แนวทางการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๕๖

กลุ่มตรวจสอบภายในระดับกระทรวง
กระทรวงศึกษาธิการ

คำนำ

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายในภาครัฐ (Internal Audit) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของสารสนเทศของหน่วยงาน ประกอบกับมาตรฐานการตรวจสอยภายในและแนวทางการประกันคุณภาพงานตรวจสอบภายในภาครัฐ กำหนดมาตรฐานด้านคุณสมบัติ รหัส 1210.A3 ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ ได้แก่ การควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแล โดยจัดให้มีระบบควบคุมในส่วนโครงสร้างพื้นฐานด้านสารสนเทศ เช่น ระบบงานข้อมูล ระบบเครือข่าย และระบบบุคลากร ซึ่งประกอบด้วย การควบคุมทั่วไปและแบบเฉพาะทาง รวมถึงเทคนิควิธีการตรวจสอบด้านเทคโนโลยีสารสนเทศ และประเด็นที่ใช้พิจารณา : การวางแผนการตรวจสอบ การเสนอ และการอนุมัติแผนการตรวจสอบ กำหนดให้การวางแผนการตรวจสอบครอบคลุมประเภทงานให้ความเชื่อมั่น ควรครอบคลุมการตรวจสอบด้านสารสนเทศ ดังนั้น เพื่อให้การดำเนินงานของส่วนราชการเป็นไปตามกฎหมาย ประกาศแนวนโยบาย และผ่านเกณฑ์การประกันคุณภาพงานตรวจสอบภายในภาครัฐกำหนด

กระทรวงศึกษาธิการ จึงได้บูรณาการงานตรวจสอบภายในร่วมกับหน่วยงานตรวจสอบภายในในสังกัด เพื่อให้มีแนวทางในการดำเนินงานไปในทิศทางเดียวกัน สามารถประมวลผลในภาพรวมของกระทรวงศึกษาธิการได้ โดยได้จัดทำแผนปฏิบัติงานตรวจสอบ และแนวทางการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศ ในปีงบประมาณ พ.ศ. 2556 ขึ้น เพื่อให้ผู้ตรวจสอบภายในสังกัดกระทรวงศึกษาธิการ นำไปใช้ในการปฏิบัติงาน และรายงานผลตรวจสอบเป็นไปในแนวทางเดียวกันต่อไป

กระทรวงศึกษาธิการ

ตุลาคม 2555

สารบัญ

หน้า

คำนำ

- แผนการปฏิบัติงานตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศ 1
- วัตถุประสงค์ของการตรวจสอบ 1
- ขอบเขตและวิธีการตรวจสอบ 2
- ขั้นตอนการดำเนินงาน 2
- ข้อมูลพื้นฐานเพื่อประกอบการตรวจสอบ 3
- กรอบประเด็นการตรวจสอบ 6
- นิยามศัพท์ 7
- แผนผังขั้นตอนการตรวจสอบ 8
- แนวทางการปฏิบัติงานการตรวจสอบระบบการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2556 11

ภาคผนวก

- **กระดาษทำการ**
  - กระดาษทำการตรวจสอบแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ IT.A1 24
  - กระดาษทำการตรวจสอบแนวนโยบายการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่กระทบ พ.ร.บ.คอมพิวเตอร์ IT.A2 25
  - กระดาษทำการตรวจสอบการควบคุมการเข้าถึงและควบคุมใช้งาน IT.A3.1 27
  - กระดาษทำการตรวจสอบการใช้งานตามภารกิจ IT.A3.2 28
  - กระดาษทำการตรวจสอบการบริหารจัดการการเข้าถึงผู้ใช้งาน IT.A3.3 29

สารบัญ

หน้า

- กระดาษทำการตรวจสอบการกำหนดหน้าที่ความรับผิดชอบ IT.A3.4 30
- กระดาษทำการตรวจสอบการเข้าถึงระบบเครือข่าย IT.A3.5 31
- กระดาษทำการตรวจสอบการเข้าถึงระบบปฏิบัติการ IT.A3.6 33
- กระดาษทำการตรวจสอบการเข้าถึงโปรแกรมประยุกต์ หรือ Application และสารสนเทศ IT.A3.7 34
- กระดาษทำการตรวจสอบการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน IT.A3.8 35
- กระดาษทำการสอบทานการจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ IT.A3.9 36

- **โครงการบูรณาการงานตรวจสอบภายในกระทรวงศึกษาธิการ ประจำปีงบประมาณ พ.ศ. 2556** 37

แผนการปฏิบัติงานตรวจสอบ
ระบบความมั่นคงปลอดภัยด้านสารสนเทศ

ปัจจุบันเทคโนโลยีสารสนเทศเพื่อการสื่อสาร มีความก้าวหน้าอย่างรวดเร็ว การทำธุรกรรมในระบบอิเล็กทรอนิกส์ขยายตัวเพิ่มมากขึ้น หน่วยงานภาครัฐจึงได้รับการสนับสนุนให้มีการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว ซึ่งจะเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการให้บริการ และเพื่อให้หน่วยงานภาครัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภายใต้มาตรฐานเดียวกัน และเพื่อเป็นการสร้างความเชื่อมั่นต่อประชาชน จึงได้มีการตราพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2549 ขึ้นตามลำดับ

แต่อย่างไรก็ตาม สิ่งที่พัฒนาพร้อมกับความก้าวหน้าทางด้านเทคโนโลยี คือ ปัญหาด้านความปลอดภัยของระบบสารสนเทศที่มีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ และมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทั้งในส่วนของผู้ประกอบการ องค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ทำให้หน่วยงานเหล่านั้นขาดความเชื่อมั่นต่อการทำธุรกิจในทุกรูปแบบ และเพื่อเป็นการป้องกันและแก้ไขปัญหาดังกล่าว จึงได้มีการกำหนดกฎหมายและประกาศเพิ่มเติม ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ตามประกาศคณะกรรมการธุรกรรมฯ ในข้อ 13 (2) กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัย (External Auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับ ความเสี่ยง และระดับความมั่นคงปลอดภัยของสารสนเทศของหน่วยงาน

กอปรกับมาตรฐานการตรวจสอบภายใน และแนวทางการประกันคุณภาพงานตรวจสอบภายในภาครัฐ กำหนดมาตรฐานด้านคุณสมบัติรหัส 1210.A3 ว่า ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ ซึ่งได้แก่ การควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแล โดยจัดให้มีระบบการควบคุมในส่วนโครงสร้างพื้นฐานด้านสารสนเทศ เช่น ระบบงานข้อมูล ระบบเครือข่าย และบุคลากร ซึ่งประกอบด้วย การควบคุมทั่วไป (General Controls) และแบบเฉพาะทาง (Technical Controls) รวมถึงเทคนิควิธีการตรวจสอบด้านเทคโนโลยีสารสนเทศ และประเด็นที่ใช้พิจารณา : การวางแผนตรวจสอบ การเสนอ และอนุมัติแผนการตรวจสอบ กำหนดให้ การวางแผนการตรวจสอบครอบคลุมประเภทงานให้ความเชื่อมั่นควรครอบคลุมการตรวจสอบด้านสารสนเทศ ด้วย

เพื่อให้การดำเนินงานของส่วนราชการเป็นไปตามกฎหมาย ประกาศแนวนโยบายฯ และผ่านเกณฑ์การประกันคุณภาพงานตรวจสอบภายในภาครัฐ กระทรวงศึกษาธิการจึงได้บูรณาการงานตรวจสอบภายในกับหน่วยงานในสังกัด ได้แก่ หน่วยงานหลัก และมหาวิทยาลัยในสังกัด

วัตถุประสงค์การตรวจสอบ

1. เพื่อให้มั่นใจว่า หน่วยงานจัดให้มีการควบคุมด้านการรักษาความปลอดภัยระบบสารสนเทศตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
2. เพื่อให้มั่นใจว่า หน่วยงานปฏิบัติงานด้านการรักษาความปลอดภัยระบบสารสนเทศตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
3. เพื่อให้ทราบปัญหา และอุปสรรคในการปฏิบัติงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอีเล็กทรอนิกส์ฯ และให้ข้อเสนอแนะเพื่อการพัฒนางาน

ขอบเขตและวิธีการตรวจสอบ

1. ดำเนินการสอบทานเอกสารหลักฐานที่เกี่ยวข้องกับการจัดให้มีการควบคุมและการปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ที่หน่วยงานใช้อยู่ในปัจจุบัน
2. ดำเนินการสุ่มสอบทานการปฏิบัติตามนโยบายและข้อปฏิบัติของหน่วยงาน
3. สังเกตการปฏิบัติงานจริงตามระบบควบคุมที่กำหนดตามนโยบายและข้อปฏิบัติ
4. สอบถามและสัมภาษณ์ ผู้บริหารและผู้ปฏิบัติงาน

ขั้นตอนการดำเนินงาน

1. ศึกษาข้อมูลพื้นฐานประกอบการตรวจสอบ แนวทางการปฏิบัติงานตรวจสอบ และกระดาษทำการ
2. ดำเนินการตรวจสอบโดย

