คู่มือแนวทางการตรวจสอบ

ด้านเทคโนโลยีสารสนเทศ

กลุ่มตรวจสอบภายใน

ประจำปี ๒๕๖๑

คำนำ

ปัจจุบันความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้น ส่งผลให้แทบทุกหน่วยงานทั้งภาครัฐและเอกชนมีความต้องการในการดูแล ความมั่นคงปลอดภัยของสารสนเทศสูงขึ้นด้วย และให้ความสำคัญในการกำหนดและจัดทำนโยบาย ระเบียบ วิธีการปฏิบัติ เพื่อให้เกิดความมั่นใจ ในการดูแลรักษาความมั่นคงปลอดภัยขององค์กร และพยายามพัฒนาให้เป็นมาตรฐานเทียบเท่าระดับสากล เพื่อการสร้างความมั่นใจ และการยอมรับ ทั้งนี้ กรมสนับสนุนบริการสุขภาพ เป็นหน่วยงานหนึ่งที่ทุกหน่วยงานในสังกัด มีการพัฒนาและใช้งานระบบเทคโนโลยีสารสนเทศในระดับหนึ่ง ซึ่งทุกหน่วยงานต้องมีการปฏิบัติงานและบริหารจัดการด้านระบบเทคโนโลยีสารสนเทศ

ดังนั้น กลุ่มตรวจสอบภายใน จึงจำเป็นต้องพัฒนาแนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพ เพื่อพัฒนาการปฏิบัติงานและบริหารจัดการด้านระบบเทคโนโลยีสารสนเทศให้เป็นเลิศ โดยเฉพาะการปฏิบัติงานใดที่เกี่ยวข้องกับการควบคุมของกฎหมาย ระเบียบ ข้อบังคับด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายใน จำเป็นต้องทราบและให้คำแนะนำหน่วยรับตรวจได้อย่างมีประสิทธิภาพ ประสิทธิผล จึงถือว่าคู่มือนี้เป็นแนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่จะทำให้ผู้ตรวจสอบภายในของกรมสนับสนุนบริการสุขภาพ สามารถตรวจสอบด้านเทคโนโลยีสารสนเทศ ได้อย่างมีประสิทธิภาพต่อไป

กลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ
๑๐ ตุลาคม ๒๕๖๑

สารบัญ

หน้า

สารบัญ

แนวทางการตรวจสอบด้านระบบเทคโนโลยีสารสนเทศ

แบบไม่มีเครื่องแม่ข่าย(Server) สำหรับหน่วยงานที่ไม่มีนักวิชาการคอมพิวเตอร์

ประเด็นการตรวจสอบที่ ๑ นโยบายความมั่นคงปลอดภัยเป็นไปตามข้อกำหนดของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าหน่วยงานกำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๑.การจัดทำนโยบายความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่านโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.หน่วยงานมีการจัดทำข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒.หน่วยงานประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบ ๓.หน่วยงานกำหนดผู้รับผิดชอบตามนโยบายชัดเจนหรือมีการแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)อย่างชัดเจนเป็นลายลักษณ์อักษร	๑.ตรวจสอบเอกสารหลักฐานว่าหน่วยงานได้กำหนดข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรหรือไม่ กรณีที่ไม่ได้ดำเนินการให้สอบถามสาเหตุจากผู้ที่เกี่ยวข้อง ๒.ตรวจสอบหลักฐานการประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบว่ามีหรือไม่โดยผ่านทางการแจ้งเวียนบันทึกหรือชี้แจงในที่ประชุมหรือผ่านทางเว็บไซด์ รายงานการประชุม เป็นต้น	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.เอกสารข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒.หลักฐานแสดงการประกาศและเผยแพร่นโยบายและข้อปฏิบัติ ๓.คำสั่งหรือหนังสือมอบหมายสั่งการ ๔.รายงานการประชุมติดตามการปฏิบัติตามข้อปฏิบัติที่ประกาศไว้ ๕.เอกสารทบทวนข้อปฏิบัติ/แนวทางปฏิบัติ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๔.กรณีมีข้อปฏิบัติ/แนวทางปฏิบัติอยู่แล้ว หน่วยงานมีการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบัน ๕.มีการปฏิบัติตามข้อปฏิบัติ/แนวปฏิบัติที่รองรับนโยบาย ซึ่งต้องมีกระบวนการติดตามประเมินผลข้อปฏิบัติที่รองรับนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน	๓.ตรวจสอบว่ามีการกำหนดผู้รับผิดชอบหรือมีคำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)เป็นลายลักษณ์อักษรหรือไม่ และเป็นปัจจุบันหรือไม่ ถ้าปีที่ผ่านมาไม่มีการเปลี่ยนแปลงคณะทำงานก็ใช้คำสั่งเดิมได้ ๔.ตรวจสอบหลักฐานการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบันโดยผู้มีอำนาจของหน่วยงาน ๕.ตรวจสอบหลักฐานรายงานการประชุมคณะกรรมการฯว่ามีการติดตามประเมินผลข้อปฏิบัติที่รองรับนโยบายหรือไม่(เป็นการประเมินรายข้อ)	

ประเด็นการตรวจสอบที่ ๒ การควบคุมการเข้าถึงเป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่ามีการปฏิบัติในการควบคุมการเข้าถึงเป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๒.๑ การควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศ (User access management) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศ (User access management) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของ	๑.มีการจัดอบรม/ชี้แจงในการประชุม/แจ้งเวียน/เผยแพร่ในเว็บไซด์ เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ๒.ต้องมีกระบวนการในการแจ้งการถอดถอนสิทธิผู้ใช้งานระบบเครือข่ายหรือระบบสารสนเทศของหน่วยงานในกรณีโอนย้ายลาออกเกษียณอายุของเจ้าหน้าที่ในหน่วยงาน	๑.ตรวจสอบว่ามีเอกสารการอบรมหรือรายงานการประชุมชี้แจงหรือบันทึกแจ้งเวียนหรือการเผยแพร่ในเว็บไซด์หน่วยงานเกี่ยวกับการสร้างความตระหนักรู้ถึงการระมัดระวังในการใช้ระบบสารสนเทศอย่างมั่นคงปลอดภัย ๒.ตรวจสอบบันทึกแจ้งการถอดถอนสิทธิผู้ใช้งานระบบเครือข่ายหรือระบบสารสนเทศของหน่วยงานในกรณีโอนย้ายลาออกเกษียณอายุของเจ้าหน้าที่ในหน่วยงานอย่างน้อยปีละ๑ครั้ง	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.เอกสารการอบรม/รายงานการประชุม/บันทึกแจ้งเวียน/หลักฐานการเผยแพร่ในเว็บไซด์ ๒.บันทึกแจ้งถอดถอนสิทธิการใช้งานระบบเครือข่าย/ระบบสารสนเทศของหน่วยงาน ๓.มาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน ๔.รายงานการประชุมควบคุมโปรแกรมอรรถประโยชน์

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
ระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๓.มีข้อปฏิบัติหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่ เช่นการกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น ๔.มีการควบคุมการใช้งานโปรแกรมอรรถประโยชน์ในหน่วยงาน	๓.มีการกำหนดข้อปฏิบัติหรือแนวทางปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่ เช่นการกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น ๔.ตรวจสอบรายงานการประชุมของคณะกรรมการCSO ว่ามีการควบคุมการใช้งานโปรแกรมอรรถประโยชน์หรือไม่และสุ่มตรวจโปรแกรมอรรถประโยชน์ที่ติดตั้งในเครื่องคอมพิวเตอร์ของหน่วยงานว่าเป็นไปตามที่คณะกรรมการฯกำหนดหรือไม่	
๒.๒ การควบคุมการเข้าถึงระบบปฏิบัติการ(Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงระบบปฏิบัติการตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ	๑.การติดตั้งโปรแกรมป้องกันไวรัสและการupdateโปรแกรมป้องกันไวรัส	๑.ตรวจสอบว่า มีการติดตั้งโปรแกรมป้องกันไวรัสครบถ้วนทุกเครื่องหรือไม่ และมีการ update โปรแกรมป้องกันไวรัสครบถ้วนหรือไม่	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** -สุ่มตรวจเครื่องคอมพิวเตอร์

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์			
๒.๓ การควบคุมการเข้าถึงทางกายภาพของห้องสำนักงาน ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีแบบปลอดภัย **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงทางกายภาพตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ๑.๑ การจัดระเบียบสายไฟฟ้าและสายสัญญาณรับ-ส่งข้อมูลอย่างเป็นระเบียบเรียบร้อย ๑.๒ มีการกำกับป้ายสายสัญญาณรับส่งข้อมูลครบถ้วนทุกสาย ๑.๓ มีแผนผังคอมพิวเตอร์ของหน่วยงาน	**<u>๑.การจัดทำบริเวณล้อมรอบ (Physical security perimeter)</u>** ๑.๑ ตรวจสอบสายไฟฟ้าและสายสัญญาณรับ-ส่งข้อมูลว่ามีความเป็นระเบียบเรียบร้อยหรือไม่ ๑.๒ ตรวจสอบป้ายกำกับสายสัญญารับส่งข้อมูลว่ามีป้ายกำกับครบถ้วนทุกสายและเห็นชัดเจน เพื่อป้องกันการดึงสายผิดเส้น ๑.๓ ตรวจสอบแผนผังคอมพิวเตอร์ว่าถูกต้องตรงกับตำแหน่งที่ตั้งของคอมพิวเตอร์และสาย LAN หรือไม่	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.ภาพถ่ายพื้นที่และการจัดระเบียบสายไฟฟ้าและสายสัญญาณรับ-ส่งข้อมูล ๒.แผนผังคอมพิวเตอร์

ประเด็นการตรวจสอบที่ ๓ การดำเนินงานควบคุมและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

วัตถุประสงค์

๑.เพื่อมั่นใจว่ามีการดำเนินการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศมิให้สูญหาย

๒.เพื่อมั่นใจว่ามีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีอย่างเหมาะสม

๓.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
การดำเนินงานควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างรัดกุม **<u>วัตถุประสงค์ย่อย</u>** ๑.เพื่อมั่นใจว่ามีการดำเนินการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศมิให้สูญหาย ๒.เพื่อมั่นใจว่ามีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีอย่างเหมาะสม	๑.ต้องมีการจัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยมีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อย CPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินโดยครอบคลุมด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ ๒.ระบบการยืม-คืนครุภัณฑ์ตามระเบียบ ๓.มีการทำความสะอาดเครื่องคอมพิวเตอร์และอุปกรณ์ อย่างน้อยทุกๆ ๓ เดือน	๑.ตรวจสอบทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อยCPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินโดยครอบคลุมด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ ๒.ตรวจสอบว่า มีระบบการยืม-คืนครุภัณฑ์ถูกต้องตามระเบียบหรือไม่ ๓.ตรวจสอบว่า มีการตรวจสอบการทำความสะอาดเครื่องคอมพิวเตอร์และอุปกรณ์ อย่างน้อยทุกๆ ๓ เดือนหรือไม่ (ขอดูหลักฐานการตรวจเช็คทำความสะอาด)	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.ทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ ๒.เอกสารเกี่ยวกับระบบการยืม-คืนครุภัณฑ์ด้านเทคโนโลยีสารสนเทศ ๓.เอกสารในการดำเนินกิจกรรมบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์

ประเด็นการตรวจสอบที่ ๔ การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่า การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

หมายเหตุ:

คุณภาพ หมายถึง ๑.ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้อง

เหมาะสมต่อการใช้งาน หมายถึง สอดคล้องกับความต้องการของผู้ใช้งานระบบสารสนเทศ

พัฒนาต่อยอดได้ในอนาคต หมายถึง ระบบสารสนเทศต้องมีเอกสารการวิเคราะห์ออกแบบระบบที่สามารถพัฒนาต่อยอดได้ในอนาคต ได้แก่ แผนผังกระแสการไหลของข้อมูล(DFD/Use case) และแผนผังโครงสร้างฐานข้อมูล(ER Diagram) รวมทั้งพจนานุกรมฐานข้อมูล และความสัมพันธ์ของฐานข้อมูล

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่า การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต	๑. ระบบสารสนเทศต้องมีระบบการนำเข้าข้อมูลที่ถูกต้องและมีการประมวลผลรวมถึงออกรายงานแสดงได้อย่างถูกต้อง ๒.ปฏิบัติตามขั้นตอนการเผยแพร่ข้อมูลต่อสาธารณะผ่านเว็บไซต์หน่วยงานตามประกาศกรมเรื่องแนวทางการเผยแพร่ข้อมูลต่อสาธารณะผ่านเว็บไซต์ของหน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ๒๕๖๒ ลงวันที่ ๑ ก.ค.๖๒	๑. ตรวจสอบว่า ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้องหรือไม่ ๒.ขอดูคำสั่งแต่งตั้ง/มอบหมายให้เป็นผู้กลั่นกรองเอกสารก่อนเผยแพร่และหลังเผยแพร่ในเว็บไซต์หน่วยงาน รวมทั้ง Flow chart ขั้นตอนกระบวนการเผยแพร่ข้อมูลสารสนเทศผ่านเว็บไซต์หน่วยงาน	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** -ระบบสารสนเทศมีการนำเข้า-ประมวลผล-ออกรายงานอย่างถูกต้อง -คำสั่งแต่งตั้ง/มอบหมาย -ขั้นตอน/ Flow chartกระบวนการเผยแพร่ข้อมูลสารสนเทศผ่านเว็บไซต์หน่วยงาน

ประเด็นการตรวจสอบที่ ๕ เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่ามีการเผยแพร่ตามพรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด วัตถุประสงค์ย่อย เพื่อให้มั่นใจว่ามีการเผยแพร่ตามพรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด	๑.ตามมติคณะรัฐมนตรี ที่ นร ๐๔๐๕/ว ๕๗ ลงวันที่ ๒๙ เมษายน ๒๕๕๔ ให้นำข้อมูลข่าวสารตามมาตรา ๗ เผยแพร่ในเว็บไซต์ของหน่วยงาน -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ ๒.ตามมติคณะรัฐมนตรี ที่ นร ๐๔๐๕/ว ๕๗ ลงวันที่ ๒๙ เมษายน ๒๕๕๔ ให้นำข้อมูลข่าวสารตามมาตรา ๙ เผยแพร่ในเว็บไซต์ของหน่วยงาน -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน)	๑.ตรวจสอบว่ามีการเผยแพร่ตามมาตรา ๗ เผยแพร่ในเว็บไซต์ของหน่วยงาน -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ ๒.ตรวจสอบว่ามีการเผยแพร่ตามมาตรา ๙ เผยแพร่ในเว็บไซต์ของหน่วยงาน -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน) -แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน	กระดาษทำการ WA_IT๐๑ **<u>หลักฐาน</u>** ๑.บันทึกภาพถ่ายการเผยแพร่ตามมาตรา๗และ๙ ผ่านเว็บไซต์หน่วยงาน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	-แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน ๓.ตามมติคณะรัฐมนตรีที่ ๒๘ ธันวาคม ๒๕๔๗ ให้นำ -ประกาศประกวดราคา ประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน	๓.ตรวจสอบว่ามีการเผยแพร่ -ประกาศประกวดราคา ประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน	

แนวทางการตรวจสอบด้านระบบเทคโนโลยีสารสนเทศ

แบบไม่มีเครื่องแม่ข่าย(Server) และมีนักวิชาการคอมพิวเตอร์

ประเด็นการตรวจสอบที่ ๑ นโยบายความมั่นคงปลอดภัยเป็นไปตามข้อกำหนดของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าหน่วยงานกำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๑.การจัดทำนโยบายความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่านโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.หน่วยงานมีการจัดทำข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒.หน่วยงานประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบ ๓.หน่วยงานกำหนดผู้รับผิดชอบตามนโยบายชัดเจนหรือมีการแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)อย่างชัดเจนเป็นลายลักษณ์อักษร	๑.ตรวจสอบเอกสารหลักฐานว่าหน่วยงานได้กำหนดข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรหรือไม่ กรณีที่ไม่ได้ดำเนินการให้สอบถามสาเหตุจากผู้ที่เกี่ยวข้อง ๒.ตรวจสอบหลักฐานการประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบว่ามีหรือไม่โดยผ่านทางการแจ้งเวียนบันทึกหรือชี้แจงในที่ประชุมหรือผ่านทางเว็บไซด์ รายงานการประชุม เป็นต้น	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.เอกสารข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒.หลักฐานแสดงการประกาศและเผยแพร่นโยบายและข้อปฏิบัติ ๓.คำสั่งหรือหนังสือมอบหมายสั่งการ ๔.รายงานการประชุมติดตามการปฏิบัติตามข้อปฏิบัติที่ประกาศไว้ ๕.เอกสารทบทวนข้อปฏิบัติ/แนวทางปฏิบัติ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๔.กรณีมีข้อปฏิบัติ/แนวทางปฏิบัติอยู่แล้ว หน่วยงานมีการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบัน ๕.มีการปฏิบัติตามข้อปฏิบัติ/แนวปฏิบัติที่รองรับนโยบาย ซึ่งต้องมีกระบวนการติดตามประเมินผลข้อปฏิบัติที่รองรับนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน	๓.ตรวจสอบว่ามีการกำหนดผู้รับผิดชอบหรือมีคำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)เป็นลายลักษณ์อักษรหรือไม่ และเป็นปัจจุบันหรือไม่ ถ้าปีที่ผ่านมาไม่มีการเปลี่ยนแปลงคณะทำงานก็ใช้คำสั่งเดิมได้ ๔.ตรวจสอบหลักฐานการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบันโดยผู้มีอำนาจของหน่วยงาน ๕.ตรวจสอบหลักฐานรายงานการประชุมคณะกรรมการฯว่ามีการติดตามประเมินผลข้อปฏิบัติที่รองรับนโยบายหรือไม่(เป็นการประเมินรายข้อ)	

