระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน ๓. การเข้าข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน ๔. . การดักข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่งของระบบคอมพิวเตอร์ ๕. การทำลาย แก้ไข เปลี่ยนแปลงเพิ่มเติมข้อมูลผู้อื่น	มีการประกาศแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ. คอมพิวเตอร์ เช่น - มีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน - มีการประกาศไม่ให้ผู้ใช้บริการมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น	กระดาษทำการ (IT ๕)

ประเด็นการตรวจสอบ/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
	๖. การระงับ ชะลอ ขัดขวาง หรือรบกวนระบบคอมพิวเตอร์ ของผู้อื่น ๗. การส่งข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์ ที่มีการปกปิดหรือปลอมแปลงแหล่งที่มาของข้อมูล เพื่อรบกวนข้อมูลการทำงานของผู้อื่น ๘. ก่อให้เกิดความเสียหายแก่ประชาชน เศรษฐกิจความมั่นคงของประเทศชาติ ๙. การจำหน่ายหรือเผยแพร่ชุดคำสั่ง ๑๐. การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบคอมพิวเตอร์ ๑๑. การเผยแพร่ข้อมูลความผิดที่เกี่ยวกับการก่อการร้ายเข้าสู่ระบบคอมพิวเตอร์ ๑๒. การนำเข้าหรือเผยแพร่เนื้อหาอันไม่เหมาะสม ๑๓. การเผยแพร่ภาพตัดต่อที่เป็นการหมิ่นประมาทเข้าสู่ระบบคอมพิวเตอร์ ๑๔. ผู้ให้บริการการเข้าถึงอินเทอร์เน็ตไม่มีการเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ ๙๐ วัน	- มีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งข้อมูล คอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้น มิได้มีไว้สำหรับตน - ฝ่าย IT มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ ๙๐ วัน	
๖. การควบคุมการเข้าถึงระบบสารสนเทศ (ระบบปฏิบัติการ) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. การควบคุมการเข้าถึงระบบปฏิบัติการ ๒. การใช้รหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์	๑. ตรวจสอบการควบคุมการเข้าถึงระบบปฏิบัติการ ๒. ตรวจสอบการใช้รหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์ การเปลี่ยนรหัสผ่าน (Password) ของหน่วยงานทุก ๓-๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล	กระดาษทำการ (IT ๖)

ประเด็นการตรวจสอบ/วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ
๗. การควบคุมการเข้าถึงระบบสารสนเทศ (ระบบเครือข่าย) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	การป้องกันจากโปรแกรมประสงค์ร้าย	๑. ตรวจสอบการป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งตรวจสอบการปรับปรุงการป้องกันให้ทันสมัยอยู่เสมอ ๒. ตรวจสอบแนวปฏิบัติการป้องกันการทำการปิดหรือยกเลิกโปรแกรมประสงค์ร้าย	กระดาษทำการ (IT ๗)
๘. การควบคุมการเข้าถึงระบบสารสนเทศ (ระบบอินเทอร์เน็ต) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	การใช้งานระบบอินเทอร์เน็ต	๑. ตรวจสอบการเชื่อมต่อระบบคอมพิวเตอร์ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้ ๒. ตรวจสอบการเข้าถึงข้อมูลตามสิทธิ์ที่ได้รับ ๓. ตรวจสอบการปกปิดความลับของข้อมูลที่ยังไม่ได้รับอนุญาตอย่างเป็นทางการ ๔. ตรวจสอบแนวปฏิบัติการละเมิดลิขสิทธิ์ด้านสารสนเทศหรือทรัพย์สินทางปัญญา ๕. ตรวจสอบการให้บริการเมื่อผู้ใช้งานใช้งานเสร็จสิ้นแล้ว	กระดาษทำการ (IT ๘)

สรุปผลการตรวจสอบภาพรวม

.....

.....

.....

.....

.....

..... ผู้ตรวจสอบ
(.....)

..... ผู้สอบทาน
(.....)

ขั้นตอนที่ ๗ ดำเนินการบันทึกข้อมูลการตรวจสอบ

ผู้ตรวจสอบภายในดำเนินการบันทึกข้อมูลการตรวจสอบลงกระดาษทำการตามรูปแบบที่กำหนดตามรูปแบบกระดาษทำการในขั้นตอนที่ ๓

๑. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (นโยบาย/แนวปฏิบัติ) รหัสกระดาษทำการ (IT ๑)

๒. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (การจัดแบ่งพื้นที่) รหัสกระดาษทำการ (IT ๒)

๓. แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (การสำรองข้อมูล) รหัสกระดาษทำการ (IT ๓)

๔. แบบสำรวจภัยคุกคาม รหัสกระดาษทำการ (IT ๔)

๕. แบบการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ที่กระทบต่อ พ.ร.บ. คอมพิวเตอร์ รหัสกระดาษทำการ (IT ๕)

๖. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบปฏิบัติการ) รหัสกระดาษทำการ (IT ๖)

๗. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบเครือข่าย) รหัสกระดาษทำการ (IT ๗)

๘. แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ (ระบบอินเทอร์เน็ต) รหัสกระดาษทำการ (IT ๘)

ขั้นตอนที่ ๘ ดำเนินการวิเคราะห์ข้อมูลเพื่อสรุปการตรวจสอบ

ผู้ตรวจสอบภายในดำเนินการตรวจสอบตามวัตถุประสงค์ ขอบเขต ระยะเวลา และกระดาษทำการตามที่ได้กำหนดไว้ในข้างต้น ผู้ตรวจสอบภายในจะต้องดำเนินการวิเคราะห์ข้อมูลดังกล่าวตามสภาพแวดล้อมที่เกิดขึ้นจริง เช่น การได้รับเอกสารจากแหล่งที่มาที่มีอยู่จริง ระยะเวลาในการประมวลผลของระบบสามารถหาผลลัพธ์ได้อย่างรวดเร็ว ถูกต้องและแม่นยำ การปฏิบัติงานของเจ้าหน้าที่ที่ได้รับมอบหมายหรือรับผิดชอบอยู่ในสภาวะที่พร้อมเข้ารับการตรวจสอบ เป็นต้น