2.1 แจ้งหน่วยรับตรวจ (หน่วยงานที่ดูแลระบบสารสนเทศขององค์กร) ถึงวันที่จะดำเนินการเปิดตรวจ

2.2 ประชุมเปิดตรวจเพื่อชี้แจงวัตถุประสงค์ ขอบเขต แนวทางและวิธีการตรวจสอบ พร้อมทั้งขอความร่วมมือในการให้ข้อมูล

2.3 ดำเนินการตรวจสอบตามแนวทางการปฏิบัติงานตรวจสอบ และบันทึกข้อมูลการตรวจสอบในกระดาษทำการ

2.4 เมื่อดำเนินการตรวจสอบแล้วเสร็จ ให้สรุปผลจากกระดาษทำการเก็บข้อมูลลงในกระดาษทำการสรุปผล

2.5 ประชุมปิดตรวจ เพื่อสรุปผลการตรวจสอบ ทำความเข้าใจ ชี้แจง และขอความเห็นเพิ่มเติมในบางประเด็นที่ยังเป็นที่สงสัย พร้อมขอบคุณผู้ที่มีส่วนเกี่ยวข้องในการให้ข้อมูลการตรวจสอบ

3. ร่างรายงานผลการตรวจสอบ พร้อมทั้งแจ้งให้หน่วยรับตรวจทราบผลเพื่อพิจารณาให้ความเห็น แล้วจัดทำรายงานผลการตรวจสอบพร้อมแนบความเห็นของหน่วยรับตรวจ เสนอผู้บริหารเพื่อพิจารณาสั่งการ

4. สำเนารายงานผลการตรวจสอบ ส่งกลุ่มตรวจสอบภายในระดับกระทรวง กระทรวงศึกษาธิการภายในเดือนมิถุนายน 2556

ข้อมูลพื้นฐานเพื่อประกอบการตรวจสอบ

1. **การตรวจสอบด้านสารสนเทศ** ตามมาตรฐานการตรวจสอบภายในของกรมบัญชีกลางที่กำหนดในมาตรฐานการตรวจสอบภายในรหัส 1210.A3 กำหนดให้ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านสารสนเทศ

2. **โครงสร้างพื้นฐานด้านสารสนเทศ** ประกอบด้วย

   2.1 อุปกรณ์: Hardware

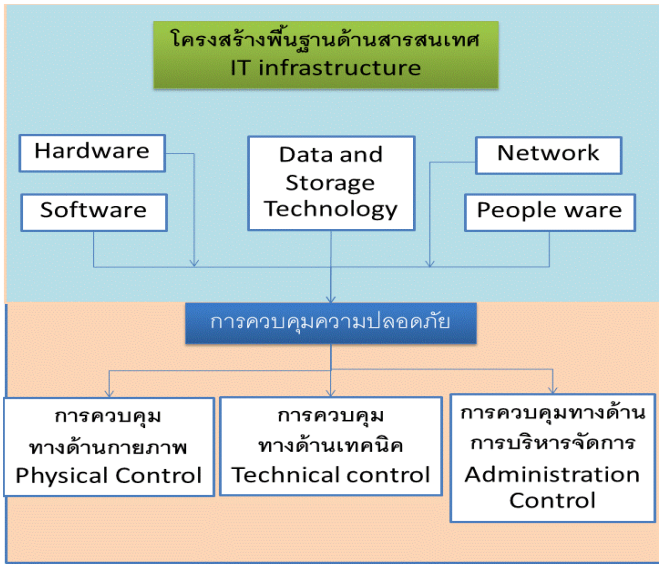
   2.2 โปรแกรม: Software

   2.3 ฐานข้อมูล: Data & Storage Technology

   2.4 เครือข่าย: Networks

   2.5 บุคลากร: People ware

ผังแสดงความเชื่อมโยงโครงสร้างพื้นฐานด้านสารสนเทศและการควบคุมความปลอดภัย



3. **การควบคุมความปลอดภัย** แบ่งเป็น 3 ด้าน คือ

   3.1 มุมมองทางด้านกายภาพ (Physical Control)

   3.2 มุมมองทางด้านเทคนิค (Technical Control)

   3.3 มุมมองทางด้านการบริหารจัดการ (Administrative Control)

การจำแนกงานตรวจสอบตามมุมมองการควบคุม จากมุมมองทางด้านการควบคุม ทำให้งานตรวจสอบทางด้าน IT แบ่งเป็น 3 ด้าน ได้แก่

3.1 ด้านกายภาพ

การตรวจสอบด้านกายภาพ (Physical Control) ได้แก่ ระบบควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์, Hardware ระบบ Backup/Restore และ ระบบไฟสำรอง เช่น มี UPS เพียงพอหรือไม่ และอุปกรณ์เฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) เป็นต้น

3.2 ด้านเทคนิค (Technical Control) ได้แก่

1). การตรวจสอบระบบปฏิบัติการ (NOS Audit) เช่น การตรวจสอบระบบ Server ที่ใช้ MS Windows เช่น Windows NT, Window 2000 Server ตลอดจน Workstation ที่ใช้ Windows XP เป็นต้น การตรวจสอบควรจะครอบคลุมถึงระบบปฏิบัติการอื่นด้วย เช่น การตรวจสอบระบบปฏิบัติการ Unix เช่น Sun Solaris, HP/UX, IBM AIX และ ระบบปฏิบัติการ Linux ที่ได้รับความนิยมเพิ่มขึ้นเรื่อยๆ

2). การตรวจสอบอุปกรณ์เครือข่าย (Network Devices Audit) เช่น การตรวจสอบ Router, การตรวจสอบ Switching และ การตรวจสอบ Remote Access Server ตลอดจน การตรวจสอบโครงสร้างของเครือข่าย (Network Infrastructure Audit) และ ประสิทธิภาพของเครือข่าย (Network Performance Audit) โดยใช้โปรแกรมตรวจสอบประเภท Packet Sniffer หรือ RMON Probe เป็นต้น

3). การตรวจสอบอุปกรณ์รักษาความปลอดภัย (Security Devices Audit) เช่น การตรวจสอบ Firewall, การตรวจสอบ Intrusion Detection System (IDS), การตรวจสอบ Intrusion Prevention System (IPS), การตรวจสอบโปรแกรม Enterprise Anti-Virus, การตรวจสอบ VPN Server เป็นต้น การตรวจสอบอุปกรณ์รักษาความปลอดภัยนั้นเป็นสิ่งที่มีความจำเป็นอย่างสูง เพราะถ้าอุปกรณ์รักษาความปลอดภัยมีปัญหาเสียเอง หรือโดน Hacker เจาะเข้ามา compromised ก็จะทำให้เกิดปัญหากับความปลอดภัยของระบบโดยรวม ผู้ตรวจสอบควรเป็นผู้ชำนาญงานด้านการใช้งาน Firewall หรือ IDS/IPS มาก่อนด้วยจะช่วยได้มาก

4). การตรวจสอบโปรแกรมฐานข้อมูล (RDBMS Audit) เช่น การตรวจสอบ Oracle, IBM DB2, Microsoft SQL Server, Informix, SYBASE หรือ MySQL RDBMS การตรวจสอบโปรแกรมฐานข้อมูลควรกระทำ ควบคู่ไปกับการตรวจสอบระบบปฏิบัติการที่โปรแกรมฐานข้อมูลทำงานอยู่ เช่น Oracle ทำงานบน Unix เป็นต้น เพื่อที่จะเจาะลึกลงไปในด้านความปลอดภัยของตัวโปรแกรมฐานข้อมูลเองว่ามีช่องโหว่หรือไม่ ผู้ตรวจสอบควรเป็นผู้เชี่ยวชาญการใช้งานโปรแกรมฐานข้อมูลนั้นๆมาก่อน เพราะการตรวจสอบต้องใช้ความรู้เชิงลึกทางด้าน RDBMS ด้วย

5). การตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการในลักษณะ Server (Application Specific Audit) เช่น การตรวจสอบ Web Server IIS บน Microsoft Windows Platform และ การตรวจสอบ Web Server Apache บน Unix/Linux Platform ซึ่งทั้ง 2 เป็นโปรแกรม Web Server ยอดนิยมอยู่ใน ขณะนี้ นอกจากการตรวจสอบ Web Server แล้ว IT Auditor ควรตรวจสอบ Mail Server, FTP Server, LDAP Server, RADIUS Server ตลอดจน DNS Server ซึ่งถือเป็นหัวใจหลักของระบบ หาก DNS Server มีปัญหาจะทำให้ระบบไม่สามารถอ้างอิง Hostname ได้ ซึ่งจะก่อให้เกิดปัญหาใหญ่กับระบบ โดยรวม

3.3 ด้านการบริหารจัดการ (Administrative Control)

การตรวจสอบกระบวนการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control) ได้แก่ การตรวจสอบ Policy, Standard, Guideline และ Procedure ที่องค์กรมีอยู่ว่าครอบคลุม และ มีการปฏิบัติตามหรือไม่ ในขั้นตอนนี้รวมถึงการตรวจสอบว่าองค์กรมีการจัด ฝึกอบรมด้านการรักษาความปลอดภัย (Security Awareness Training) หรือไม่ ซึ่งตามปกติควรจะมีเป็นประจำทุกปี การตรวจสอบการบริหารจัดการนั้นต้องพิจารณาจากโครงสร้างหน่วยงาน, การแบ่งแยกหน้าที่ต่างๆ ในหน่วยงาน, การจัดทำแผนสำรองฉุกเฉิน และแผนรับเหตุการณ์ (Business Continuity Planning , Disaster Recovery Planning and Incident Response Procedure) ตลอดจนการควบคุมการเปลี่ยนแปลงระบบงาน (Change Control Management)

สำหรับการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศตามที่กำหนดนี้จะเป็นการตรวจสอบทางด้านกายภาพ และการตรวจสอบทางด้านการบริหารจัดการ

4. การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดในเรื่องต่อไปนี้

4.1 การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้แก่

1). การควบคุมระบบคอมพิวเตอร์ของหน่วยงานตาม มาตรา 15 เพื่อป้องกันผู้ใช้บริการที่เข้าไปกระทำความผิดตามพระราชบัญญัติคอมพิวเตอร์ เช่น นำเข้าข้อมูลอันเป็นเท็จทำให้เกิดความเสียหายต่อความมั่นคง สร้างความตื่นตระหนกต่อประชาชน หรือเผยแพร่ภาพลามกอนาจาร เป็นต้น

2). การเก็บข้อมูลจราจร ซึ่งหมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ และอื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ตามมาตรา 26 กำหนดให้หน่วยงานต้องจัดเก็บข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วันนับตั้งแต่การใช้บริการสิ้นสุดลง

การควบคุมทั้ง 2 เรื่องที่กล่าวมาข้างต้น หน่วยงานดำเนินการ ด้วยวิธีการ ดังนี้คือ

1). การควบคุมการเข้าสู่ระบบ (Access Control) ด้วยการกำหนด Username และ Password ให้กับผู้ใช้งาน

2). การเก็บ Log file ข้อมูลจราจรทางคอมพิวเตอร์ของหน่วยงาน

โดยปกติ Log file เป็นไฟล์ที่ถูกสร้างขึ้นอัตโนมัติ โดยโปรแกรม (ซึ่งผู้เขียนโปรแกรมต้องเขียนเรื่องนี้ไว้) เพื่อใช้ในการเก็บข้อมูลสถานะต่างๆ โดยจะบันทึกข้อมูลทั้งหมดที่เกิดขึ้นตั้งแต่ผู้ใช้บริการเข้าสู่ระบบ (Log - In) จนกระทั่งผู้ใช้บริการออกนอกระบบ (Log - Out) หรือปิดการใช้งาน และในบางโปรแกรม เช่น โปรแกรม GFMIS จะมีการเก็บ Log file ไว้เพื่อการตรวจสอบ และบางโปรแกรม Log file สามารถใช้เพื่อสั่งให้ระบบย้อนกลับไปปฏิบัติงานได้ในกรณีที่เกิดปัญหาได้

4.2 การควบคุมประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดดังนี้

1). ให้จัดทำนโยบายและข้อปฏิบัติให้ครอบคลุมเนื้อหาตามที่ประกาศกำหนด

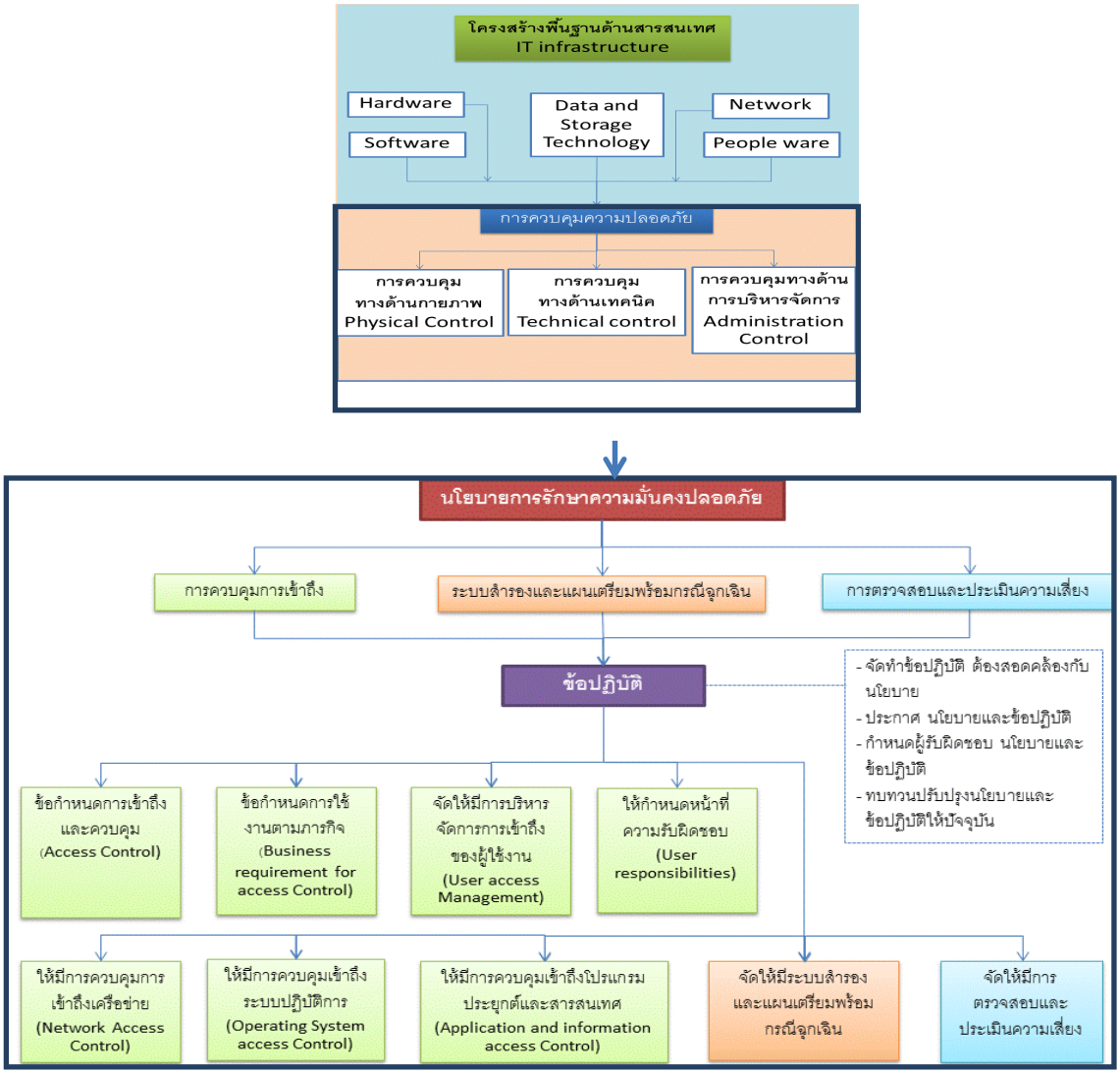
2). ให้ประกาศเผยแพร่นโยบายและข้อปฏิบัติ พร้อมทั้งทบทวนให้เป็นปัจจุบัน

3). ให้ปฏิบัติตามนโยบายและข้อปฏิบัติที่กำหนดและประกาศไว้

4). กรณีที่เกิดความเสียหายหรืออันตรายต่อองค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติ ผู้บริหารระดับสูงต้องรับผิดชอบต่อความเสียหายดังกล่าว

5). หน่วยงานสามารถเลือกใช้ข้อปฏิบัติที่ต่างจากประกาศได้ หากมีความเหมาะสมกว่าหรือเทียบเท่า

ผังแสดง ความเชื่อมโยงการควบคุมความปลอดภัยกับนโยบายและข้อปฏิบัติตามประกาศของหน่วยงาน



กรอบประเด็นการตรวจสอบ

ประเด็นที่ 1 นโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ

1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติ คลอบคลุมข้อกำหนดตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ

1.2 การเผยแพร่นโยบายและข้อปฏิบัติ ให้ผู้ที่เกี่ยวข้องทราบสามารถเข้าถึงเข้าใจและปฏิบัติตามได้

1.3 กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติที่ชัดเจน

1.4 ทบทวนนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ประเด็นที่ 2 การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ประเด็นที่ 3 การควบคุมตามประกาศคณะกรรมการธุรกรรมฯ

3.1 การเข้าถึงและการควบคุมการใช้งาน (Access Control)

