แนวทางการตรวจประเมินเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศ

ข้อมูลเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศ	เกณฑ์การตรวจประเมิน	แนวทางการตรวจประเมิน	ตัวอย่างเอกสารประกอบการตรวจประเมิน
1. มีฐานข้อมูลที่ครอบคลุมที่ใช้สนับสนุนการปฏิบัติงาน	☐ มีฐานข้อมูลที่ครอบคลุมอย่างน้อยทุกประเด็นยุทธศาสตร์ของแผนปฏิบัติราชการ ซึ่งสนับสนุนการปฏิบัติงานได้อย่างเหมาะสม	- พิจารณาจากเอกสารที่แสดงให้เห็นถึงรายชื่อฐานข้อมูล ที่นำมาใช้สนับสนุนการปฏิบัติงาน ในแต่ละประเด็นยุทธศาสตร์ - สุ่มตรวจการใช้งานฐานข้อมูลว่านำไปสนับสนุนการปฏิบัติงานอย่างไร	- รายชื่อฐานข้อมูลสนับสนุนการปฏิบัติงานแยกตามประเด็นยุทธศาสตร์ - รายงานการประชุมที่เกี่ยวข้อง ที่แสดงให้เห็นถึงการจัดทำฐานข้อมูลสนับสนุนการปฏิบัติงาน
2. มีระบบสนับสนุนการวิเคราะห์ผลการดำเนินการ	☐ มีการนำข้อมูลและสารสนเทศของส่วนราชการ มาใช้ในการวิเคราะห์ผลการดำเนินการ และนำไปปรับปรุง/พัฒนางาน	- พิจารณาจากเอกสารหรือระบบที่แสดงให้เห็นว่าส่วนราชการได้นำข้อมูลและสารสนเทศจากฐานข้อมูลหรือช่องทางอื่นๆ มาใช้วิเคราะห์ผลการดำเนินการ - พิจารณาจากหลักฐานใดๆ ที่แสดงให้เห็นว่าส่วนราชการได้นำเอาผลจากการวิเคราะห์ไปใช้ในการปรับปรุง/พัฒนางาน	- ระบบสารสนเทศสำหรับผู้บริหาร (EIS) หรือระบบสารสนเทศทางภูมิศาสตร์ (GIS) - รายงานผลการดำเนินการ ที่มีการวิเคราะห์ข้อมูลผลการดำเนินการและข้อเสนอเพื่อการปรับปรุง - หลักฐานที่แสดงให้เห็นถึงผลของการปรับปรุง/พัฒนางาน
3. มีระบบตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลที่จัดเก็บ ในระบบฐานข้อมูล	☐ มีการกำหนดผู้รับผิดชอบในการตรวจสอบข้อมูลและการจัดเก็บข้อมูล รวมถึงการดำเนินการตามแผนการจัดเก็บและตรวจสอบ	- พิจารณาจากเอกสารที่แสดงให้เห็นว่าส่วนราชการได้กำหนดผู้รับผิดชอบในการตรวจสอบข้อมูลและการจัดเก็บ	- แผนการจัดเก็บและตรวจสอบข้อมูลแต่ละประเภทในระบบฐานข้อมูล ซึ่งต้องมีการกำหนดผู้รับผิดชอบในการ