ประเด็นการตรวจสอบที่ ๒ การควบคุมการเข้าถึงเป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่ามีการปฏิบัติในการควบคุมการเข้าถึงเป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๒.๑ การควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศ (User access management) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศ (User access management) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของ	๑.มีการจัดอบรม/ชี้แจงในการประชุม/แจ้งเวียน/เผยแพร่ในเว็บไซด์ เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ๒.มีการวางระบบการลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ	๑.ตรวจสอบหลักฐานว่ามีการจัดอบรม/ชี้แจง/แจ้งเวียน เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน ๒.ตรวจสอบว่ามีระบบการลงทะเบียนผู้ใช้งาน คือ การลงทะเบียนสมัครเข้าใช้ระบบงานเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงาน โดยต้องมีการกำหนดขั้นตอนการปฏิบัติสำหรับการลงทะเบียน ๓.ตรวจสอบบันทึกแจ้งการถอดถอนสิทธิผู้ใช้งานระบบเครือข่ายหรือระบบสารสนเทศของหน่วยงานในกรณีโอนย้ายลาออกเกษียณอายุของ	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.เอกสารการจัดอบรม/ชี้แจง/แจ้งเวียน เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน ๒.Flowchart ขั้นตอนระบบการลงทะเบียนผู้ใช้งาน ๓.เอกสารประกอบระบบการลงทะเบียนผู้ใช้งาน ๔.เอกสารที่ได้จากการพิมพ์ในระบบการบริหารจัดการรหัสผ่าน ๕.มาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
ระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๓.ต้องมีกระบวนการในการแจ้งการถอดถอนสิทธิผู้ใช้งานระบบเครือข่ายหรือระบบสารสนเทศของหน่วยงานในกรณีโอนย้ายลาออกเกษียณอายุของเจ้าหน้าที่ในหน่วยงาน ๔.มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน(user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ๕.ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ๖.มีข้อปฏิบัติหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่ เช่นการกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น ๗.มีการควบคุมการใช้งานโปรแกรมอรรถประโยชน์ในหน่วยงาน	เจ้าหน้าที่ในหน่วยงานอย่างน้อยปีละ๑ครั้ง ๔.ตรวจสอบว่า มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน เช่น มีระบบการเปลี่ยนรหัสผ่าน/ระบบกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น ๕.ตรวจสอบว่า ระบบการ authentication หรือระบบเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงานมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละครั้งหรือไม่ หรือแจ้งรายชื่อผู้ที่โอนย้ายลาออกส่งไปยกเลิกในระบบ authenticationของกรมหรือไม่ ๖.มีการกำหนดข้อปฏิบัติหรือแนวทางปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่ เช่นการกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		๗.ตรวจสอบรายงานการประชุมของคณะกรรมการCSO ว่ามีการควบคุมการใช้งานโปรแกรมอรรถประโยชน์หรือไม่และสุ่มตรวจโปรแกรมอรรถประโยชน์ที่ติดตั้งในเครื่องคอมพิวเตอร์ของหน่วยงานว่าเป็นไปตามที่คณะกรรมการฯกำหนดหรือไม่	
๒.๒ การควบคุมการเข้าถึงระบบปฏิบัติการ(Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงระบบปฏิบัติการตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ	๑.การติดตั้งโปรแกรมป้องกันไวรัสและการupdateโปรแกรมป้องกันไวรัส	๑.ตรวจสอบว่า มีการติดตั้งโปรแกรมป้องกันไวรัสครบถ้วนทุกเครื่องหรือไม่และมีการ update โปรแกรมป้องกันไวรัสครบถ้วนหรือไม่	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** -สุ่มตรวจเครื่องคอมพิวเตอร์

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์			
๒.๓ การควบคุมการเข้าถึงทางกายภาพของห้องสำนักงาน ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีแบบปลอดภัย **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงทางกายภาพตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ๑.๑ การจัดระเบียบสายไฟฟ้าและสายสัญญาณรับ-ส่งข้อมูลอย่างเป็นระเบียบเรียบร้อย ๑.๒ มีการกำกับป้ายสายสัญญาณรับส่งข้อมูลครบถ้วนทุกสาย ๑.๓ มีแผนผังคอมพิวเตอร์ของหน่วยงาน	**<u>๑.การจัดทำบริเวณล้อมรอบ (Physical security perimeter)</u>** ๑.๑ ตรวจสอบสายไฟฟ้าและสายสัญญาณรับ-ส่งข้อมูลว่ามีความเป็นระเบียบเรียบร้อยหรือไม่ ๑.๒ ตรวจสอบป้ายกำกับสายสัญญารับส่งข้อมูลว่ามีป้ายกำกับครบถ้วนทุกสายและเห็นชัดเจน เพื่อป้องกันการดึงสายผิดเส้น ๑.๓ ตรวจสอบแผนผังคอมพิวเตอร์ว่าถูกต้องตรงกับตำแหน่งที่ตั้งของคอมพิวเตอร์และสาย LAN หรือไม่	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.ภาพถ่ายพื้นที่และการจัดระเบียบสายไฟฟ้าและสายสัญญาณรับ-ส่งข้อมูล ๒.แผนผังคอมพิวเตอร์
๒.๔การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑.หน่วยงานต้องมีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑.ตรวจสอบว่าหน่วยงานมีการจัดทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศหรือไม่ และการประเมินความเสี่ยงได้ดำเนินการอย่างถูกต้องเหมาะสมหรือไม่	**<u>หลักฐาน</u>** -เอกสารประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเด็นการตรวจสอบที่ ๓ การดำเนินงานควบคุมและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

วัตถุประสงค์

๑.เพื่อมั่นใจว่ามีการดำเนินการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศมิให้สูญหาย

๒.เพื่อมั่นใจว่ามีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีอย่างเหมาะสม

๓.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
การดำเนินงานควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างรัดกุม **<u>วัตถุประสงค์ย่อย</u>** ๑.เพื่อมั่นใจว่ามีการดำเนินการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศมิให้สูญหาย ๒.เพื่อมั่นใจว่ามีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีอย่างเหมาะสม	๑.ต้องมีการจัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยมีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อย CPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินโดยครอบคลุมด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ ๒.ระบบการยืม-คืนครุภัณฑ์ตามระเบียบ ๓.มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย(ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิงป้องกันและเชิงแก้ไข)	๑.ตรวจสอบทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อยCPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินโดยครอบคลุมด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ ๒.ตรวจสอบว่า มีระบบการยืม-คืนครุภัณฑ์ถูกต้องตามระเบียบหรือไม่ ๓.ตรวจสอบว่า มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย(ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิงป้องกันและเชิงแก้ไข)	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.ทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ ๒.เอกสารเกี่ยวกับระบบการยืม-คืนครุภัณฑ์ด้านเทคโนโลยีสารสนเทศ ๓.แผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ ๔.เอกสารในการดำเนินกิจกรรมบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์

ประเด็นการตรวจสอบที่ ๔ หน่วยงานต้องมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าหน่วยงานมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงาน รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๔.มีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด วัตถุประสงค์ย่อย เพื่อให้มั่นใจว่าหน่วยงานมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด	๑.ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม ๒.มีแผนในการสำรองข้อมูลเป็นลายลักษณ์อักษรและปฏิบัติตรงตามแผนที่กำหนด ๓.กำหนดผู้รับผิดชอบในการสำรองข้อมูล ๔.กำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง ๕.ต้องติดฉลากที่มีรายละเอียดชัดเจนเพื่อให้สามารถค้นหาได้โดยเร็วและป้องกันการใช้งานสื่อบันทึกผิดพลาด ๖.กำหนดขั้นตอนการทดสอบข้อมูลที่สำรอง ๗.มีรายงานผลการทดสอบข้อมูลที่สำรอง	๑.สัมภาษณ์มีกระบวนการในการสำรองข้อมูลอย่างเป็นระบบได้แก่ (๑)คัดเลือกข้อมูลที่สำคัญต่อองค์กรนำมาจัดเรียงลำดับความสำคัญ (๒)กำหนดความถี่ในการสำรองข้อมูลตามระดับความสำคัญที่กำหนดไว้ (๓)จัดทำแผนในการสำรองข้อมูลอย่างเป็นระบบ (๔)ดำเนินการสำรองข้อมูลและสุ่มตรวจข้อมูลที่สำรองว่ามีความสมบูรณ์หรือไม่และมีหลักฐานบันทึกกิจกรรมการสำรองข้อมูล ๒.ขอดูแผนการสำรองข้อมูลและผลการปฏิบัติในการสำรองข้อมูลว่าตรงตามแผนหรือไม่และมีการสุ่มตรวจการสำรองข้อมูล ๓.สัมภาษณ์และขอดูเอกสารหลักฐานการแต่งตั้ง/มอบหมายผู้รับผิดชอบในการสำรองข้อมูล	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.รายงานการประชุมคัดเลือกข้อมูลและจัดลำดับความสำคัญของข้อมูลองค์กรรวมทั้งการกำหนดความถี่ในการสำรองข้อมูล ๒.แผนในการสำรองข้อมูล ๓.ผลการสำรองข้อมูลและการสุ่มตรวจการสำรองข้อมูล ๔.แผนเตรียมความพร้อมกรณีฉุกเฉิน ๕.รายงานผลการซักซ้อมแผนเตรียมความพร้อมกรณีฉุกเฉิน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		๔.สัมภาษณ์และขอดูพื้นที่เก็บรักษาข้อมูลที่สำรอง ๕.ขอดูสื่อในการบันทึกการสำรองข้อมูลว่ามีการติดฉลากที่มีรายละเอียดชัดเจนหรือไม่ ๖.ขอดูเอกสารการกำหนดขั้นตอนการทดสอบข้อมูลที่สำรอง ๗.ขอดูรายงานผลการทดสอบข้อมูลที่สำรอง	

ประเด็นการตรวจสอบที่ ๔ การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่า การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

หมายเหตุ:

คุณภาพ หมายถึง ๑.ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้อง

เหมาะสมต่อการใช้งาน หมายถึง สอดคล้องกับความต้องการของผู้ใช้งานระบบสารสนเทศ

พัฒนาต่อยอดได้ในอนาคต หมายถึง ระบบสารสนเทศต้องมีเอกสารการวิเคราะห์ออกแบบระบบที่สามารถพัฒนาต่อยอดได้ในอนาคต ได้แก่ แผนผังกระแสการไหลของข้อมูล(DFD/Use case) และแผนผังโครงสร้างฐานข้อมูล(ER Diagram) รวมทั้งพจนานุกรมฐานข้อมูล และความสัมพันธ์ของฐานข้อมูล

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่า การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต	๑.ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว ๑.๑ ระบบสารสนเทศต้องมีระบบการนำเข้าข้อมูลที่ถูกต้องและมีการประมวลผลรวมถึงออกรายงานแสดงได้อย่างถูกต้อง ๑.๒ ระบบสารสนเทศต้องมีการทำงานที่สอดคล้องกับความต้องการของผู้ใช้งาน ๑.๓ ระบบต้องมีเอกสารที่สามารถพัฒนาต่อยอดในอนาคตได้ คือเอกสารการวิเคราะห์ออกแบบระบบ	๑.ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว ๑.๑ ตรวจสอบว่า ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้องหรือไม่ ๑.๒ ตรวจสอบว่า มีเอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งานหรือไม่ ๑.๓ ตรวจสอบว่า ระบบที่พัฒนาสอดคล้องกับความต้องการของ	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.เอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งาน ๒.เอกสารการวิเคราะห์ออกแบบระบบ ๓.เอกสารการศึกษาความเป็นไปได้ ๔.รายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา ๕.รายงานผลการทดสอบระบบ ๖.รายงานผลการฝึกอบรมการใช้งาน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๒.ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้นตาม SDLC ๒.๑ต้องมีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งาน ๒.๒ต้องมีเอกสารการวิเคราะห์ออกแบบระบบ ๒.๓ต้องมีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา ๒.๔ต้องมีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน ๒.๕ต้องมีรายงานผลการฝึกอบรมการใช้งานและคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ ๒.๖รายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๒.๗ประเมินความพึงพอใจของผู้ใช้งานระบบ	ผู้ใช้งานหรือไม่ โดยการเปรียบเทียบกับเอกสารการวิเคราะห์การใช้งาน ๑.๔ตรวจสอบว่ามีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล (DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล ๒.ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้น ๒.๑มีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งาน ๒.๒มีเอกสารการวิเคราะห์ออกแบบระบบ ๒.๓มีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา	๗.คู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ ๘.รายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๙.สรุปผลการประเมินความพึงพอใจของผู้ใช้งานระบบ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		๒.๔มีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน ๒.๕มีรายงานผลการฝึกอบรมการใช้งานและคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ ๒.๖มีรายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๒.๗มีประเมินความพึงพอใจของผู้ใช้งานระบบ	

ประเด็นการตรวจสอบที่ ๕ ระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
ระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่าระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย	๑.มีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบ ได้แก่ (๑)มีเกณฑ์การตรวจสอบคุณภาพข้อมูล (๒)มีการตรวจสอบคุณภาพข้อมูลตามเกณฑ์ที่กำหนด (๓)มีรายงานผลคุณภาพข้อมูลให้ผู้บังคับบัญชาทราบ (๔)มีแนวทางแก้ไขพัฒนาระบบข้อมูลสารสนเทศหรือฐานข้อมูลของหน่วยงาน ๒.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้อง ๓.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความครบถ้วน ๔.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัยเป็นปัจจุบัน	๑.ตรวจสอบว่า หน่วยงานมีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบหรือไม่ ๒.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้องหรือไม่ ๓.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความครบถ้วนหรือไม่ ๔.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัยเป็นปัจจุบันหรือไม่	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.ระบบการตรวจสอบคุณภาพข้อมูล ๒.รายงานผลคุณภาพข้อมูล ๓.หน้าwebpageที่มีการแสดงข้อมูลที่ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่ทันสมัย

ประเด็นการตรวจสอบที่ ๖ เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่ามีการเผยแพร่ตามพรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด วัตถุประสงค์ย่อย เพื่อให้มั่นใจว่ามีการเผยแพร่ตามพรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด	๑.ตามมติคณะรัฐมนตรี ที่ นร ๐๔๐๕/ว ๕๗ ลงวันที่ ๒๙ เมษายน ๒๕๕๔ ให้นำข้อมูลข่าวสารตามมาตรา ๗ เผยแพร่ในเว็บไซต์ของหน่วยงาน -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ ๒.ตามมติคณะรัฐมนตรี ที่ นร ๐๔๐๕/ว ๕๗ ลงวันที่ ๒๙ เมษายน ๒๕๕๔ ให้นำข้อมูลข่าวสารตามมาตรา ๙ เผยแพร่ในเว็บไซต์ของหน่วยงาน -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน)	๑.ตรวจสอบว่ามีการเผยแพร่ตามมาตรา ๗ เผยแพร่ในเว็บไซต์ของหน่วยงาน -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ ๒.ตรวจสอบว่ามีการเผยแพร่ตามมาตรา ๙ เผยแพร่ในเว็บไซต์ของหน่วยงาน -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน) -แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน	กระดาษทำการ WA_IT๐๑ **<u>หลักฐาน</u>** ๑.บันทึกภาพถ่ายการเผยแพร่ตามมาตรา๗และ๙ ผ่านเว็บไซต์หน่วยงาน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	-แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน ๓.ตามมติคณะรัฐมนตรีที่ ๒๘ ธันวาคม ๒๕๔๗ ให้นำ -ประกาศประกวดราคา ประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน	๓.ตรวจสอบว่ามีการเผยแพร่ -ประกาศประกวดราคา ประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน	

แนวทางการตรวจสอบด้านระบบเทคโนโลยีสารสนเทศ

หน่วยงานที่มีเครื่องแม่ข่าย(Server)

ประเด็นการตรวจสอบที่ ๑ นโยบายความมั่นคงปลอดภัยเป็นไปตามข้อกำหนดของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าหน่วยงานกำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๑.การจัดทำนโยบายความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่านโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.หน่วยงานมีการจัดทำข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒.หน่วยงานประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบ ๓.หน่วยงานกำหนดผู้รับผิดชอบตามนโยบายชัดเจนหรือมีการแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)อย่างชัดเจนเป็นลายลักษณ์อักษร	๑.ตรวจสอบเอกสารหลักฐานว่าหน่วยงานได้กำหนดข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรหรือไม่ กรณีที่ไม่ได้ดำเนินการให้สอบถามสาเหตุจากผู้ที่เกี่ยวข้อง ๒.ตรวจสอบหลักฐานการประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบว่ามีหรือไม่โดยผ่านทางการแจ้งเวียนบันทึกหรือชี้แจงในที่ประชุมหรือผ่านทางเว็บไซด์ รายงานการประชุม เป็นต้น	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.เอกสารข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒.หลักฐานแสดงการประกาศและเผยแพร่นโยบายและข้อปฏิบัติ ๓.คำสั่งหรือหนังสือมอบหมายสั่งการ ๔.รายงานการประชุมติดตามการปฏิบัติตามข้อปฏิบัติที่ประกาศไว้ ๕.เอกสารทบทวนข้อปฏิบัติ/แนวทางปฏิบัติ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๔.กรณีมีข้อปฏิบัติ/แนวทางปฏิบัติอยู่แล้ว หน่วยงานมีการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบัน ๕.มีการปฏิบัติตามข้อปฏิบัติ/แนวปฏิบัติที่รองรับนโยบาย ซึ่งต้องมีกระบวนการติดตามประเมินผลข้อปฏิบัติที่รองรับนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน	๓.ตรวจสอบว่ามีการกำหนดผู้รับผิดชอบหรือมีคำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)เป็นลายลักษณ์อักษรหรือไม่ และเป็นปัจจุบันหรือไม่ ถ้าปีที่ผ่านมาไม่มีการเปลี่ยนแปลงคณะทำงานก็ใช้คำสั่งเดิมได้ ๔.ตรวจสอบหลักฐานการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบันโดยผู้มีอำนาจของหน่วยงาน ๕.ตรวจสอบหลักฐานรายงานการประชุมคณะกรรมการฯว่ามีการติดตามประเมินผลข้อปฏิบัติที่รองรับนโยบายหรือไม่(เป็นการประเมินรายข้อ)	

ประเด็นการตรวจสอบที่ ๒ การควบคุมการเข้าถึงเป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่ามีการปฏิบัติในการควบคุมการเข้าถึงเป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๒.๑ การควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศ (User access management) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศ (User access management) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของ	๑.มีการจัดอบรม/ชี้แจงในการประชุม/แจ้งเวียน/เผยแพร่ในเว็บไซต์ เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ๒.มีการวางระบบการลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว	๑.ตรวจสอบหลักฐานว่ามีการจัดอบรม/ชี้แจง/แจ้งเวียน เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน ๒.ตรวจสอบว่ามีระบบการลงทะเบียนผู้ใช้งาน เช่นระบบการ authentication หรือการลงทะเบียนสมัครเข้าใช้ระบบงานเว็บไซต์/ระบบสารสนเทศอื่นใดของหน่วยงาน โดยต้องมีการกำหนดขั้นตอนการปฏิบัติสำหรับการลงทะเบียนและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาต	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.เอกสารการจัดอบรม/ชี้แจง/แจ้งเวียนเพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน ๒.Flowchart ขั้นตอนระบบการลงทะเบียนผู้ใช้งาน ๓.เอกสารประกอบระบบการลงทะเบียนผู้ใช้งาน ๔.เอกสารที่ได้จากการพิมพ์ในระบบการบริหารจัดการรหัสผ่าน ๕.มาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
ระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๓.มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆที่เกี่ยวข้องกับการเข้าถึง ๔.มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน(user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ๕.ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ๖.มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน(User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต	๓.ตรวจสอบว่า ระบบการ authentication หรือการลงทะเบียนสมัครเข้าใช้ระบบงานเว็บไซต์/ระบบสารสนเทศอื่นใดของหน่วยงานมีเมนูระบบบริหารจัดการและกำหนดสิทธิของผู้ใช้งานที่เหมาะสมหรือไม่ ๔.ตรวจสอบว่า มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน เช่น มีระบบการเปลี่ยนรหัสผ่าน/ระบบกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษร และต้องมีอักขระปน เป็นต้น ๕.ตรวจสอบว่า ระบบการ authentication หรือระบบเว็บไซต์/ระบบสารสนเทศอื่นใดของหน่วยงานมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละครั้งหรือไม่ ๖.ตรวจสอบว่ามีมาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	โดยต้องมีเนื้อหาการใช้งานรหัสผ่านต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่านและการเปลี่ยนรหัสผ่านที่มีคุณภาพ	๗.จากข้อ ๖ ผู้ใช้ได้ดำเนินการตามแนวปฏิบัติหรือไม่	
๒.๒ การควบคุมการเข้าถึงเครือข่าย (network access control) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงเครือข่ายตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.ต้องมีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร(user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายได้ ๒.การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่ระบบ(remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับ	๑.ตรวจสอบว่า มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กรก่อนที่จะเข้ามาใช้งานระบบเครือข่ายภายในองค์กร ๒. การตรวจ IP แบบ Fix IP ๓.ตรวจสอบ มีการเปิดใช้งานพอร์ตเฉพาะพอร์ตที่กรมกำหนดไว้เท่านั้น	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.บัญชีรหัสผู้ใช้งานในการยืนยันตัวบุคคล ๒.เอกสารที่พิมพ์ออกมาจากระบบไฟร์วอลล์เกี่ยวกับการเปิดใช้งานพอร์ต ๓.แผนผังเครือข่ายว่ามีการแบ่งแยกเครือข่าย

