แนวทางการปฏิบัติงานการตรวจสอบระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ประจำปีงบประมาณ พ.ศ. 2556

ประเด็นการตรวจสอบที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์
1. เพื่อให้มั่นใจว่า หน่วยงานกำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
2. เพื่อทราบปัญหาอุปสรรคในการดำเนินการ

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
1. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ **วัตถุประสงค์** เพื่อให้มั่นใจว่า การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	1. หน่วยงานมีการจัดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร 2. นโยบายมีเนื้อหาครอบ - คลุมเรื่องต่อไปนี้ 2.1 การเข้าถึงหรือการควบคุมการใช้สารสนเทศ 2.2 จัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน 2.3 จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ 3. หน่วยงานประกาศนโยบายให้ผู้ที่เกี่ยว-ข้องทราบ 4. หน่วยงานกำหนดผู้รับผิดชอบตามนโยบายที่ชัดเจน 5. หน่วยงานมีการทบทวนนโยบายให้เป็นปัจจุบัน	1. ตรวจสอบเอกสารหลักฐานว่าหน่วย-งานได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรหรือไม่ กรณีที่ไม่ได้ดำเนินการให้สอบถามสาเหตุจากผู้ที่เกี่ยวข้อง 2. กรณีที่จัดทำให้ตรวจสอบเนื้อหาในนโยบายว่า ครอบคลุมประเด็นที่กำหนดตามเกณฑ์ และมีหลักฐานเชื่อได้ว่ามีการทบทวนเป็นปัจจุบัน 3. ตรวจสอบว่า มีการออกคำสั่งหรือมอบหมายสั่งการให้รับผิดชอบ ตามนโยบายที่กำหนดหรือไม่ 4. ตรวจสอบ/สังเกต การประกาศนโยบายให้ผู้ที่เกี่ยวข้องทราบ 5. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ พร้อมถ่ายเอกสารนโยบายที่จัดทำ (ถ้ามี) แนบกระดาษทำการเป็นหลักฐาน	<u>เครื่องมือ</u> กระดาษทำการ IT.A1.1 <u>หลักฐาน</u> 1. เอกสารนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 2. หลักฐานแสดงการประกาศเผยแพร่ 3. คำสั่งหรือหนังสือมอบหมายสั่งการ <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT ภาพรวมขององค์กร 2. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง
2.การจัดทำข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	1. ข้อปฏิบัติสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัย 2. ข้อปฏิบัติมีเนื้อหาอย่างน้อยต่อไปนี้	1. ตรวจสอบเอกสารหลักฐานว่าหน่วยงานได้กำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสอดคล้องกับนโยบายที่กำหนดทุกข้อหรือไม่	<u>เครื่องมือ</u> กระดาษทำการ IT.A1.2 <u>หลักฐาน</u> 1. เอกสารนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
วัตถุประสงค์ เพื่อให้มั่นใจว่า การจัดทำข้อปฏิบัติในการรักษาความ-มั่นคงปลอดภัย เป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	2.1 มีข้อกำหนดการควบคุมการเข้าถึง 2.2 มีข้อกำหนดการใช้งานตามภารกิจ 2.3 มีการจัดการการเข้าถึงของผู้ใช้งาน 2.4 มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน 2.5 มีการควบคุมการเข้าถึงเครือข่าย 2.6 มีการควบคุมการเข้าถึงระบบปฏิบัติการ 2.7 มีการควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ 2.8 จัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน 2.9 จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ 3. หน่วยงานประกาศข้อปฏิบัติให้ผู้ที่เกี่ยว ข้องทราบ 4. หน่วยงานกำหนดผู้รับ - ผิดชอบตามข้อปฏิบัติที่ชัดเจน 5. หน่วยงานมีการทบทวนข้อปฏิบัติเป็นปัจจุบัน	2. ตรวจสอบข้อปฏิบัติที่กำหนดครอบคลุมทุกประเด็นตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และมีหลักฐานเชื่อได้ว่ามีการทบทวนเป็นปัจจุบัน 3. ตรวจสอบว่า มีการออกคำสั่งหรือมอบหมายสั่งการให้รับผิดชอบ ตามข้อปฏิบัติที่กำหนดหรือไม่ 4. ตรวจสอบ/สังเกต การประกาศข้อปฏิบัติฯ ให้ผู้ที่เกี่ยวข้องทราบ 5. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ พร้อมถ่ายเอกสารข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยแนบกระดาษทำการเป็นหลักฐาน	2. หลักฐานแสดงการประกาศเผยแพร่ 3. คำสั่งหรือหนังสือมอบหมายสั่งการ <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT ภาพรวมขององค์กร 2. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นการตรวจสอบที่ 2 หน่วยงานดำเนินการควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