ขั้นตอนที่ ๙ ผู้ตรวจสอบภายในสรุปผลการตรวจสอบเสนอหัวหน้าหน่วยตรวจสอบภายในพิจารณา

ผู้ตรวจสอบภายในดำเนินการรายงานสรุปผลการตรวจสอบเสนอหัวหน้าหน่วยตรวจสอบภายในพิจารณา โดยใช้ข้อมูลจากการตรวจสอบที่ได้บันทึกลงกระดาษทำการมารายงานผลให้ครบถ้วน ในกรณีที่มีการตรวจสอบแล้วพบประเด็นที่นอกเหนือจากขอบเขตหรือกระดาษทำการที่กำหนดไว้ให้ผู้ตรวจสอบภายในแนบสิ่งที่ตรวจพบดังกล่าวแนบรายงานผลการตรวจสอบนั้นให้หัวหน้าหน่วยตรวจสอบภายในได้พิจารณาประกอบกันได้

- ร่าง -

รายงานผลการตรวจสอบภายใน มหาวิทยาลัยราชภัฏสกลนคร
ประจำปีงบประมาณ พ.ศ. ๒๕XX

หน่วยรับตรวจ .....หน่วยรับตรวจ.....

ระยะเวลาการตรวจสอบ .....

รายงานผลการตรวจสอบ .....หน่วยรับตรวจ..... เวลา .....

สถานที่ .....

วัตถุประสงค์ของการตรวจสอบ

เพื่อให้มั่นใจว่าหน่วยงานได้กำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีการประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และการควบคุมการปฏิบัติที่เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยการตรวจสอบดังกล่าวเป็นไปตามมาตรฐาน COBIT (Control Objectives for Information and related Technology) ทั้งนี้ รวมถึงการตรวจสอบการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ขอบเขตการตรวจสอบ

๑. ตรวจสอบตามกระดาษทำการ IT๑ – IT๘ (ตามเอกสารแนบท้าย)
๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย
๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย
๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย

ลงชื่อ.....ผู้ตรวจสอบ ลงชื่อ.....ผู้ตรวจสอบ
( ) ( )
นักตรวจสอบภายใน นักตรวจสอบภายในปฏิบัติการ

ลงชื่อ..... ผู้สอบทาน
( )
หัวหน้าหน่วยตรวจสอบภายใน

ภาพที่ ๑๓ – ๑ แสดงร่างรายงานผลการตรวจสอบภายใน

รายงานผลการตรวจสอบ.....หน่วยรับตรวจ.....

ประจำปีงบประมาณ พ.ศ. ๒๕XX

ลำดับ	ขอบเขตการตรวจสอบ	รายงานผลการตรวจสอบ	ข้อเสนอแนะ
๑	ตรวจสอบตามกระดาษทำการ IT๑ – IT๘		
	๑.๑ แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (IT ๑)		
	๑.๒ แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (IT ๒)		
	๑.๓ แบบการตรวจสอบแนวปฏิบัติเพื่อความต่อเนื่องทางธุรกิจ (IT ๓)		
	๑.๔ แบบสำรวจภัยคุกคาม (IT ๔)		
	๑.๕ แบบการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่กระทบ พ.ร.บ. คอมพิวเตอร์ (IT ๕)		
	๑.๖ แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย (IT ๖)		
	๑.๗ แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย (IT ๗)		
	๑.๘ แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย(IT ๘)		
๒	การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย		
๓	การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์		
๔	การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย		
๕	การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย		

ภาพที่ ๑๓ – ๒ แสดงร่างรายงานผลการตรวจสอบภายใน

รายงานผลการตรวจสอบภายใน มหาวิทยาลัยราชภัฏสกลนคร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

หน่วยรับตรวจ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ระยะเวลาการตรวจสอบ วันที่ ๑๕ พฤษภาคม – ๙ มิถุนายน ๒๕๖๖

รายงานผลการตรวจสอบ วันศุกร์ที่ ๒ กุมภาพันธ์ ๒๕๖๗ เวลา ๑๐.๐๐ - ๑๒.๐๐ น.

สถานที่ ห้องประชุม ๑๑๑๑ อาคารศูนย์ภาษาและคอมพิวเตอร์ (อาคาร ๑๑) ชั้น ๑

วัตถุประสงค์ของการตรวจสอบ

เพื่อให้มั่นใจว่าหน่วยงานได้กำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีการประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และการควบคุมการปฏิบัติที่เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ โดยการตรวจสอบดังกล่าวเป็นไปตามมาตรฐาน COBIT (Control Objectives for Information and related Technology) ทั้งนี้ รวมถึงการตรวจสอบการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ และการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ขอบเขตการตรวจสอบ

๑. ตรวจสอบตามกระดาษทำการ IT.A ๑ – IT.A ๘ (ตามเอกสารแนบท้าย)
๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย
๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย
๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย

ปกปิด

ลงชื่อ.....ผู้ตรวจสอบ
(นางสาวขวัญหทัย ใจสมุทร)
นักตรวจสอบภายใน

ปกปิด

ลงชื่อ.....ผู้ตรวจสอบ
(นายพงศกร หาแก้ว)
นักตรวจสอบภายในปฏิบัติการ

ปกปิด

ลงชื่อ..... ผู้สอบทาน
(นางสาวธิดารัตน์ อุปชัย)
ปฏิบัติหน้าที่หัวหน้าหน่วยตรวจสอบภายใน

