แนวทางการควบคุมภายในด้านการกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ระบบสารสนเทศเพื่อการศึกษากรุงเทพมหานคร

.....

๑. แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ ในกรณีระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียนความเสียหายหรืออันตรายใด ๆ ต่อกรุงเทพมหานคร หรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืน การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน และป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่น รวมถึงการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยได้กำหนดบทบาทและความรับผิดชอบให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ดังนี้

(๑) ผู้อำนวยการสถานศึกษา หรือรองผู้อำนวยการสถานศึกษาที่ได้รับมอบหมายให้กำกับดูแลระบบสารสนเทศเพื่อการศึกษาระดับโรงเรียน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน

(๒) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติงานในระบบสารสนเทศเพื่อการศึกษาระดับโรงเรียน เป็นผู้รับผิดชอบควบคุม ติดตาม และตรวจสอบการใช้งาน ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน

(๓) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียนตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน

<u>หน้าที่ความรับผิดชอบของผู้ดูแลระบบ</u>

(๑) จัดทำบัญชีทรัพย์สินด้านระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียนโดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

(๒) บริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์ และระบบเครือข่าย เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหาย ใช้งานไม่ได้ หรือสูญหาย

(๓) เก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

(๔) กำหนดสิทธิ์การเข้าถึงระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียนตามที่ได้รับมอบหมาย โดยกำหนดสิทธิ์ให้ผู้ใช้งานสามารถใช้งานได้ตามภารกิจของผู้ใช้งาน และสามารถเข้าใช้ได้แต่เพียงงานที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๕) บริหารจัดการการใช้งานระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียนให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันทีเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้น ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

(๖) ติดตั้งและเปลี่ยนแปลงค่าต่าง ๆ ของระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียนที่ได้รับมอบหมายและทบทวนการกำหนดค่าต่างๆ อย่างน้อยเดือนละ ๑ ครั้ง

(๗) บริหารจัดการข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงาน สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงให้มีความปลอดภัยอยู่เสมอ

(๘) จัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานและต้องเก็บรักษาไว้อย่างครบถ้วน ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศกระทรวงไอซีที เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

(๙) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

(๑๐) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

(๑๑) คืนทรัพย์สิน ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และมอบให้ผู้บริหารหรือผู้ที่ได้รับมอบหมายเพื่อทำการตรวจสอบการคืนทรัพย์สินดังกล่าวให้ถูกต้องและครบถ้วน

<u>หน้าที่ความรับผิดชอบของผู้ใช้งาน</u>

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงและใช้งานระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวทางปฏิบัติ ดังนี้

๑. การใช้งานรหัสผ่าน (Password Use) ผู้ใช้งานระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน ควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ควรกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (save password)

(๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๒) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ตนใช้งาน

(๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๕) ผู้ดูแลระบบต้องเปลี่ยนรหัสถี่กว่าผู้ใช้งานทั่วไป

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องมีการดำเนินการดังนี้

(๑) ผู้ใช้งานต้องป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

(๒) ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือไม่มีการใช้งานนานเกินกว่า ๑ ชั่วโมง

(๓) ผู้ดูแลระบบต้องสร้างความตระหนักกับผู้ใช้งานเพื่อให้เข้าใจในมาตรการป้องกันที่ได้กำหนดไว้

(๔) ผู้ใช้งานและผู้ดูแลระบบต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๕) ผู้ใช้งานและผู้ดูแลระบบต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๒๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๖) ผู้ใช้งานและผู้ดูแลระบบต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) ผู้ใช้งานต้องป้องกันทรัพย์สินของระบบงานสารสนเทศเพื่อการศึกษากรุงเทพมหานครระดับโรงเรียน และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศ ที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมเรื่องต่าง ๆ ประกอบด้วย

- การจัดการบริเวณล้อมรอบ
- การควบคุมการเข้า-ออก
- การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(๓) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(๔) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒. แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชั่นโดยไม่ได้รับอนุญาตโดยมีแนวปฏิบัติดังนี้

๒.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยมีวิธีการปฏิบัติ ดังนี้

(๑) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการพิสูจน์ตัวตนทุกครั้งของผู้ใช้งาน เมื่อมีการเข้าถึงแอพพลิเคชั่น

(๒) เจ้าของข้อมูลหรือเจ้าของระบบสารสนเทศต้องกำหนดรายการข้อมูลสำหรับการให้บริการประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้ เข้าถึง และช่องทางการเข้าถึง เป็นต้น