วัตถุประสงค์
1. เพื่อให้มั่นใจว่า หน่วยงานดำเนินการควบคุมความปลอดภัย ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
2. เพื่อทราบปัญหาอุปสรรคในการดำเนินการ

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
1. การควบคุมป้องกันมิให้ผู้ใช้งานเข้าไปกระทำความผิดตามตามพระราช - บัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 **วัตถุประสงค์** เพื่อให้มั่นใจว่าหน่วยงานได้ดำเนินการเพื่อเป็นการป้องกันมิให้ผู้ใช้งานเข้าไปกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงาน	หน่วยงานได้มีการประกาศเผยแพร่การกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงาน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้กับผู้ใช้งานทราบ	1. ตรวจสอบเอกสารหลักฐานว่ามีการประกาศเผยแพร่ข้อมูลเกี่ยวกับการกระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้กับผู้ใช้งานทราบ 2. สอบถามสัมภาษณ์ผู้บริหาร และผู้ปฏิบัติานที่เกี่ยวข้อง 3. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ	<u>เครื่องมือ</u> กระดาษทำการ IT.A2 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการประกาศเผยแพร่ <u>ข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง
2. การเก็บข้อมูลจราจรทางคอมพิวเตอร์ **วัตถุประสงค์** เพื่อให้มั่นใจว่า หน่วยงานมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	หน่วยงานที่รับผิดชอบดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ไว้จำนวนไม่น้อยกว่า 90 วัน	1. สอบถามสัมภาษณ์ผู้บริหาร และผู้ปฏิบัติงานที่เกี่ยวข้องถึงกระบวนการและหลักฐานที่แสดงว่ามีการจัดเก็บ 2. ตรวจสอบหลักฐานให้มั่นใจว่ามีการจัดเก็บครบตามวันเวลาที่กำหนดจริง 3. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ	<u>เครื่องมือ</u> กระดาษทำการ IT.A2 <u>หลักฐาน</u> เอกสารหลักฐานแสดงจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ <u>ข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นการตรวจสอบที่ 3 หน่วยงานดำเนินการควบคุมตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

วัตถุประสงค์
1. เพื่อให้มั่นใจว่า ดำเนินการควบคุมตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
2. เพื่อทราบปัญหาอุปสรรคในการดำเนินการ

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
1. การควบคุมการเข้าถึงและการควบคุมการใช้งาน (Access Control) สารสนเทศ[1] **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	1. มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลทางกายภาพเช่น โดยบัตรผ่านหรือรหัสในการเข้าสู่ส่วนที่สำคัญล็อคประตูเมื่อไม่มีการเข้าใช้งาน มีระบบ CCTV หรือยามรักษาความปลอดภัย ฯลฯ 2. มีการกำหนดสิทธิในการเข้าถึง การอนุญาต และการมอบอำนาจ 3. มีการกำหนดเกี่ยวกับ 3.1 ประเภทของข้อมูล 3.2 ชั้นความลับของข้อมูล 3.3 ระดับชั้นการเข้าถึง 3.4 เวลาที่เข้าถึง 3.5 ช่องทางที่เข้าถึง	1. ตรวจสอบหลักฐานที่แสดงว่ามีการควบคุมการเข้าถึงข้อมูลอุปกรณ์ในการประมวลผลข้อมูลทางกายภาพของหน่วยงานหรือไม่อย่างไร 2. สอบทานสิทธิ การอนุญาต และการมอบอำนาจให้เป็นไปตามคำสั่งหรือการมอบหมายสั่งการของหัวหน้าส่วนราชการ 3. มีเอกสารแสดงการจัดประเภท และลำดับความสำคัญของข้อมูล เพื่อกำหนดการเข้าถึงและช่องทางที่เข้าถึง 4. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.1 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ศูนย์ควบคุมคอมพิวเตอร์ของหน่วยงาน 3. ผู้บริหารหรือผู้ปฏิบัติ งานที่เกี่ยวข้อง
2. การกำหนดการใช้งานตามภารกิจ (Business requirements for access control)	มีข้อปฏิบัติสำหรับการใช้งานสารสนเทศตามภารกิจ โดยมีการควบคุมเป็น 2 ส่วน คือ 1. การควบคุมการเข้าถึงสารสนเทศ	1. ตรวจสอบหน่วยงานได้จัดทำข้อปฏิบัติสำหรับการใช้งานสารสนเทศตามภารกิจหรือไม่ 2. ถ้ามีให้ตรวจสอบข้อกำหนดดังกล่าวว่าครอบคลุม การควบคุมการเข้าถึงและการควบคุมด้านความปลอดภัยหรือไม่	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.2 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม

[1] หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้น ต่อบุคคลภายนอกตลอดจนอานกำหนดข้อกำหนดเกี่ยวกับการเข้าถึงโดยมิชอบไว้ด้วยก็ได้

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
วัตถุประสงค์ เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการใช้งานตามภารกิจเป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	2. การปรับปรุงให้สอดคล้องกับข้อกำหนดในการปฏิบัติงานและข้อกำหนดด้านความปลอดภัย	3. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ	<u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง
3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access Management) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานบริหารจัดการการเข้าถึงของผู้ใช้งาน ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	1. มีการให้ความรู้ ความเข้าใจให้แก่ผู้ใช้งานถึงภัยและผลกระทบจากการใช้งานระบบโดยไม่ระมัดระวังและรู้เท่าไม่ถึงการณ์ 2. มีกำหนดให้ลงทะเบียนผู้ใช้งาน เพื่ออนุญาตและเพิกถอนสิทธิ 3. มีการควบคุมและจำกัดสิทธิ โดยให้เป็นไปตามหลัก Need to know [2] 4. การให้รหัสผ่านและการ	1. สอบทานว่าหน่วยงานได้จัดให้มีการให้ความรู้ ความเข้าใจแก่ผู้ใช้งาน เป็นประจำหรือไม่ ด้วยวิธีการใด 2. สอบทานว่า 2.1 มีข้อกำหนดในการลงทะเบียนและผังขั้นตอนการปฏิบัติในการลงทะเบียน 2.2 มีข้อปฏิบัติหรือหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ 2.3 มีข้อปฏิบัติหรือหลักเกณฑ์ในการยกเลิก เพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ 3. สอบทานเอกสารแสดงการกำหนดสิทธิใน(ตารางกำหนดสิทธิ) แต่ละระบบว่า มี User จำนวนกี่คน มีการสร้าง User ร่วมได้หรือไม่ สิทธิที่ให้ในแต่ละกลุ่มเป็นอย่างไร เหมาะสมหรือไม่ ทั้งนี้อาจดำเนินการตรวจสอบทุกระบบหรือสุ่มตรวจเฉพาะระบบสำคัญๆ โดยให้พิจารณาตามความจำเป็นและเหมาะสม 4. สอบทานกระบวนการในการให้รหัส	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.3 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