ภาพที่ ๑๔ - ๑ แสดงตัวอย่างร่างรายงานผลการตรวจสอบภายใน

รายงานผลการตรวจสอบสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

ลำดับ	ขอบเขตการตรวจสอบ	รายงานผลการตรวจสอบ	ข้อเสนอแนะ
๑	ตรวจสอบตามกระดาษทำการ IT.A ๑ – IT.A ๘	สืบเนื่องจากกระดาษทำการ IT.A ๑ – IT.A ๘ นั้น เป็นรูปแบบของการตรวจสอบที่เป็นแนวปฏิบัติที่ต้องใช้หลักฐานหรือเอกสารในการอ้างอิงข้อมูล ซึ่งเอกสารหลักฐานประกอบการตรวจสอบนั้น ไม่สามารถอ้างอิงได้ตามห้วงระยะเวลาที่ดำเนินการตรวจสอบ จึงส่งผลให้การรายงานผลการตรวจสอบยังไม่สมบูรณ์ ซึ่งขอบเขตในการตรวจสอบของกระดาษทำการจะต้องดำเนินการปรับปรุงใหม่เพื่อให้การตรวจสอบสอดคล้องกับภารกิจของหน่วยรับตรวจ	ผู้ตรวจสอบดำเนินการปรับรูปแบบกระดาษทำการเพื่อให้เกิดความสอดคล้องกับหน่วยรับตรวจ ทั้งนี้ กระดาษทำการดังกล่าวจะต้องเป็นไปตามรูปแบบที่มีความครบถ้วนทั้งระบบ และครอบคลุมตามพันธะ ภารกิจของหน่วยรับตรวจ
	๑.๑ แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (IT ๑)		
	๑.๒ แบบการตรวจสอบแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพ (IT ๒)		
	๑.๓ แบบการตรวจสอบแนวปฏิบัติเพื่อความต่อเนื่องทางธุรกิจ (IT ๓)		
	๑.๔ แบบสำรวจภัยคุกคาม (IT ๔)		
	๑.๕ แบบการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือขายที่กระทบ พ.ร.บ. คอมพิวเตอร์ (IT ๕)		
	๑.๖ แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย (IT ๖)		
	๑.๗ แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย (IT ๗)		
	๑.๘ แบบการตรวจสอบแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย(IT ๘)		
๒	การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ยังคงใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร พ.ศ. ๒๕๕๗	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ควรมีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร พ.ศ. ๒๕๕๙ เพื่อให้นโยบายดังกล่าวสามารถใช้งานและตอบสนองต่อการปฏิบัติงานของส่วนราชการ และผู้มีส่วนได้ส่วนเสียในระดับมหาวิทยาลัยได้

ลำดับ	ขอบเขตการตรวจสอบ	รายงานผลการตรวจสอบ	ข้อเสนอแนะ
๓	การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์	ไม่พบ การประกาศใช้การรักษาความมั่นคงปลอดภัยไซเบอร์	สำนักวิทยบริการและเทคโนโลยีสารสนเทศควรประกาศใช้การรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้เป็นไปตามพระราชบัญญัติที่กำหนดไว้
๔	การกำหนดกระบวนการกำกับดูแลการประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีการกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในของหน่วยงาน แต่การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศยังไม่มีการกำหนดความเสี่ยงที่ชัดเจน ซึ่งความเสี่ยงดังกล่าวอาจส่งผลกระทบต่อความเสี่ยงในสภาวะวิกฤตด้านสารสนเทศทันที และอาจทำให้มหาวิทยาลัยเกิดความเสียหายได้ ดังนั้น สำนักฯ ควรจะมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศแบบเฉพาะเจาะจง เพื่อเป็นการป้องกันเหตุที่อาจจะเกิดขึ้นในอนาคตได้	๑. สำนักฯ ควรจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับหน่วยงานและระดับมหาวิทยาลัย ๒. สำนักฯ ควรมีแผนรองรับเหตุสภาวะวิกฤตด้านเทคโนโลยีสารสนเทศ และ ควรทบทวนแผนดังกล่าวอย่างน้อยปีละ ๑ ครั้ง
๕	การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีการประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัยซึ่งการประกาศใช้ข้อมูลส่วนบุคคลดังกล่าวเป็นไปตามกฎหมาย ว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล เป็นการสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาตโดยกฎหมาย PDPA Thailand (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล)	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ควรมีการทบทวนการประกาศใช้ข้อมูลส่วนบุคคลของมหาวิทยาลัย เพื่อรองรับการเปลี่ยนแปลงที่เป็นไปตามข้อกฎหมาย เป็นต้น

ภาพที่ ๑๔ - ๒ แสดงตัวอย่างร่างรายงานผลการตรวจสอบภายใน

ขั้นตอนที่ ๑๐ แจ้งรายงานผลการตรวจสอบให้หน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบ (ปิดตรวจ)

เมื่อหัวหน้าหน่วยตรวจสอบภายในได้พิจารณาการรายงานสรุปผลการตรวจสอบจากผู้ตรวจสอบภายในเสร็จสิ้นแล้ว และรายงานผลการตรวจสอบดังกล่าวมีความถูกต้อง ครบถ้วน สมบูรณ์ ผู้ตรวจสอบภายในจะต้องดำเนินการแจ้งรายงานผลการตรวจสอบให้หน่วยรับตรวจเพื่อดำเนินการยืนยันหรือทักท้วงการรายงานผลการตรวจสอบ (ปิดตรวจ) โดยผู้ตรวจสอบภายในจะต้องประสานงานกับหน่วยรับตรวจเพื่อให้การดำเนินงานในการรายงานผลการตรวจเป็นไปด้วยความเรียบร้อย

การรายงานผลการตรวจสอบดังกล่าวเป็นการยืนยันผลการตรวจสอบภายในที่ผู้ตรวจสอบภายในได้ดำเนินการตรวจสอบตามระยะเวลาที่กำหนด โดยการรายงานผลการตรวจสอบต้องดำเนินการอย่างเป็นทางการและมีลายลักษณ์อักษรอย่างชัดเจน ผู้ตรวจสอบภายในจะต้องรายงานผลการตรวจสอบให้หน่วยรับตรวจได้รับทราบถึงผลการตรวจสอบ รวมไปถึงรับทราบข้อเสนอแนะหรือแนวทางปฏิบัติที่ถูกต้อง

หากหน่วยรับตรวจทราบการรายงานผลการตรวจสอบแล้ว และเห็นด้วยกับรายงานผลการตรวจสอบ ให้หน่วยรับตรวจจัดทำหนังสือบันทึกข้อความเพื่อยืนยันผลการรายงานผลการตรวจสอบดังกล่าวตามที่ผู้ตรวจสอบภายในได้รายงานผล หากหน่วยรับตรวจไม่เห็นด้วยกับการรายงานผลการตรวจสอบ ให้หน่วยรับตรวจจัดทำหนังสือบันทึกข้อความทักท้วงการรายงานผลการตรวจสอบ และหน่วยรับตรวจจะต้องแนบเอกสารหรือหลักฐานอ้างอิงในการทักท้วงรายงานผลการตรวจสอบ เพื่อให้ผู้ตรวจสอบภายในได้ดำเนินการตรวจสอบ วิเคราะห์ข้อมูลเพื่อดำเนินการหักล้างข้อมูลในรายงานผลการตรวจสอบดังกล่าว

บันทึกข้อความ

ส่วนราชการ XXX

ที่ XXX / XXX **วันที่** XXX

เรื่อง ยืนยันหรือหักท้วงรายงานผลการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕XX

หน่วยรับตรวจ : .....**หน่วยรับตรวจ**.....

เรียน .....**หน่วยรับตรวจ**.....

ตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕XX หน่วยตรวจสอบภายในได้ดำเนินการรายงานผลการตรวจสอบภายในหน่วยรับตรวจ .....**หน่วยรับตรวจ**.....ประจำปีงบประมาณ พ.ศ. ๒๕XX เมื่อ .....XXX..... เวลา .....XXX..... ณ ห้อง..... XXX ..... นั้น หน่วยตรวจสอบภายในได้ดำเนินการตรวจสอบตามภารกิจของ.....**หน่วยรับตรวจ**.....โดยมีขอบเขตการตรวจสอบ ดังนี้

๑. ตรวจสอบตามกระดาษทำการ IT๑ – IT๘
๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ....**หน่วยรับตรวจ**....
๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ....**หน่วยรับตรวจ**....
๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของ...**หน่วยรับตรวจ**....

ในการนี้ หน่วยตรวจสอบภายใน ได้ดำเนินการรายงานผลการตรวจสอบตามขอบเขตการตรวจสอบเสร็จสิ้น แล้วรวมถึงได้ให้ข้อเสนอแนะกับ.....**หน่วยรับตรวจ**.....ทั้งนี้ หน่วยตรวจสอบภายในขอให้.....**หน่วยรับตรวจ**.....ดำเนินการยืนยันหรือหักท้วงรายงานผลการตรวจสอบภายในดังกล่าว (ปิดตรวจ) หากมีข้อหักท้วงในรายงานผลการตรวจสอบดังกล่าว ให้.....**หน่วยรับตรวจ**.....หักท้วงรายงานผลการตรวจสอบโดยแนบเอกสารหลักฐานในการหักท้วงรายงานผลการตรวจสอบด้วย นำส่งหน่วยตรวจสอบภายใน ภายในวันที่ .....XXX..... เพื่อที่หน่วยตรวจสอบภายในจะได้รวบรวมรายงานผลการตรวจสอบดังกล่าวเสนอต่อหัวหน้าส่วนราชการและคณะกรรมการตรวจสอบประจำ มหาวิทยาลัยราชภัฏสกลนครต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการ

( )
หัวหน้าหน่วยตรวจสอบภายใน

แบบยืนยันหรือหักท้วงรายงานผลการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕XX
หน่วยรับตรวจ : .....XXX.....

ข้อเสนอแนะจากการตรวจสอบภายใน	แบบยืนยันหรือหักท้วงรายงานผลการตรวจสอบภายใน		กรณีหักท้วงแนบหลักฐานหรือเอกสารอ้างอิง
	ยืนยัน	หักท้วง	

ลงชื่อ.....**หัวหน้าหน่วยรับตรวจ**.....
( )
วันที่ ...../...../.....

ภาพที่ ๑๕ แสดงการยืนยันหรือหักท้วงรายงานผลการตรวจสอบภายใน

บันทึกข้อความ

ส่วนราชการ หน่วยตรวจสอบภายใน สำนักงานอธิการบดี มหาวิทยาลัยราชภัฏสกลนคร IP Phone ๑๖๕

ที่ อว ๐๖๒๑.๐๑(๑)/ ๔๑๔ **วันที่** ๘ กุมภาพันธ์ ๒๕๖๗

เรื่อง ยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

หน่วยรับตรวจ : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

เรียน ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ หน่วยตรวจสอบภายในได้ดำเนินการรายงานผลการตรวจสอบภายในหน่วยรับตรวจ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ เมื่อวันศุกร์ที่ ๒ กุมภาพันธ์ ๒๕๖๗ เวลา ๑๐.๐๐ – ๑๒.๐๐ น. ณ ห้องประชุม ๑๑๑๑ ชั้น ๓ อาคารศูนย์ภาษาและคอมพิวเตอร์ นั้น หน่วยตรวจสอบภายในได้ดำเนินการตรวจสอบตามภารกิจของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ โดยมีขอบเขตการตรวจสอบ ดังนี้

๑. ตรวจสอบตามกระดาษทำการ IT.A ๑ – IT.A ๘
๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย
๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย
๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย

ในการนี้ หน่วยตรวจสอบภายใน ได้ดำเนินการรายงานผลการตรวจสอบตามขอบเขตการตรวจสอบเสร็จสิ้น แล้วรวมถึงได้ให้ข้อเสนอแนะกับหน่วยรับตรวจ ทั้งนี้หน่วยตรวจสอบภายใน ขอให้หน่วยรับตรวจดำเนินการยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายในดังกล่าว (ปิดตรวจ) หากมีข้อทักท้วงในรายงานผลการตรวจสอบดังกล่าว ให้หน่วยรับตรวจทักท้วงรายงานผลการตรวจสอบโดยแนบเอกสารหลักฐานในการทักท้วงรายงานผลการตรวจสอบด้วย นำส่งหน่วยตรวจสอบภายใน ชั้น ๔ อาคาร ๑๐ ภายในวันที่ ๙ กุมภาพันธ์ ๒๕๖๗ เพื่อที่หน่วยตรวจสอบภายในจะได้รวบรวมรายงานผลการตรวจสอบดังกล่าว เสนอต่อหัวหน้าส่วนราชการและคณะกรรมการตรวจสอบประจำ มหาวิทยาลัยราชภัฏสกลนครต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการ

ปกปิด

(นางสาวธิดารัตน์ อุปชัย)
ปฏิบัติหน้าที่หัวหน้าหน่วยตรวจสอบภายใน

ภาพที่ ๑๖ แสดงตัวอย่างแบบบันทึกข้อความเพื่อให้หน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบ

ขั้นตอนที่ ๑๑ สรุปรายงานผลการตรวจสอบหลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบ

ผู้ตรวจสอบภายในดำเนินการสรุปรายงานผลการตรวจสอบหลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลกการตรวจสอบ โดยการยืนยันหรือทักท้วงรายงานผลกการตรวจสอบดังกล่าวนั้น ผู้ตรวจสอบภายในจะสรุปรายงานผลการตรวจสอบอีกครั้งเมื่อหน่วยรับตรวจได้แนบเอกสารหรือหลักฐานอ้างอิงในการทักท้วงรายงานผลการตรวจสอบดังกล่าว ภายใน ๑๕ วันตามกำหนด หากหน่วยรับตรวจแนบเอกสารหลักฐานอ้างอิง ไม่มีความสอดคล้องในการหักล้างข้อมูลในรายงานผลการตรวจสอบดังกล่าว ให้ผู้ตรวจสอบภายในยึดการรายงานผลการตรวจสอบก่อนมีการทักท้วงรายงานผลการตรวจสอบได้ ทั้งนี้ ผู้ตรวจสอบภายในสามารถสรุปรายงานผลการตรวจสอบหลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบได้ทันที และผู้ตรวจสอบภายในต้องจัดทำหนังสือบันทึกข้อความแจ้งต่อหน่วยรับตรวจว่าผู้ตรวจสอบภายในยืนยันใช้รายงานผลการตรวจสอบเดิม

บันทึกข้อความ

ส่วนราชการ .....**หน่วยรับตรวจ**.....

ที่ XXX / XXX **วันที่** XXX

เรื่อง ยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕XX

หน่วยรับตรวจ : .....**หน่วยรับตรวจ**.....

เรียน หัวหน้าหน่วยตรวจสอบภายใน

ตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕XX หน่วยตรวจสอบภายในได้ดำเนินการรายงานผลการตรวจสอบภายในหน่วยรับตรวจ .....**หน่วยรับตรวจ**..... ประจำปีงบประมาณ พ.ศ. ๒๕XX เมื่อ.....XXX ..... เวลา .....XXX ..... ณ ห้อง .....XXX .....นั้น หน่วยตรวจสอบภายในได้ดำเนินการตรวจสอบตามภารกิจของ.....**หน่วยรับตรวจ**.....เสร็จสิ้นแล้วนั้น

ในการนี้ .....**หน่วยรับตรวจ**.....ซึ่งเป็นหน่วยรับตรวจขอยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายในดังกล่าว (ปิดตรวจ) ตามวันและเวลาข้างต้นแล้วนั้น .....**หน่วยรับตรวจ**.....ขอยืนยันหรือทักท้วงรายงานผลการตรวจสอบ ทั้งนี้.....**หน่วยรับตรวจ**.....ได้แนบเอกสารหลักฐานในการทักท้วงรายงานผลการตรวจสอบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบและพิจารณา

.....**หัวหน้าหน่วยรับตรวจ**.....

( )

วันที่...../...../.....

ภาพที่ ๑๗-๑ แสดงแบบบันทึกข้อความการยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายในจากหน่วยรับตรวจ

แบบยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕XX

หน่วยรับตรวจ : .....หน่วยรับตรวจ.....

ข้อเสนอแนะจากการตรวจสอบภายใน	แบบยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายใน		กรณีทักท้วงแนบหลักฐานหรือเอกสารอ้างอิง
	ยืนยัน	ทักท้วง	

.....หัวหน้าหน่วยรับตรวจ.....

( )

วันที่...../...../.....

ภาพที่ ๑๗-๒ แสดงแบบบันทึกข้อความการยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายในจากหน่วยรับตรวจ

บันทึกข้อความ

ส่วนราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร IP Phone ๒๒๑

ที่ อว ๐๖๒๑.๑๐/ ๑๐๕ **วันที่** ๙ กุมภาพันธ์ ๒๕๖๗

เรื่อง ยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

หน่วยรับตรวจ : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

เรียน หัวหน้าหน่วยตรวจสอบภายใน

ตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ หน่วยตรวจสอบภายในได้ดำเนินการรายงานผลการตรวจสอบภายในหน่วยรับตรวจ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ เมื่อวันศุกร์ที่ ๒ กุมภาพันธ์ ๒๕๖๗ เวลา ๑๐.๐๐ – ๑๒.๐๐ น. ณ ห้องประชุม ๑๑๑๑ ชั้น ๓ อาคารศูนย์ภาษาและคอมพิวเตอร์ นั้น หน่วยตรวจสอบภายในได้ดำเนินการตรวจสอบตามภารกิจของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ นั้น