ข้อมูลเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศ	เกณฑ์การตรวจประเมิน	แนวทางการตรวจประเมิน	ตัวอย่างเอกสารประกอบการตรวจประเมิน
	ข้อมูลแต่ละประเภทในระบบฐานข้อมูล ในระยะเวลาที่เหมาะสม	ข้อมูล - ตรวจสอบการดำเนินการตามแผนการจัดเก็บและตรวจสอบข้อมูลแต่ละประเภทในระบบฐานข้อมูล	จัดเก็บและตรวจสอบข้อมูล - รายงานผลการดำเนินการตามแผนการจัดเก็บและตรวจสอบข้อมูล
	☐ มีระบบการตรวจสอบสิทธิ์การเข้าถึง (Login) ที่สามารถ Verify User name และ Password	- พิจารณาความสามารถของระบบในการตรวจสอบสิทธิ์การเข้าถึง (Login) ของระบบ Intranet หรือ Back Office ได้ถูกต้อง	
4. มีการอัพเดทข้อมูลที่จำเป็นอย่างสม่ำเสมอและทันท่วงที	☐ มีการตรวจรอบของการจัดเก็บข้อมูลแต่ละประเภท พร้อมที่จะนำไปใช้ประโยชน์อยู่เสมอ	- พิจารณาจากเอกสารหลักฐานที่แสดงให้เห็นถึงวิธีการ/ข้อกำหนดเกี่ยวกับการอัพเดทข้อมูลที่จำเป็น และหลักฐานที่บันทึกการจัดเก็บข้อมูล โดยการสุ่มตรวจ	- เอกสารแสดงวิธีการ/ข้อกำหนดเกี่ยวกับรอบของการจัดเก็บข้อมูล เช่น รายงาน/บันทึกการจัดเก็บข้อมูล เป็นต้น
5. มีระบบสืบค้นข้อมูลบนเว็บไซต์ของส่วนราชการที่มีประสิทธิภาพ	☐ มีระบบการสืบค้นข้อมูล (Search Engine) บนเว็บไซต์ของส่วนราชการ ที่สามารถค้นหาได้ถูกต้องสอดคล้องกับความต้องการ และในระยะเวลาที่เหมาะสม	- พิจารณาจากระยะเวลาที่เหมาะสมในการค้นหาข้อมูล และความถูกต้องของผลการค้นหาที่สอดคล้องกับคำค้น โดยการทดสอบ Search Engine บนเว็บไซต์ของส่วนราชการ	

ข้อมูลเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศ	เกณฑ์การตรวจประเมิน	แนวทางการตรวจประเมิน	ตัวอย่างเอกสารประกอบการตรวจประเมิน
6. มีการพัฒนาปรับปรุงเทคโนโลยีสารสนเทศจากข้อคิดเห็น/ข้อเสนอแนะ/ ข้อร้องเรียนของผู้ใช้งาน	☐ มีการนำข้อคิดเห็น/ข้อเสนอแนะ/ข้อร้องเรียนจากผู้ใช้งานสารสนเทศมาพัฒนาปรับปรุงให้ดีขึ้น	- พิจารณาจากเอกสาร/หลักฐาน ที่แสดงให้เห็นว่าส่วนราชการมีการสำรวจข้อคิดเห็น/ข้อเสนอแนะ/ข้อร้องเรียนจากผู้ใช้งานสารสนเทศ และได้นำข้อคิดเห็นดังกล่าวมาพัฒนาปรับปรุงระบบเทคโนโลยีสารสนเทศ	- แบบสำรวจความพึงพอใจ/ความคิดเห็นจากผู้ใช้งานสารสนเทศ - เอกสารที่แสดงให้เห็นถึงการดำเนินการพัฒนาปรับปรุงเทคโนโลยีสารสนเทศจากข้อคิดเห็น/ข้อเสนอแนะ/ข้อร้องเรียนของผู้ใช้งานจากผู้ใช้งานสารสนเทศ เช่น รายงานการประชุม เป็นต้น
7. มีแนวทาง/มาตรการป้องกันความเสียหายและมีการสำรองข้อมูลสารสนเทศ (Backup)	☐ มีการสำรองข้อมูลสารสนเทศ (back up) ในระบบ Intranet อย่างน้อย 2 ครั้ง/สัปดาห์ และในระบบ Internet อย่างน้อย 1-2 ครั้ง/เดือนหรือตามความเหมาะสมของแต่ละหน่วยงาน ซึ่งสามารถพิจารณาจากความสำคัญ ปริมาณงาน Transaction และสถิติความเสียหายที่พบในอดีตที่ผ่านมา	- พิจารณาจากเอกสารแนวทาง/มาตรการ/แผนการสำรองข้อมูล - ผู้ตรวจสุ่มตรวจความพร้อมใช้งานของระบบการสำรองข้อมูลตามรูปแบบของสื่อที่ส่วนราชการใช้ในการเก็บข้อมูล เช่น เทป ซีดี ฮาร์ดดิส เป็นต้น	- แผนการสำรองข้อมูล หรือปฏิทินกิจกรรมการสำรองข้อมูล - รายงานหรือบันทึกการดำเนินการสำรองข้อมูล - รายงานหรือบันทึกการกู้คืนข้อมูลหรือการทดสอบการกู้คืนข้อมูล