[2] ให้เข้าถึง/รู้ได้เท่าที่จำเป็นต้องรู้

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
	เพิกถอนรหัสให้กับผู้ใช้งาน มีการดำเนินการผ่านกระบวนการด้านการบริหาร 5. มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานเป็นระยะ	กับผู้ใช้งาน และเพิกถอนรหัสว่ามีการควบคุมอย่างรัดกุม และมีการดำเนินการผ่านกระบวนการบริหาร โดยควรกำหนดเงื่อนไขให้ผู้งานเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้หน่วยงานได้มีการพิจารณาถึงลำดับชั้นความลับของระบบ/ ข้อมูล ในการเข้าถึงแล้ว 5. สอบทานว่าหน่วยงานจัดให้มีการทบทวนสิทธิของผู้ใช้งานเป็นปกติประจำ เช่น ทุก 3 เดือน หรือทุก 6 เดือน เป็นต้น และตรวจสอบจากเอกสารหลักฐานว่าดำเนินการทบทวนหรือไม่ 6. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ 7. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	
4. การกำหนดหน้าที่ความรับผิดชอบ (User Responsibilities) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมกำหนดหน้าที่ความรับผิดชอบเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือลักลอบทำสำเนาข้อมูลสารสนเทศ หรือ ลักขโมยอุปกรณ์ประมวลผลตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	1. กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้รหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ 2. กำหนดข้อปฏิบัติในการป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน	1. สอบทานกระบวนการในการกำหนดรหัสผ่านว่ามีข้อแนะนำในการกำหนดรหัสข้อกำหนดในการใช้งาน รวมถึงการเปลี่ยนรหัส หรือไม่ กรณีที่ผู้ใช้งานไม่ดำเนินการ ตามที่กำหนด ดำเนินการอย่างไร 2. สอบทานว่ามีข้อปฏิบัติในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานหรือไม่ ดำเนินการสร้างความตระหนักให้ผู้ใช้งาน เอาใจใส่ต่อการป้องกันอุปกรณ์ของสำนักงานขณะที่ไม่มีผู้ใช้งาน ด้วยวิธีการใด	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.4 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
	3. กำหนดวิธีการควบคุมข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์[3] ด้านสารสนเทศ	3. หน่วยงานมีการกำหนดวิธีการควบคุมไม่ให้มีการทิ้งหรือปล่อยให้ข้อมูลสารสนเทศ หรืออุปกรณ์สารสนเทศที่สำคัญ ไว้ในที่ที่ไม่ปลอดภัย ตามนโยบายเคลียร์โต๊ะเคลียร์หน้าจอ (Clear desk clear screen policy) และมีการดำเนินการตามนั้นหรือไม่	
	4. กำหนดการควบคุมป้องกัน ผู้ใช้งานนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ	4. หน่วยงานได้มีการกำหนดข้อปฏิบัติและหลักเกณฑ์สำหรับการเข้าถึงข้อมูลลับและข้อมูลที่สำคัญขององค์กรหรือไม่อย่างไร	
		5. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ	
		6. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	
5. การควบคุมการเข้าถึงระบบเครือข่าย (Network access control) **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานระบบเครือข่ายตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	1. ผู้ใช้งานสามารถเข้าถึงได้เฉพาะบริการที่ได้รับสิทธิให้เข้าถึงเท่านั้น	1.1 หน่วยงานต้องมีเอกสารหลักฐานที่แสดงว่ามีระบบสารสนเทศอะไรบ้างในหน่วยงานที่ต้องควบคุมการเข้าถึง 1.2 หน่วยงานต้องแสดงข้อปฏิบัติที่กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่อนุญาตให้เข้าถึงเท่านั้น 1.3 สำหรับหน่วยงานที่มีระบบคอมพิวเตอร์ขนาดใหญ่ที่มีการเชื่อมต่อเครื่อง terminal ให้สำหรับผู้ใช้งานหน่วยงานได้มีการควบคุมที่เข้มงวดในการเชื่อมต่อระหว่างเครื่อง Terminal ของผู้ใช้งาน กับระบบของหน่วยงานหรือไม่	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.5 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

[3] นิยามตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดให้หมายถึง สิ่งใดๆ ก็ตามที่คุณค่าสำหรับองค์กร

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
	2. การเข้าใช้งานจากภายนอกต้องได้รับการยืนยันบุคคลก่อนจึงจะสามารถเข้าใช้งานได้	2. หน่วยงานต้องแสดงข้อปฏิบัติหรือกระบวนการที่จะช่วยยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้จากภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายหรือระบบสารสนเทศของหน่วยงานได้	
	3. ต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้	3. หน่วยงานต้องแสดงวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึงได้	
	4. กำหนดการควบคุมป้องกัน Portที่ใช้สำหรับการตรวจสอบและการปรับแต่งระบบทั้งจากการเข้าถึงภายในระบบ และการเข้าถึงจากเครือข่าย	4. หน่วยงานต้องกำหนดขั้นตอน/หลักเกณฑ์ในการควบคุมการเข้าถึง Portที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ โดยจำแนกเป็น 4.1 การเข้าถึงทางกายภาพ 4.2 การเข้าถึงทางเครือข่าย อย่างไรก็ตาม เนื่องจากการเข้าถึง Port เป็นเรื่องที่มีความเสี่ยงสูง การกำหนดขั้นตอน/หลักเกณฑ์ในการควบคุมจึงต้องไม่ระบุ Port ไว้ และต้องไม่กำหนดรายละเอียดใดๆ ไว้ในขั้นตอน/หลักเกณฑ์การควบคุมที่จะทำให้เข้าถึง Port ได้	
	5. แบ่งแยกเครือข่ายสำหรับให้บริการ สารสนเทศตามกลุ่มการให้บริการ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ	5. หน่วยงานมีการแบ่งแยกเครือข่ายสำหรับกลุ่มต่าง ๆ ดังนี้ (1) กลุ่มของบริการสารสนเทศ (2) กลุ่มของผู้ใช้งาน (3) กลุ่มของระบบสารสนเทศ ทั้งนี้ผู้ตรวจสอบสามารถสอบทานได้จากเอกสาร Network diagram	