(๓) ผู้ดูแลระบบสารสนเทศต้องตัดเวลาในการใช้งานเครื่องลูกข่าย เมื่อไม่มีการใช้งานเป็นเวลา ๑๕ นาที หรือแล้วแต่กรณี

(๔) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ระบบสารสนเทศจำกัดเวลาการเชื่อมต่อ รวมถึงต้องระบุตัวตนก่อนการเข้าใช้งานระบบสารสนเทศใหม่ทุกครั้ง

(๕) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ระบบสารสนเทศไม่อนุญาตให้ใช้งานชื่อผู้ใช้งานซ้ำกันในเวลาเดียวกันเพื่อความปลอดภัยของระบบสารสนเทศ

(๖) ผู้ดูแลระบบสารสนเทศต้องบันทึกข้อมูลพฤติกรรมการใช้งานข้อมูลโดยจัดเก็บ log file ในการเข้าถึงระบบสารสนเทศของผู้ใช้งาน เพื่อให้สามารถตรวจสอบได้ภายหลังและนำมาวิเคราะห์ ตรวจสอบเมื่อเกิดการบุกรุกระบบสารสนเทศและระบบเครือข่าย

(๗) มีการแสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ล็อคอินเสร็จแล้ว

(๘) มีข้อความแสดงเตือน ห้ามผู้ไม่มีสิทธิ์เข้าถึงระบบงาน

(๙) มีการกำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบงานได้ ภายหลังจากที่ใส่ข้อมูลการล็อกอินผิดเกินกว่าจำนวนครั้งที่กำหนด

(๑๐) มีการส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามล็อกอินแต่ผิดพลาดเป็นจำนวนหลายครั้ง

๓. แนวปฏิบัติการจัดทำระบบสำรองข้อมูลและสารสนเทศ รวมถึงการเตรียมความพร้อมกรณีฉุกเฉิน

๓.๑ เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวปฏิบัติต่อไปนี้

(๑) มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

(๒) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- ผู้ดูแลระบบต้องกำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง โดยประกอบด้วยข้อมูลคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล
- ผู้ดูแลระบบต้องกำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)
- มีการบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ผู้ดูแลระบบต้องตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล เป็นต้น
- ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
- มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ผู้ดูแลระบบต้องทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- ผู้ดูแลระบบต้องจัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ผู้ดูแลระบบต้องกำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

(๓) การปฏิบัติเกี่ยวกับการสำรองข้อมูล ดังนี้

ชนิดอุปกรณ์	รายการ	ความถี่	ผู้รับผิดชอบ
Network Equipment	-ค่า Configuration, policy , rules	- รายสัปดาห์ - ก่อนและหลังการเปลี่ยนแปลง	- ผู้ดูแลระบบ - เจ้าของระบบงานหรือเจ้าของอุปกรณ์
Server อื่นๆ	-ค่า Configuration ของระบบปฏิบัติการ -ค่า Configuration Service ต่างๆ - ข้อมูลอื่นๆ ที่มีความสำคัญสำหรับระบบนั้นๆ	- รายสัปดาห์ - ก่อนและหลังการเปลี่ยนแปลง	- ผู้ดูแลระบบ - ผู้ดูแลระบบ Server - เจ้าของระบบงานหรือเจ้าของอุปกรณ์

(๔) ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การสำรองข้อมูลตามรายละเอียดข้างต้นนั้น ถูกต้อง สมบูรณ์หรือไม่ และมีการตรวจสอบเป็นระยะ รวมถึงการประเมินสถานที่ในการจัดเก็บข้อมูลสำรองประจำทุกปีหรือตามความเหมาะสม

(๕) สื่อบันทึกข้อมูลต้องการการเปลี่ยนแปลงตามอายุการใช้งาน

๓.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม

(๑) จัดทำแผนเตรียมความพร้อมฉุกเฉินในกรณีไม่สามารถดำเนินวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดดังนี้

- กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินของระบบเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ ฉุกเฉินจากภัยพิบัติ
- ผู้ดูแลระบบต้องทดสอบ/ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้ หากเกิดเหตุการณ์ขึ้นจริง
- ผู้ดูแลระบบต้องบันทึกเหตุการณ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น โดยพิจารณาถึงประเภท ปริมาณและหลักฐานสำหรับอ้างอิง เพื่อใช้ในกรณีที่เหตุการณ์มีความเกี่ยวข้องกับการดำเนินการ ทางกฎหมาย