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	ตรวจสอบและปรับแต่ระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ๔.การแบ่งแยกเครือข่าย(segregation in network) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ	ได้แก่ Web Access: ๘๐,๔๔๓ Remote Desktop: ๓๓๘๙ snmp: ๑๖๒ smtp: ๒๕ Printer-Sharing: ๑๓๙ ftp: ๒๑ ssh: ๒๒ ๔.ตรวจสอบการกำหนดแผนผังเครือข่ายว่ามีการแบ่งแยกเครือข่ายตามกลุ่มที่เหมาะสมหรือไม่	
๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ(Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงระบบปฏิบัติการตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.การใช้งานโปรแกรมอรรถประโยชน์(user of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ๒.เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น(session time-out) ๓.การติดตั้งโปรแกรมป้องกันไวรัสและการupdateโปรแกรมป้องกันไวรัส	๑.ตรวจสอบว่ามีการควบคุมการใช้โปรแกรมอรรถประโยชน์หรือไม่ โดยการสุ่มตรวจที่เครื่องคอมพิวเตอร์และหากมีการกำหนดต้องรายงานการประชุมเพื่อควบคุมการใช้โปรแกรมอรรถประโยชน์ ๒.ตรวจสอบว่ามีการตัดสัญญาณอินเทอร์เน็ตในระยะเวลา ๕-๑๕ นาทีหรือไม่ โดยตรวจสอบการตั้งค่าที่ไฟร์วอลล์(Firewall)ไปที่เมนู User	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.รายงานการประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน(CSO) เกี่ยวกับการควบคุมการใช้โปรแกรมอรรถประโยชน์ ๒.เอกสารที่พิมพ์มาจากไฟร์วอลล์(Firewall)เกี่ยวกับการตั้งค่าการตัดสัญญาณอินเตอร์เน็ต(session time-out)

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		Device →authentication Setting →TimeOutauthentication ๓.ตรวจสอบว่า มีการติดตั้งโปรแกรมป้องกันไวรัสครบถ้วนทุกเครื่องหรือไม่ และมีการ update โปรแกรมป้องกันไวรัสครบถ้วนหรือไม่	
๒.๔ การควบคุมการเข้าถึงทางกายภาพของห้องแม่ข่าย ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีแบบปลอดภัย **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงทางกายภาพตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ๑.๑ ให้มีการป้องกันขอบเขตพื้นที่ของหน่วยงานที่มีการติดตั้ง จัดเก็บหรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศ ๑.๒มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพเพื่อป้องกันภัยจากภายนอกภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น	**<u>๑.การจัดทำบริเวณล้อมรอบ (Physical security perimeter)</u>** ๑.๑ มีการแยกพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศขององค์กร (เช่น ห้องเครื่อง/ห้องแม่ข่าย) ออกจากพื้นที่ส่วนที่เป็นสำนักงานของผู้ให้บริการภายนอกหรือไม่ ๑.๒ มีการจัดแสงสว่างในบริเวณต่างๆ อย่างเพียงพอ ๑.๓ มีการใช้ผนังล้อมรอบเป็นผนังทึบและควรมิดชิด เมื่อมองจากด้านนอกเข้าไปข้างในจะต้องไม่รู้ว่าเป็นห้อง	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.ภาพถ่ายบริเวณพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศขององค์กร ๒.ภาพถ่ายป้ายหน้าห้องแม่ข่าย ๓.ภาพถ่ายกล้องวงจรปิดที่ติดตั้งบริเวณหน้าห้องและภายในห้องแม่ข่าย ๔.ภาพถ่ายเครื่องมือการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้ลายนิ้วมือ ๕.ภาพถ่ายเครื่องมือวัดอุณหภูมิและความชื้นภายในห้องแม่ข่าย

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๑.๓ จัดวางและป้องกันอุปกรณ์สารสนเทศเพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่างๆและเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ๑.๔มีการป้องกันอุปกรณ์สารสนเทศที่อาจเกิดจากไฟฟ้าขัดข้องหรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน ๑.๕มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธีเพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ	แม่ข่ายหรือหากผนังเป็นกระจกใส ต้องทำการติดฟิล์มทึบทับไว้ ๑.๔ มีการใช้ประตูและหน้าต่างของสำนักงานให้ล็อคอยู่เสมอ ๑.๕ ประตูทางเข้า จะต้องมีกล้องวงจรปิดบันทึกภาพบริเวณประตูเข้าออกห้อง ๑.๖ มีการจัดระบบการรักษาความปลอดภัยอย่างเพียงพอหรือไม่ มีการตรวจตาพื้นที่ภายในองค์กรอย่างไร ตรวจตราบ่อยเพียงไร มีผู้ตรวจตราหรือกวดขันงานของ รปภ.อย่างสม่ำเสมอหรือไม่ **๒.การควบคุมการเข้า-ออก(Physical entry control)**	๖.ภาพถ่ายสัญญาณเตือนภัยต่างๆและเครื่องแม่ข่าย รวมทั้งมาตรการข้อห้ามมิให้ปฏิบัติต่างๆ ๗.ภาพถ่ายสัญญาณและสายไฟฟ้าที่เดินในห้องแม่ข่าย รวมทั้งแผนผังสายสัญญาณ ๘.ภาพถ่ายการจัดวางอุปกรณ์เครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องเช่นUPS ๙.ภาพถ่ายตู้ Rack และระบบปรับอากาศ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		๒.๑ มีมาตรการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้ลายนิ้วมือ เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญหรือไม่ ๒.๒ มีการลงและจัดเก็บบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญ **๓.ภายในห้องแม่ข่ายที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)** ๓.๑ ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น ๓.๒ ห้ามสูญบุหรี่ และนำอาหารเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง ๓.๓ ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องให้ปิดล็อคอยู่เสมอ ๓.๔ ความสะอาดและความเป็นระเบียบเรียบร้อยของห้องแม่ข่าย ๓.๕ มีการดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องแม่ข่าย	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		อย่างสม่ำเสมอหรือไม่ ให้ตรวจสอบแผนการทำความสะอาดของห้องแม่ข่ายว่ามีการจดบันทึกและทำแผนไว้หรือไม่ และมีการทำความสะอาดเพื่อให้อุปกรณ์ปลอดจากฝุ่นอย่างสม่ำเสมอหรือไม่ ๓.๖ ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย ๓.๗ ไม่มีการจัดวางอุปกรณ์คอมพิวเตอร์ไว้ใต้ตู้เครื่องปรับอากาศ (ซึ่งอาจมีน้ำรั่วไหลลงมายังอุปกรณ์คอมพิวเตอร์ได้) ๓.๘ มีการตรวจสอบระดับอุณหภูมิในห้องแม่ข่ายหรือไม่ ๓.๙ มีการตรวจสอบความชื้นในห้องแม่ข่ายหรือไม่ ๓.๑๐ มีการติดตามระบบปรับอากาศอย่างน้อยมีแอร์ ๒ ตัว ตั้งเวลาเปิดปิดสลับทำงาน	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		๓.๑๑ มีการป้องกันไฟไหม้หรือไม่ เช่น การติดตั้งอุปกรณ์ดับเพลิงและเครื่องดักจับควันไฟ ๓.๑๒ ตู้ Rack ทุกตู้ต้องล็อคอยู่เสมอ ห้ามเปิดค้างไว้ ๓.๑๓ ตู้ Rack มีพัดลมดูดอากาศติดตั้งไว้ด้านบน ๓.๑๔ ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย ๓.๑๕ มีการจัดทำป้ายชื่อสำหรับสายสัญญาณสื่อสารเพื่อป้องกันการตัดต่อสัญญาณผิดเส้น ๓.๑๖ มีการจัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง ๓.๑๗ มีการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน (แรงดันไฟฟ้าไม่คงที่ มีการผันแปรอย่างต่อเนื่อง) หรือไฟฟ้ากระชากหรือไม่ เช่น การใช้ยูพีเอส	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๒.๔การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑.หน่วยงานต้องมีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑.ตรวจสอบว่าหน่วยงานมีการจัดทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศหรือไม่ และการประเมินความเสี่ยงได้ดำเนินการอย่างถูกต้องเหมาะสมหรือไม่	**<u>หลักฐาน</u>** -เอกสารประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเด็นการตรวจสอบที่ ๓ หน่วยงานมีการดำเนินงานควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐

วัตถุประสงค์

๑..เพื่อให้มั่นใจหน่วยงานมีการดำเนินงานควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๓.มีการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ตามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐กำหนด **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่าได้ดำเนินการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ตามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐กำหนด	มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์	๑.ตรวจสอบไฟร์วอลล์(Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ โดย ๑.๑ ตรวจสอบว่าเวลาของไฟร์วอลล์(Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ถูกต้องเป็นปัจจุบัน -เมนู Dachbord→Main→ Time -เมนู Log&Report→ Forward Traffic→ดู log เวลาตรงกับปัจจุบันหรือไม่ ๑.๒ ตรวจสอบการตั้งเวลาในการจัดเก็บการจารจรคอมพิวเตอร์ไว้ ๙๐ วันตามที่กำหนด	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.ภาพถ่ายไฟร์วอลล์(Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์เพื่อดูสถานะการทำงาน ๒.เอกสารพิมพ์จากไฟร์วอลล์(Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์

ประเด็นการตรวจสอบที่ ๔ มีการประเมินขีดสมรรถนะของระบบสารสนเทศให้มีความพร้อมใช้งาน

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าระบบสารสนเทศของหน่วยงานมีความพร้อมใช้ตลอดเวลา

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๔.ระบบสารสนเทศมีความพร้อมใช้งานตลอดเวลา **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่าระบบสารสนเทศของหน่วยงานมีความพร้อมใช้งานตลอดเวลา	๑.ต้องมีการจัดทำแผนการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ๒.มีการประเมินขีดสมรรถนะของระบบดังกล่าวตามแผนที่กำหนด ๓.ต้องวิเคราะห์ผลการประเมินขีดสมรรถนะของระบบดังกล่าวอย่างสม่ำเสมอ ๔.ต้องรายงานผลการวิเคราะห์ขีดสมรรถนะของระบบดังกล่าวให้ผู้บังคับบัญชาทราบอย่างน้อยปีละครั้ง ยกเว้นในกรณีที่ค่าขีดสมรรถนะเกินค่า Threshold หน่วยงานต้องมีการประเมินค่าขีดสมรรถนะของระบบถี่มากขึ้นตามความเหมาะสมและรายงานผู้บังคับบัญชาทราบพร้อมทั้งหาสาเหตุและแนวทางการแก้ไขปัญหา	๑.มีแผนการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิชหรือไม่ ๒.ตรวจสอบว่ามีการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ตามแผนที่กำหนดหรือไม่ ๓.ตรวจสอบว่ามีการวิเคราะห์ขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิชหรือไม่ ๔.ตรวจสอบว่า เครื่องแม่ข่ายและสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิชเกินค่า Thresholdหรือไม่หากเกินว่าค่า Threshold ที่กำหนดไว้ต้องหาสาเหตุและแนวทางการแก้ไข รวมถึงรายงาน	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.แผนการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ๒.การบันทึกกิจกรรมการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ตามแผนที่กำหนด ๓.รายงานผลการวิเคราะห์ขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ๔.การบันทึกเหตุการณ์ที่เป็นปัญหา ๕.รายงานผลการบันทึกเหตุการณ์ที่เป็นปัญหา เช่น กรณีที่ค่าขีดสมรรถนะเกินค่า Thresholdที่กำหนดหรือการDownของระบบ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๕.หากมีการDownของระบบดังกล่าวต้องมีการจดบันทึกปัญหาและรายงานผู้บังคับบัญชาทราบพร้อมทั้งหาสาเหตุและแนวทางการแก้ไขปัญหา	ผู้บังคับบัญชาทราบ ๕.ตรวจสอบว่า มีการจดบันทึกเหตุการณ์ปัญหาที่เกิดขึ้นหรือไม่ ๖.ตรวจสอบว่า มีการ Downของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิชหรือไม่ กี่ครั้งและสาเหตุใด ได้แก้ไขอย่างไร มีการรายงานผู้บังคับบัญชาหรือไม่	

ประเด็นการตรวจสอบที่ ๕ การดำเนินงานควบคุมและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

วัตถุประสงค์

๑.เพื่อมั่นใจว่ามีการดำเนินการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศมิให้สูญหาย

๒.เพื่อมั่นใจว่ามีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีอย่างเหมาะสม

๓.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๖.การดำเนินงานควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างรัดกุม **<u>วัตถุประสงค์ย่อย</u>** ๑.เพื่อมั่นใจว่ามีการดำเนินการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศมิให้สูญหาย ๒.เพื่อมั่นใจว่ามีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีอย่างเหมาะสม	๑.ต้องมีการจัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยมีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อย CPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินโดยครอบคลุมด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ ๒.ระบบการยืม-คืนครุภัณฑ์ตามระเบียบ ๓.มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย(ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิงป้องกันและเชิงแก้ไข)	๑.ตรวจสอบทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อยCPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินโดยครอบคลุมด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ ๒.ตรวจสอบว่า มีระบบการยืม-คืนครุภัณฑ์ถูกต้องตามระเบียบหรือไม่ ๓.ตรวจสอบว่า มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย(ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิงป้องกันและเชิงแก้ไข)	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.ทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ ๒.เอกสารเกี่ยวกับระบบการยืม-คืนครุภัณฑ์ด้านเทคโนโลยีสารสนเทศ ๓.แผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ ๔.เอกสารในการดำเนินกิจกรรมบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์

ประเด็นการตรวจสอบที่ ๖ การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่า การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

หมายเหตุ:

คุณภาพ หมายถึง ๑.ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้อง

เหมาะสมต่อการใช้งาน หมายถึง สอดคล้องกับความต้องการของผู้ใช้งานระบบสารสนเทศ

พัฒนาต่อยอดได้ในอนาคต หมายถึง ระบบสารสนเทศต้องมีเอกสารการวิเคราะห์ออกแบบระบบที่สามารถพัฒนาต่อยอดได้ในอนาคต ได้แก่ แผนผังกระแสการไหลของข้อมูล(DFD/Use case) และแผนผังโครงสร้างฐานข้อมูล(ER Diagram) รวมทั้งพจนานุกรมฐานข้อมูล และความสัมพันธ์ของฐานข้อมูล

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่า การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต	๑.ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว ๑.๑ ระบบสารสนเทศต้องมีระบบการนำเข้าข้อมูลที่ถูกต้องและมีการประมวลผลรวมถึงออกรายงานแสดงได้อย่างถูกต้อง ๑.๒ ระบบสารสนเทศต้องมีการทำงานที่สอดคล้องกับความต้องการของผู้ใช้งาน ๑.๓ ระบบต้องมีเอกสารที่สามารถพัฒนาต่อยอดในอนาคตได้ คือเอกสารการวิเคราะห์ออกแบบระบบ	๑.ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว ๑.๑ ตรวจสอบว่า ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้องหรือไม่ ๑.๒ ตรวจสอบว่า มีเอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งานหรือไม่ ๑.๓ ตรวจสอบว่า ระบบที่พัฒนาสอดคล้องกับความต้องการของ	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.เอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งาน ๒.เอกสารการวิเคราะห์ออกแบบระบบ ๓.เอกสารการศึกษาความเป็นไปได้ ๔.รายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา ๕.รายงานผลการทดสอบระบบ ๖.รายงานผลการฝึกอบรมการใช้งาน ๗.คู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๒.ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้นตาม SDLC ๒.๑ต้องมีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งาน ๒.๒ต้องมีเอกสารการวิเคราะห์ออกแบบระบบ ๒.๓ต้องมีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา ๒.๔ต้องมีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน ๒.๕ต้องมีรายงานผลการฝึกอบรมการใช้งานและคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ ๒.๖รายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๒.๗ประเมินความพึงพอใจของผู้ใช้งานระบบ	ผู้ใช้งานหรือไม่ โดยการเปรียบเทียบกับเอกสารการวิเคราะห์การใช้งาน ๑.๔ตรวจสอบว่ามีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล (DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล ๒.ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้น ๒.๑มีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งาน ๒.๒มีเอกสารการวิเคราะห์ออกแบบระบบ ๒.๓มีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา	๘.รายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๙.สรุปผลการประเมินความพึงพอใจของผู้ใช้งานระบบ

ประเด็นย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ

วัตถุประสงค์ย่อย			แหล่งข้อมูล
		๒.๔มีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน ๒.๕มีรายงานผลการฝึกอบรมการใช้งานและคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ ๒.๖มีรายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๒.๗มีประเมินความพึงพอใจของผู้ใช้งานระบบ	

ประเด็นการตรวจสอบที่ ๗ ระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
ระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่าระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย	๑.มีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบ ได้แก่ (๑)มีเกณฑ์การตรวจสอบคุณภาพข้อมูล (๒)มีการตรวจสอบคุณภาพข้อมูลตามเกณฑ์ที่กำหนด (๓)มีรายงานผลคุณภาพข้อมูลให้ผู้บังคับบัญชาทราบ (๔)มีแนวทางแก้ไขพัฒนาระบบข้อมูลสารสนเทศหรือฐานข้อมูลของหน่วยงาน ๒.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้อง ๓.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความครบถ้วน ๔.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัยเป็นปัจจุบัน	๑.ตรวจสอบว่า หน่วยงานมีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบหรือไม่ ๒.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้องหรือไม่ ๓.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความครบถ้วนหรือไม่ ๔.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัยเป็นปัจจุบันหรือไม่	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.ระบบการตรวจสอบคุณภาพข้อมูล ๒.รายงานผลคุณภาพข้อมูล ๓.หน้าwebpageที่มีการแสดงข้อมูลที่ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่ทันสมัย

ประเด็นการตรวจสอบที่ ๘ เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่ามีการเผยแพร่ตามพรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด วัตถุประสงค์ย่อย เพื่อให้มั่นใจว่ามีการเผยแพร่ตามพรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด	๑.ตามมติคณะรัฐมนตรี ที่ นร ๐๔๐๕/ว ๕๗ ลงวันที่ ๒๙ เมษายน ๒๕๕๔ ให้นำข้อมูลข่าวสารตามมาตรา ๗ เผยแพร่ในเว็บไซต์ของหน่วยงาน -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ ๒.ตามมติคณะรัฐมนตรี ที่ นร ๐๔๐๕/ว ๕๗ ลงวันที่ ๒๙ เมษายน ๒๕๕๔ ให้นำข้อมูลข่าวสารตามมาตรา ๙ เผยแพร่ในเว็บไซต์ของหน่วยงาน -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน)	๑.ตรวจสอบว่ามีการเผยแพร่ตามมาตรา ๗ เผยแพร่ในเว็บไซต์ของหน่วยงาน -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ ๒.ตรวจสอบว่ามีการเผยแพร่ตามมาตรา ๙ เผยแพร่ในเว็บไซต์ของหน่วยงาน -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน) -แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน	กระดาษทำการ WA_IT๐๑ **<u>หลักฐาน</u>** ๑.บันทึกภาพถ่ายการเผยแพร่ตามมาตรา๗และ๙ ผ่านเว็บไซต์หน่วยงาน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	-แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน ๓.ตามมติคณะรัฐมนตรีที่ ๒๘ ธันวาคม ๒๕๔๗ ให้นำ -ประกาศประกวดราคา ประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน	๓.ตรวจสอบว่ามีการเผยแพร่ -ประกาศประกวดราคา ประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน	