3.1.1 การกำหนดการเข้าถึงสารสนเทศ

1). การควบคุมการเข้าถึงระบบสารสนเทศ

2). การควบคุมการเข้าถึงระบบเครือข่าย

3). การควบคุมการเข้าถึงระบบปฏิบัติการ

4). การควบคุมการเข้าถึงโปรแกรมประยุกต์ (Applications) และสารสนเทศ

3.1.2 การกำหนดการใช้งานตามภารกิจ

3.1.3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

3.1.4 การกำหนดหน้าที่ความรับผิดชอบ

3.2 การจัดให้มีระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

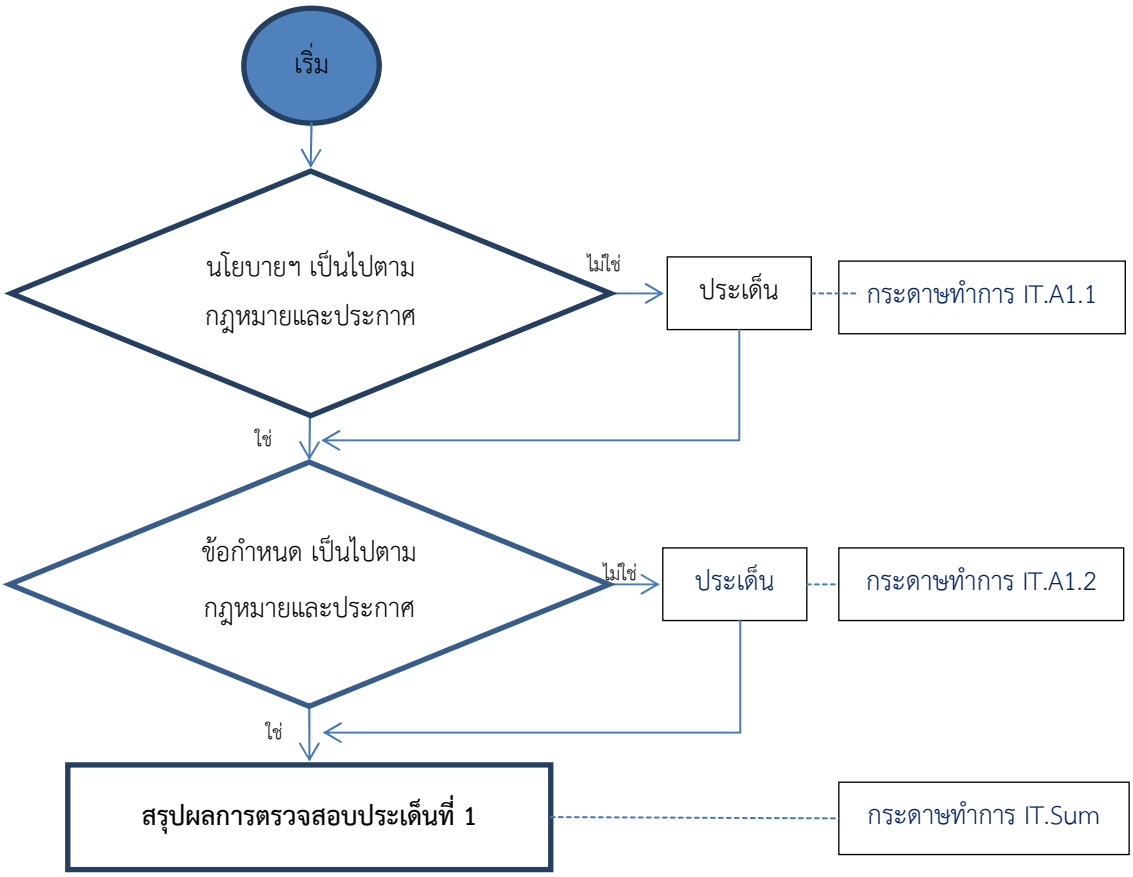
3.3 การจัดให้มีการตรวจสอบและประเมินความเสี่ยง

นิยามศัพท์ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

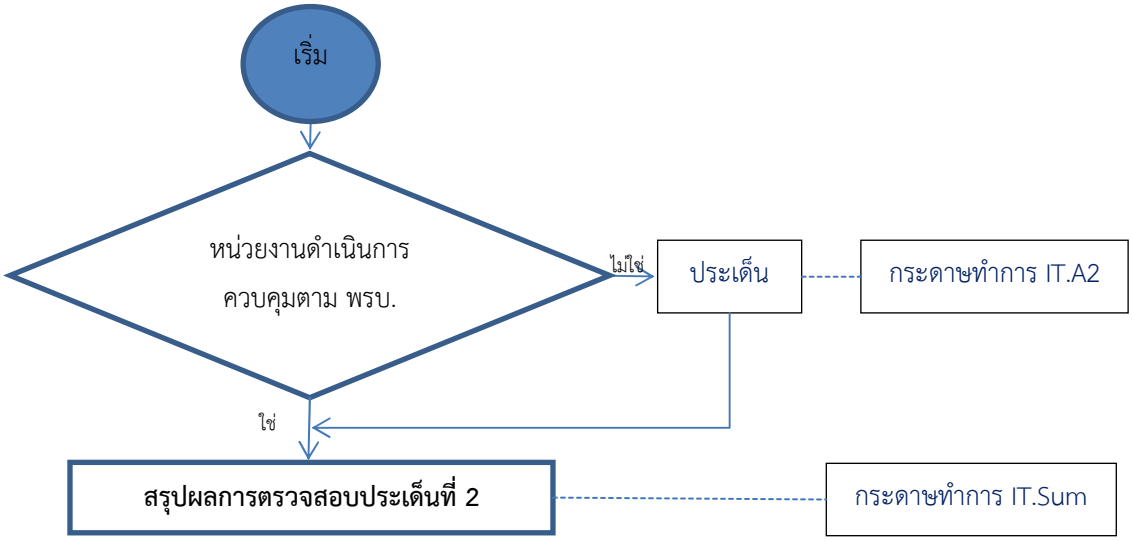
รายการ	ความหมาย
ผู้ใช้งาน	ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป
สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
ความมั่นคงปลอดภัยด้านสารสนเทศ	การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

แผนผังขั้นตอนการตรวจสอบ

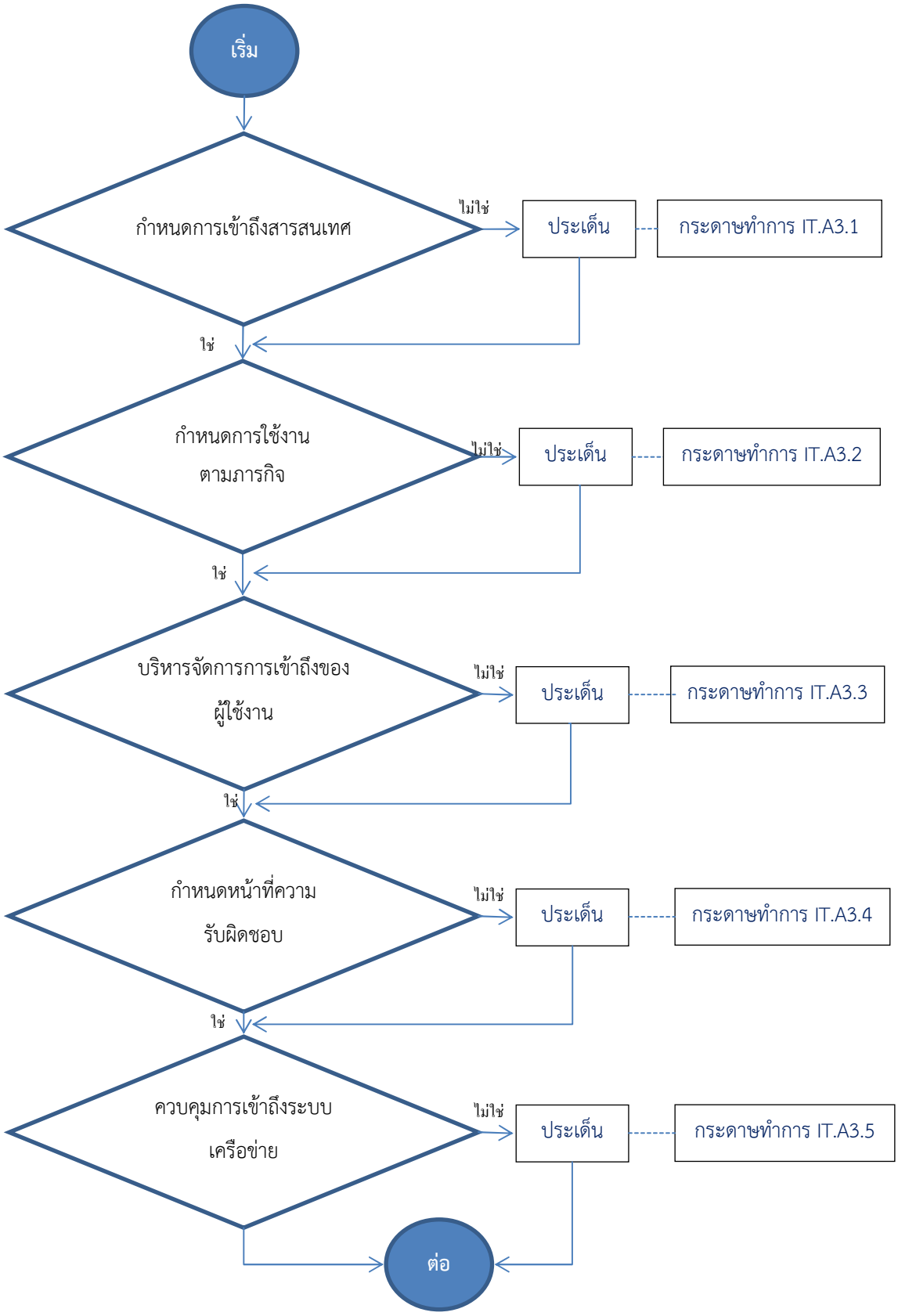
ประเด็นที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศ

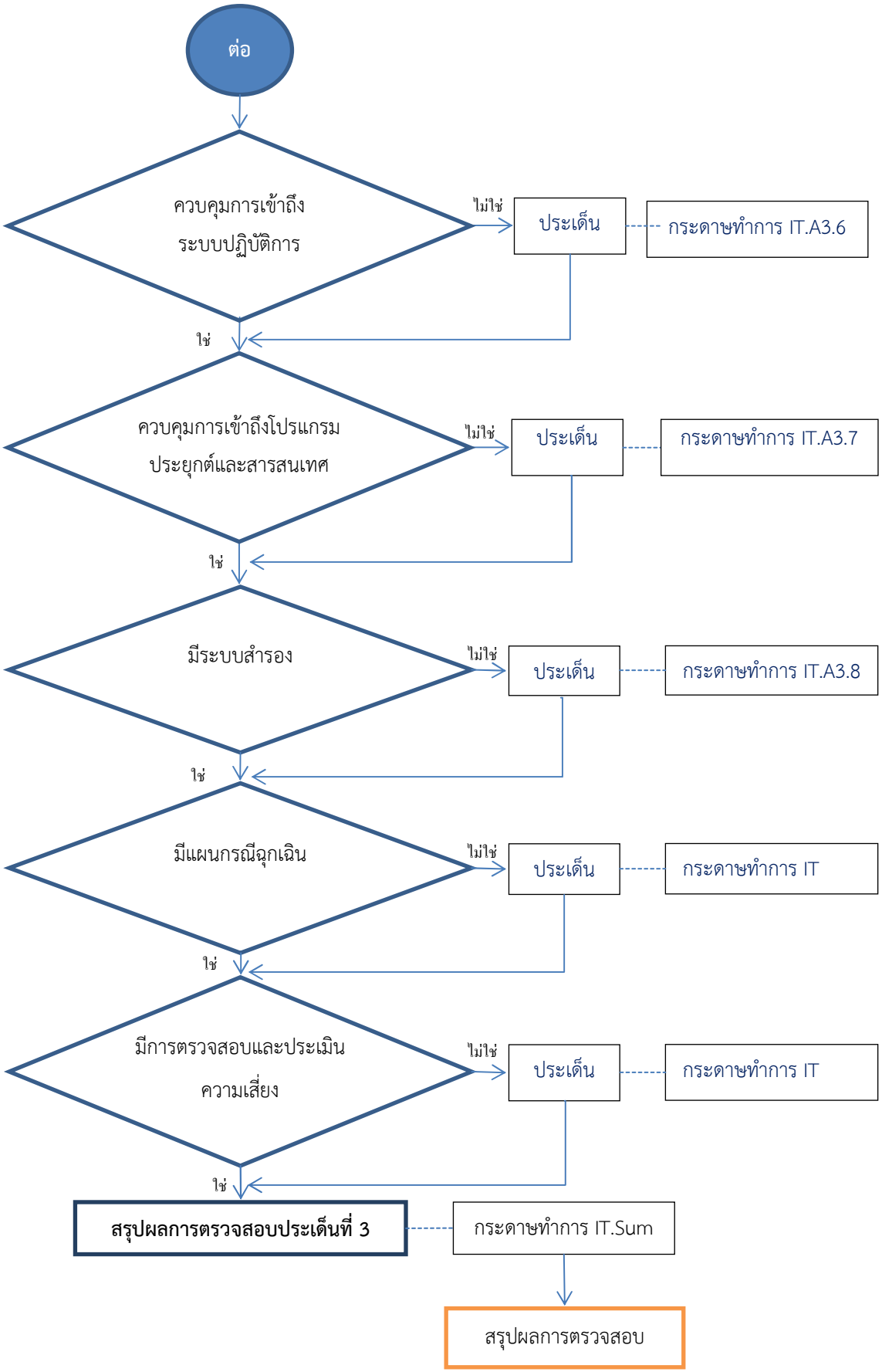


ประเด็นที่ 2 หน่วยงานดำเนินการควบคุม ตามพระราชบัญญัติว่าด้วยคอมพิวเตอร์ พ.ศ. 2550



ประเด็นที่ 3 การควบคุมตามประกาศคณะกรรมการธุรกรรมฯ




ต่อ
ควบคุมการเข้าถึง
ระบบปฏิบัติการ
ไม่ใช่
ประเด็น
กระดาษทำการ IT.A3.6
ใช่
ควบคุมการเข้าถึงโปรแกรม
ประยุกต์และสารสนเทศ
ไม่ใช่
ประเด็น
กระดาษทำการ IT.A3.7
ใช่
มีระบบสำรอง
ไม่ใช่
ประเด็น
กระดาษทำการ IT.A3.8
ใช่
มีแผนกรณีฉุกเฉิน
ไม่ใช่
ประเด็น
กระดาษทำการ IT
ใช่
มีการตรวจสอบและประเมิน
ความเสี่ยง
ไม่ใช่
ประเด็น
กระดาษทำการ IT
ใช่
สรุปผลการตรวจสอบประเด็นที่ 3
กระดาษทำการ IT.Sum
สรุปผลการตรวจสอบ

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.....

กระดาษทำการ IT.A1

กระดาษทำการตรวจสอบแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงาน .....

ลำดับ	แนวนโยบาย	ผลการตรวจสอบ		ข้อปฏิบัติ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
		มี/ใช่	ไม่มี/ไม่ใช่		มี/ใช่	ไม่มี/ไม่ใช่		
1	มีการจัดทำนโยบายเป็นลายลักษณ์อักษร			1. มีการจัดทำข้อปฏิบัติเป็นลายลักษณ์อักษร				
2	มีการจัดทำนโยบายเกี่ยวกับการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ครอบคลุม							
	2.1 การเข้าถึงระบบสารสนเทศ			2. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับข้อกำหนดการควบคุมการเข้าถึง				
				3. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับข้อกำหนดการใช้งานตามภารกิจ				
				4. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการจัดการการเข้าถึงของผู้ใช้งาน				
				5. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ใช้งาน				
	2.2 การเข้าถึงระบบเครือข่าย			6. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการควบคุมการเข้าถึงระบบเครือข่าย				
	2.3 การเข้าถึงระบบปฏิบัติการ			7. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการควบคุมการเข้าถึงระบบปฏิบัติการ				
	2.4 การเข้าถึงโปรแกรมประยุกต์หรือ Application			8. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ				
3	มีกำหนดนโยบายเกี่ยวข้องกับการจัดทำระบบสำรองโดยมีเนื้อหาอย่างน้อย 2 เรื่อง			9. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการจัดทำระบบสำรองข้อมูลสารสนเทศ				
	3.1 การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน			10. ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน				
	3.2 การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน							
4	มีการตรวจสอบประเมินผลไว้เป็นนโยบายข้อหนึ่งด้านสารสนเทศ			11. ข้อปฏิบัติกำหนดเดี่ยวกับการตรวจสอบและประเมินความเสี่ยง				
				12. ข้อปฏิบัติสอดคล้องกับนโยบายรักษาความมั่นคงปลอดภัย				
5	มีการประกาศเผยแพร่นโยบายให้ผู้ใช้งานทราบ โดย			13. มีการประกาศเผยแพร่ข้อปฏิบัติให้ผู้ใช้งานทราบ โดย				
	5.1 ทางwebsite			13.1 ทางwebsite				
	5.2 แจ้งเวียน			13.2 แจ้งเวียน				
	5.2 อื่นๆ ระบุ.....			13.3 อื่นๆ ระบุ.....				
6	หน่วยงานมีการกำหนดผู้รับผิดชอบตามนโยบายที่ชัดเจน			14. หน่วยงานมีการกำหนดผู้รับผิดชอบตามข้อปฏิบัติที่ชัดเจน				
7	หน่วยงานมีการทบทวนนโยบายเป็นปัจจุบัน โดยฉบับที่ใช้ในปัจจุบัน คือ ฉบับลงวันที่.....			15. หน่วยงานมีการทบทวนข้อปฏิบัติเป็นปัจจุบัน โดยฉบับที่ใช้ในปัจจุบัน คือ ฉบับลงวันที่.....				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่กระทบ พ.ร.บ. คอมพิวเตอร์

หน่วยงาน .....

