แผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
จังหวัดสระแก้ว

ส่วนที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

สารสนเทศเป็นทรัพยากรที่สำคัญยิ่งขององค์การ เป็นข้อมูลที่มีความหมาย และมีประโยชน์ต่อการตัดสินใจองค์การต่าง ๆ จึงจัดให้มีระบบสารสนเทศเพื่อช่วยให้การดำเนินงานมีประสิทธิภาพยิ่งขึ้น มีการตัดสินใจที่รวดเร็วและถูกต้อง ตลอดจนเสริมสร้างภาพลักษณ์ที่ดีขององค์การ ดังนั้นระบบสารสนเทศที่มีประสิทธิภาพจึงเป็นหัวใจสำคัญของหน่วยงาน การรักษาความปลอดภัยให้กับระบบสารสนเทศเพื่อป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อระบบเป็นเรื่องที่ต้องตระหนักเป็นอันดับแรก

๑.๒ วิสัยทัศน์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด

เป็นศูนย์กลางการบริหารจัดการ การพัฒนาบุคลากรของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค และส่วนท้องถิ่นในจังหวัด โดยใช้เทคโนโลยีสารสนเทศที่เหมาะสม มีความทันสมัย และมีประสิทธิภาพ

๑.๓ พันธกิจ

พัฒนาศักยภาพการจัดการ ระบบเทคโนโลยีสารสนเทศเพื่อประโยชน์ในการบริหารจัดการการพัฒนาคุณภาพ การรายงานผลที่มีประสิทธิภาพ เพื่อการบริหารจัดการพัฒนาจังหวัดแบบบูรณาการให้เกิดการพัฒนาอย่างมีประสิทธิภาพ ประสิทธิผลก่อให้เกิดการพัฒนาอย่างยั่งยืน

๑.๔ ยุทธศาสตร์ในการพัฒนา

๑) ศึกษาวิเคราะห์ วางแผน ออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศ ของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่ายให้มีความเหมาะสม ตอบสนองต่อการพัฒนาจังหวัดแบบบูรณาการได้อย่างมีประสิทธิภาพ ประสิทธิผลก่อให้เกิดการพัฒนาอย่างยั่งยืน

๒) การเชื่อมโยงระบบข้อมูลสารสนเทศ การดูแลรักษาเทคโนโลยีสารสนเทศ ของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่าย ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

๓) เป็นศูนย์กลางการประสานงานด้านข้อมูลสารสนเทศของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่าย เพื่อให้มีการจัดระบบข้อมูลสารสนเทศ การบริการข้อมูลสารสนเทศ และการเผยแพร่ข้อมูลสารสนเทศให้เกิดประโยชน์ในการบริหารจัดการพัฒนาจังหวัดแบบบูรณาการ

๔) พัฒนาศักยภาพบุคลากรของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่ายให้มีความรู้ความสามารถในด้านการใช้เทคโนโลยีสารสนเทศในการจัดระบบข้อมูลสารสนเทศได้อย่างมีประสิทธิภาพ ส่งผลให้เกิดการพัฒนาจังหวัดอย่างยั่งยืน

๑.๕ วัตถุประสงค์

เพื่อควบคุมความเสี่ยงและสร้างความปลอดภัยให้กับระบบสารสนเทศของจังหวัด

ส่วนที่ ๒
ความเสี่ยงและปัจจัยความเสี่ยง

๒.๑ นิยามความเสี่ยง

- Australian and New Zealand Public Sector Guidelines for Managing Risk ได้ให้คำจำกัดความว่า ความเสี่ยง หมายถึง โอกาสของบางสิ่งบางอย่างซึ่งเมื่อเกิดขึ้นแล้วจะมีผลกระทบต่อการบรรลุวัตุประสงค์ โดยสามารถวัดความเสี่ยงได้จากผลที่ติดตามมา (Consequences) เป็นโอกาสที่น่าจะเกิดขึ้น (Likelihood)