ประเด็นการตรวจสอบที่ ๙ หน่วยงานต้องมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าหน่วยงานมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงาน รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๔.มีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด วัตถุประสงค์ย่อย เพื่อให้มั่นใจว่าหน่วยงานมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด	๑.ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม ๒.มีแผนในการสำรองข้อมูลเป็นลายลักษณ์อักษรและปฏิบัติตรงตามแผนที่กำหนด ๓.กำหนดผู้รับผิดชอบในการสำรองข้อมูล ๔.กำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง ๕.ต้องติดฉลากที่มีรายละเอียดชัดเจนเพื่อให้สามารถค้นหาได้โดยเร็วและป้องกันการใช้งานสื่อบันทึกผิดพลาด ๖.กำหนดขั้นตอนการทดสอบข้อมูลที่สำรอง ๗.มีรายงานผลการทดสอบข้อมูลที่สำรอง ๘.กำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว	๑.สัมภาษณ์มีกระบวนการในการสำรองข้อมูลอย่างเป็นระบบได้แก่ (๑)คัดเลือกข้อมูลที่สำคัญต่อองค์กรนำมาจัดเรียงลำดับความสำคัญ (๒)กำหนดความถี่ในการสำรองข้อมูลตามระดับความสำคัญที่กำหนดไว้ (๓)จัดทำแผนในการสำรองข้อมูลอย่างเป็นระบบ (๔)ดำเนินการสำรองข้อมูลและสุ่มตรวจข้อมูลที่สำรองว่ามีความสมบูรณ์หรือไม่และมีหลักฐานบันทึกกิจกรรมการสำรองข้อมูล ๒.ขอดูแผนการสำรองข้อมูลและผลการปฏิบัติในการสำรองข้อมูลว่าตรงตามแผนหรือไม่และมีการสุ่มตรวจการสำรองข้อมูล ๓.สัมภาษณ์และขอดูเอกสารหลักฐานการแต่งตั้ง/มอบหมายผู้รับผิดชอบในการสำรองข้อมูล	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.รายงานการประชุมคัดเลือกข้อมูลและจัดลำดับความสำคัญของข้อมูลองค์กรรวมทั้งการกำหนดความถี่ในการสำรองข้อมูล ๒.แผนในการสำรองข้อมูล ๓.ผลการสำรองข้อมูลและการสุ่มตรวจการสำรองข้อมูล ๔.แผนเตรียมความพร้อมกรณีฉุกเฉิน ๕.รายงานผลการซักซ้อมแผนเตรียมความพร้อมกรณีฉุกเฉิน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๙.มีการดำเนินการการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้วตามขั้นตอนที่กำหนดไว้ ๑๐.ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องโดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ๑๑.มีการรายงานผลการซักซ้อมแผนฉุกเฉินอย่างเป็นลายลักษณ์อักษร	๔.สัมภาษณ์และขอดูพื้นที่เก็บรักษาข้อมูลที่สำรอง ๕.ขอดูสื่อในการบันทึกการสำรองข้อมูลว่ามีการติดฉลากที่มีรายละเอียดชัดเจนหรือไม่ ๖.ขอดูเอกสารการกำหนดขั้นตอนการทดสอบข้อมูลที่สำรอง ๗.ขอดูรายงานผลการทดสอบข้อมูลที่สำรอง ๘.ขอดูเอกสารการกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ๙.สัมภาษณ์การดำเนินการการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้วตามขั้นตอนที่กำหนดไว้ ๑๐.ตรวจสอบว่า หน่วยงานมีแผนเตรียมความพร้อมกรณีฉุกเฉินหรือไม่และมีการซักซ้อมแผนหรือไม่ ๑๑.ขอดูการรายงานผลการซักซ้อมแผนฉุกเฉิน	

แนวทางการตรวจสอบด้านระบบเทคโนโลยีสารสนเทศ

ของศูนย์เทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ประเด็นการตรวจสอบที่ ๑ นโยบายความมั่นคงปลอดภัยเป็นไปตามข้อกำหนดของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าหน่วยงานกำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๑.การจัดทำนโยบายความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่านโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.หน่วยงานมีการจัดทำข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒.หน่วยงานประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบ ๓.หน่วยงานกำหนดผู้รับผิดชอบตามนโยบายชัดเจนหรือมีการแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)อย่างชัดเจนเป็นลายลักษณ์อักษร	๑.ตรวจสอบเอกสารหลักฐานว่าหน่วยงานได้กำหนดข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรหรือไม่ กรณีที่ไม่ได้ดำเนินการให้สอบถามสาเหตุจากผู้ที่เกี่ยวข้อง ๒.ตรวจสอบหลักฐานการประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบว่ามีหรือไม่โดยผ่านทางการแจ้งเวียนบันทึกหรือชี้แจงในที่ประชุมหรือผ่านทางเว็บไซด์ รายงานการประชุม เป็นต้น	กระดาษทำการ WAIT๐๑ **<u>หลักฐาน</u>** ๑.เอกสารข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒.หลักฐานแสดงการประกาศและเผยแพร่นโยบายและข้อปฏิบัติ ๓.คำสั่งหรือหนังสือมอบหมายสั่งการ ๔.รายงานการประชุมติดตามการปฏิบัติตามข้อปฏิบัติที่ประกาศไว้ ๕.เอกสารทบทวนข้อปฏิบัติ/แนวทางปฏิบัติ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๔.กรณีมีข้อปฏิบัติ/แนวทางปฏิบัติอยู่แล้ว หน่วยงานมีการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบัน ๕.มีการปฏิบัติตามข้อปฏิบัติ/แนวปฏิบัติที่รองรับนโยบาย ซึ่งต้องมีกระบวนการติดตามประเมินผลข้อปฏิบัติที่รองรับนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน	๓.ตรวจสอบว่ามีการกำหนดผู้รับผิดชอบหรือมีคำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)เป็นลายลักษณ์อักษรหรือไม่ และเป็นปัจจุบันหรือไม่ ถ้าปีที่ผ่านมาไม่มีการเปลี่ยนแปลงคณะทำงานก็ใช้คำสั่งเดิมได้ ๔.ตรวจสอบหลักฐานการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบันโดยผู้มีอำนาจของหน่วยงาน ๕.ตรวจสอบหลักฐานรายงานการประชุมคณะกรรมการฯว่ามีการติดตามประเมินผลข้อปฏิบัติที่รองรับนโยบายหรือไม่(เป็นการประเมินรายข้อ)	

ประเด็นการตรวจสอบที่ ๒ การควบคุมการเข้าถึงเป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่ามีการปฏิบัติในการควบคุมการเข้าถึงเป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๒.๑ การควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศ (User access management) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศ (User access management) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของ	๑.มีการจัดอบรม/ชี้แจงในการประชุม/แจ้งเวียน/เผยแพร่ในเว็บไซต์ เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ๒.มีการวางระบบการลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว	๑.ตรวจสอบหลักฐานว่ามีการจัดอบรม/ชี้แจง/แจ้งเวียน เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน ๒.ตรวจสอบว่ามีระบบการลงทะเบียนผู้ใช้งาน เช่นระบบการ authentication หรือการลงทะเบียนสมัครเข้าใช้ระบบงานเว็บไซต์/ระบบสารสนเทศอื่นใดของหน่วยงาน โดยต้องมีการกำหนดขั้นตอนการปฏิบัติสำหรับการลงทะเบียนและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาต	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.เอกสารการจัดอบรม/ชี้แจง/แจ้งเวียนเพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน ๒.Flowchart ขั้นตอนระบบการลงทะเบียนผู้ใช้งาน ๓.เอกสารประกอบระบบการลงทะเบียนผู้ใช้งาน ๔.เอกสารที่ได้จากการพิมพ์ในระบบการบริหารจัดการรหัสผ่าน ๕.มาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
ระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๓.มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆที่เกี่ยวข้องกับการเข้าถึง ๔.มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน(user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ๕.ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ๖.มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน(User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต	๓.ตรวจสอบว่า ระบบการ authentication หรือการลงทะเบียนสมัครเข้าใช้ระบบงานเว็บไซต์/ระบบสารสนเทศอื่นใดของหน่วยงานมีเมนูระบบบริหารจัดการและกำหนดสิทธิของผู้ใช้งานที่เหมาะสมหรือไม่ ๔.ตรวจสอบว่า มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน โดยการตั้งรหัสผ่านต้องมีคุณภาพ เช่น มีระบบการเปลี่ยนรหัสผ่าน/ระบบกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษร และต้องมีอักขระปน เป็นต้น ๕.ตรวจสอบว่า ระบบการ authentication หรือระบบเว็บไซต์/ระบบสารสนเทศอื่นใดของหน่วยงานมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละครั้งหรือไม่ ๖.ตรวจสอบว่ามีมาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	โดยต้องมีเนื้อหาการใช้งานรหัสผ่านต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ		
๒.๒ การควบคุมการเข้าถึงเครือข่าย (network access control) เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงเครือข่ายตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ๒.ต้องมีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร(user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายได้ ๓.การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่ระบบ(remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับ	๑.ตรวจสอบว่ามีการใช้งานบริการเครือข่ายที่ให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่เปิด/อนุญาตให้เข้าถึงเท่านั้น เช่นไม่มีการรีโมลเข้ามาในระบบภายในเครือข่ายโดยไม่รับอนุญาตหรือออกเครือข่ายโดยไม่ผ่านการ authenticationเป็นต้น ๒. การตรวจ IP แบบ Fix IP ๓.ตรวจสอบว่า มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กรก่อนที่จะเข้ามาใช้งานระบบเครือข่ายภายในองค์กร ๔.ตรวจสอบ มีการเปิดใช้งานพอร์ตเฉพาะพอร์ตที่กรมกำหนดไว้เท่านั้น	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.บัญชีรหัสผู้ใช้งานในการยืนยันตัวบุคคล ๒.เอกสารที่พิมพ์ออกมาจากระบบไฟร์วอลล์เกี่ยวกับการเปิดใช้งานพอร์ต ๓.แผนผังเครือข่ายว่ามีการแบ่งแยกเครือข่าย

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	ตรวจสอบและปรับแต่ระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ๔.การแบ่งแยกเครือข่าย(segregation in network) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ	ได้แก่ Web Access: ๘๐,๔๔๓ Remote Desktop: ๓๓๘๙ snmp: ๑๖๒ smtp: ๒๕ Printer-Sharing: ๑๓๙ ftp: ๒๑ ssh: ๒๒ ๕.ตรวจสอบการกำหนดแผนผังเครือข่ายว่ามีการแบ่งแยกเครือข่ายตามกลุ่มที่เหมาะสมหรือไม่	
๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ(Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงระบบปฏิบัติการตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.การใช้งานโปรแกรมอรรถประโยชน์ (user of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ๒.เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น(session time-out) ๓.การติดตั้งโปรแกรมป้องกันไวรัสและการupdateโปรแกรมป้องกันไวรัส	๑.ตรวจสอบว่ามีการควบคุมการใช้โปรแกรมอรรถประโยชน์หรือไม่ โดยการสุ่มตรวจที่เครื่องคอมพิวเตอร์และหากมีการกำหนดต้องรายงานการประชุมเพื่อควบคุมการใช้โปรแกรมอรรถประโยชน์ ๒.ตรวจสอบว่ามีการตัดสัญญาณอินเทอร์เน็ตในระยะเวลา ๕-๑๕ นาที หรือไม่ โดยตรวจสอบการตั้งค่าที่ไฟร์วอลล์(Firewall)ไปที่เมนู User	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.รายงานการประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน(CSO) เกี่ยวกับการควบคุมการใช้โปรแกรมอรรถประโยชน์ ๒.เอกสารที่พิมพ์มาจากไฟร์วอลล์(Firewall)เกี่ยวกับการตั้งค่าการตัดสัญญาณอินเตอร์เน็ต(session time-out)

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		Device →authentication Setting →TimeOutauthentication ๓.ตรวจสอบว่า มีการติดตั้งโปรแกรมป้องกันไวรัสครบถ้วนทุกเครื่องหรือไม่ และมีการ update โปรแกรมป้องกันไวรัสครบถ้วนหรือไม่	
๒.๔ การควบคุมการเข้าถึงทางกายภาพของห้องแม่ข่าย ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีแบบปลอดภัย **วัตถุประสงค์ย่อย** เพื่อให้มั่นใจว่ามีการปฏิบัติในการการควบคุมการเข้าถึงทางกายภาพตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑.การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ๑.๑ ให้มีการป้องกันขอบเขตพื้นที่ของหน่วยงานที่มีการติดตั้ง จัดเก็บหรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศ ๑.๒มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพเพื่อป้องกันภัยจากภายนอกภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น	**๑.การจัดทำบริเวณล้อมรอบ (Physical security perimeter)** ๑.๑ มีการแยกพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศขององค์กร (เช่น ห้องเครื่อง/ห้องแม่ข่าย) ออกจากพื้นที่ส่วนที่เป็นสำนักงานของผู้ให้บริการภายนอกหรือไม่ ๑.๒ มีการจัดแสงสว่างในบริเวณต่างๆ อย่างเพียงพอ ๑.๓ มีการใช้ผนังล้อมรอบเป็นผนังทึบและควรมิดชิด เมื่อมองจากด้านนอกเข้าไปข้างในจะต้องไม่รู้ว่าเป็นห้อง	ตสน.กระดาษทำการ WA_IT๐๒ **หลักฐาน** ๑.ภาพถ่ายบริเวณพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศขององค์กร ๒.ภาพถ่ายป้ายหน้าห้องแม่ข่าย ๓.ภาพถ่ายกล้องวงจรปิดที่ติดตั้งบริเวณหน้าห้องและภายในห้องแม่ข่าย ๔.ภาพถ่ายเครื่องมือการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้ลายนิ้วมือ ๕.ภาพถ่ายเครื่องมือวัดอุณหภูมิและความชื้นภายในห้องแม่ข่าย

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๑.๓ จัดวางและป้องกันอุปกรณ์สารสนเทศเพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่างๆและเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ๑.๔มีการป้องกันอุปกรณ์สารสนเทศที่อาจเกิดจากไฟฟ้าขัดข้องหรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน ๑.๕มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธีเพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ	แม่ข่ายหรือหากผนังเป็นกระจกใส ต้องทำการติดฟิล์มทึบทับไว้ ๑.๔ ห้องแม่ข่าย (Server) ห้ามมีป้ายบอกว่าเป็นห้อง Server Room เพื่อป้องกันการแอบเข้ามาขโมยทรัพย์สินหรือเข้ามาทำลายในกรณีเกิดเหตุการณ์ประท้วงของพนักงาน ๑.๕ มีการใช้ประตูและหน้าต่างของสำนักงานให้ล็อคอยู่เสมอ ๑.๖ ประตูทางเข้า จะต้องมีกล้องวงจรปิดบันทึกภาพบริเวณประตูเข้าออกห้อง ๑.๗ มีการจัดระบบการรักษาความปลอดภัยอย่างเพียงพอหรือไม่ มีการตรวจตาพื้นที่ภายในองค์กรอย่างไร ตรวจตราบ่อยเพียงไร มีผู้ตรวจตราหรือกวดขันงานของ รปภ.อย่างสม่ำเสมอหรือไม่ **๒.การควบคุมการเข้า-ออก(Physical entry control)**	๖.ภาพถ่ายสัญญาณเตือนภัยต่างๆและเครื่องแม่ข่าย รวมทั้งมาตรการข้อห้ามมิให้ปฏิบัติต่างๆ ๗.ภาพถ่ายสัญญาณและสายไฟฟ้าที่เดินในห้องแม่ข่าย รวมทั้งแผนผังสายสัญญาณ ๘.ภาพถ่ายการจัดวางอุปกรณ์เครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องเช่นUPS ๙.ภาพถ่ายตู้ Rack และระบบปรับอากาศ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		๒.๑ มีมาตรการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้ลายนิ้วมือ เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญหรือไม่ ๒.๒ มีการลงและจัดเก็บบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญ **๓.ภายในห้องแม่ข่ายที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)** ๓.๑ ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น ๓.๒ ห้ามสูญบุหรี่ และนำอาหารเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง ๓.๓ ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องให้ปิดล็อคอยู่เสมอ ๓.๔ ความสะอาดและความเป็นระเบียบเรียบร้อยของห้องแม่ข่าย ๓.๕ มีการดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องแม่ข่าย	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		อย่างสม่ำเสมอหรือไม่ ให้ตรวจสอบแผนการทำความสะอาดของห้องแม่ข่ายว่ามีการจดบันทึกและทำแผนไว้หรือไม่ และมีการทำความสะอาดเพื่อให้อุปกรณ์ปลอดจากฝุ่นอย่างสม่ำเสมอหรือไม่ ๓.๖ ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย ๓.๗ ไม่มีการจัดวางอุปกรณ์คอมพิวเตอร์ไว้ใต้ตู้เครื่องปรับอากาศ (ซึ่งอาจมีน้ำรั่วไหลลงมายังอุปกรณ์คอมพิวเตอร์ได้) ๓.๘ มีการตรวจสอบระดับอุณหภูมิในห้องแม่ข่ายหรือไม่ ๓.๙ มีการตรวจสอบความชื้นในห้องแม่ข่ายหรือไม่ ๓.๑๐ มีการติดตามระบบปรับอากาศอย่างน้อยมีแอร์ ๒ ตัว ตั้งเวลาเปิดปิดสลับทำงาน	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		๓.๑๑ มีการป้องกันไฟไหม้หรือไม่ เช่น การติดตั้งอุปกรณ์ดับเพลิงและเครื่องดักจับควันไฟ ๓.๑๒ ตู้ Rack ทุกตู้ต้องล็อคอยู่เสมอ ห้ามเปิดค้างไว้ ๓.๑๓ ตู้ Rack มีพัดลมดูดอากาศติดตั้งไว้ด้านบน ๓.๑๔ ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย ๓.๑๕ มีการจัดทำป้ายชื่อสำหรับสายสัญญาณสื่อสารเพื่อป้องกันการตัดต่อสัญญาณผิดเส้น ๓.๑๖ มีการจัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง ๓.๑๗ มีการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน (แรงดันไฟฟ้าไม่คงที่ มีการผันแปรอย่างต่อเนื่อง) หรือไฟฟ้ากระชากหรือไม่ เช่น การใช้ยูพีเอส	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๒.๕การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่ามีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑.หน่วยงานต้องมีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑.ตรวจสอบว่าหน่วยงานมีการจัดทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศหรือไม่ และการประเมินความเสี่ยงได้ดำเนินการอย่างถูกต้องเหมาะสมหรือไม่	**<u>หลักฐาน</u>** -เอกสารประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเด็นการตรวจสอบที่ ๓ หน่วยงานมีการดำเนินงานควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐

วัตถุประสงค์

๑..เพื่อให้มั่นใจหน่วยงานมีการดำเนินงานควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานที่ไม่เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๓.มีการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ตามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐กำหนด **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่าได้ดำเนินการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ตามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐กำหนด	มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์	๑.ตรวจสอบไฟร์วอลล์(Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ โดย ๑.๑ ตรวจสอบว่าเวลาของไฟร์วอลล์(Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ถูกต้องเป็นปัจจุบัน -เมนู Dachbord→Main→ Time -เมนู Log&Report→ Forward Traffic→ดู log เวลาตรงกับปัจจุบันหรือไม่ ๑.๒ ตรวจสอบการตั้งเวลาในการจัดเก็บการจารจรคอมพิวเตอร์ไว้ ๙๐ วันตามที่กำหนด	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.ภาพถ่ายไฟร์วอลล์(Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์เพื่อดูสถานะการทำงาน ๒.เอกสารพิมพ์จากไฟร์วอลล์(Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์

ประเด็นการตรวจสอบที่ ๔ มีการประเมินขีดสมรรถนะของระบบสารสนเทศให้มีความพร้อมใช้งาน

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าระบบสารสนเทศของหน่วยงานมีความพร้อมใช้ตลอดเวลา

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๔.ระบบสารสนเทศมีความพร้อมใช้งานตลอดเวลา **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่าระบบสารสนเทศของหน่วยงานมีความพร้อมใช้งานตลอดเวลา	๑.ต้องมีการจัดทำแผนการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ๒.มีการประเมินขีดสมรรถนะของระบบดังกล่าวตามแผนที่กำหนด ๓.ต้องวิเคราะห์ผลการประเมินขีดสมรรถนะของระบบดังกล่าวอย่างสม่ำเสมอ ๔.ต้องรายงานผลการวิเคราะห์ขีดสมรรถนะของระบบดังกล่าวให้ผู้บังคับบัญชาทราบอย่างน้อยปีละครั้ง ยกเว้นในกรณีที่ค่าขีดสมรรถนะเกินค่า Threshold หน่วยงานต้องมีการประเมินค่าขีดสมรรถนะของระบบถี่มากขึ้นตามความเหมาะสมและรายงานผู้บังคับบัญชาทราบพร้อมทั้งหาสาเหตุและแนวทางการแก้ไขปัญหา	๑.มีแผนการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิชหรือไม่ ๒.ตรวจสอบว่ามีการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ตามแผนที่กำหนดหรือไม่ ๓.ตรวจสอบว่ามีการวิเคราะห์ขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิชหรือไม่ ๔.ตรวจสอบว่า เครื่องแม่ข่ายและสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิชเกินค่า Thresholdหรือไม่หากเกินว่าค่า Threshold ที่กำหนดไว้ต้องหาสาเหตุและแนวทางการแก้ไข รวมถึงรายงาน	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.แผนการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ๒.การบันทึกกิจกรรมการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ตามแผนที่กำหนด ๓.รายงานผลการวิเคราะห์ขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิช ๔.การบันทึกเหตุการณ์ที่เป็นปัญหา ๕.รายงานผลการบันทึกเหตุการณ์ที่เป็นปัญหา เช่น กรณีที่ค่าขีดสมรรถนะเกินค่า Thresholdที่กำหนดหรือการDownของระบบ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๕.หากมีการDownของระบบดังกล่าวต้องมีการจดบันทึกปัญหาและรายงานผู้บังคับบัญชาทราบพร้อมทั้งหาสาเหตุและแนวทางการแก้ไขปัญหา	ผู้บังคับบัญชาทราบ ๕.ตรวจสอบว่า มีการจดบันทึกเหตุการณ์ปัญหาที่เกิดขึ้นหรือไม่ ๖.ตรวจสอบว่า มีการ Downของเครื่องแม่ข่ายและไฟร์วอลล์(Firewall)รวมถึงแบนด์วิชหรือไม่ กี่ครั้งและสาเหตุใด ได้แก้ไขอย่างไร มีการรายงานผู้บังคับบัญชาหรือไม่	

ประเด็นการตรวจสอบที่ ๕ การดำเนินงานควบคุมและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

วัตถุประสงค์

๑.เพื่อมั่นใจว่ามีการดำเนินการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศมิให้สูญหาย

๒.เพื่อมั่นใจว่ามีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีอย่างเหมาะสม

๓.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๖.การดำเนินงานควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างรัดกุม **<u>วัตถุประสงค์ย่อย</u>** ๑.เพื่อมั่นใจว่ามีการดำเนินการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศมิให้สูญหาย ๒.เพื่อมั่นใจว่ามีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีอย่างเหมาะสม	๑.ต้องมีการจัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยมีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อย CPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินโดยครอบคลุมด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ ๒.ระบบการยืม-คืนครุภัณฑ์ตามระเบียบ ๓.มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย(ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิงป้องกันและเชิงแก้ไข)	๑.ตรวจสอบทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อยCPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินโดยครอบคลุมด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ ๒.ตรวจสอบว่า มีระบบการยืม-คืนครุภัณฑ์ถูกต้องตามระเบียบหรือไม่ ๓.ตรวจสอบว่า มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย(ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิงป้องกันและเชิงแก้ไข)	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.ทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ ๒.เอกสารเกี่ยวกับระบบการยืม-คืนครุภัณฑ์ด้านเทคโนโลยีสารสนเทศ ๓.แผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ ๔.เอกสารในการดำเนินกิจกรรมบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์

ประเด็นการตรวจสอบที่ ๖ การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่า การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

หมายเหตุ:

คุณภาพ หมายถึง ๑.ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้อง

เหมาะสมต่อการใช้งาน หมายถึง สอดคล้องกับความต้องการของผู้ใช้งานระบบสารสนเทศ

พัฒนาต่อยอดได้ในอนาคต หมายถึง ระบบสารสนเทศต้องมีเอกสารการวิเคราะห์ออกแบบระบบที่สามารถพัฒนาต่อยอดได้ในอนาคต ได้แก่ แผนผังกระแสการไหลของข้อมูล(DFD/Use case) และแผนผังโครงสร้างฐานข้อมูล(ER Diagram) รวมทั้งพจนานุกรมฐานข้อมูล และความสัมพันธ์ของฐานข้อมูล

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่า การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต	๑.ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว ๑.๑ ระบบสารสนเทศต้องมีระบบการนำเข้าข้อมูลที่ถูกต้องและมีการประมวลผลรวมถึงออกรายงานแสดงได้อย่างถูกต้อง ๑.๒ ระบบสารสนเทศต้องมีการทำงานที่สอดคล้องกับความต้องการของผู้ใช้งาน ๑.๓ ระบบต้องมีเอกสารที่สามารถพัฒนาต่อยอดในอนาคตได้ คือเอกสารการวิเคราะห์ออกแบบระบบ	๑.ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว ๑.๑ ตรวจสอบว่า ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้องหรือไม่ ๑.๒ ตรวจสอบว่า มีเอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งานหรือไม่ ๑.๓ ตรวจสอบว่า ระบบที่พัฒนาสอดคล้องกับความต้องการของ	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.เอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งาน ๒.เอกสารการวิเคราะห์ออกแบบระบบ ๓.เอกสารการศึกษาความเป็นไปได้ ๔.รายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา ๕.รายงานผลการทดสอบระบบ ๖.รายงานผลการฝึกอบรมการใช้งาน ๗.คู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๒.ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้นตาม SDLC ๒.๑ต้องมีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งาน ๒.๒ต้องมีการศึกษาความเป็นไปได้ (ถ้ามี) ๒.๓ต้องมีเอกสารการวิเคราะห์ออกแบบระบบ ๒.๔ต้องมีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา ๒.๕ต้องมีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน ๒.๖ต้องมีรายงานผลการฝึกอบรมการใช้งานและคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ ๒.๗รายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๒.๘ประเมินความพึงพอใจของผู้ใช้งานระบบ	ผู้ใช้งานหรือไม่ โดยการเปรียบเทียบกับเอกสารการวิเคราะห์การใช้งาน ๑.๔ตรวจสอบว่ามีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล (DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล ๒.ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้น ๒.๑มีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งาน ๒.๒มีการศึกษาความเป็นไปได้ (ถ้ามี) ๒.๓มีเอกสารการวิเคราะห์ออกแบบระบบ ๒.๔มีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา	๘.รายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๙.สรุปผลการประเมินความพึงพอใจของผู้ใช้งานระบบ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
		๒.๕มีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน ๒.๖มีรายงานผลการฝึกอบรมการใช้งานและคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ ๒.๗มีรายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง ๒.๘มีประเมินความพึงพอใจของผู้ใช้งานระบบ	

ประเด็นการตรวจสอบที่ ๗ ระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงานรวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
ระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย **<u>วัตถุประสงค์ย่อย</u>** เพื่อให้มั่นใจว่าระบบข้อมูลและสารสนเทศรวมถึงฐานข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย	๑.มีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบ ได้แก่ (๑)มีเกณฑ์การตรวจสอบคุณภาพข้อมูล (๒)มีการตรวจสอบคุณภาพข้อมูลตามเกณฑ์ที่กำหนด (๓)มีรายงานผลคุณภาพข้อมูลให้ผู้บังคับบัญชาทราบ (๔)มีแนวทางแก้ไขพัฒนาระบบข้อมูลสารสนเทศหรือฐานข้อมูลของหน่วยงาน ๒.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้อง ๓.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความครบถ้วน ๔.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัยเป็นปัจจุบัน	๑.ตรวจสอบว่า หน่วยงานมีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบหรือไม่ ๒.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้องหรือไม่ ๓.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความครบถ้วนหรือไม่ ๔.ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัยเป็นปัจจุบันหรือไม่ ๕.มีการนำข้อมูลจากฐานข้อมูลมาตรวจสอบด้านคุณภาพข้อมูล	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.ระบบการตรวจสอบคุณภาพข้อมูล ๒.รายงานผลคุณภาพข้อมูล ๓.หน้าwebpageที่มีการแสดงข้อมูลที่ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่ทันสมัย

ประเด็นการตรวจสอบที่ ๘ เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่ามีการเผยแพร่ตามพรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด วัตถุประสงค์ย่อย เพื่อให้มั่นใจว่ามีการเผยแพร่ตามพรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด	๑.ตามมติคณะรัฐมนตรี ที่ นร ๐๔๐๕/ว ๕๗ ลงวันที่ ๒๙ เมษายน ๒๕๕๔ ให้นำข้อมูลข่าวสารตามมาตรา ๗ เผยแพร่ในเว็บไซต์ของหน่วยงาน -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ ๒.ตามมติคณะรัฐมนตรี ที่ นร ๐๔๐๕/ว ๕๗ ลงวันที่ ๒๙ เมษายน ๒๕๕๔ ให้นำข้อมูลข่าวสารตามมาตรา ๙ เผยแพร่ในเว็บไซต์ของหน่วยงาน -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน)	๑.ตรวจสอบว่ามีการเผยแพร่ตามมาตรา ๗ เผยแพร่ในเว็บไซต์ของหน่วยงาน -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ ๒.ตรวจสอบว่ามีการเผยแพร่ตามมาตรา ๙ เผยแพร่ในเว็บไซต์ของหน่วยงาน -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน) -แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.บันทึกภาพถ่ายการเผยแพร่ตามมาตรา๗และ๙ ผ่านเว็บไซต์หน่วยงาน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	-แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน ๓.ตามมติคณะรัฐมนตรีที่ ๒๘ ธันวาคม ๒๕๔๗ ให้นำ -ประกาศประกวดราคา ประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน	๓.ตรวจสอบว่ามีการเผยแพร่ -ประกาศประกวดราคา ประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน	

ประเด็นการตรวจสอบที่ ๙ หน่วยงานต้องมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

วัตถุประสงค์

๑.เพื่อให้มั่นใจว่าหน่วยงานมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๒.เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินงาน รวมทั้งให้ข้อเสนอแนะ ข้อคิดเห็น และ/หรือการแก้ไขปรับปรุงเพื่อให้การปฏิบัติงานมีประสิทธิภาพ

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๔.มีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด วัตถุประสงค์ย่อย เพื่อให้มั่นใจว่าหน่วยงานมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด	๑.ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม ๒.มีแผนในการสำรองข้อมูลเป็นลายลักษณ์อักษรและปฏิบัติตรงตามแผนที่กำหนด ๓.กำหนดผู้รับผิดชอบในการสำรองข้อมูล ๔.กำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง ๕.ต้องติดฉลากที่มีรายละเอียดชัดเจนเพื่อให้สามารถค้นหาได้โดยเร็วและป้องกันการใช้งานสื่อบันทึกผิดพลาด ๖.กำหนดขั้นตอนการทดสอบข้อมูลที่สำรอง ๗.มีรายงานผลการทดสอบข้อมูลที่สำรอง ๘.กำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว	๑.สัมภาษณ์มีกระบวนการในการสำรองข้อมูลอย่างเป็นระบบได้แก่ (๑)คัดเลือกข้อมูลที่สำคัญต่อองค์กรนำมาจัดเรียงลำดับความสำคัญ (๒)กำหนดความถี่ในการสำรองข้อมูลตามระดับความสำคัญที่กำหนดไว้ (๓)จัดทำแผนในการสำรองข้อมูลอย่างเป็นระบบ (๔)ดำเนินการสำรองข้อมูลและสุ่มตรวจข้อมูลที่สำรองว่ามีความสมบูรณ์หรือไม่และมีหลักฐานบันทึกกิจกรรมการสำรองข้อมูล ๒.ขอดูแผนการสำรองข้อมูลและผลการปฏิบัติในการสำรองข้อมูลว่าตรงตามแผนหรือไม่และมีการสุ่มตรวจการสำรองข้อมูล ๓.สัมภาษณ์และขอดูเอกสารหลักฐานการแต่งตั้ง/มอบหมายผู้รับผิดชอบในการสำรองข้อมูล	ตสน.กระดาษทำการ WA_IT๐๒ **<u>หลักฐาน</u>** ๑.รายงานการประชุมคัดเลือกข้อมูลและจัดลำดับความสำคัญของข้อมูลองค์กรรวมทั้งการกำหนดความถี่ในการสำรองข้อมูล ๒.แผนในการสำรองข้อมูล ๓.ผลการสำรองข้อมูลและการสุ่มตรวจการสำรองข้อมูล ๔.แผนเตรียมความพร้อมกรณีฉุกเฉิน ๕.รายงานผลการซักซ้อมแผนเตรียมความพร้อมกรณีฉุกเฉิน

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๙.มีการดำเนินการการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้วตามขั้นตอนที่กำหนดไว้ ๑๐.ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องโดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ๑๑.มีการรายงานผลการซักซ้อมแผนฉุกเฉินอย่างเป็นลายลักษณ์อักษร	๔.สัมภาษณ์และขอดูพื้นที่เก็บรักษาข้อมูลที่สำรอง ๕.ขอดูสื่อในการบันทึกการสำรองข้อมูลว่ามีการติดฉลากที่มีรายละเอียดชัดเจนหรือไม่ ๖.ขอดูเอกสารการกำหนดขั้นตอนการทดสอบข้อมูลที่สำรอง ๗.ขอดูรายงานผลการทดสอบข้อมูลที่สำรอง ๘.ขอดูเอกสารการกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ๙.สัมภาษณ์การดำเนินการการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้วตามขั้นตอนที่กำหนดไว้ ๑๐.ตรวจสอบว่า หน่วยงานมีแผนเตรียมความพร้อมกรณีฉุกเฉินหรือไม่และมีการซักซ้อมแผนหรือไม่ ๑๑.ขอดูการรายงานผลการซักซ้อมแผนฉุกเฉิน	

ประเด็นการตรวจสอบที่ ๑๐ การตรวจสอบการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกระบวนการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ ประสิทธิผล

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
๑.การกำหนดขั้นตอนการปฏิบัติในการแก้ไขปัญหาหรือการแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ วัตถุประสงค์ เพื่อให้ทราบแนวทาง/ขั้นตอนการปฏิบัติในการแก้ไขปัญหาหรือการแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพ	๑.มีการกำหนดขั้นตอนการปฏิบัติในการแก้ไขปัญหาหรือการแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Flowchart) และกำหนดผู้รับผิดชอบในแต่ละขั้นตอน ๒.มีการกำหนดเกณฑ์ในการประเมินการตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยหรือไม่ เช่น ระดับความเสี่ยงสูงต้องรายงานด้วยวาจาทันทีแล้วจึงแก้ไขทันที ระดับความเสี่ยงปานกลางแก้ไขก่อนแล้วจึงรายงานเป็นลายลักษณ์อักษร ระดับความเสี่ยงต่ำรายงานเป็นลายลักษณ์อักษรแล้วจึงแก้ไข ๓.มีการจดบันทึกเหตุการณ์ความไม่มั่นคงปลอดภัยเป็นลายลักษณ์อักษร ๔.มีการรายงานต่อผู้บังคับบัญชาเป็นระดับชั้นที่เหมาะสมและรวดเร็วทันต่อการแก้ไขปัญหา	๑.ขอดูขั้นตอนการปฏิบัติในการแก้ไขปัญหาหรือการแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Flowchart) ๒.ขอดูการกำหนดเกณฑ์ที่เป็นลายลักษณ์อักษรหรือรายงานการประชุมหรือระเบียบปฏิบัติ และประเมินดูการปฏิบัติงานได้ดำเนินการตามที่กำหนดหรือไม่ ๓.ขอดูหลักฐานการจดบันทึกเหตุการณ์ความไม่มั่นคงปลอดภัยเป็นลายลักษณ์อักษร ๔.ขอดูบันทึกการรายงานต่อผู้บังคับบัญชาเป็นระดับชั้นว่าช่องทางเหมาะสมหรือไม่และรวดเร็วทันต่อการแก้ไขปัญหาหรือไม่ ๕.ขอดูสรุปวิเคราะห์ปัญหาและค้นหาสาเหตุของปัญหารายงานต่อผู้บังคับบัญชา ปีละ๑ครั้ง	

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
	๕.มีการสรุปวิเคราะห์ปัญหาและค้นหาสาเหตุของปัญหา เพื่อมิให้เกิดปัญหาซ้ำและรายงานต่อผู้บังคับบัญชา ปีละ๑ครั้ง		

ประเด็นการตรวจสอบที่ ๑๑ การตรวจสอบการเข้ารหัสตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ
วัตถุประสงค์ เพื่อสอบทานระบบแอปพลิเคชั่น (Application) มีการรับส่งข้อมูลอย่างปลอดภัย

ประเด็นย่อย วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล
เพื่อสอบทานระบบแอปพลิเคชั่น (Application) มีการรับส่งข้อมูลอย่างปลอดภัย	๑.ระบบแอปพลิเคชั่น (Application)ของหน่วยงานมีการเข้ารหัสในการรับส่งข้อมูลอย่างปลอดภัย	๑.ดำเนินการดักจับข้อมูลด้วยโปรแกรมดักจับข้อมูลระหว่างการรับ-ส่งข้อมูลผ่านระบบเครือข่าย(โปรแกรม wire shark) ๒.เปิดแอปพลิเคชั่น (Application)ที่จะตรวจสอบ URL ต้องนำหน้าด้วย Https://	แหล่งข้อมูล ๑.รายงานในการดักจับข้อมูลจากโปรแกรม wire shark ๒. การคัดลอกหน้าต่างในการเปิดแอปพลิเคชั่น (Application)ที่จะตรวจสอบ URL ต้องนำหน้าด้วย Https://

กระดาษทำการระบบการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ

สำหรับกลุ่มเทคโนโลยีสารสนเทศและหน่วยงานที่ไม่มี server

กระดาษทำการที่ WA_IT๐๑

หน่วยที่ตรวจ.....