ในการนี้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยรับตรวจขอยืนยันและทักท้วงรายงานผลการตรวจสอบภายในดังกล่าว (ปิดตรวจ) ในวันดังกล่าวข้างต้น ดังรายงานผลการตรวจสอบและได้แนบเอกสารหลักฐานในการทักท้วงรายงานผลการตรวจสอบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบและพิจารณา

ปกปิด

(อาจารย์กรกช มาตะรัตน์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ภาพที่ ๑๘ แสดงตัวอย่างแบบบันทึกข้อความจากหน่วยรับตรวจในการยืนยันหรือทักท้วงรายงานผลการตรวจสอบภายในเสนอหัวหน้าหน่วยตรวจสอบภายใน

ขั้นตอนที่ ๑๒ ผู้ตรวจสอบภายในสรุปรายงานผลการตรวจสอบหลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบเสนอต่อหัวหน้าตรวจสอบภายในพิจารณา

ผู้ตรวจสอบภายในสรุปรายงานผลการตรวจสอบหลังจากหน่วยรับตรวจยืนยันหรือทักท้วงรายงานผลการตรวจสอบเสนอต่อหัวหน้าตรวจสอบภายในพิจารณา หากหัวหน้าหน่วยตรวจสอบภายในพิจารณาแล้วเห็นชอบในการรายงานสรุปผลการตรวจสอบหลังจากหน่วยรับตรวจได้ดำเนินการยืนยันหรือทักท้วงรายงานผลการตรวจสอบ ให้ผู้ตรวจสอบภายในดำเนินการจัดทำระเบียบวาระการประชุมเพื่อเสนอให้คณะกรรมการตรวจสอบประจำให้ความเห็นชอบในการรายงานผลการตรวจสอบดังกล่าว

บันทึกข้อความ

ส่วนราชการ หน่วยตรวจสอบภายใน สำนักงานอธิการบดี มหาวิทยาลัยราชภัฏสกลนคร IP Phone ๑๖๕

ที่ อว ๐๖๒๑.๐๑(๑)/ ๖๘๑ **วันที่** ๕ มีนาคม ๒๕๖๗

เรื่อง รายงานผลการตรวจสอบภายใน หน่วยรับตรวจ : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

เรียน หัวหน้าหน่วยตรวจสอบภายใน

สืบเนื่องจากหน่วยตรวจสอบภายใน มหาวิทยาลัยราชภัฏสกลนคร ได้เข้าดำเนินการรายงานผลการตรวจสอบภายใน หน่วยรับตรวจ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ เมื่อวันศุกร์ที่ ๒ กุมภาพันธ์ ๒๕๖๗ เวลา ๑๐.๐๐ – ๑๒.๐๐ น. ณ ห้องประชุม ๑๑๑๑ ชั้น ๓ อาคารศูนย์ภาษาและคอมพิวเตอร์ นั้น หน่วยตรวจสอบภายในได้ดำเนินการตรวจสอบตามภารกิจของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ (Information Auditing) โดยมีขอบเขตการตรวจสอบ ดังนี้

๑. ตรวจสอบตามกระดาษทำการ IT.A ๑ – IT.A ๘
๒. การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย
๓. การประกาศใช้ตามแนวพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. การกำหนดกระบวนการกำกับดูแล การประเมินความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย
๕. การประกาศใช้ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองส่วนบุคคลของมหาวิทยาลัย

ในการนี้ หน่วยตรวจสอบภายใน ได้ดำเนินการรายงานผลการตรวจสอบตามขอบเขตและภารกิจของหน่วยรับตรวจเสร็จสิ้นแล้ว รวมถึงได้ให้ข้อเสนอแนะกับหน่วยรับตรวจโดยข้อเสนอแนะที่ให้หน่วยรับตรวจนั้น หน่วยรับตรวจสอบต้องรายงานผลการยืนยันหรือทักท้วงรายงานผลการตรวจสอบเพื่อให้เป็นไปตามหลักเกณฑ์การประเมินการประกันและการปรับปรุงคุณภาพงานตรวจสอบภายในภาครัฐจากองค์กรภายนอก หน่วยตรวจสอบภายในจึงขอรายงานผลการตรวจสอบดังกล่าวเสนอต่อหัวหน้าหน่วยตรวจสอบภายในและคณะกรรมการตรวจสอบประจำ มหาวิทยาลัยราชภัฏสกลนครในลำดับถัดไป

จึงเรียนมาเพื่อโปรดพิจารณา

ปกปิด

(นางสาวธิดารัตน์ อุปชัย)
ปฏิบัติหน้าที่หัวหน้าหน่วยตรวจสอบภายใน

ภาพที่ ๑๙ แสดงตัวอย่างแบบบันทึกข้อความการรายงานผลการตรวจสอบภายในเสนอหัวหน้าหน่วยตรวจสอบภายใน

ขั้นตอนที่ ๑๓ หัวหน้าหน่วยตรวจสอบภายในรายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบประจำเพื่อพิจารณาให้ความเห็นชอบและให้หัวหน้าส่วนราชการพิจารณาสั่งการ

หัวหน้าหน่วยตรวจสอบภายในดำเนินการรายงานผลการตรวจสอบตามระเบียบวาระการประชุมซึ่งการรายงานผลการตรวจสอบคณะกรรมการตรวจสอบประจำ หัวหน้าหน่วยตรวจสอบภายในจะต้องรายงานผลการตรวจสอบเสนอที่ประชุมเพื่อให้ที่ประชุมพิจารณาให้ความเห็นชอบ และให้หัวหน้าส่วนราชการพิจารณาสั่งการโดยการรายงานผลการตรวจสอบดังกล่าวอยู่ในระเบียบวาระที่ ๔ เรื่องเสนอให้ที่ประชุมพิจารณา

ระเบียบวาระการประชุมคณะกรรมการตรวจสอบ.....ชื่อองค์กร.....
ครั้งที่ ...../๒๕XX
วัน.....ที่.....เดือน.....พ.ศ. ๒๕XX เวลา ..... น.
ณ .....