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
	6. กำหนดการควบคุมการเชื่อมต่อเครือข่ายที่มาใช้ร่วมกันหรือใช้เชื่อมกันระหว่างหน่วยงาน ให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง	6. ให้สอบทานว่าหน่วยงานได้มีการกำหนดขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงและการใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อกันระหว่างหน่วยงานว่าสอดคล้องหรือเป็นไปตามข้อปฏิบัติการควบคุมการเข้าถึงที่หน่วยงานกำหนดหรือไม่ และในกรณีที่หน่วยงานมีการ Share network โดยอาจมีการโอนfile ระหว่างกัน (file transfers) ต้องควบคุมให้มั่นใจว่า ไม่สามารถขยายออกไปนอกหน่วยงานได้	
	7. กำหนดการควบคุมการจัดเส้นทางบนเครือข่าย ให้สอดคล้องกับข้อปฏิบัติในการเข้าถึง และการประยุกต์ใช้งานตามภารกิจ	7. ให้สอบทานว่าหน่วยงานได้มีการกำหนดขั้นตอนหรือหลักเกณฑ์ในการควบคุมการจัดเส้นทางบนเครือข่ายดังนี้ 7.1 การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านข้อมูลหรือไหลเวียนของข้อมูลหรือสารสนเทศ ต้องไม่ทำให้เกิดช่องโหว่ในการควบคุมการเข้าถึงหรือใช้งานในโปรแกรมประยุกต์ 7.2 ข้อกำหนดต้องสอดคล้องกับข้อปฏิบัติ การควบคุมการเข้าถึง และการประยุกต์ใช้งานตามภารกิจ 8. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ 9. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	
6. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)	1. มีขั้นตอนปฏิบัติเพื่อเข้าใช้งานที่มั่นคงปลอดภัย และต้องควบคุมโดยการยืนยันตัวตน	1. หน่วยงานต้องสามารถแสดงขั้นตอนการปฏิบัติในการเข้าถึงเรื่องต่อไปนี้ ว่าต้องใช้วิธีการยืนยันตัวตนจึงจะสามารถเข้าถึงได้	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.6 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
วัตถุประสงค์ เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานระบบปฏิบัติการ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์		1.1 การควบคุมการเข้าใช้งานในที่มั่นคงปลอดภัย 1.2 การเข้าถึงระบบปฏิบัติ	<u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติ งานที่เกี่ยวข้อง
	2. กำหนดให้ผู้ใช้งานมีข้อมูลจำเพาะที่สามารถระบุตันตนของผู้ใช้งานได้	2. สอบทานหลักฐานที่แสดงให้เห็นว่า 2.1 หน่วยงานได้มีการกำหนดให้ผู้ใช้งานแสดงข้อมูลจำเพาะในการยืนยันตัวตนของผู้ใช้งานได้ 2.2 หน่วยงานได้กำหนดขั้นตอนการยืนยันตัวตนของผู้ใช้งาน	
	3. กำหนดระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบได้ (interactive)	3. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบหรือทำงานอัตโนมัติได้	
	4. มีการจำกัดหรือควบคุมการใช้งานโปรแกรมอรรถประโยชน์[4]	4. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการใช้งานโปรแกรมอรรถประโยชน์ได้ โดยข้อกำหนดต้องครอบคลุม การป้องกันการละเมิด และการหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย	
	5. กำหนดให้เครื่องยุติการใช้งาน หากว่างเว้นการใช้งานใดๆ ระยะเวลาหนึ่ง (เช่น การเปิดเครื่องทิ้งไว้โดยไม่ดำเนินการใดๆ)	5. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการให้เครื่องยุติการใช้งานหากว่างเว้นการใช้งานใดๆ ระยะเวลาหนึ่ง (session time-out)	
	6. จำกัดเวลาในการ	6. ให้หน่วยงานแสดงข้อปฏิบัติหรือ	

[4] โปรแกรมอรรถประโยชน์ หรือ Utility Program คือ โปรแกรมที่ติดมาพร้อมกับระบบปฏิบัติการวินโดว์ เรียกง่ายๆว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดว์เพราะมีหลากหลายประเภทเช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บีบอัดไฟล์ ฯลฯ