งวดที่ตรวจ.....

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
ประเด็นที่ ๑ การจัดทำนโยบายความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์							
๑	*มีข้อปฏิบัติ/แนวทางปฏิบัติรองรับนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร						
๒	หน่วยงานมีการประกาศ/สื่อสารนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบหรือไม่						
๓	*หน่วยงานกำหนดผู้รับผิดชอบหรือคำสั่งแต่งตั้งคณะกรรมการCSO ชัดเจนหรือไม่						
๔	*หน่วยงานมีการทบทวนข้อปฏิบัติ/แนวทางปฏิบัติให้เป็นปัจจุบัน(กรณีที่มีข้อปฏิบัติ/แนวทางปฏิบัติอยู่แล้ว ถ้าไม่มีให้ข้ามทำข้ออื่น)						
๖	*ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน						
ประเด็นที่ ๒ การควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศและเครือข่าย รวมทั้งระบบปฏิบัติการ เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์							

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๗	มีการจัดอบรม/ชี้แจงในการประชุม/แจ้งเวียน/เผยแพร่ในเว็บไซด์ เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์						
๙	มีระบบการลงทะเบียนผู้ใช้งาน เช่นระบบการ authentication หรือการลงทะเบียนสมัครเข้าใช้ระบบงานเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงาน โดยต้องมีการกำหนดขั้นตอนการปฏิบัติสำหรับการลงทะเบียน						
๑๐	การตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาต						
๑๑	ระบบการauthentication หรือเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงานมีเมนูระบบบริหารจัดการและกำหนดสิทธิของผู้ใช้งานที่เหมาะสมหรือไม่						
๑๒	มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน เช่น มีระบบการเปลี่ยนรหัสผ่าน/ระบบมีการล็อก						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	รหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น						
๑๓	ระบบการ authentication หรือระบบเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงาน มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละครั้งหรือไม่						
๑๔	มีมาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่ เช่นการกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น						
๑๕	มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กรก่อนที่จะเข้ามาใช้งานระบบเครือข่ายภายในองค์กร						
๑๖	มีการควบคุมการใช้โปรแกรมอรรถประโยชน์หรือไม่						
๑๗	มีการติดตั้งโปรแกรมป้องกันไวรัสครบถ้วนหรือไม่						
๑๘	มีการ update โปรแกรมป้องกันไวรัสครบถ้วนหรือไม่						
ประเด็นที่ **๓** การควบคุมการเข้าถึงทางกายภาพ **ตรวจในห้องแม่ข่าย**							

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๑๙	มีการจัดแสงสว่างในบริเวณต่างๆอย่างเพียงพอ						
๒๐	มีการจัดระเบียบสายไฟฟ้าและสายสัญญาณรับ-ส่งข้อมูลที่เป็นระเบียบเรียบร้อย						
๒๑	มีการกำกับป้ายสายสัญญาณรับ-ส่งข้อมูลอย่างคราบถ้วน						
๒๒	มีการจัดทำแผนผังคอมพิวเตอร์และเครือข่าย						
ประเด็นการตรวจสอบที่ ๔ การดำเนินงานควบคุมและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม							
๒๓	มีทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อย CPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ						
๒๔	มีระบบการยืม-คืนครุภัณฑ์ถูกต้องตามระเบียบ						
๒๕	มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย (ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิง						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ป้องกันและเชิงแก้ไข)						
ประเด็นการตรวจสอบที่ ๕ การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต							
๗.๑ ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว							
๒๖	ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้องหรือไม่						
๒๗	มีเอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งานหรือไม่						
๒๘	ระบบที่พัฒนาสอดคล้องกับความต้องการของผู้ใช้งานหรือไม่						
๒๙	มีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล						
๗.๒ ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้น							
๓๐	มีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งานหรือไม่						
๓๑	มีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	(๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล						
๓๒	มีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา						
๓๓	มีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน						
๓๔	มีรายงานผลการฝึกอบรมการใช้งาน						
๓๕	มีคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ						
๓๖	มีรายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง						
๓๗	มีรายงานผลการประเมินความพึงพอใจของผู้ใช้งานระบบ						
๓๘	หน่วยงานมีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบหรือไม่โดยต้องมีสิ่งเหล่านี้ครบถ้วน (๑)มีเกณฑ์การตรวจสอบคุณภาพข้อมูล (๒)มีการตรวจสอบคุณภาพ						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ข้อมูลตามเกณฑ์ที่กำหนด (๓)มีรายงานผลคุณภาพข้อมูลให้ผู้บังคับบัญชาทราบ (๔)มีแนวทางแก้ไขพัฒนาระบบข้อมูล						
๓๙	ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้อง						
๔๐	ข้อมูลของระบบสารสนเทศของหน่วยงานมีครบถ้วน						
๔๑	ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัย						
๔๒	เผยแพร่บนเว็บไซต์หน่วยงานตามพรบ.ข้อมูลข่าวสารปี ๒๕๔๐ ครบถ้วน **<u>มาตรา ๗</u>** -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ **<u>มาตรา๙</u>** -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่าย						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ประจำปี(ปีปัจจุบัน) -แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน -ประกาศประกวดราคาประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซต์หน่วยงาน						
ประเด็นการตรวจสอบที่ ๕ หน่วยงานต้องมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด							
๔๓	มีกระบวนการในการสำรองข้อมูลอย่างเป็นระบบได้แก่ (๑)คัดเลือกข้อมูลที่สำคัญต่อองค์กรนำมาจัดเรียงลำดับความสำคัญ (๒)กำหนดความถี่ในการสำรองข้อมูลตามระดับความสำคัญที่กำหนดไว้ (๓)จัดทำแผนในการสำรองข้อมูลอย่างเป็นระบบ (๔)ดำเนินการสำรองข้อมูลและสุ่มตรวจข้อมูลที่สำรองว่ามีความสมบูรณ์หรือไม่และมีหลักฐานบันทึกกิจกรรมการสำรองข้อมูล						
๕๔	แผนในการสำรองข้อมูลมีหรือไม่						
๕๕	ผลกิจกรรมการสำรองข้อมูลตามแผนที่กำหนด						
๕๖	กำหนดผู้รับผิดชอบในการ						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	สำรองข้อมูล						
๕๗	กำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง						
๕๘	ต้องติดฉลากที่มีรายละเอียดชัดเจนเพื่อให้สามารถค้นหาได้โดยเร็วและป้องกันการใช้งานสื่อบันทึกผิดพลาด						
๕๙	กำหนดขั้นตอนการทดสอบข้อมูลที่สำรอง						
๖๐	มีรายงานผลการทดสอบข้อมูลที่สำรอง						
๖๑	กำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว						
๖๒	มีการดำเนินการการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้วตามขั้นตอนที่กำหนดไว้						
๖๓	แผนเตรียมความพร้อมกรณีฉุกเฉินมีหรือไม่						
๖๔	มีการซักซ้อมแผนฯและรายงานผลการซักซ้อมแผนเตรียมความพร้อมกรณีฉุกเฉิน						
๖๕	มีการรายงานผลการซักซ้อมแผนฉุกเฉินอย่างเป็นลายลักษณ์อักษร						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
ผลรวม n๑, n๒ , n๓						N/A	

รวมคะแนนทั้งหมด (N = n๑ + n๒ + n๓)	
ผลรวมจำนวนข้อ (โดยไม่นับรวมข้อที่เป็น N/A) = (๑๐๐%)	
คิดเป็นร้อยละ (N / ผลรวมจำนวนข้อ x ๑๐๐)	

สรุปผลการตรวจสอบและประเมินผล

.....

.....

.....

.....

ข้อเสนอแนะ

.....

.....

.....

.....

เกณฑ์การประเมินผลระบบการควบคุมภายใน

คะแนน	ระดับ
๙๐ – ๑๐๐	ดีมาก
๘๐ – ๘๙.๙๙	ดี
๗๐ – ๗๙.๙๙	พอใช้
ต่ำกว่า ๗๐	ต้องปรับปรุง

ผู้รับตรวจ .....

(.....)

.....

ผู้ตรวจ/สอบทาน.....

(.....)

.....

วันที่.....เดือน.....พ.ศ.....

กระดาษทำการระบบการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ

สำหรับกลุ่มเทคโนโลยีสารสนเทศและหน่วยงานที่มี server

กระดาษทำการที่ WA_IT๐๑

หน่วยที่ตรวจ .....

งวดที่ตรวจ .....

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
ประเด็นที่ ๑ การจัดทำนโยบายความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์							
๑	*มีข้อปฏิบัติ/แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร						
๒	หน่วยงานมีการประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบหรือไม่						
๓	*หน่วยงานกำหนดผู้รับผิดชอบตามนโยบายชัดเจนหรือมีการแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ(CSO)อย่างชัดเจนเป็นลายลักษณ์อักษร						
๔	*หน่วยงานมีการทบทวนนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน						
๕	*ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน						
๖	มีการประชุมคณะทำงาน(CSO)ของหน่วยงานอย่าง						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	น้อยปีละ ๒ ครั้ง ครั้งแรกจัดประชุมเพื่อสื่อสารและกำหนดข้อปฏิบัติ ครั้งที่๒ เป็นการติดตามประเมินผลการปฏิบัติตามข้อปฏิบัติที่ประกาศใช้						
ประเด็นที่ **๒** การควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศและเครือข่าย รวมทั้งระบบปฏิบัติการ เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์							
๗	มีการจัดอบรม/ชี้แจงในการประชุม/แจ้งเวียน/เผยแพร่ในเว็บไซด์ เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์						
๘	มีระบบการลงทะเบียนผู้ใช้งาน เช่นระบบการ authentication หรือการลงทะเบียนสมัครเข้าใช้ระบบงานเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงาน โดยต้องมีการกำหนดขั้นตอนการปฏิบัติสำหรับการลงทะเบียน						
๙	การตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาต						
๑๐	ระบบการauthentication หรือเว็บไซด์/ระบบ						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	สารสนเทศอื่นใดของหน่วยงานมีเมนูระบบบริหารจัดการและกำหนดสิทธิของผู้ใช้งานที่เหมาะสมหรือไม่						
๑๑	มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน เช่น มีระบบการเปลี่ยนรหัสผ่าน/ระบบมีการล็อกรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น						
๑๒	ระบบการ authentication หรือระบบเว็บไซต์/ระบบสารสนเทศอื่นใดของหน่วยงาน มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละครั้งหรือไม่						
๑๓	มีมาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่ เช่นการกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น						
๑๔	ไม่มีการรีโมลเข้ามาในระบบภายในเครือข่ายโดยไม่รับอนุญาตหรือออกเครือข่ายโดยไม่ผ่านการ authentication เป็นต้น						
๑๕	มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ภายนอกองค์กรก่อนที่จะเข้ามาใช้งานระบบเครือข่ายภายในองค์กร						
๑๖	แผนผังเครือข่ายว่ามีการแบ่งแยกเครือข่าย ตามกลุ่มที่เหมาะสมหรือไม่						
๑๗	มีการควบคุมการใช้โปรแกรมอรรถประโยชน์หรือไม่						
๑๘	มีการตัดสัญญาณอินเทอร์เน็ต (session time-out) ในระยะเวลา ๕-๑๕ นาทีหรือไม่						
๑๙	มีการติดตั้งโปรแกรมป้องกันไวรัสครบถ้วนหรือไม่						
๒๐	มีการ update โปรแกรมป้องกันไวรัสครบถ้วนหรือไม่						
ประเด็นที่ ๓ การควบคุมการเข้าถึงทางกายภาพ **ตรวจในห้องแม่ข่าย**							
๒๑	มีการแยกพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศขององค์กร (เช่น ห้องเครื่อง/ห้องแม่ข่าย) ออกจากพื้นที่ส่วนที่เป็นสำนักงานของผู้ให้บริการภายนอกหรือไม่						
๒๒	มีการจัดแสงสว่างในบริเวณต่างๆอย่างเพียงพอ						
๒๓	มีการใช้ผนังล้อมรอบเป็นผนังทึบและควรมิดชิด เมื่อมองจากด้านนอกเข้าไปข้าง						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ในจะต้องไม่รู้ว่าเป็นห้องแม่ข่ายหรือหากผนังเป็นกระจกใส ต้องทำการติดฟิล์มทึบทับไว้						
๒๔	มีการใช้ประตูและหน้าต่างของสำนักงานให้ล็อคอยู่เสมอ						
๒๕	ประตูทางเข้า จะต้องมีกล้องวงจรปิดบันทึกภาพบริเวณประตูเข้าออกห้อง						
๒๖	มีการจัดระบบการรักษาความปลอดภัยอย่างเพียงพอหรือไม่ มีการตรวจตาพื้นที่ภายในองค์กรอย่างไร ตรวจตราบ่อยเพียงไร มีผู้ตรวจตราหรือกวดขันงานของ รปภ.อย่างสม่ำเสมอหรือไม่						
๒๗	มีมาตรการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้ลายนิ้วมือ เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญหรือไม่						
๒๘	มีการลงและจัดเก็บบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญ ในกรณีเป็นบุคคลอื่นที่ไม่ใช้เจ้าหน้าที่ เช่น ผู้ตรวจสอบ บริษัทล้างแอร์ เป็นต้น						
๒๙	ห้ามนำบุคคลภายนอกเข้า						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น						
๓๐	ห้ามสูญบุหรี่ และนำอาหาร เครื่องดื่มเข้าไปในบริเวณห้องเครื่อง						
๓๑	ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องให้ปิดล็อคอยู่เสมอ						
๓๒	ความสะอาดและความเป็นระเบียบเรียบร้อยของห้องแม่ข่าย						
๓๓	ตรวจสอบแผนการทำความสะอาดของห้องแม่ข่ายว่ามีการจดบันทึกและทำแผนไว้หรือไม่ และมีการทำความสะอาดเพื่อให้อุปกรณ์ปลอดจากฝุ่นอย่างสม่ำเสมอหรือไม่						
๓๔	ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย						
๓๕	ไม่มีการจัดวางอุปกรณ์คอมพิวเตอร์ไว้ใต้ตู้เครื่องปรับอากาศ (ซึ่งอาจมีน้ำรั่วไหลลงมายังอุปกรณ์คอมพิวเตอร์ได้)						
๓๖	มีการตรวจสอบระดับอุณหภูมิในห้องแม่ข่ายหรือไม่						
๓๗	มีการตรวจสอบความชื้นใน						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ห้องแม่ข่ายหรือไม่						
๓๘	มีการติดตามระบบปรับอากาศอย่างน้อยมีแอร์ ๒ ตัว ตั้งเวลาเปิดปิดสลับทำงาน						
๓๙	มีการป้องกันไฟไหม้หรือไม่ เช่น การติดตั้งอุปกรณ์ดับเพลิงและเครื่องดักจับควันไฟ						
๔๐	ห้องแม่ข่าย (Server) ห้ามมีป้ายบอกว่าเป็นห้อง Server Room เพื่อป้องกันการแอบเข้ามาขโมยทรัพย์สิน หรือเข้ามาทำลายในกรณีเกิดเหตุการณ์ประท้วงของพนักงาน						
๔๑	ตู้ Rack ทุกตู้ต้องล็อคอยู่เสมอห้ามเปิดค้างไว้						
๔๒	ตู้ Rack มีพัดลมดูดอากาศติดตั้งไว้ด้านบน						
๔๓	มีการจัดทำป้ายชื่อสำหรับสายสัญญาณสื่อสารเพื่อป้องกันการตัดต่อสัญญาณผิดเส้น						
๔๔	มีการจัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง						
๔๕	มีการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน (แรงดันไฟฟ้าไม่คงที่ มีการผันแปรอย่างต่อเนื่อง) หรือ						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ไฟฟ้ากระชากหรือไม่ เช่น การใช้ยูพีเอส						
ประเด็นการตรวจสอบที่ ๔ หน่วยงานมีการดำเนินงานควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐							
๔๖	เวลาของไฟร์วอลล์ (Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ถูกต้องเป็นปัจจุบัน						
๔๗	การตั้งเวลาในการจัดเก็บการจารจรคอมพิวเตอร์ไว้ ๙๐ วันตามที่กำหนด						
ประเด็นการตรวจสอบที่ ๕ หน่วยงานต้องมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด							
๔๘	มีกระบวนการในการสำรองข้อมูลอย่างเป็นระบบได้แก่ (๑)คัดเลือกข้อมูลที่สำคัญต่อองค์กรนำมาจัดเรียงลำดับความสำคัญ (๒)กำหนดความถี่ในการสำรองข้อมูลตามระดับความสำคัญที่กำหนดไว้ (๓)จัดทำแผนในการสำรองข้อมูลอย่างเป็นระบบ (๔)ดำเนินการสำรองข้อมูลและสุ่มตรวจข้อมูลที่สำรองว่ามีความสมบูรณ์หรือไม่และมีหลักฐานบันทึกกิจกรรมการสำรองข้อมูล						
๔๙	แผนในการสำรองข้อมูลมีหรือไม่						
๕๐	ผลกิจกรรมการสำรอง						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ข้อมูลตามแผนที่กำหนด						
๕๑	กำหนดผู้รับผิดชอบในการสำรองข้อมูล						
๕๒	กำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง						
๕๓	ต้องติดฉลากที่มีรายละเอียดชัดเจนเพื่อให้สามารถค้นหาได้โดยเร็ว และป้องกันการใช้งานสื่อบันทึกผิดพลาด						
๕๔	กำหนดขั้นตอนการทดสอบข้อมูลที่สำรอง						
๕๕	มีรายงานผลการทดสอบข้อมูลที่สำรอง						
๕๖	กำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว						
๕๗	มีการดำเนินการการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้วตามขั้นตอนที่กำหนดไว้						
๕๘	แผนเตรียมความพร้อมกรณีฉุกเฉินมีหรือไม่						
๕๙	มีการซักซ้อมแผนฯและรายงานผลการซักซ้อมแผนเตรียมความพร้อมกรณีฉุกเฉิน						
๖๐	มีการรายงานผลการซักซ้อมแผนฉุกเฉินอย่างเป็นลายลักษณ์อักษร						
ประเด็นการตรวจสอบที่ ๖ มีการประเมินขีดสมรรถนะของระบบสารสนเทศให้มีความพร้อมใช้งาน							
๖๑	มีแผนการประเมินขีด						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	สมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์ (Firewall)รวมถึงแบนด์วิชหรือไม่						
๖๒	มีการบันทึกกิจกรรมการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์ (Firewall)รวมถึงแบนด์วิชตามแผนที่กำหนด						
๖๓	มีรายงานผลการวิเคราะห์ขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์ (Firewall)รวมถึงแบนด์วิชอย่างน้อยปีละครั้ง						
๖๔	มีการจดบันทึกเหตุการณ์ที่เป็นปัญหา เช่น มีค่า Threshold เกินหรือมีการล่ม/downของระบบเครื่องแม่ข่ายและไฟร์วอลล์ (Firewall) รวมถึงแบนด์วิช เป็นต้น						
๖๕	มีการรายงานกรณีที่ มีค่า Threshold เกินหรือมีการล่ม/downของระบบเครื่องแม่ข่ายและไฟร์วอลล์(Firewall) รวมถึงแบนด์วิช						
ประเด็นการตรวจสอบที่ ๗ การดำเนินงานควบคุมและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม							
๖๖	มีทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะ						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	อย่างน้อย CPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ						
๖๗	มีระบบการยืม-คืนครุภัณฑ์ถูกต้องตามระเบียบ						
๖๘	มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย (ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิงป้องกันและเชิงแก้ไข)						
ประเด็นการตรวจสอบที่ ๘ การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต							
๗.๑ ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว							
๖๙	ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้องหรือไม่						
๗๐	มีเอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งานหรือไม่						
๗๑	ระบบที่พัฒนาสอดคล้องกับความต้องการของผู้ใช้งานหรือไม่						
๗๒	มีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วน						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล						
๗.๒ ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้น							
๗๓	มีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งานหรือไม่						
๗๔	มีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล						
๗๕	มีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา						
๗๖	มีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน						
๗๗	มีรายงานผลการฝึกอบรม						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	การใช้งาน						
๗๘	มีคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ						
๗๙	มีรายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง						
๘๐	มีรายงานผลการประเมินความพึงพอใจของผู้ใช้งานระบบ						
๘๑	หน่วยงานมีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบหรือไม่โดยต้องมีสิ่งเหล่านี้ครบถ้วน (๑)มีเกณฑ์การตรวจสอบคุณภาพข้อมูล (๒)มีการตรวจสอบคุณภาพข้อมูลตามเกณฑ์ที่กำหนด (๓)มีรายงานผลคุณภาพข้อมูลให้ผู้บังคับบัญชาทราบ (๔)มีแนวทางแก้ไขพัฒนาระบบข้อมูล						
๘๒	ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้อง						
๘๓	ข้อมูลของระบบสารสนเทศของหน่วยงานมีครบถ้วน						
๘๔	ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัย						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
ประเด็นการตรวจสอบที่ ๙ เผยแพร่ตาม พรบ.ข้อมูลข่าวสารพ.ศ.๒๕๔๐ กำหนด							
๘๕	เผยแพร่บนเว็บไซด์หน่วยงานตามพรบ.ข้อมูลข่าวสารปี ๒๕๔๐ ครบถ้วน **<u>มาตรา ๗</u>** -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับหน่วยงานรัฐ **<u>มาตรา๙</u>** -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน) -แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน -ประกาศประกวดราคาประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซด์หน่วยงาน						
ประเด็นการตรวจสอบที่ ๑๐ การตรวจสอบการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ							
๘๖	มีการกำหนดขั้นตอนการปฏิบัติในการแก้ไขปัญหา						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	หรือการแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Flowchart) และกำหนดผู้รับผิดชอบในแต่ละขั้นตอน						
๘๗	มีการจดบันทึกเหตุการณ์ความไม่มั่นคงปลอดภัยเป็นลายลักษณ์อักษร						
๘๘	มีการรายงานต่อผู้บังคับบัญชาเป็นระดับชั้นที่เหมาะสมและรวดเร็วทันต่อการแก้ไขปัญหา						
๘๙	มีการสรุปวิเคราะห์ปัญหาและค้นหาสาเหตุของปัญหาเพื่อมิให้เกิดปัญหาซ้ำและรายงานต่อผู้บังคับบัญชา ปีละ๑ครั้ง						
๙๐	มีการประเมินความเสี่ยงด้านสารสนเทศ ปีละ๑ ครั้ง						
		ผลรวม n๑, n๒ , n๓				N/A	