ระเบียบวาระที่ ๑ เรื่องประธานแจ้งที่ประชุม

๑.๑
๑.๒
๑.๓

ระเบียบวาระที่ ๒ เรื่องรับรองรายงานการประชุม

รายงานการประชุมคณะกรรมการตรวจสอบประจำมหาวิทยาลัยราชภัฏสกลนคร ครั้งที่ ..../๒๕XX เมื่อวันที่ .....

ระเบียบวาระที่ ๓ เรื่องที่เสนอให้ที่ประชุมทราบ

๓.๑
๓.๒
๓.๓

ระเบียบวาระที่ ๔ เรื่องเสนอให้ที่ประชุมพิจารณา

๔.๑ รายงานผลการตรวจสอบระบบความมั่นคงปลอดภัยปลอดภัยด้านสารสนเทศ (Information Technology)
๔.๒
๔.๓

ระเบียบวาระที่ ๕ เรื่องอื่น ๆ

๕.๑
๕.๒
๕.๓

ภาพที่ ๒๐ แสดงระเบียบวาระการประชุมเพื่อรายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบประจำ

จากเทคนิคการปฏิบัติงานข้างต้น จะเห็นได้ว่า ผู้จัดทำได้เรียบเรียงขั้นตอนการปฏิบัติงานด้านการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศไว้ได้ ๑๓ ขั้นตอนหลัก โดยการจัดทำคู่มือการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศที่ได้จัดทำขึ้นมานี้ ผู้จัดทำได้เล็งเห็นว่าหน่วยงานที่มีข้อมูลด้านสารสนเทศที่มีขนาดใหญ่ และมีความสำคัญต่อการบริหารจัดการนั้นจะต้องได้รับการปกป้องหรือป้องกันเหตุการณ์ที่อาจส่งผลกระทบทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศดังกล่าว ซึ่งข้อมูลในส่วนต่าง ๆ ที่มีความเกี่ยวข้องในด้านสารสนเทศนั้น อาจจะประกอบด้วย ข้อมูลส่วนบุคคล ข้อมูลการบริหารงาน ข้อมูลการเงินและงบประมาณ หรือข้อมูลที่มีการเชื่อมโยงด้านสารสนเทศในมิติที่หลากหลาย ดังนั้น หน่วยงานที่มีหน้าที่รับผิดชอบในการดูแลข้อมูลด้านสารสนเทศนั้นจะต้องสร้างมาตรการ แนวทางปฏิบัติ มาตรฐานการดูแลรักษาข้อมูลด้านสนเทศให้มีความปลอดภัย เพื่อเป็นการป้องกันจากผู้ไม่ประสงค์ดีเข้าบุกรุกหรือเจตนาทำลายข้อมูลด้านสารสนเทศที่สร้างความสียหายต่อตัวบุคคลหรือองค์กร

หน่วยงานที่มีความสนใจในเรื่องการป้องกันข้อมูลสารสนเทศ สามารถนำคู่มือการปฏิบัติงานการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศไปใช้เป็นแนวทางในการปฏิบัติงาน เพื่อตรวจสอบข้อมูลสารสนเทศของหน่วยงานตนเองในเบื้องต้น และสามารถปรับใช้คู่มือปฏิบัติงานดังกล่าวให้มีความเหมาะสมกับบริบทของหน่วยงานหรือองค์กรได้

บทที่ ๕
ปัญหา อุปสรรค และข้อเสนอแนะ

๑. ปัญหา อุปสรรค และแนวทางการแก้ไข

ผู้จัดทำได้ดำเนินการรวบรวมปัญหา อุปสรรค แนวทางแก้ไข พร้อมด้วยข้อเสนอแนะในการพัฒนาให้กับผู้ปฏิบัติงานที่มีความเกี่ยวข้องกันการใช้คู่มือการปฏิบัติงาน เรื่อง การตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ โดยสรุปได้ดังนี้