- The Canadian Institute of Charteres Accounts (CICA) ให้คำจำกัดความว่า ความเสี่ยง คือ ความเป็นไปได้ที่บุคคลใดบุคคลหนึ่งหรือกลุ่มหนึ่ง หรือองค์การจะประสบความยากลำบากซึ่งเป็นผลจากเหตุการณ์หรือกรณีบางอย่าง

- Treasury Board of Canada ได้ให้ความหมายของความเสี่ยงว่า เป็นความไม่แน่นอนที่อยู่ห้อมล้อมเหตุการณ์ในอนาคตและผลลัพธ์ ซึ่งสามารถแสดงออกในลักษณะของโอกาสที่น่าจะเกิดขึ้นและผลกระทบของเหตุการณ์ที่มีแนวโน้มว่าจะส่งผลกระทบต่อความสำเร็จของวัตถุประสงค์ขององค์การ โดยสรุปความเสี่ยง (Risk) เป็นสิ่งที่มนุษย์ทุกคนไม่อาจหลีกเลี่ยงได้และเกิดขึ้นในชีวิตประจำวันทั่วไป

๒.๒ ปัจจัยความเสี่ยง

ความเสี่ยงที่อาจผลกระทบต่อระบบสารสนเทศ ประกอบด้วย

๑) Access Risk : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือบุคคลมีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานไม่ได้มีวิธีจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปใช้ก่อให้เกิดความเสียกายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยอาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งานการไม่ได้มีการกำหนดรหัสผ่าน (Password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอการไม่ได้จำกัดควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

๒) Integrity Risk : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานระบบคอมพิวเตอร์ ซึ่งอาจเกิดจาการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ (acess risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ เพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการ และการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช่งานได้

๓) Availability Risk : เป็นความเสี่ยงเกี่ยวกับไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการซึ่งอาจทำให้การปฏิบัติงานหรือการให้บริการด้านต่าง ๆ อาจจะหยุดชะงักได้ โดยอาจเกิดจากการที่ไม่ได้มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ การไม่ได้ทำการสำรองข้อมูลและระบบงานคอมพิวเตอร์ การไม่ได้จัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน รวมถึง ไม่ได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ (access risk) ก็อาจส่งผลให้เกิดความเสียหายได้

๔) Infrastructure Risk : เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี รวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการปฏิบัติงาน โดยอาจเกิดจากการแบ่งอำนาจหน้าที่ไม่เหมาะสม ซึ่งทำให้ขาดการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการที่ไม่ได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่าง ๆ หรืออาจเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานที่สำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน

ส่วนที่ ๓
การบริหารจัดการความเสี่ยง

๓.๑ องค์ประกอบสำคัญของความเสี่ยง

ความเสี่ยงอาจก่อให้เกิดการสูญเสียหรือเกิดสิ่งที่ไม่พึงประสงค์ การบริหารจัดการความเสี่ยงจึงมีวัตถุประสงค์เพื่อรับรู้ จำกัด และควบคุมความเสี่ยง จากปัจจัยความเสี่ยงดังกล่าว สามารถกำหนดเป็นองค์ประกอบหลักที่จะต้องบริหารจัดการได้ ๓ องค์ประกอบ คือ

๑) บุคลากร หากบุคลากรไม่เข้าใจเกี่ยวกับการใช้งาน/การรักษาความปลอดภัยให้กับเทคโนโลยีสารสนเทศอาจทำให้ระบบสารสนเทศเกิดความเสียหายได้

๒) เทคโนโลยี ความผิดพลาดในการประมวลผลอาจมีผลต่อการให้บริการข้อมูล ซึ่งจะทำให้กระทบต่อการตัดสินใจและการวางแผน

๓) การบริหารจัดการ หากไม่มีการบริหารจัดการที่ดีอาจส่งผลให้เกิดปัญหาหลายประการ เช่น การไม่มีนโยบายด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ทำให้ผู้ใช้งาน/ผู้ดูแลระบบไม่มีแนวทางในการปฏิบัติงานได้อย่างถูกต้อง