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
	เชื่อมต่อระบบสารสนเทศ (เช่น ต่ออินเตอร์เน็ตทิ้งไว้โดยไม่ใช้งานใดๆ)	หลักเกณฑ์ในการจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศหรือโปรแกรมประยุกต์ (Application) ที่มีความสำคัญหรือมีความเสี่ยงสูง 7. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ 8. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	
7. การควบคุมการเข้าถึงโปรแกรมประยุกต์ และสารสนเทศ **วัตถุประสงค์** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานโปรแกรมประยุกต์และสารสนเทศตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	1. จำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชันต่างๆของโปรแกรมประยุกต์หรือ Application จากผู้ใช้งานและบุคลากรฝ่ายสนับสนุน 2. จัดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน	1. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการจำกัดเวลาและการควบคุมการเข้าถึงหรือใช้งานของผู้ใช้งานหรือบุคลากร โดยให้สอดคล้องกับนโยบายการควบคุมการเข้าถึงสารสนเทศ 2. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน 3. ให้สอบทานว่าหน่วยงานได้มีการกำหนดข้อปฏิบัติและมาตรการเพื่อป้องกันสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ 4. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ 5. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.7 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติ งานที่เกี่ยวข้อง

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
8. การจัดให้มีการสำรองและเตรียมความพร้อมกรณีฉุกเฉิน **วัตถุประสงค์** เพื่อให้มั่นใจว่าหน่วยงานมีการจัดระบบสำรองและจัดแผนเตรียมความพร้อมกรณีฉุกเฉินตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	1. มีการพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมและอยู่ในสภาพพร้อมใช้	1.1 ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการคัดเลือกระบบสารสนเทศ 1.2 ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการจัดทำระบบสำรองที่เหมาะสมและพร้อมใช้งาน ทั้งนี้ให้สอบทานขั้นตอนปฏิบัติว่าได้มีการกำหนดให้มีการกู้คืนและรายงานผลการสำรองข้อมูลในทุกระบบด้วย	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.8 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติ งานที่เกี่ยวข้อง
	2. มีแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติและต่อเนื่อง	2. ให้หน่วยงานแสดงแผนเตรียมความพร้อมกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ รวมทั้งในกรณีที่ Site หลักทำงานไม่ได้ ว่าในระยะสั้น (เร่งด่วน) ดำเนินการอย่างไร ระยะยาวดำเนินการอย่างไร และควรทบทวนแผน 3 เดือนครั้ง	
	3. กำหนดหน้าที่ความรับผิดชอบของบุคลากรที่ทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และจัดทำแผนความพร้อมกรณีฉุกเฉิน	3. ให้หน่วยงานระบุบุคลากร พร้อมทั้งแสดงรายละเอียดหน้าที่ความรับผิดชอบของบุคลากรในเรื่องดังต่อไปนี้ 3.1 ระบบสารสนเทศ 3.2 ระบบสำรอง 3.3 แผนเตรียมความพร้อมกรณีฉุกเฉิน	
	4. มีการทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง และการดำเนินการตามแผนเตรียมความพร้อม อย่างสม่ำเสมอ	4. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการทดสอบสภาพความพร้อมใช้ในเรื่องต่อไปนี้ 4.1 ระบบสารสนเทศ 4.2 ระบบสำรอง 4.3 แผนเตรียมความพร้อมกรณีฉุกเฉินและควรแสดงความถี่ในการปฏิบัติในเรื่องที่กล่าวมาข้างต้นด้วย	

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
		5. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ 6. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	
9. การจัดให้มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ **วัตถุประสงค์** เพื่อให้มั่นใจว่า หน่วยงานจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ	หน่วยงานจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายในหรือผู้ประเมินความเสี่ยงจากภายนอกหน่วยงาน	1. หน่วยงานมีการกำหนดนโยบายและมาตรการให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้น 2. มีการรายงานผลการตรวจสอบหรือประเมินความเสี่ยงจากผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกแล้วแต่กรณี 3. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	<u>เครื่องมือ</u> กระดาษทำการ IT.A3.9 <u>หลักฐาน</u> เอกสารหลักฐานแสดงการควบคุม <u>แหล่งข้อมูล</u> 1. หน่วยงานที่ดูแลด้าน IT 2. ผู้บริหารหรือผู้ปฏิบัติ งานที่เกี่ยวข้อง

งบประมาณที่ใช้ในการตรวจสอบ

แผนงาน.....งบประมาณ.....

ผู้จัดทำ.....

วันที่.....

ผู้อนุมัติ.....

วันที่.....