ลำดับ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
			มี	ไม่มี		
1	การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	มีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเข้าถึงโดยโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน				
2	การเปิดเผยวิธีการที่จะเข้าไปยังระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกันของผู้อื่นที่มีการป้องกัน	มีการประกาศไม่ให้ผู้ใช้บริการมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น				
3	การเข้าข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	มีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน				
4	การดักข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่งของระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์				
5	การทำลาย แก้ไข เปลี่ยนแปลงเพิ่มเติมโดยมิได้รับ อนุญาต	มีการประกาศไม่ให้ผู้ใช้บริการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงหรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ				
6	การระงับ ชะลอ ขัดขวาง หรือรบกวนคอมพิวเตอร์ของผู้อืน	มีการประกาศไม่ให้ผู้ใช้บริการกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้				
7	การส่งข้อมูลคอมพิวเตอร์หรือจดหมายทีมีการปกปิดหรือปลอมแปลงแหล่งทีมาเพื่อรบกวนข้อมูลการทำงานของผู้อืน	มีการประกาศไม่ให้ผู้ใช้บริการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดตปกปิดหรือปลอมแปลงที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข				
8	ก่อให้เกิดความเสียงหายแก่ประชาชน ความมันคงของประเทศชาติ	มีการประกาศไม่ให้ผู้ใช้บริการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศชาติ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรฐกิจของประเทศหรือการบริการสาธารณะผรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ				
9	การจำหน่วยหรือเผยแพร่ชุดคำสั่ง	มีการประกาศไม่ให้ผู้ใช้บริการจำหน่วยหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม พ.ร.บ.คอมพิวเตอร์				

กระดาษทำการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่กระทบ พ.ร.บ. คอมพิวเตอร์

หน่วยงาน .....

ลำดับ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
			มี	ไม่มี		
10	การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน				
11	การเผยแพร่ข้อมูลที่เท็จเข้าสู่ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น				
12	การนำเข้าหรือเผยแพร่เนื้อหาอันไม่เหมาะสม	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน				
13	การเผยแพร่ข้อมูลความผิดที่เกียวกับการเข้าสู่ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา				
14	การเผยแพร่ข้อมูลที่มีลักษณะ ลามก ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะ ลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้				
15	การเผยแพร่ภาพตัดต่อที่เป็นการหมิน ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการใดๆทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง				
16	ผู้ให้บริการการเข้าถึงอนเทอร์เน็ต ไม่มีจราจรคอมพิวเตอร์ไว้ 90 วัน	ฝ่าย IT มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ 90 วัน				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการตรวจสอบการควบคุมการเข้าถึงและควบคุมการใช้งาน กระดาษทำการ IT.A3.1

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
		มี/ใช่	ไม่มี/ไม่ใช่		
1	การควบคุมทางกายภาพ				
	1.1 พื้นที่ศูนย์สารสนเทศเป็นพื้นที่เฉพาะสำหรับบุคคลที่ได้รับอนุญาตเท่านั้น				
	1.2 ศูนย์ฯ รวมถึงห้องเก็บสารสนเทศภายใน และห้องทำงานปิดล็อก เมื่อไม่มีการใช้งาน				
	1.3 ศูนย์ฯ มีการควบคุมเพื่อป้องกันภัย				
	- ขโมย				
	- ไฟไหม้				
	- น้ำท่วม				
	1.4 มีนโยบายไม่ให้กิน ดื่ม และสูบบุหรี่ภายในศูนย์				
	1.5 มีอุปกรณ์ UPS สำรองไฟ เพื่อป้องกันข้อมูลสารสนเทศเสียหายกรณีไฟฟ้าดับ/ตก/ไม่สม่ำเสมอ				
	1.6 อุปกรณ์ UPS มีระยะเวลาการใช้งานเพียงพอที่จะสำรองข้อมูลได้				
	1.7 มีการตรวจสอบ และบำรุงรักษาสายไฟฟ้าภายในศูนย์ฯอย่างสม่ำเสมอ				
	1.8 มีการตรวจสอบ และบำรุงรักษาสายเคเบิลโทรคมนาคมที่อยู่ในความรับผิดชอบของหน่วยงานอย่างสม่ำเสมอ				
	1.9 มีการบำรุงรักษาอุปกรณ์ คอมพิวเตอร์ และ Hardware ของหน่วยงานเป็นระยะ				
2	มีการกำหนดสิทธิในการเข้าถึงสอดคล้องกับการอนุญาตและการมอบอำนาจ				
3	มีการดำเนินการเกี่ยวกับข้อมูลและสารสนเทศต่างๆ ในเรื่องต่อไปนี้				
	3.1 จัดประเภทของข้อมูลและสารสนเทศ				
	3.2 จัดชั้นความลับของข้อมูลและสารสนเทศ				
	3.3 จัดชั้นการเข้าถึง				
	3.4 กำหนดเวลาในการเข้าถึง				
	3.5 กำหนดช่องทางในการเข้าถึง				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการตรวจสอบการใช้งานตามภารกิจ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
1	หน่วยงานได้กำหนดข้อปฏิบัติสำหรับการใช้งานตามภารกิจ				
2	กรณีที่กำหนดข้อปฏิบัติ ดำเนินการแยกรายภารกิจหรือไม่				
3	ข้อปฏิบัติครอบคลุม เรื่องต่อไปนี้หรือไม่				
	3.1 มีการควบคุมการเข้าถึงสารสนเทศ หรือไม่				
	3.2 การควบคุมการเข้าถึงสารสนเทศ สอดคล้องกับนโยบายและข้อปฏิบัติ หรือไม่				
	3.3 มีการกำหนดในส่วนของการปรับปรุงหรือไม่				
	3.4 การควบคุมการปรับปรุงสอดคล้องกับนโยบายและข้อปฏิบัติ				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการตรวจสอบการบริหารจัดการการเข้าถึงผู้ใช้งาน

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
1	หน่วยงานจัดให้มีการให้ความรู้ ความเข้าใจกับกับผู้ปฏิบัติงานอย่างต่อเนื่อง				
	โดยวิธีการ ต่อไปนี้				
	1.1 เผยแพร่ทาง Website				
	1.2 จัดอบรม				
	1.3 วิธีอื่นๆ ระบุ.....				
2	มีการให้ลงทะเบียนสำหรับผู้เข้าใช้งาน				
	2.1 มีข้อกำหนดในการลงทะเบียน				
	2.2 มีข้อกำหนดและหลักเกณฑ์ในการอนุญาตให้ใช้งาน				
	2.3 มีข้อกำหนดและหลักเกณฑ์ในการยกเลิก/เพิกถอนการอนุญาตให้เข้าใช้งานในระบบ				
3	มีการควบคุมและจำกัดสิทธิ				
	3.1 มีเอกสารแสดงการกำหนดสิทธิ (ตารางกำหนดสิทธิ)				
	3.2 ไม่มีการสร้าง User ร่วม				
	3.3 สิทธิที่กำหนดในแต่ละกลุ่มชัดเจนและเหมาะสม				
4	มีการกำหนดเงื่อนไขการให้รหัสและเพิกถอนการให้รหัสโดยผ่านกระบวนการด้านการบริหาร				
	4.1 กระบวนการให้รหัสผ่านความเห็นชอบตามเงื่อนไขที่ฝ่ายบริหารกำหนด				
	4.2 มีการดำเนินการเพิกถอบรหัสตามเงื่อนไขที่กำหนด				
	4.3 มีการกำหนดเงื่อนไขให้ผู้ใช้งานเก็บรหัสไว้เป็นความลับ				
5	มีการทบทวนสิทธิเข้าถึงของผู้ใช้งานหรือไม่				
	- การทบทวนสิทธิดำเนินการอย่างต่อเนื่องเป็นระยะ โดยมีการกำหนดระยะเวลาในการทบทวนที่แน่นอน หรือไม่				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการ IT.A3.5

กระดาษทำการตรวจสอบการเข้าถึงระบบเครือข่าย

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
1	กำหนดให้ผู้ใช้งานสามารถเข้าได้เฉพาะบริการที่ได้รับสิทธิเท่านั้น				
	1.1 หน่วยงานมีเอกสารที่แสดงว่ามีระบบสารสนเทศใดที่หน่วยงานต้องควบคุมการเข้าถึง				
	1.2 หน่วยงานได้แสดงข้อปฏิบัติในการเข้าถึงให้ผู้ใช้งานทราบ				
	1.3 หน่วยงานมีการควบคุมการเชื่อมต่อ Terminal กับระบบคอมพิวเตอร์หลัก อย่างรัดกุม				
2	ผู้ใช้งานรับทราบแนวปฏิบัติเกี่ยวกับการเข้าถึงบริการ ผ่านช่องทางใด				
	2.1 ทาง website				
	2.2 หนังสือเวียน				
	2.3 อื่นๆ ระบุ.....				
3	หน่วยงานมีข้อปฏิบัติหรือกระบวนการในการยืนยันตัวบุคคลก่อนอนุญาตให้ผู้ใช้งานจากภายนอกเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน				
4	หน่วยงานสามารถระบุอุปกรณ์บนเครือข่ายได้				
5	หน่วยงานใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึงได้				
6	หน่วยงานกำหนดให้มีการควบคุม Port ต่อไปนี้				
	6.1 Port สำหรับการตรวจสอบ				
	(1) การเข้าถึงทางกายภาพ				
	(2) การเข้าถึงทางเครือข่าย				
	6.2 Port สำหรับการปรับแต่งระบบ				
	(1) การเข้าถึงทางกายภาพ				
	(2) การเข้าถึงทางเครือข่าย				
7	ข้อห้าม				
	7.1 ไม่มีการระบุ Port ตามข้อ 6.1 และ 6.2 ไว้ในเอกสารการควบคุมหรือข้อปฏิบัติ				
	7.1 ไม่มีการระบุวิธีการเข้าถึง Port ตามข้อ 6.1 และ6.2 ไว้ในเอกสารการควบคุมหรือข้อปฏิบัติ				