๓.๒ แนวทางการลดความเสี่ยง

๑) ด้านบุคลากร

๑.๑) สร้างความตระหนักให้กับบุคลากรในการรักษาความปลอดภัยให้กับเทคโนโลยีสารสนเทศ โดยมุ่งเน้นพฤติกรรมการใช้งานระบบเครือข่าย ได้แก่ การตรวจสอบไวรัสก่อนการดาวน์โหลดไฟล์ การออกจากระบบ (Logout) เมื่อไม่ได้ใช้งาน เป็นต้น

๑.๒) ฝึกอบรมเพื่อเพิ่มทักษะความชำนาญ และสร้างความเข้าใจที่ถูกต้องเกี่ยวกับการใช้งานและการรักษาความปลอดภัยของข้อมูลและระบบงานคอมพิวเตอร์

๒) ด้านเทคโนโลยีสารสนเทศ

๒.๑) ติดตั้งระบบปฏิบัติการให้ทำงานอย่างปลอดภัย

๒.๒) จัดให้มีการบำรุงรักษาที่ต่อเนื่องเหมาะสม และควบคุมครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ทุกประเภท

๒.๓) ติดตั้งระบบป้องกันการบุกรุก

๒.๔) ติดตั้งระบบเตือนภัย

๒.๕) ติดตั้งระบบสำรองไฟ

๓) ด้านการบริหารจัดการ

๓.๑) กำหนดการ/แนวทางในการควบคุมการปฏิบัติงาน

๓.๒) ตรวจสอบกระบวนการหรือวิธีการจัดเก็บเอกสาร หรือ Media ที่ใช้ประกอบการออกแบบระบบงาน รวมทั้งวิธีการเก็บและดูแลรักษา Source Program อย่างสม่ำเสมอ

๓.๓) กำหนดให้มีการจัดทำทะเบียนคุมการติดตั้งการนำ Software จากภายนอกเข้ามาใช้กับเครื่องคอมพิวเตอร์ในหน่วยงาน

๓.๔) กำหนดผู้ที่มีหน้าที่รับผิดชอบศึกษา ทบทวนระบบรักษาความปลอดภัย และกำหนดสิทธิในการเข้าถึงระบบงานและฐานข้อมูลที่สำคัญ

๓.๕) การปรับปรุงพัฒนาระบบและสิทธิ หรือ User ID ในการเข้าถึงระบบงานและระบบข้อมูลเป็นระยะ

๓.๖) จัดให้มีการตรวจสอบข้อมูลหรือเอกสารที่จะนำเข้าระบบ รวมทั้งจัดให้มีรายงานจากโปรแกรมระบบงานสำหรับใช้ในการตรวจสอบหรือสอบทานความถูกต้องของข้อมูลก่อนการส่งต่อ

๓.๗) กำหนดระบบการจัดเก็บและสำรองแฟ้มข้อมูล ฐานข้อมูล และรายงานต่าง ๆ ให้เหมาะสมกับการใช้งาน

๓.๘) กำหนดให้มีวิธีการ Backup หรือทำสำเนา Source Program ระบบงานที่สำคัญอย่างน้อย ๒ ชุด และแยกสถานที่จัดเก็บ รวมทั้งจัดทำทะเบียนไว้เป็นหลักฐาน

๓.๙) จัดให้มีการสำรองข้อมูลให้ครบถ้วนตามความเหมาะสมของแต่ละระบบงานตามเวลาที่กำหนด เช่น จัดเก็บทุกสิ้นวัน ทุกสัปดาห์ หรือทุกเดือนตามความจำเป็นและเหมาะสม

๓.๑๐) จัดให้มีการทดสอบความถูกต้องของข้อมูลที่สำรองไว้เป็นครั้งคราวและทำรายงานผลการทดสอบ

