**นโยบายและแนวปฏิบัติการจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน (Disaster Recovery Plan)**

นโยบายและแนวปฏิบัติการจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน จัดทำขึ้นเพื่อให้ระบบสารสนเทศความปลอดภัยห้องปฏิบัติการ (Lab Safety) มีสภาพพร้อมใช้งานและให้บริการได้อย่างต่อเนื่อง อีกทั้งเพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่าย และผู้ดูแลระบบสารสนเทศถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น ดังนี้

**๑. ระบบสำรอง (Backup System)**

๑.๑ จัดทำบัญชีครุภัณฑ์เครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง โดยกองระบบและบริหารข้อมูลเชิงยุทธศาสตร์ด้านวิทยาศาสตร์ วิจัยและนวัตกรรม (กบข.)

๑.๒ ระบบสำรองต้องอยู่ในสถานที่ๆ ปลอดภัย และมีการควบคุม ดังนี้

๑) มีระบบควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

๒) มีระบบไฟฟ้าสำรอง

๓) มีระบบปรับอากาศและความชื้นที่เหมาะสม

๔) มีระบบป้องกันอัคคีภัย

๕) มีระบบส่องสว่างที่เหมาะสม

๖) มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดหรือหยุดการทำงาน

๑.๓ มีแผนบำรุงรักษาสำรองระบบที่สำคัญอย่างต่อเนื่อง

**๒. การสำรองข้อมูล (Data Backup)**

๒.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดขององค์กรที่จะทำการสำรองข้อมูล และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง โดยกองระบบและบริหารข้อมูลเชิงยุทธศาสตร์ด้านวิทยาศาสตร์ วิจัยและนวัตกรรม (กบข.)

๒.๒ กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศในแต่ละระบบ

๒.๓ กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยกำหนดให้ทำการสำรองข้อมูล แบบ Incremental ทุกวัน และแบบ Full backup ทุกสัปดาห์

๒.๔ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และข้อมูลการตั้งค่าระบบ เป็นต้น

๒.๕ จัดเก็บข้อมูลสำรองที่สำคัญไว้ในระบบสำรองส่วนกลางที่กลุ่มเทคโนโลยีสารสนเทศจัดไว้ หรือที่เครื่องของผู้รับผิดชอบดูแลในแต่ละระบบ

๒.๖ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่ใช้จัดเก็บข้อมูลสำรอง

๒.๗ มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๒.๘ มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๙ กำหนดหน้าที่ความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศและระบบสำรองกรณีเกิดเหตุการณ์ผิดปกติเกี่ยวกับเครือข่ายสื่อสาร ตามแผนเตรียมความพร้อมกรณีฉุกเฉินของ วช.

**๓. การกู้คืนข้อมูล (Data Recovery)**

๓.๑ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนการปฏิบัติอย่างสม่ำเสมอ

๓.๒ ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๓.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Last Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

๓.๔ มีการเตรียมศูนย์คอมพิวเตอร์สำรอง (DR site) ในเครือข่ายหรือการสำรองข้อมูลบนเทคโนโลยี Cloud เพื่อเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบงานตามลำดับความสำคัญคืนมาให้ใช้งานได้ภายในระยะเวลาที่เหมาะสม โดยมีการทดสอบการกู้คืนข้อมูลและตรวจสอบสภาพพร้อมใช้งานอย่างน้อยปีละ ๑ ครั้ง โดยกองระบบและบริหารข้อมูลเชิงยุทธศาสตร์ด้านวิทยาศาสตร์ วิจัยและนวัตกรรม (กบข.)