ตารางที่ ๕ ปัญหา อุปสรรค และแนวทางการแก้ไข

ปัญหา	อุปสรรค	แนวทางการแก้ไข
๑. การวางแผนการตรวจสอบภายในประจำปี	หน่วยตรวจสอบภายในมีความยุ่งยากในการวางแผนการตรวจสอบภายในประจำปี ซึ่งการกำหนดแผนการตรวจสอบในแต่ละปีงบประมาณจะต้องมีการจัดเตรียมข้อมูล ข้อวิเคราะห์ข้อมูล รวมถึงการกำหนดเกณฑ์บริหารจัดการความเสี่ยงทำให้การวางแผนการตรวจสอบภายในประจำปีงบประมาณต้องใช้ความละเอียดรอบคอบในการปฏิบัติ	ผู้ตรวจสอบภายในจะต้องเร่งดำเนินการวางแผนในการจัดทำแผนการตรวจสอบภายในดังกล่าว โดยการขอข้อมูลจากหน่วยรับตรวจเพื่อใช้ประเมินผลการจัดทำแผนการตรวจสอบภายใน โดยการจัดทำแผนการตรวจสอบด้านสารสนเทศ หน่วยรับตรวจจะต้องทำการประเมินความเสี่ยงขององค์กรโดยเน้นปัจจัยเสี่ยงที่มีความเกี่ยวข้องกับระบบสารสนเทศโดยตรงเป็นอันดับแรก
๒. แนวทางการตรวจสอบ (Engagement)	กระดาษทำการไม่สอดคล้องกับบริบทของหน่วยรับตรวจ	ผู้ตรวจสอบภายในจะต้องดำเนินการวิเคราะห์ข้อมูลของหน่วยรับตรวจ และวิเคราะห์ความเชื่อมโยงของกระดาษทำการให้มีความสัมพันธ์กันอย่างมีนัยยสำคัญที่ไม่สร้างความเสียหายต่อหน่วยรับตรวจและองค์กร
๓. การดำเนินการ (เปิดตรวจ) กับหน่วยรับตรวจ	เนื่องจากหน่วยรับตรวจมีภารกิจที่ต้องรับผิดชอบค่อนข้างมากทำให้การเข้าตรวจสอบของผู้ตรวจสอบภายในไม่เป็นไปตามแผนการตรวจสอบภายในส่งผลให้การตรวจสอบนั้นกระทบต่อหน่วยรับตรวจอื่น	ก่อนดำเนินการประสานงานเพื่อเข้าตรวจสอบผู้ตรวจสอบภายในจะต้องสอบถามความชัดเจนกับหน่วยรับตรวจ หรือจัดทำหนังสือเพื่อยืนยันการอนุญาตให้ผู้ตรวจสอบภายในเข้าดำเนินการตรวจสอบตามแผนการตรวจสอบของผู้ตรวจสอบภายใน
๔. การดำเนินการบันทึกข้อมูลการตรวจสอบ	การบันทึกข้อมูลการตรวจสอบลงกระดาษทำการขาดความครบถ้วนของข้อมูล เนื่องจากระยะเวลาในการประมวลผลของแต่ละระบบใช้เวลาค่อนข้างนานจึงไม่สามารถสรุปผลการตรวจสอบในระยะเวลาที่กำหนดการตรวจสอบได้	ผู้ตรวจสอบภายในอาจจะต้องวิเคราะห์ข้อมูลในการตรวจสอบระบบแต่ละประเภท เพื่อสามารถกำหนดระยะเวลาในการตรวจสอบและได้ข้อมูลจากระบบที่แท้จริง
๕. การรายงานสรุปผลการตรวจสอบเสนอหัวหน้าหน่วยตรวจสอบภายในพิจารณา	การรายงานผลการตรวจสอบต่อหัวหน้าหน่วยตรวจสอบภายในเพื่อรายงานผลการตรวจสอบนั้น ไม่ทันกาลต่อการให้หน่วยรับตรวจนำไปปฏิบัติงานจริง	ผู้ตรวจสอบภายในต้องเร่งดำเนินการสรุปผลการตรวจสอบจากกระดาษทำการ หากการตรวจสอบได้ข้อมูลจากการตรวจสอบไม่ครบถ้วนให้ผู้ตรวจสอบภายในเร่งดำเนินการติดตามอย่างเร่งด่วนเพื่อเป็นการป้องกันเหตุการณ์ความเสียหายที่อาจเกิดขึ้นในอนาคตได้

๒. ข้อเสนอแนะเพื่อการพัฒนา

๑. มหาวิทยาลัยควรตระหนักและให้ความสำคัญต่อระบบสารสนเทศเป็นอย่างมากเนื่องจากปัจจุบันนี้เทคโนโลยีเป็นปัจจัยหลักในการดำเนินงานที่ส่งผลต่อการใช้ชีวิตและสะท้อนถึงความปลอดภัยในการใช้ระบบสารสนเทศจึงทำให้ความปลอดภัยในข้อมูลด้านสารสนเทศนั้นมีความสำคัญสูงมาก ทั้งนี้มหาวิทยาลัยอาจจำเป็นต้องจัดอันดับความสำคัญของข้อมูลโดยอาจแบ่งเป็นข้อมูลระดับพื้นฐานและข้อมูลระดับสูง และกำหนดให้มีหน่วยงานหลักในการรับผิดชอบข้อมูลดังกล่าว โดยข้อมูลระดับพื้นฐานอาจเป็นการกำหนดนโยบายของส่วนราชการที่ได้รับการอนุมัติและเผยแพร่อย่างชัดเจน หรือข้อมูลระดับสูงควรกำหนดทิศทางการบริหารงานด้านสารสนเทศเป็นส่วนราชการนั้น ๆ ได้

๒. ผู้บริหาร บุคลากร เจ้าหน้าที่ นักศึกษา ควรได้ตระหนักถึงข้อมูล และสิทธิส่วนบุคคลของตนเองในการกรอกข้อมูลให้กับมหาวิทยาลัย ทั้งนี้ ผู้บริหาร บุคลากร เจ้าหน้าที่ นักศึกษา ควรได้รับการอบรมในเรื่องของความปลอดภัยของข้อมูลที่มีความเกี่ยวข้องกับระบบสารสนเทศ เป็นการป้องกันข้อมูลของตนเองเพื่อมิให้บุคคลอื่นเข้ามาล่วงรู้ข้อมูลของตนเองได้

๓. ปัจจุบันหลายองค์กรได้นำ ISO ๒๗๐๐๑ เข้ามาเป็นส่วนหนึ่งในการบริหารองค์กรและมหาวิทยาลัยควรนำมาตรฐาน ISO ๒๗๐๐๑ เข้ามาวางรากฐานและสร้างมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศทั้งองค์กร เนื่องจากมาตรฐาน ISO ๒๗๐๐๑ เป็นมาตรฐานและข้อกำหนดสำหรับการรักษาความมั่นคงปลอดภัย (ISMS requirements) ซึ่งหน่วยงานสามารถใช้เป็นมาตรฐานในการอ้างอิงให้ระบบสารสนเทศมีความน่าเชื่อถือและปลอดภัยมากยิ่งขึ้น

ผู้จัดทำคู่มือดังกล่าวนี้ หวังเป็นอย่างยิ่งว่าจะทำให้ผู้ปฏิบัติงานคนอื่นสามารถนำไปปฏิบัติงานแทนกันได้ และหวังเป็นอย่างยิ่งว่าคู่มือฉบับนี้จะเป็นประโยชน์หรือเป็นแนวทางในการจัดทำคู่มือเรื่องอื่น ๆ ต่อการปฏิบัติงานของหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาการปฏิบัติงาน และเพื่อสนับสนุนการจัดทำผลงานของบุคลากรสายสนับสนุนให้เข้าสู่ตำแหน่งที่สูงขึ้น