ส่วนที่ ๔
การควบคุมการปฏิบัติงาน

เพื่อรักษาความปลอดภัยให้กับระบบสารสนเทศ และควบคุมความเสี่ยงที่อาจเกิดขึ้นได้ตลอดเวลา จำเป็นต้องมีการควบคุมการปฏิบัติงาน เพื่อเป็นมาตรการป้องกันผลกระทบที่จะเกิดตามมา โดยกำหนดแนวทางในการควบคุมความเสี่ยง และผู้รับผิดชอบให้ชัดเจน ดังนี้

โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยงและผลกระทบต่อองค์กร

โอกาสที่จะปิด	ความถี่ที่เกิดขึ้น (เฉลี่ย)	ผลกระทบ/ความเสียหายต่อองค์กร
สูงมาก	มากกว่า ๑ ครั้งต่อเดือน	มากกว่า ๑๐ ล้านบาท
สูง	ระหว่าง ๑ – ๖ เดือนต่อครั้ง	๕ แสนบาท – ๑๐ ล้านบาท
ปานกลาง	ระหว่าง ๖ – ๑๒ เดือนต่อครั้ง	๑ – ๕ แสนบาท
น้อย	มากกว่า ๑ ปีต่อครั้ง	๑ หมื่นบาท – ๑ แสนบาท
น้อยมาก	มากกว่า ๕ ปีต่อครั้ง	น้อยกว่า ๑ หมื่นบาท

การควบคุมความเสี่ยง

องค์ประกอบ	ความเสี่ยง	การวิเคราะห์ความเสี่ยง		การควบคุม	หน่วยรับผิดชอบ
		โอกาสที่จะเกิดความเสี่ยง	ระดับความเสี่ยง		
๑. บุคลากร **วัตถุประสงค์** ๑.๑ เพื่อให้บุคลากรมีความตระหนักในการรักษาความปลอดภัยให้กับเทคโนโลยีสารสนเทศ ๑.๒ เพื่อให้บุคลากรมีทักษะความชำนาญและความเข้าใจที่ถูกต้องกับปัญหาเรื่องความปลอดภัยข้อมูลคอมพิวเตอร์	พฤติกรรมการใช้งานระบบเครือข่ายขาดความระมัดระวังในการป้องกัน	มีโอกาสเกิดขึ้นซึ่งมีผลทำให้ฐานข้อมูลอาจได้รับความเสียหายจกไวรัสหรือการถูกบุกรุก	ปานกลาง	๑. จากกฎ ระเบียบควบคุมการใช้งาน กำหนดรหัสการใช้งาน ๒. การจัดฝึกอบรมให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศ	ทุกส่วนราชการ
๒. เทคโนโลยีสารสนเทศ วัตถุประสงค์ เพื่อให้ระบบปฏิบัติการสามารถใช้งานได้อย่างมีประสิทธิภาพไม่สร้างปัญหาให้กับฐานข้อมูล	๑. เครื่องคอมพิวเตอร์ทั้งแฟ้มข้อมูลเสียหายเนื่องจากถูกไวรัสการถูกคุกคามทางอินเตอร์เน็ต	๑. ระบบคอมพิวเตอร์เสียหายไม่สามารถใช้งานได้	ปานกลาง	๑. ติดตั้งระบบปฏิบัติการให้ทำงานอย่างปลอดภัย ๒. จัดให้มีระบบการบำรุงรักษาที่ต่อเนื่องและเหมาะสม	ทุกส่วนราชการ