รวมคะแนนทั้งหมด (N = n๑ + n๒ + n๓)	
ผลรวมจำนวนข้อ (โดยไม่นับรวมข้อที่เป็น N/A) = (๑๐๐%)	
คิดเป็นร้อยละ (N / ผลรวมจำนวนข้อ x ๑๐๐)	

สรุปผลการตรวจสอบและประเมินผล

.....

.....

.....

ข้อเสนอแนะ

.....

.....

.....

.....

ผู้รับตรวจ .....

(.....)

.....

เกณฑ์การประเมินผลระบบการควบคุมภายใน

คะแนน	ระดับ
๙๐ – ๑๐๐	ดีมาก
๘๐ – ๘๙.๙๙	ดี
๗๐ – ๗๙.๙๙	พอใช้
ต่ำกว่า ๗๐	ต้องปรับปรุง

ผู้ตรวจ/สอบทาน

.....

(นางณัฐณิชา กลัมพสุต)

นักวิชาการตรวจสอบภายในชำนาญการพิเศษ

วันที่.....เดือน.....พ.ศ..๒๕๖๓..

กระดาษทำการระบบการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ

สำหรับกลุ่มเทคโนโลยีสารสนเทศและหน่วยงานที่มี server

กระดาษทำการที่ WA_IT๐๑

หน่วยที่ตรวจ.....

งวดที่ตรวจ.....

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
ประเด็นที่ ๑ การจัดทำนโยบายความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์							
๑	มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร						
๒	เนื้อหานโยบายมีความครอบคลุมเกี่ยวกับ (๑)การเข้าถึงหรือการควบคุมการใช้สารสนเทศ (๒)จัดระบบการสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน (๓)จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ						
๓	หน่วยงานมีการประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทราบหรือไม่						
๔	หน่วยงานกำหนดผู้รับผิดชอบตามนโยบายชัดเจนหรือไม่						
๕	หน่วยงานมีการทบทวนนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
ประเด็นที่ **๒** การควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศและเครือข่าย รวมทั้งระบบปฏิบัติการ เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์							
๖	มีการจัดอบรม/ชี้แจงในการประชุม/แจ้งเวียน/เผยแพร่ในเว็บไซด์ เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์						
๗	มีระบบการลงทะเบียนผู้ใช้งาน เช่นระบบการ authentication หรือการลงทะเบียนสมัครเข้าใช้ระบบงานเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงาน โดยต้องมีการกำหนดขั้นตอนการปฏิบัติสำหรับการลงทะเบียนและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาต						
๘	มีระบบการauthentication หรือเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงานมีเมนูระบบบริหารจัดการและกำหนดสิทธิของผู้ใช้งานที่เหมาะสมหรือไม่						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๙	มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน เช่น มีระบบการเปลี่ยนรหัสผ่าน/ระบบมีการล็อกรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น						
๑๐	ระบบการ authentication หรือระบบเว็บไซด์/ระบบสารสนเทศอื่นใดของหน่วยงาน มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละครั้งหรือไม่						
๑๑	มีมาตรการหรือแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่านหรือไม่ เช่นการกำหนดรหัสผ่านที่มีความยาว ๖-๘ ตัวอักษรและต้องมีอักขระปน เป็นต้น						
๑๒	มีการใช้งานบริการเครือข่ายที่ให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่เปิด/อนุญาตให้เข้าถึงเท่านั้น เช่นไม่มีการรีโมลเข้ามาในระบบภายในเครือข่ายโดยไม่รับอนุญาต หรือออกเครือข่ายโดยไม่ผ่านการ authentication เป็นต้น						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๑๓	มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กรก่อนที่จะเข้ามาใช้งานระบบเครือข่ายภายในองค์กร						
๑๔	มีการเปิดใช้งานพอร์ตเฉพาะพอร์ตที่กรมกำหนดไว้เท่านั้นหรือไม่						
๑๕	แผนผังเครือข่ายว่ามีการแบ่งแยกเครือข่าย ตามกลุ่มที่เหมาะสมหรือไม่						
๑๖	มีการควบคุมการใช้โปรแกรมอรรถประโยชน์หรือไม่						
๑๗	มีการตัดสัญญาณอินเทอร์เน็ต (session time-out) ในระยะเวลา ๕-๑๕ นาทีหรือไม่						
๑๘	มีการติดตั้งโปรแกรมป้องกันไวรัสครบถ้วนหรือไม่						
๑๙	มีการ update โปรแกรมป้องกันไวรัสครบถ้วนหรือไม่						
ประเด็นที่ **๒** การควบคุมการเข้าถึงทางกายภาพ **ตรวจในห้องแม่ข่าย**							
๒๐	มีการแยกพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศขององค์กร (เช่น ห้องเครื่อง/ห้องแม่ข่าย) ออกจากพื้นที่ส่วนที่เป็นสำนักงานของผู้ให้บริการภายนอกหรือไม่						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๒๑	มีการจัดแสงสว่างในบริเวณต่างๆอย่างเพียงพอ						
๒๒	มีการใช้ผนังล้อมรอบเป็นผนังทึบและควรมิดชิด เมื่อมองจากด้านนอกเข้าไปข้างในจะต้องไม่รู้ว่าเป็นห้องแม่ข่ายหรือหากผนังเป็นกระจกใส ต้องทำการติดฟิล์มทึบทับไว้						
๒๓	ห้องแม่ข่าย (Server) ห้ามมีป้ายบอกว่าเป็นห้อง Server Room เพื่อป้องกันการแอบเข้ามาขโมยทรัพย์สิน หรือเข้ามาทำลายในกรณีเกิดเหตุการณ์ประท้วงของพนักงาน						
๒๔	มีการใช้ประตูและหน้าต่างของสำนักงานให้ล็อคอยู่เสมอ						
๒๕	ประตูทางเข้า จะต้องมีกล้องวงจรปิดบันทึกภาพบริเวณประตูเข้าออกห้อง						
๒๖	มีการจัดระบบการรักษาความปลอดภัยอย่างเพียงพอหรือไม่ มีการตรวจตาพื้นที่ภายในองค์กรอย่างไร ตรวจตราบ่อยเพียงไร มีผู้ตรวจตราหรือกวดขันงานของ รปภ.อย่างสม่ำเสมอหรือไม่						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๒๗	มีมาตรการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้ลายนิ้วมือ เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญหรือไม่						
๒๘	มีการลงและจัดเก็บบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญ						
๒๙	ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น						
๓๐	ห้ามสูบบุหรี่ และนำอาหาร เครื่องดื่มเข้าไปในบริเวณห้องเครื่อง						
๓๑	ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องให้ปิดล็อคอยู่เสมอ						
๓๒	ความสะอาดและความเป็นระเบียบเรียบร้อยของห้องแม่ข่าย						
๓๓	มีการดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องแม่ข่ายอย่างสม่ำเสมอหรือไม่ ให้ตรวจสอบแผนการทำความสะอาดของห้องแม่ข่ายว่ามีการจดบันทึกและทำแผนไว้หรือไม่ และมีการทำความสะอาดเพื่อให้อุปกรณ์ปลอดจากฝุ่นอย่างสม่ำเสมอหรือไม่						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๓๔	ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย						
๓๕	ไม่มีการจัดวางอุปกรณ์คอมพิวเตอร์ไว้ใต้ตู้เครื่องปรับอากาศ (ซึ่งอาจมีน้ำรั่วไหลลงมายังอุปกรณ์คอมพิวเตอร์ได้)						
๓๖	มีการตรวจสอบระดับอุณหภูมิในห้องแม่ข่ายหรือไม่						
๓๗	มีการตรวจสอบความชื้นในห้องแม่ข่ายหรือไม่						
๓๘	มีการติดตามระบบปรับอากาศอย่างน้อยมีแอร์ ๒ ตัว ตั้งเวลาเปิดปิดสลับทำงาน						
๓๙	มีการป้องกันไฟไหม้หรือไม่ เช่น การติดตั้งอุปกรณ์ดับเพลิงและเครื่องดักจับควันไฟ						
๔๐	ตู้ Rack ทุกตู้ต้องล็อคอยู่เสมอห้ามเปิดค้างไว้						
๔๑	ตู้ Rack มีพัดลมดูดอากาศติดตั้งไว้ด้านบน						
๔๒	ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๔๓	มีการจัดทำป้ายชื่อสำหรับสายสัญญาณสื่อสารเพื่อป้องกันการตัดต่อสัญญาณผิดเส้น						
๔๔	มีการจัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง						
๔๕	มีการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน (แรงดันไฟฟ้าไม่คงที่ มีการผันแปรอย่างต่อเนื่อง) หรือไฟฟ้ากระชากหรือไม่ เช่น การใช้ยูพีเอส						
ประเด็นการตรวจสอบที่ ๓ หน่วยงานมีการดำเนินงานควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๖๐							
๔๖	เวลาของไฟร์วอลล์ (Firewall)และเครื่องบันทึกการจัดเก็บข้อมูลการจารจรคอมพิวเตอร์ถูกต้องเป็นปัจจุบัน						
๔๗	การตั้งเวลาในการจัดเก็บการจารจรคอมพิวเตอร์ไว้ ๙๐ วันตามที่กำหนด						
ประเด็นการตรวจสอบที่ ๔ หน่วยงานต้องมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด							
๔๘	มีกระบวนการในการสำรองข้อมูลอย่างเป็นระบบได้แก่ (๑)คัดเลือกข้อมูลที่สำคัญต่อองค์กรนำมาจัดเรียงลำดับความสำคัญ (๒)กำหนดความถี่ในการ						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	สำรองข้อมูลตามระดับความสำคัญที่กำหนดไว้ (๓)จัดทำแผนในการสำรองข้อมูลอย่างเป็นระบบ (๔)ดำเนินการสำรองข้อมูลและสุ่มตรวจข้อมูลที่สำรองว่ามีความสมบูรณ์หรือไม่ และมีหลักฐานบันทึกกิจกรรมการสำรองข้อมูล						
๔๙	แผนในการสำรองข้อมูลมีหรือไม่						
๕๐	ผลกิจกรรมการสำรองข้อมูลตามแผนที่กำหนด						
๕๑	แผนเตรียมความพร้อมกรณีฉุกเฉินมีหรือไม่						
๕๒	มีการซักซ้อมแผนฯและรายงานผลการซักซ้อมแผนเตรียมความพร้อมกรณีฉุกเฉิน						
ประเด็นการตรวจสอบที่ ๕ มีการประเมินขีดสมรรถนะของระบบสารสนเทศให้มีความพร้อมใช้งาน							
๕๓	มีแผนการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์ (Firewall)รวมถึงแบนด์วิชหรือไม่						
๕๔	มีการบันทึกกิจกรรมการประเมินขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์ (Firewall)รวมถึงแบนด์วิชตามแผนที่กำหนด						
๕๕	มีรายงานผลการวิเคราะห์						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ขีดสมรรถนะของเครื่องแม่ข่ายและไฟร์วอลล์ (Firewall)รวมถึงแบนด์วิชอย่างน้อยปีละครั้ง						
๕๖	มีการจดบันทึกเหตุการณ์ที่เป็นปัญหา เช่น มีค่า Threshold เกินหรือมีการล่ม/downของระบบเครื่องแม่ข่ายและไฟร์วอลล์ (Firewall) รวมถึงแบนด์วิช เป็นต้น						
๕๗	มีการรายงานกรณีที่ มีค่า Threshold เกินหรือมีการล่ม/downของระบบเครื่องแม่ข่ายและไฟร์วอลล์(Firewall) รวมถึงแบนด์วิช						
ประเด็นการตรวจสอบที่ ๖ การดำเนินงานควบคุมและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม							
๕๘	มีทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการคุม (๑)เครื่องคอมพิวเตอร์ต้องจัดเก็บคุณลักษณะเฉพาะอย่างน้อย CPU RAM HD (๒)มีการควบคุมประเภทของทรัพย์สินด้าน Hardware,Network,Database,Software (๓)มีการจัดเก็บชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ						
๕๙	มีระบบการยืม-คืนครุภัณฑ์ถูกต้องตามระเบียบ						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๖๐	มีการตรวจสอบบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งเครือข่าย (ถ้ามี) อย่างน้อยปีละครั้ง(มีการบำรุงรักษาทั้งในเชิงป้องกันและเชิงแก้ไข)						
ประเด็นการตรวจสอบที่ ๗ การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต							
๗.๑ ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว							
๖๑	ระบบสารสนเทศมีการนำเข้าข้อมูลได้อย่างถูกต้อง มีการประมวลผลและออกรายงานผลแสดงได้อย่างถูกต้องหรือไม่						
๖๒	มีเอกสารการกำหนด/วิเคราะห์ความต้องการของผู้ใช้งานหรือไม่						
๖๓	ระบบที่พัฒนาสอดคล้องกับความต้องการของผู้ใช้งานหรือไม่						
๖๔	มีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล						
๗.๒ ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้น							
๖๕	มีเอกสารการวิเคราะห์						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ความต้องการของผู้ใช้งานหรือไม่						
๖๖	มีการศึกษาความเป็นไปได้						
๖๗	มีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) (๓)พจนานุกรมฐานข้อมูล (๔)ความสัมพันธ์ของฐานข้อมูล						
๖๘	มีรายงานการประชุมการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา						
๖๙	มีรายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน						
๗๐	มีรายงานผลการฝึกอบรมการใช้งาน						
๗๑	มีคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ						
๗๒	มีรายงานผลการติดตั้งทดสอบระบบขึ้นใช้งานจริง						
๗๓	มีรายงานผลการประเมินความพึงพอใจของผู้ใช้งานระบบ						
๗๔	หน่วยงานมีระบบการตรวจสอบคุณภาพข้อมูล						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	สารสนเทศหรือฐานข้อมูลอย่างเป็นระบบหรือไม่โดยต้องมีสิ่งเหล่านี้ครบถ้วน (๑)มีเกณฑ์การตรวจสอบคุณภาพข้อมูล (๒)มีการตรวจสอบคุณภาพข้อมูลตามเกณฑ์ที่กำหนด (๓)มีรายงานผลคุณภาพข้อมูลให้ผู้บังคับบัญชาทราบ (๔)มีแนวทางแก้ไขพัฒนาระบบข้อมูล						
๗๕	ข้อมูลของระบบสารสนเทศของหน่วยงานมีความถูกต้อง						
๗๖	ข้อมูลของระบบสารสนเทศของหน่วยงานมีครบถ้วน						
๗๗	ข้อมูลของระบบสารสนเทศของหน่วยงานมีความทันสมัย						
๗๘	เผยแพร่บนเว็บไซด์หน่วยงานตามพรบ.ข้อมูลข่าวสารปี ๒๕๔๐ ครบถ้วน **<u>มาตรา ๗</u>** -โครงสร้างและการจัดองค์กรในการดำเนินงาน -สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน/กระบวนงานที่ทำ -สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสารหรือคำแนะนำในการติดต่อกับ						

ลำดับที่	รายการที่ตรวจ	ข้อตรวจพบ	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	หน่วยงานรัฐ **<u>มาตรา๙</u>** -ผลการพิจารณาการจัดซื้อจัดจ้าง -แผนงานโครงการและงบประมาณรายจ่ายประจำปี(ปีปัจจุบัน) -แผนการจัดซื้อจัดจ้างของหน่วยงาน -คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงาน -ประกาศประกวดราคาประกาศสอบราคา -ผลการจัดซื้อประจำเดือนเผยแพร่ผ่านเว็บไซต์หน่วยงาน							
ผลรวม n๑, n๒ , n๓						N/A	
รวมคะแนนทั้งหมด (N = n๑ + n๒ + n๓)							
ผลรวมจำนวนข้อ (โดยไม่นับรวมข้อที่เป็น N/A) = (๑๐๐%)							
คิดเป็นร้อยละ (N / ผลรวมจำนวนข้อ x ๑๐๐)							

สรุปผลการตรวจสอบและประเมินผล

.....

.....

.....

.....

ข้อเสนอแนะ

.....

.....

.....

.....

ผู้รับตรวจ .....

(.....)

.....

ผู้ตรวจ/สอบทาน

.....

(.....)

.....

วันที่.....เดือน.....พ.ศ.....

เกณฑ์การประเมินผลระบบการควบคุมภายใน

คะแนน	ระดับ
๙๐ – ๑๐๐	ดีมาก
๘๐ – ๘๙.๙๙	ดี
๗๐ – ๗๙.๙๙	พอใช้
ต่ำกว่า ๗๐	ต้องปรับปรุง

การตรวจสอบ Firewall

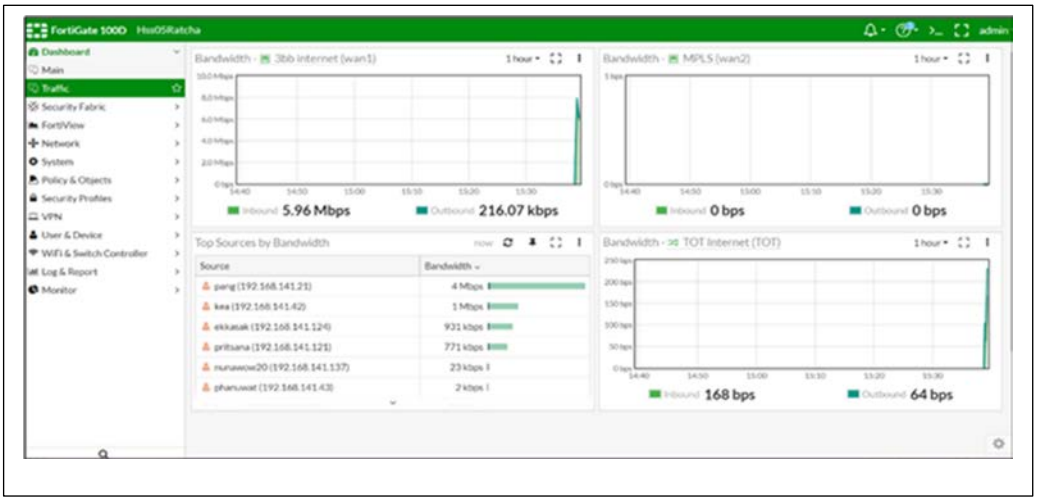
๑.ตรวจขีดสมรรถนะของ Firewall

ตรวจสอบค่า CPU RAM Traffic โดยมีรายละเอียดดังนี้

๑.๑ ตรวจสอบค่า CPU และ RAM ค่าเหล่านี้ไม่ควรเกิน ๘๐% โดยเข้าไปที่ Firewall Dashboard -> Main ตรวจเช็คดูค่า Memory, CPU และ Session ที่ใช้งาน

๑.๒ ตรวจสอบค่า Traffic ไม่ควรเกิน ๘๐%

ไปที่ Dashboard -> Traffic เช็คดูการใช้งานลักษณะต่างๆ



๒.ตรวจสอบการจัดเก็บ Log ว่าเป็นไปตามพรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ๒๕๖๐ หรือไม่ ซึ่งต้องตรวจเช็คเวลาของ Firewall ก่อนว่าตรงกับเวลาสากลหรือไม่

๒.๑ ตรวจสอบเวลาของ Firewall ว่าตรงกับเวลาสากลหรือไม่

Dashboard -> Main ดูค่า Time

๒.๒ ตรวจสอบ Log ของ Firewall ว่ามีการจัดเก็บตรงกับเวลาสากลหรือไม่

Log&Report -> Log

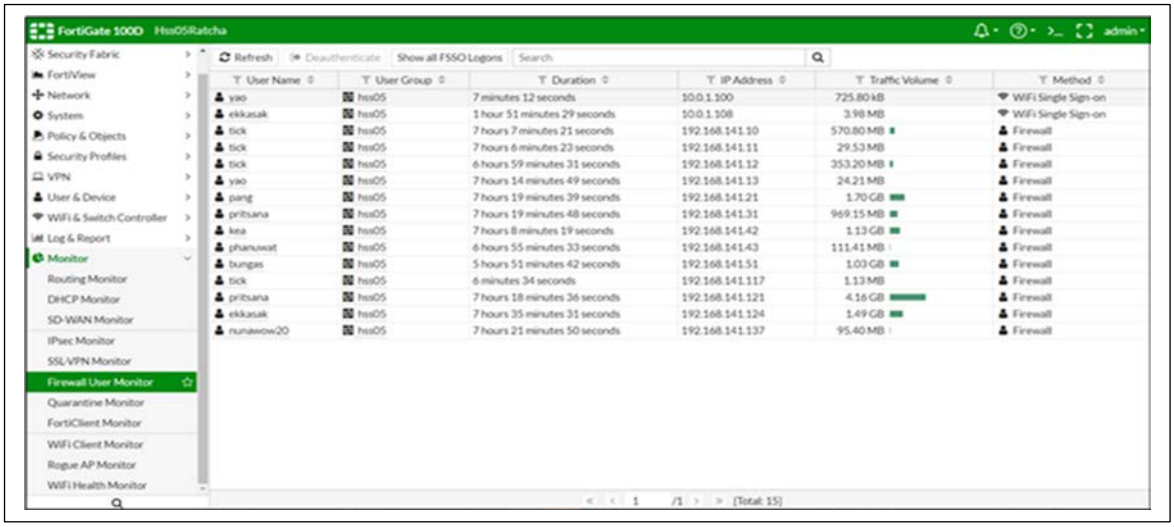
๒.๓ กรณีที่หน่วยงานใดไม่มีเครื่องบันทึกล็อกหรือD-log เสีย ให้ดูว่าLogจัดเก็บไว้ที่ใดและจัดเก็บครบอย่างน้อย ๙๐ วันหรือไม่

๓.ตรวจสอบ User Authentication ในการทบทวนสิทธิและถอดถอนสิทธิ

๓.๑ ตรวจสอบว่ามีการจัดทำบัญชี User Authentication หรือไม่ และบัญชีดังกล่าวมีการจัดเก็บไว้อย่างปกปิดมิดชิดหรือไม่ รวมทั้งมีการทบทวนบัญชีอย่างน้อยปีละครั้งหรือไม่ โดยสุ่มตรวจ User ที่เกษียณหรือโอนย้าย/ลาออก ยังมีชื่ออยู่ในบัญชีหรือไม่

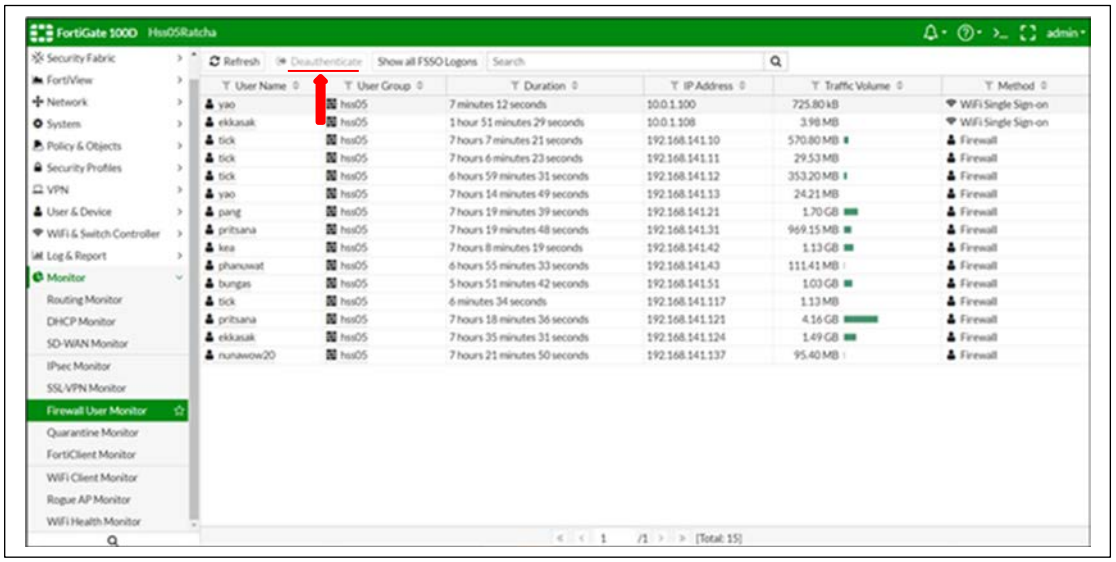
๓.๒ ตรวจสอบ User Authentication ที่อยู่บน Firewall

ไปที่ Monitor -> Firewall User Monitor



๓.๓ กรณีพบว่ามีผู้ที่ไม่มีสิทธิเข้าระบบเครือข่าย แต่ยังมีอยู่ในทะเบียนให้ดำเนินการดังนี้

ไปที่ Monitor -> Firewall User Monitor สามารถดีด User ที่เราต้องการถอดถอนออกได้ด้วยการกด Deauthenticate



๔.ตรวจสอบการ Backup file config

๔.๑ ผู้ตรวจสอบภายในต้องทดสอบผู้ดูแลระบบด้วยว่ามีความรู้ทักษะเพียงต่อการดูแลหรือไม่ การ Backup file config เป็นกระบวนการหนึ่งที่ผู้ดูแลระบบต้องดำเนินการประจำอย่างน้อย เดือนละ 1 ครั้ง ประจำอย่างน้อย เดือนละ 1 ครั้ง

ไปที่ xxx (ชื่อผู้ดูแลระบบ อยู่มุมบนขวา) -> Configuration -> Backup -> OK

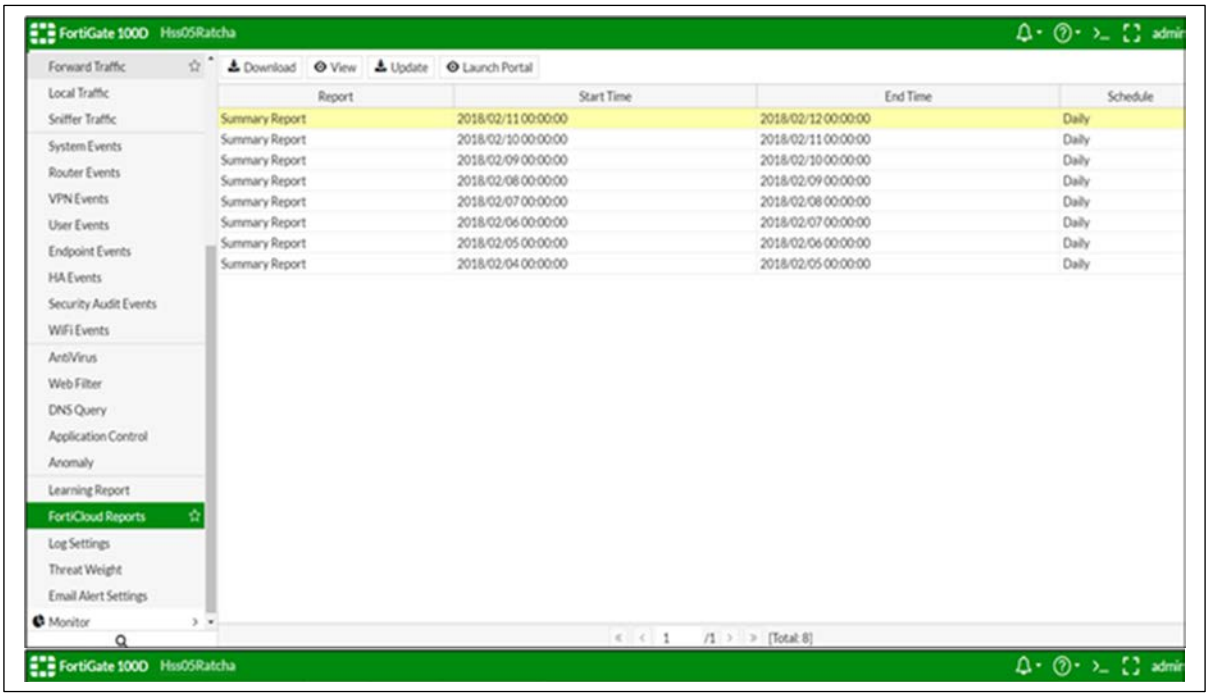
๔.๒ การ Restore File Config

ไปที่ xxx (ชื่อผู้ดูแลระบบ อยู่มุมบนขวา) -> Configuration -> Restore -> เลือก File backup ที่ต้องการ -> OK

๕.การดาวน์โหลดรายงานประจำวัน

ผู้ดูแลระบบต้องดาวน์โหลดรายงานประจำวันมาวิเคราะห์การใช้งานระบบเครือข่าย ดังนี้

ไปที่ Log &Report -> FortiCloud Reports -> เลือก Report ที่ต้องการ คลิก Download



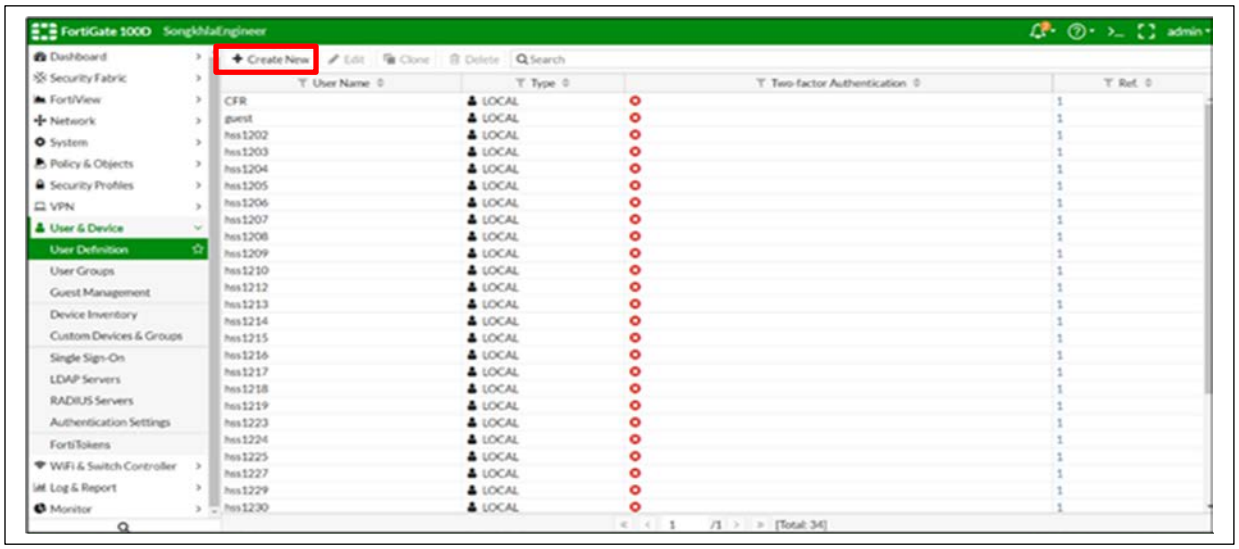
๖.ตรวจสอบการตัดสัญญาณอินเทอร์เน็ต(session timeout)

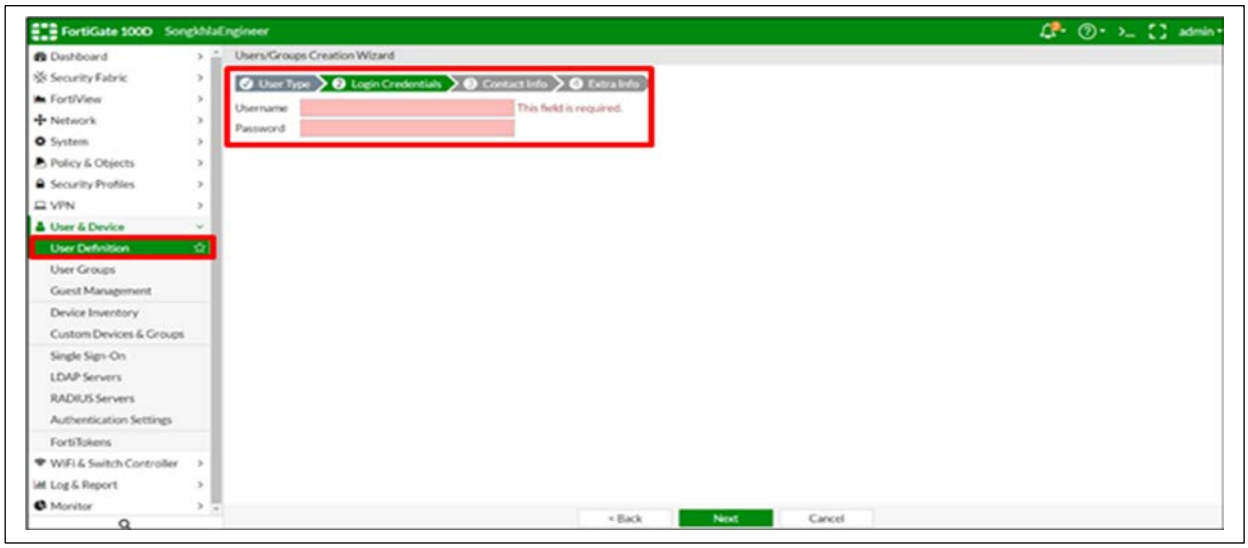
๗.การจัดการ User Authentication

๗.๑ การเพิ่ม User

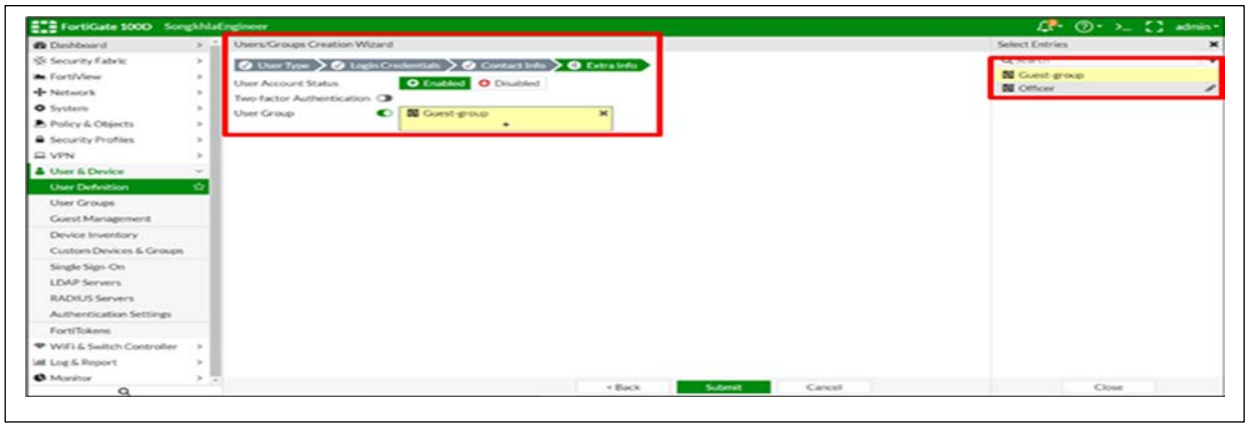
๗.๑.๑ ไปที่ User &Device -> User Definication -> คลิก Create New

๗.๑.๒ User Type เลือก Local User -> Login Credential ใส่ User/Pass ที่ต้องการ





๗.๑.๓ Contact Info ข้ามได้เลย -> Extra Info คลิกเปิด User Group ->เลือก User Group ที่ใช้งานอยู่ (แต่ละศูนย์อาจจะตั้งไม่เหมือนกัน) -> Submit



ไปที่ User &Device -> User Definication ->ดับเบิลคลิก User ที่ต้องการเปลี่ยน ->ใส่ password ใหม่ -> OK