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
8	หน่วยงานมีการแบ่งแยกเครือข่ายดังนี้				
	8.1 สำหรับกลุ่มบริการสารสนเทศ				
	8.2 สำหรับกลุ่มผู้ใช้งาน				
	8.3 สำหรับกลุ่มระบบสารสนเทศ				
9	หน่วยงานมีเอกสาร Network diagram เป็นปัจจุบัน				
10	หน่วยงานกำหนดการควบคุมเส้นทางบนเครือข่าย ดังนี้				
	- กำหนดขั้นตอนและหลักเกณฑ์ การเชื่อมต่อคอมพิวเตอร์ และการส่งผ่านข้อมูลสอดคล้องกับการควบคุมการเข้าถึงและการใช้โปรแกรมในนโยบายและข้อปฏิบัติ				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการตรวจสอบการเข้าถึงระบบปฏิบัติการ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
1	หน่วยงานกำหนดขั้นตอนการปฏิบัติต่อไปนี้				
	1.1 การควบคุมการเข้าใช้งานในที่มั่นคง				
	1.2 การควบคุมการเข้าถึงระบบปฏิบัติการ				
2	หน่วยงานมีหลักฐานที่แสดงให้เห็นว่า				
	2.1 หน่วยงานกำหนดให้ผู้ใช้งานแสดงข้อมูลจำเพาะในการยืนยันตัวตนของผู้ใช้งาน				
	2.2 หน่วยงานกำหนดขั้นตอนการยืนยันตัวตนของผู้ใช้งาน				
3	หน่วยงานมีการบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบ หรือทำงานอัตโนมัติได้				
4	หน่วยงานกำหนดการจำกัดหรือการควบคุมการใช้งานโปรแกรมอรรถประโยชน์				
5	หน่วยงานกำหนดให้เครื่องยุติ หากมีการว่างเว้นการใช้งาน				
6	หน่วยงานแจ้งข้อปฏิบัติในการให้เครื่องยุติการใช้งานหากว่างเว้นการใช้งานใดๆ ระยะเวลาหนึ่ง ให้ผู้ใช้งานทราบ				
7	หน่วยงานจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศหรือโปรแกรมประยุกต์สำคัญๆ				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการตรวจสอบการเข้าถึงโปรแกรมประยุกต์ หรือApplication และสารสนเทศ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
1	หน่วยงานมีการจำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชัน ต่างๆ ของโปรแกรมประยุกต์จากผู้ใช้งาน				
2	หน่วยงานมีการจำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชัน ต่างๆ ของโปรแกรมประยุกต์จากบุคลากรฝ่ายสนับสนุน				
3	ข้อจำกัดที่กำหนดเป็นไปตามนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน				
4	หน่วยงานมีข้อกำหนดในการควบคุมคอมพิวเตอร์เคลื่อนที่การเข้าถึงสารสนเทศ				
5	หน่วยงานมีข้อกำหนดในการควบคุมโทรศัพท์เคลื่อนที่การเข้าถึงสารสนเทศ				
6	หน่วยงานมีข้อกำหนดในการควบคุมการใช้จากภายนอกผ่านคอมพิวเตอร์เคลื่อนที่และโทรศัพท์เคลื่อนที่				
7	หน่วยงานมีข้อปฏิบัติหรือข้อกำหนดและมาตรการเพื่อป้องกันความเสี่ยงจากการใช้คอมพิวเตอร์เคลื่อนที่และโทรศัพท์เคลื่อนที่				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการ IT.A3.8

กระดาษทำการตรวจสอบการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
1	หน่วยงานมีการพิจารณาคัดเลือกและจัดทำระบบสำรองโดย				
	1.1 หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการคัดเลือกระบบสารสนเทศ				
	1.2 หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการจัดทำระบบสำรอง				
	1.3 ระบบที่จัดทำกำหนดให้มีการกู้คืนและรายงานผลได้				
	1.4 ทุกระบบที่จัดทำสำรองมีการรายงานผลการสำรอง				
2	หน่วยงานมีการเตรียมแผนการเตรียมความพร้อมกรณีฉุกเฉิน ดังนี้				
	2.1 กรณีที่ไม่สามารถดำเนินงานด้วยระบบอิเล็กทรอนิกส์ได้				
	2.2 กรณีที่ Site หลักไม่ทำงาน				
	2.3 มีการกำหนดแผนระยะสั้น				
	2.4 มีการกำหนดแผนระยะยาว				
	2.5 มีการทบทวนแผน 3 เดือนครั้ง				
3	หน่วยงานกำหนดหน้าที่ความรับผิดชอบของบุคลากร ดังนี้				
	3.1 ด้านระบบสารสนเทศ				
	3.2 ด้านระบบสำรอง				
	3.3 ด้านการจัดทำแผนและทบทวนแผน				
4	หน่วยงานจัดให้มีการทดสอบระบบให้อยู่ในสภาพพร้อมใช้งาน				
	4.1 ระบบสารสนเทศ ทดสอบครั้งสุดท้ายเมื่อ.....				
	4.2 ระบบสำรอง ทดสอบครั้งสุดท้ายเมื่อ.....				
	4.3 แผนฉุกเฉิน ทดสอบครั้งสุดท้ายเมื่อ.....				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....
วันที่.....

ผู้สอบทาน.....
วันที่.....

กระดาษทำการสอบทานการจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
1	หน่วยงานกำหนดนโยบายหรือมาตรการให้มีการตรวจสอบ โดยหน่วยตรวจสอบภายใน				
2	หน่วยงานกำหนดนโยบายหรือมาตรการให้มีการตรวจสอบหรือประเมินความเสี่ยง โดยผู้ประเมินภายนอก				
3	มีการกำหนดให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง				
4	มีการรายงานผลการตรวจสอบหรือประเมินเสนอต่อผู้บริหารหน่วยงานเพื่อทราบและพิจารณาสั่งการ				

สรุปผลการตรวจสอบ

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....

โครงการบูรณาการงานตรวจสอบภายใน
กระทรวงศึกษาธิการ
ประจำปีงบประมาณ พ.ศ. 2556

หลักการและเหตุผล

ตามพระราชบัญญัติระเบียบบริหารราชการกระทรวงศึกษาธิการ พ.ศ. 2546 กำหนดให้มีการรวมทบวงมหาวิทยาลัย และกระทรวงศึกษาธิการเดิมเข้าด้วยกัน ทำให้กระทรวงศึกษาธิการมีขนาดใหญ่ขึ้นครอบคลุมสถานศึกษาในสังกัด ตั้งแต่ระดับประถมศึกษาถึงระดับอุดมศึกษาทั่วประเทศ จำนวนมากกว่า 30,000 แห่ง และเป็นกระทรวงที่ได้รับงบประมาณมากเป็นอันดับ 1 ของประเทศ โดยในปีงบประมาณ 2556 ได้รับงบประมาณมากกว่า 460,000 ล้านบาท ดังนั้นเพื่อเป็นการเสริมสร้างความน่าเชื่อถือและความมั่นใจแก่สาธารณชนต่อการดำเนินการตามนโยบาย ยุทธศาสตร์ และผลการดำเนินงานของกระทรวงศึกษาธิการ ว่ามีกระบวนการในการกำกับดูแล ควบคุม และบริหารความเสี่ยงที่มีประสิทธิภาพ จึงได้กำหนดให้มีการตรวจสอบภายในทั้งในส่วนกลางและส่วนภูมิภาค และอาจกล่าวได้ว่า กระทรวงศึกษาธิการมีหน่วยตรวจสอบภายในและผู้ตรวจสอบภายในในสังกัดมากที่สุดในประเทศ กล่าวคือ มีหน่วยตรวจสอบภายในในสังกัดจำนวน 298 แห่ง และมีผู้ตรวจสอบภายใน จำนวนมากกว่า 850 คน ทั้งนี้เพื่อให้การปฏิบัติครอบคลุมทุกพื้นที่และทุกระดับ

เพื่อให้งานตรวจสอบภายในได้รับการพัฒนาให้มีประสิทธิภาพมากยิ่งขึ้น คณะรัฐมนตรีได้มีมติเมื่อวันที่ 22 มิถุนายน 2553 กำหนดให้หัวหน้าส่วนราชการกำกับดูแลการปฏิบัติงานของผู้ตรวจสอบภายในให้มีประสิทธิภาพเพื่อประโยชน์ต่อการปฏิบัติราชการ ตามเจตนารมณ์ของหลักการบริหารกิจการบ้านเมืองที่ดี พร้อมทั้งให้ส่งเสริมสนับสนุน และพัฒนาระบบการตรวจสอบภายในให้เข้มแข็งสามารถให้คำปรึกษาแนะนำแก่หัวหน้าส่วนราชการได้อย่างมืออาชีพ กรมบัญชีกลางในฐานะหน่วยงานที่กำกับและพัฒนาระบบการตรวจสอบภายใน จึงได้ปรับปรุงมาตรฐานการตรวจสอบภายในและจริยธรรมการปฏิบัติงานตรวจสอบภายใน รวมทั้งกำหนดแนวทางการประกันคุณภาพงานตรวจสอบภายในภาครัฐ พ.ศ. 2554 ขึ้นเพื่อผลักดันให้เกิดการพัฒนางานตรวจสอบภายในให้เป็นไปตามมาตรฐาน โดยจะทำการประเมินหน่วยงานด้านการศึกษาตามเกณฑ์การประกันคุณภาพฯ ในปีงบประมาณ 2557

แต่อย่างไรก็ตาม สภาพปัจจุบัน การตรวจสอบภายในกระทรวงศึกษาธิการ แม้จะมีหน่วยตรวจสอบภายใน และผู้ตรวจสอบภายในในสังกัดจำนวนมาก แต่หน่วยงานตรวจสอบภายในหลายแห่งมีผู้ตรวจสอบภายในเพียงคนเดียว และส่วนใหญ่เป็นอาจารย์ พนักงานมหาวิทยาลัย พนักงานราชการและลูกจ้างชั่วคราว ซึ่งบุคลากรกลุ่มดังกล่าวมีการเปลี่ยนแปลงบ่อยครั้ง จึงทำให้การปฏิบัติงานขาดความต่อเนื่อง และบุคลากรขาดทักษะความชำนาญ งานการตรวจสอบภายในจึงขาดความเป็นเอกภาพ และผลการตรวจสอบภายในยังไม่สามารถสนับสนุนการบริหารและการดำเนินงานของส่วนราชการได้เท่าที่ควร

กอปรกับการพัฒนาบุคลากรจำนวนมากเพื่อให้มีความรู้ความสามารถตามมาตรฐานการตรวจสอบภายในภาครัฐที่กรมบัญชีกลางกำหนดด้วยการฝึกอบรม ต้องดำเนินการอย่างต่อเนื่องและใช้งบประมาณสูง

ด้วยเหตุดังกล่าวข้างต้น กระทรวงศึกษาธิการโดยกลุ่มตรวจสอบภายในระดับกระทรวง ในฐานะเลขานุการคณะกรรมการตรวจสอบและประเมินผลประจำกระทรวงศึกษาธิการซึ่งมีหน้าที่ในการสอบทานและพัฒนางานด้านการตรวจสอบภายในของกระทรวงศึกษาธิการให้เข้มแข็ง จึงได้ดำเนินการบูรณาการงานตรวจสอบภายใน กระทรวงศึกษาธิการขึ้น เพื่อเป็นการสร้างเครื่องมือ และเพิ่มทักษะในการปฏิบัติงานตรวจสอบ รวมทั้งเป็นการสนับสนุนการปฏิบัติงานของหน่วยงานตรวจสอบภายในให้เป็นไปตามมาตรฐานพร้อมรองรับการประเมินตามเกณฑ์การประกันคุณภาพงานตรวจสอบภายในภาครัฐ ทั้งยังเป็นการเพิ่มประสิทธิภาพงานการตรวจสอบภายในภาพรวมของกระทรวงศึกษาธิการ โดยในปีงบประมาณ 2556 จะดำเนินการบูรณาการงานตรวจสอบภายใน 2 เรื่อง คือ การตรวจสอบระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการตรวจสอบการบริหารงบลงทุน ซึ่งกระทรวงศึกษาธิการจะได้นำมากำหนดเป็นตัวชี้วัดหนึ่งในการประเมินผลการปฏิบัติงานการตรวจสอบภายในของส่วนราชการสังกัดกระทรวงศึกษาธิการเสนอคณะกรรมการตรวจสอบและประเมินผลประจำกระทรวงศึกษาธิการ ต่อไป

วัตถุประสงค์ของโครงการ

1. เพื่อทราบการดำเนินงานด้านสารสนเทศ และการบริหารงบลงทุนภาพรวมของกระทรวงศึกษาธิการว่าเป็นไปตามกฎระเบียบ แนวนโยบาย ตลอดจนความมีประสิทธิภาพ และประสิทธิผลของการดำเนินงานและการบริหารจัดการ รวมถึงปัญหา อุปสรรค เพื่อเสนอแนะแนวทางในการพัฒนา และปรับปรุงแก้ไข
2. เพื่อพัฒนาผู้ตรวจสอบภายในหน่วยงานในสังกัด ให้สามารถดำเนินการตรวจสอบด้านสารสนเทศ และด้านการบริหาร ตามเกณฑ์การประกันคุณภาพงานตรวจสอบภายในภาครัฐเพื่อให้พร้อมรองรับการประเมิน

แนวทางการดำเนินงาน

1. ขอความอนุเคราะห์หัวหน้าส่วนราชการ โปรดพิจารณามอบหมายสั่งการให้หน่วยตรวจสอบภายในในสังกัดของท่าน กำหนดการตรวจสอบระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการตรวจสอบการบริหารงบลงทุนไว้ในแผนการตรวจสอบภายในประจำปี 2556 โดยให้สามารถรายงานผลการตรวจสอบได้ภายในเดือนมิถุนายน 2556
2. สำนักงานปลัดกระทรวงศึกษาธิการ โดยกลุ่มตรวจสอบภายในระดับกระทรวง ได้จัดประชุมเชิงปฏิบัติการร่วมกับหน่วยงานในสังกัด ซึ่งได้แก่ หน่วยงานหลักและมหาวิทยาลัยในสังกัด เพื่อจัดทำแผนการปฏิบัติงานตรวจสอบภายใน (Engagement plans) พร้อมกระดาษทำการ ในการตรวจสอบระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการตรวจสอบการบริหารงบลงทุน ระหว่างวันที่

19 - 21 กันยายน 2555 นั้น บัดนี้กลุ่มตรวจสอบภายในระดับกระทรวงได้รวบรวมและปรับปรุงแผนการปฏิบัติงานดังกล่าวเรียบร้อยแล้ว (รายละเอียดเอกสารดังแนบ) จึงขอให้ผู้ตรวจสอบภายในที่ได้รับมอบหมายให้ดำเนินการตรวจสอบในเรื่องดังกล่าว ศึกษาแผนการปฏิบัติงานตรวจสอบ (Engagement plans) และกระดาษทำการที่ส่งมาพร้อมนี้ แล้วดำเนินการตรวจสอบตามระยะเวลาที่กำหนดในแผนการตรวจสอบภายในประจำปีของหน่วยงาน

3. เมื่อดำเนินการตรวจสอบแล้วเสร็จให้รายงานผลการตรวจสอบเสนอหัวหน้าหน่วยงานเพื่อทราบผลการดำเนินงานตรวจสอบและพิจารณาสั่งการ

4. สำเนารายงานผลการตรวจสอบภายในแจ้งกลุ่มตรวจสอบภายในระดับกระทรวงภายในเดือนมิถุนายน 2556 เพื่อจัดทำรายงานผลการตรวจสอบภาพรวมเสนอคณะกรรมการตรวจสอบประเมินผลประจำกระทรวงศึกษาธิการต่อไป

ประโยชน์ที่คาดว่าจะได้รับ

1. ผู้บริหารระดับสูง และผู้บริหารของหน่วยงาน ทราบผลการดำเนินงานด้านสารสนเทศ และการบริหารงบลงทุนภาพรวมของกระทรวงศึกษาธิการว่าเป็นไปตามกฎระเบียบ แนวนโยบาย ตลอดจนความมีประสิทธิภาพ และประสิทธิผลของการดำเนินงานและการบริหารจัดการ รวมถึงปัญหา อุปสรรค และแนวทางในการพัฒนา ปรับปรุงแก้ไข

2. เพื่อให้หน่วยงานตรวจสอบภายในมีเครื่องมือในการตรวจสอบครอบคลุมการตรวจสอบด้านสารสนเทศ และการตรวจสอบด้านการบริหาร ให้เลือกใช้ในการปฏิบัติงาน ซึ่งการตรวจสอบทั้ง 2 ประเภทจะสนับสนุนการปฏิบัติงานตรวจสอบ ให้ผ่านเกณฑ์การประกันคุณภาพงานตรวจสอบภายในภาครัฐ ประเด็นการวางแผนการตรวจสอบ ในระดับสูงกว่ามาตรฐาน