องค์ประกอบ	ความเสี่ยง	การวิเคราะห์ความเสี่ยง		การควบคุม	หน่วยรับผิดชอบ
		โอกาสที่จะเกิดความเสี่ยง	ระดับความเสี่ยง		
				๓. ติดตั้งระบบป้องกันการบุกรุก ๔. ติดตั้งระบบเตือนภัย	
	๒. ระบบการควบคุมความปลอดภัยจากเหตุการณ์ไฟฟ้าดับ ไฟฟ้าลัดวงจรซึ่งส่งผลให้อุปกรณ์ต่าง ๆ เกิดการเสียหาย	๒. ข้อมูลอาจเกิดความเสียหาย	ปานกลาง	ติดตั้งระบบสำรองไฟ	ทุกส่วนราชการ
๓. การบริหารจัดการวัตถุประสงค์เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพมีระบบที่เอื้ออำนายต่อการให้บริการและลดโอกาสที่จะเกิดความเสียหาย	๑. ไม่สามารถตอบสนองความต้องการด้านสารสนเทศได้อย่างทันท่วงที ๒. การให้บริการด้านสารสนเทศไม่มีประสิทธิภาพ ๓. ข้อมูลอาจถูกเปิดเผยหรือใช้โดยไม่ได้รับอนุญาต	ความเสี่ยงมีโอกาสเกิดขึ้นมีผลทำให้ไม่สามารถนำระบบสารสนเทศไปใช้ทางปฏิบัติได้ไม่สามารถเพิ่มมูลค่าให้กับองค์กรและไม่สามารถเสนอบริการใหม่ ๆ ให้กับผู้ใช้รวมทั้งทำให้ผู้บริหารขาดข้อมูลในการตัดสินใจและวางแผน	ปานกลาง	๑. วางกฎระเบียบควบคุมการปฏิบัติงาน ๒. การสอบทานกระบวนการหรือวิธีการจัดเก็บเอกสารหรือ Media ที่ใช้ประกอบการออกแบบระบบงานรวมทั้งวิธการเก็บหรือดูแลรักษา Source Program อย่างสม่ำเสมอ ๓. กำหนดให้มีการจัดทำทะเบียนคุมการติดตั้งหรือการนำ Software จากภายนอกเข้ามาใช้กับเครื่องคอมพิวเตอร์ในหน่วยงาน	ทุกส่วนราชการ

องค์ประกอบ	ความเสี่ยง	การวิเคราะห์ความเสี่ยง		การควบคุม	หน่วยรับผิดชอบ
		โอกาสที่จะเกิดความเสี่ยง	ระดับความเสี่ยง		
				๔. กำหนดผู้มีหน้าที่รับผิดชอบศึกษาทบทวนระบบรักษาความปลอดภัยและกำหนดสิทธิในการเข้าถึงระบบงานและฐานข้อมูลที่สำคัญ ๕. การปรับปรุงพัฒนา ระบบและสิทธิ User ID ในการเข้าถึงระบบงานและระบบข้อมูลเป็นระยะ ๖. จัดให้มีการตรวจสอบข้อมูลหรือเอกสารที่จะนำเข้าระบบรวมทั้งจัดให้มีการรายงานจากโปรแกรมระบบงานสำหรับใช้ในการตรวจสอบหรือสอบทานความถูกต้องของข้อมูลก่อนการส่งต่อ ๗. กำหนดระบบการจัดเก็บและสำรองแฟ้มข้อมูลฐานข้อมูลและรายงานต่าง ๆ ให้เหมาะสมกับการใช้งาน ๘. กำหนดให้มี	

องค์ประกอบ	ความเสี่ยง	การวิเคราะห์ความเสี่ยง		การควบคุม	หน่วยรับผิดชอบ
		โอกาสที่จะเกิดความเสี่ยง	ระดับความเสี่ยง		
				วิธีการ Backup หรือทำสำนา Source Program ระบบงานและเอกสารประกอบที่สำคัญอย่างน้อย ๒ ชุด และแยกสถานที่จัดเก็บ รวมทั้งจัดทำทะเบียนคุมไว้เป็นหลักฐาน ๙. จัดให้มีการสำรองข้อมูลให้ครบถ้วนตามความเหมาะสมของแต่ละระบบงานและตามเวลาที่กำหนด เช่น จัดเก็บทุกสิ้นวัน ทุกสัปดาห์ หรือทุกเดือนตามความจำเป็นและเหมาะสม ๑๐. จัดให้มีการทดสอบความถูกต้องของข้อมูลที่สำรองไว้เป็นครั้งคราว และทำรายงานผลการทดสอบ	