ข้อมูลเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศ	เกณฑ์การตรวจประเมิน	แนวทางการตรวจประเมิน	ตัวอย่างเอกสารประกอบการตรวจประเมิน
8. มีระบบรักษาความมั่นคงและปลอดภัยของระบบฐานข้อมูลและสารสนเทศ	☐ มีระบบการตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่ายครอบคลุมทุกโฮสต์ (Host) รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน	- พิจารณาจากเอกสารที่แสดงให้เห็นถึงระบบตรวจสอบการบุกรุกฯ ตามที่ส่วนราชการใช้ เช่น Firewall, Proxy, IDS/IPS เป็นต้น - ให้ส่วนราชการแสดงการทำงานของระบบตรวจสอบการบุกรุกฯ	- เอกสารตัวอย่างแสดงภาพหน้าจอ (Capture) ของระบบตรวจสอบการบุกรุกฯ
	☐ มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล ที่เป็นไปตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	- พิจารณาจากเอกสารที่แสดงให้เห็นถึงระบบบันทึกและติดตามการใช้งานระบบสารสนเทศ และตรวจตราการละเมิดความปลอดภัย เช่น Log Server ระบบ Block Website ระบบตรวจสอบ IP Address เครื่องคอมพิวเตอร์ เป็นต้น - ให้ส่วนราชการแสดงการทำงานของระบบตรวจสอบการบุกรุกฯ	- เอกสารตัวอย่างแสดงภาพหน้าจอ (Capture) ของระบบบันทึกและติดตามฯ
9. มีแผนบริหารความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศ	☐ มีแผนบริหารความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศ และกระบวนการที่แสดงถึงการตอบสนองต่อการบุกรุกที่เสี่ยงต่อการทำงานของระบบสารสนเทศ ที่ครอบคลุมถึงการ	- พิจารณาจากแผนบริหารความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศ และเอกสารที่แสดง กระบวนการตอบสนอง (Warnning) และการป้องกันการบุกรุก	- แผนบริหารความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศ - รายงานผลการดำเนินการตามแผนบริหารความเสี่ยงด้านคอมพิวเตอร์

ข้อมูลเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศ	เกณฑ์การตรวจประเมิน	แนวทางการตรวจประเมิน	ตัวอย่างเอกสารประกอบการตรวจประเมิน
	สนับสนุนการปฏิบัติงานได้อย่างต่อเนื่องภายใต้ภาวะวิกฤต (เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว เป็นต้น) เพื่อให้สามารถลดความเสียหายได้อย่างรวดเร็ว รวมถึงการป้องกันเหตุการณ์ที่อาจเกิดขึ้นและดำเนินการตามแผน	ระบบสารสนเทศ เช่น ระบบ Anti-Virus ระบบตรวจสอบการถูก Hack ระบบตรวจสอบ IP Address เครื่องคอมพิวเตอร์ ระบบยืนยันตัวตน (Pin Code) เป็นต้น	และสารสนเทศ - เอกสารตัวอย่างแสดงภาพหน้าจอ (Capture) ของกระบวนการตอบสนอง (Warnning) และการป้องกันการบุกรุกระบบสารสนเทศ
10. มีระบบ Access Right ที่ถูกต้องและทันสมัย	☐ มีการกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมถึงการเปลี่ยนแปลงหรือยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก พ้นจากตำแหน่ง หรือยกเลิกการใช้งาน และมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ	- พิจารณาจากเอกสารที่แสดงให้เห็นว่าส่วนราชการมีแนวทาง/วิธีการ/หลักเกณฑ์ ในการกำหนดสิทธิ์ และทบทวนสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูล - ส่วนราชการแสดงความถูกต้องของระบบ Access Right โดยเปรียบเทียบสิทธิ์การเข้าถึงตามจริง กับในระบบ โดยอาจเป็นระบบ Intranet หรือ Back Office ก็ได้	- เอกสารแสดงการกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูล - เอกสารแสดงการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน