นโยบายการควบคุมการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ
และการควบคุมรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

ระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น ได้จัดทำขึ้น เพื่อให้บริการแก่ประชาชนทั่วไป องค์กรปกครองส่วนท้องถิ่น และบุคลากรในสังกัดกรมส่งเสริมการปกครองท้องถิ่นในการใช้บริการเว็บไซต์ของผู้ใช้บริการจะอยู่ภายใต้เงื่อนไข และข้อกำหนด ผู้ใช้บริการจึงควรศึกษาเงื่อนไข และข้อกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศ และหรือเงื่อนไขและข้อตกลง อื่นใดที่ กรมส่งเสริมการปกครองท้องถิ่น ได้แจ้งให้ทราบบนเว็บไซต์โดยละเอียดก่อนการเข้าใช้บริการ ทั้งนี้ ในการใช้บริการ ให้ถือว่าผู้ใช้บริการได้ตกลงที่จะปฏิบัติตามเงื่อนไขและข้อกำหนดการให้บริการที่กำหนดไว้นี้ หากผู้ใช้บริการไม่ประสงค์ที่จะผูกพันตามข้อกำหนดและเงื่อนไขการให้บริการ ขอความกรุณาท่านยุติการเข้าชมและใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นนี้ ในทันที

2. เงื่อนไขและข้อกำหนดการใช้งานระบบสารสนเทศ

2.1 ผู้ใช้บริการอาจได้รับ เข้าถึง สร้าง ส่งหรือแสดงข้อมูล เช่น ไฟล์ข้อมูล ข้อความลายลักษณ์อักษร ซอฟต์แวร์คอมพิวเตอร์ ดนตรี ไฟล์เสียง หรือเสียงอื่นๆ ภาพถ่าย วิดีโอ หรือรูปภาพอื่นๆ โดยเป็นส่วนหนึ่งของบริการ หรือโดยผ่านการใช้บริการ ซึ่งต่อไปนี้จะเรียกว่า “เนื้อหา”

2.2 เนื้อหาที่นำเสนอต่อผู้ใช้บริการ อาจได้รับการคุ้มครองโดยสิทธิ์ในทรัพย์สินทางปัญญาของเจ้าของเนื้อหา นั้น ผู้ใช้บริการไม่มีสิทธิ์เปลี่ยนแปลงแก้ไข จำหน่ายจ่ายโอนหรือสร้างผลงานต่อเนื่องโดยอาศัยเนื้อหาดังกล่าว ไม่ว่าจะทั้งหมดหรือบางส่วน เว้นแต่ผู้ใช้บริการจะได้รับอนุญาตโดยชัดแจ้งจากเจ้าของเนื้อหานั้น

2.3 ผู้ใช้บริการอาจพบเนื้อหาที่ไม่เหมาะสม หรือหยาบคาย อันก่อให้เกิดความไม่พอใจ ภายใต้ความเสี่ยงของตนเอง

2.4 กรมส่งเสริมการปกครองท้องถิ่น ทรงไว้ซึ่งสิทธิ์ในการคัดกรอง ตรวจทาน ทำเครื่องหมาย เปลี่ยนแปลง แก้ไข ปฏิเสธ หรือลบเนื้อหาใดๆ ที่ไม่เหมาะสมออกจากบริการ ซึ่งกรมส่งเสริมการปกครองท้องถิ่นอาจจัดเตรียม เครื่องมือในการคัดกรองเนื้อหาอย่างชัดเจน โดยไม่ขัดต่อกฎหมาย กฎระเบียบของทางราชการที่เกี่ยวข้อง

2.5 กรมส่งเสริมการปกครองท้องถิ่น อาจหยุดให้บริการเป็นการชั่วคราวหรือถาวร หรือยกเลิกการให้บริการ แก่ผู้ใช้บริการรายใดเป็นการเฉพาะ หากการให้บริการดังกล่าวส่งผลกระทบต่อผู้ใช้บริการอื่นๆ หรือขัดแย้ง ต่อกฎหมาย โดยไม่ต้องแจ้งให้ผู้ใช้บริการทราบล่วงหน้า

2.6 การหยุดหรือการยกเลิกบริการตามข้อ 2.5 ผู้ใช้บริการจะไม่สามารถเข้าใช้บริการ และเข้าถึงรายละเอียด บัญชีของผู้ใช้บริการ ไฟล์เอกสารใดๆ หรือเนื้อหาอื่นๆ ที่อยู่ในบัญชีของผู้ใช้บริการได้

3. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

3.1 การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

3.1.1 ผู้ดูแลระบบต้องดำเนินการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่ผู้ใช้งานได้รับอนุญาตหรือได้รับการมอบอำนาจตามที่กำหนดใน “การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่”

3.1.2 ผู้ดูแลระบบมีการกำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้ อ่านข้อมูล, สร้างข้อมูล,นำเข้าข้อมูล แก้ไขข้อมูล, อนุมัติ และดูข้อมูลได้เท่านั้น

3.1.3 ผู้ดูแลระบบดำเนินการควบคุมการเข้าถึงที่เหมาะสมต่อหมวดหมู่ของสารสนเทศที่จัดไว้ตามระดับชั้นความลับ

3.1.4 ผู้ดูแลระบบมีการถอดสิทธิ์การเข้าถึงเข้าถึงการใช้งานสารสนเทศ ตามที่กำหนดใน “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

3.1.5 ผู้ดูแลระบบเป็นผู้ควบคุมการเข้าถึงจากประเภทของการเชื่อมต่อทั้งหมด

3.1.6 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน จะต้องได้รับการพิจารณาจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษรและหรือตามแบบฟอร์มที่ศูนย์เทคโนโลยีสารสนเทศท้องถิ่นกำหนด

3.1.7 ผู้ดูแลระบบกำหนดประเภทของข้อมูล ได้แก่ ข้อมูลภายนอกสามารถเปิดเผยได้ ข้อมูลภายในเป็นไปตามลำดับขั้นความลับของข้อมูล

3.1.8 ผู้ดูแลระบบกำหนดลำดับชั้นความลับของข้อมูล ได้แก่ ลับที่สุด ลับมาก ลับ และทั่วไป

3.1.9 ผู้ดูแลระบบกำหนดลำดับความสำคัญของข้อมูล ได้แก่ สำคัญมากที่สุด สำคัญมาก และทั่วไป

3.1.10 ผู้ดูแลระบบกำหนดระดับชั้นการเข้าถึง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ เจ้าของระบบ และผู้ใช้ระบบ

3.1.11 ผู้ดูแลระบบกำหนดเวลาและช่องทางที่เข้าถึงได้ ให้เหมาะสมตามแต่ละระบบงาน

3.2 การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

3.2.1 ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บริหารของหน่วยงานต้นสังกัด และเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานเพื่อเข้าใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษรและหรือตามแบบฟอร์มที่ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น กำหนด ตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

3.2.2 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบเฉพาะ ในส่วนที่จำเป็น โดยต้องคำนึงถึงประเภทข้อมูลและชั้นความลับ โดยต้องมีการอนุญาตเข้าใช้งานเป็นลายลักษณ์อักษรจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศท้องถิ่น หรือผู้อำนวยการกลุ่มงานสารสนเทศ เพื่อการจัดเก็บไว้เป็นหลักฐาน

3.2.3 เจ้าของข้อมูลและหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานหรือตามความจำเป็นขั้นต่ำเท่านั้น โดยไม่อนุญาตให้กำหนดสิทธิ์เกินความจำเป็นในการใช้งาน โดยต้องมีการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและหรือเจ้าของระบบงาน

3.3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3.3.1การลงทะเบียนเจ้าหน้าที่ใหม่กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน เจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเมื่อลาออก โอน ย้าย หรือเมื่อเปลี่ยนตำแหน่งงาน

3.3.2 ผู้ดูแลระบบกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสารสนเทศ โปรแกรมประยุกต์ (Application) ภายในหน่วยงาน จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต ระบบเครือข่ายไร้ สาย (Wireless LAN) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

3.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที

3.4.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติ ตามที่ กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

3.4.2 การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ผู้ดูแลระบบต้องปฏิบัติตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

3.4.3 กรณีผู้ดูแลระบบมีความจำเป็นต้องให้สิทธิ์เพิ่มเป็นกรณีพิเศษแก่ผู้ใช้งานที่มีสิทธิ์พื้นฐานต้อง ได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานต้นสังกัด และต้องมีการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุม เพียงพอ โดยต้องดำเนินการอย่างน้อย ดังนี้

3.4.3.1 ควบคุมการใช้งานอย่างเข้มงวดและอนุญาตให้เข้าใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

3.4.3.2 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.4.3.3 กรณีมีการใช้งานไม่ต่อเนื่อง ให้มีการเปลี่ยนรหัสผ่านทุกครั้ง ภายหลังจากเสร็จสิ้นการใช้งานในแต่ละครั้ง หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานให้มีการเปลี่ยนรหัสผ่านทุก 3 เดือน

3.4.4 กำหนดขั้นตอนในการลงทะเบียนผู้ใช้งาน (user registration) ดังนี้

3.4.4.1 มีการระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล

3.4.4.2 การกำหนดผู้ใช้งาน (Username) ให้กำหนดเป็นรหัสบัตรประจำตัวประชาชน 13 หลัก

3.4.4.3 มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาต จากหัวหน้าหน่วยงานต้นสังกัดหรือผู้ดูแลระบบของหน่วยงาน

3.4.4.4 มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศการการตัด ออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดสัญญาจ้าง เป็นต้น

3.5 การกำหนดชั้นความสำคัญหรือความลับของข้อมูล (data classification)

ใช้เกณฑ์ระดับของผู้ใช้งานระบบสารสนเทศหรือสิทธิการเข้าใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น เพื่อกำหนดระดับชั้นการเข้าถึงข้อมูล ดังนี้

3.5.1. Single Sign-On กรมส่งเสริมการปกครองท้องถิ่น

3.5.1.1 ผู้ดูแลระบบของกรมส่งเสริมการปกครองท้องถิ่น (Supper SSO-ADMIN) สามารถสร้าง ยกเลิก และกำหนดสิทธิ์ผู้ใช้งานของระบบได้

3.5.1.2 ผู้ใช้งานระดับหน่วยงาน สำนักงานส่งเสริมการปกครองท้องถิ่นจังหวัด (สถจ.), สำนักงานส่งเสริมการปกครองท้องถิ่นอำเภอ (สถอ.) และ องค์กรปกครองส่วนท้องถิ่น (อปท.) (SSO-ADMIN) สามารถสร้าง แก้ไข ลบ และกำหนดสิทธิ์ของผู้ใช้งานในหน่วยงานได้

3.5.2 ระบบงานย่อยของกรมส่งเสริมการปกครองท้องถิ่น

3.5.2.1 ผู้ดูแลระบบงานของกรมส่งเสริมการปกครองท้องถิ่น (ADMIN) สามารถกำหนดสิทธิ์การเข้าใช้งานของผู้ใช้งานทั้งหมดในระบบได้

3.5.2.2 ผู้ใช้งานระดับสำนัก/กอง สามารถเข้าถึงข้อมูลของ อปท. ได้ทั้งประเทศ

3..5.2.3 ผู้ใช้งานสำนักงานส่งเสริมการปกครองท้องถิ่นจังหวัด สามารถเข้าถึงข้อมูลของ อปท. และรับรองข้อมูลในระดับจังหวัด เฉพาะในจังหวัดเท่านั้น

3.5.2.4 ผู้ใช้งานองค์กรปกครองส่วนท้องถิ่น สามารถเข้าถึงข้อมูลเฉพาะหน่วยงานเท่านั้น

3.5.4.1 ผู้ใช้งานสำหรับการบันทึกข้อมูลต่าง ๆ (create, edit, del, export รายงาน)

3.5.4.2 ผู้ใช้งานสำหรับดูข้อมูลได้อย่างเดียว (viewer, export รายงาน)

3.5.4.3 ผู้ใช้งานสำหรับการรับรองข้อมูลในระบบ (Approve)

3.6 การควบคุมการเข้าใช้งานระบบจากภายนอก

3.6.1 ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ เพื่อขอใช้สิทธิ์ในการเข้าถึงระบบจากระยะไกล และต้องได้รับอนุมัติจากหน่วยงาน

3.6.2 ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น เป็นผู้ควบคุมการเข้าถึงระบบจากระยะไกล (Remote access)

3.6.3 ผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศท้องถิ่น หรือผู้อำนวยการกลุ่มงานสารสนเทศ และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบ และข้อมูลอย่างเคร่งครัด

3.6.4 ผู้ดูแลระบบต้องควบคุมช่องทางหรือ firewall ที่ระบบสารสนเทศเทศให้บริการ ใช้ในการเข้าสู่ระบบ อย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการ อนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

3.6.5 การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของความจำเป็นเท่านั้น และให้ปิดช่องทางเมื่อผู้ใช้งานได้ใช้งานเสร็จสิ้นแล้วทันที

3.7 การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบของหน่วยงาน ต้องผ่านการพิสูจน์ตัวตนจากระบบของ หน่วยงาน โดยมีแนวทางปฏิบัติดังนี้

3.7.1 การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)

3.7.2 การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

3.7.3 การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ตนั้น จะต้องมีการตรวจสอบผู้ใช้งาน

3.7.4 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส

3.8 การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านการบริหารรหัสผ่าน

3.8.1 ศูนย์เทคโนโลยีสารสนเทศท้องถิ่นต้องกำหนด ชื่อผู้ใช้(Username) ระบบคอมพิวเตอร์เฉพาะบุคคลไม่ซ้ำ กัน และกำหนดชื่อผู้ใช้ในส่วนของ ชื่อผู้ใช้ของผู้ใช้งาน ชื่อผู้ใช้ของผู้ดูแลระบบ ชื่อผู้ใช้ของผู้ดูแลฐานข้อมูล ชื่อผู้ใช้ของผู้พัฒนาระบบ ชื่อผู้ใช้ของเจ้าหน้าที่ทางเทคนิค หรืออื่น ๆ ให้มีความแตกต่างกัน

3.8.2 ผู้ใช้งานต้องเก็บรักษารหัสผ่าน (Password) ของตนเองและของกลุ่มไว้เป็นความลับ

3.8.3 ห้ามทำการบันทึกรหัสผ่าน (Password) ไว้ในไปรษณีย์อิเล็กทรอนิกส์ หรือแบบฟอร์มอิเล็กทรอนิกส์ ต่าง ๆ

3.8.4 ไม่จดหรือบันทึกรหัสผ่าน (Password) ส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

3.8.5 ผู้ใช้งานทุกคนต้องเปลี่ยนรหัสผ่าน (Password) เริ่มต้นทันที หลังจากได้รับมอบรหัสผ่านเริ่มต้นจาก ผู้ดูแลระบบของศูนย์เทคโนโลยีสารสนเทศท้องถิ่น

3.8.6 กำหนดให้รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยควรมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน และไม่ควรกำหนดรหัสผ่านส่วนบุคคลจาก ชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

3.8.7 ไม่ใช้รหัสผ่าน (Password) ส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

3.8.8 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับ เครื่องคอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่

3.8.9 ในกรณีที่ลืมรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบดำเนินการเปลี่ยนแปลง รหัสผ่านทันที หรือแจ้งให้ศูนย์เทคโนโลยีสารสนเทศท้องถิ่นทราบ เพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง

3.8.10 หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้น ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง

3.8.11 กรณีผู้ใช้งานของหน่วยงานภายในหน่วยงานลาออก ให้ศูนย์เทคโนโลยีสารสนเทศท้องถิ่นดำเนินการยกเลิกสิทธิ ของผู้ที่ลาออก ออกจากระบบทันที

3.8.12 กรณีผู้ใช้งานของหน่วยงานภายในหน่วยงาน มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอ สิทธิ์การใช้งาน ให้หน่วยงานต้นสังกัด แจ้งศูนย์เทคโนโลยีสารสนเทศท้องถิ่น เพื่อดำเนินการเปลี่ยนแปลงสิทธิ์ในการใช้งาน

3.8.13 ผู้ใช้งานทุกคนของหน่วยงาน มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอม ให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ของตน

4. การควบคุมการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ

การกำหนดนโยบายปรับปรุงแก้ไขเปลี่ยนแปลงระบบโดยไม่ได้รับอนุญาต อาจมีผลให้เกิดความผิดพลาด ในโปรแกรม หรือมีข้อมูลที่ไม่ถูกต้องในระบบสารสนเทศและรายงานต่าง และการแก้ไขเปลี่ยนแปลงแก้ไขฐานข้อมูลโดยตรง และอาจทำให้ระบบล้มเหลวหรือหยุดชะงักการทำงานได้ การเปลี่ยนแปลงแก้ไขระบบหรือโปรแกรมที่ใช้อยู่ จึงควรมีการกำหนดเป็นขั้นตอน โดยมีการอนุมัติและจัดทำเอกสารประกอบ โดยเจ้าหน้าที่ระบบสารสนเทศจะต้องดำเนินการควบคุมกระบวนการและขั้นตอนของการแก้ไขเปลี่ยนแปลงระบบงาน หรือโปรแกรมที่มีการเปลี่ยนแปลงแก้ไขนั้นประกอบด้วย

4.1 การกำหนดระเบียบวิธีการปฏิบัติในการเปลี่ยนแปลงแก้ไขระบบที่เป็นลายลักษณ์อักษร และมีการอนุมัติจากเจ้าของระบบงานเป็นลายลักษณ์อักษร

4.2 มีการศึกษาผลกระทบต่าง ๆ ทั้งผลกระทบงานด้านเทคนิค ผลกระทบที่มีต่อระบบอื่น และความเสี่ยงจากการเปลี่ยนแปลง

4.3 มีการทดสอบระบบที่แก้ไขแล้ว ก่อนนำมาใช้งาน

4.4 จัดทำเอกสารคู่มือประกอบการแก้ไขเปลี่ยนแปลงทั้งหมด และมีการแก้ไขเอกสารที่เกี่ยวข้อง เช่น คู่มือการใช้งาน คู่มือการแก้ไขระบบงาน และตารางการทำงานของผู้เกี่ยวของของการปฏิบัติงาน เป็นต้น

4.5 มีการประเมินผลและทดสอบระบบงานหรือโปรแกรมภายหลังจากเริ่มใช้งานในระยะเวลาหนึ่ง

5. สิทธิ หน้าที่ และความรับผิดชอบของผู้ใช้บริการ

5.1 ผู้ใช้บริการจะให้ข้อมูลเกี่ยวกับตนเอง เช่น ข้อมูลระบุตัวตนหรือรายละเอียดการติดต่อที่ถูกต้องเป็นจริง และเป็นปัจจุบันเสมอแก่กรมส่งเสริมการปกครองท้องถิ่น อันเป็นส่วนหนึ่งของกระบวนการลงทะเบียนใช้บริการ หรือการใช้บริการที่ต่อเนื่อง

5.2 ผู้ใช้บริการจะใช้บริการเว็บไซต์นี้ เพื่อวัตถุประสงค์ที่ได้รับอนุญาตตามข้อกำหนดของกรมส่งเสริมการปกครองท้องถิ่น และไม่ขัดต่อกฎหมาย กฎ ระเบียบ ข้อบังคับ หลักปฏิบัติที่เป็นที่ยอมรับโดยทั่วไป

5.3 ผู้ใช้บริการจะไม่เข้าใช้หรือพยายามเข้าใช้บริการหนึ่งบริการใดโดยวิธีอื่น รวมถึงการใช้วิธีการอัตโนมัติ (การใช้สคริปต์) นอกจากช่องทางที่กรมส่งเสริมการปกครองท้องถิ่นจัดเตรียมไว้ให้เว้นแต่ผู้ใช้บริการจะได้รับอนุญาตเป็นลายลักษณ์อักษรจากกรมส่งเสริมการปกครองท้องถิ่นกระทำได้

5.4 ผู้ใช้บริการจะไม่ทำหรือมีส่วนร่วมในการขัดขวางหรือรบกวนบริการของกรมส่งเสริมการปกครองท้องถิ่น รวมทั้งเครื่องแม่ข่ายและเครือข่ายที่เชื่อมต่อกับบริการ

5.5 ผู้ใช้บริการจะไม่ทำสำเนา คัดลอก ทำซ้ำ ขาย แลกเปลี่ยน หรือขายต่อบริการ เพื่อวัตถุประสงค์ใดๆ เว้นแต่ผู้ใช้บริการจะได้รับอนุญาตเป็นลายลักษณ์อักษรจากกรมส่งเสริมการปกครองท้องถิ่นกระทำได้

5.6 ผู้ใช้บริการมีหน้าที่ในการรักษาความลับของรหัสผ่านที่เชื่อมโยงกับบัญชีใดๆ ที่ใช้ในการเข้าถึงบริการ

5.7 ผู้ใช้บริการจะเป็นผู้รับผิดชอบแต่เพียงผู้เดียวต่อบุคคลใดๆ รวมถึงกรมส่งเสริมการปกครองท้องถิ่น ในความเสียหายอันเกิดจากการละเมิดข้อกำหนด

6. การเชื่อมโยงระบบอื่น ๆ

6.1 การเชื่อมโยงไปยังเว็บไซต์หรือระบบเทคโนโลยีสารสนเทศอื่นเป็นเพียงการให้บริการเพื่ออำนวยความสะดวกแก่ผู้ใช้บริการเท่านั้น กรมส่งเสริมการปกครองท้องถิ่นมิได้มีส่วนเกี่ยวข้องหรือมีอำนาจควบคุม รับรอง ความถูกต้องความน่าเชื่อถือ ตลอดจนความรับผิดชอบในเนื้อหาข้อมูลของเว็บไซต์นั้นๆ และกรมส่งเสริมการปกครองท้องถิ่นไม่รับผิดชอบ ต่อเนื้อหาใดๆ ที่แสดงบนเว็บไซต์อื่นที่เชื่อมโยงมายังเว็บไซต์ของกรมส่งเสริมการปกครองท้องถิ่นหรือต่อความเสียหายใดๆ ที่เกิดขึ้นจากการเข้าเยี่ยมชมเว็บไซต์ดังกล่าวการเชื่อมโยงมายังเว็บไซต์ระบบข้อมูลกลางองค์กรปกครองส่วนท้องถิ่น

6.2 กรณีต้องการเชื่อมโยงมายังเว็บไซต์หรือระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น ผู้ใช้บริการสามารถเชื่อมโยงมายังหน้าแรกของเว็บไซต์ของกรมส่งเสริมการปกครองท้องถิ่นได้ โดยแจ้งความประสงค์เป็นหนังสือ แต่หากต้องการเชื่อมโยงมายังหน้าภายในของเว็บไซต์นี้ จะต้องได้รับความยินยอมเป็นหนังสือจากกรมส่งเสริมการปกครองท้องถิ่น แล้วเท่านั้น และในการให้ความยินยอมดังกล่าว กรมส่งเสริมการปกครองท้องถิ่น ขอสงวนสิทธิ์ที่จะกำหนดเงื่อนไขใดๆ ไว้ด้วยก็ได้ ในการที่เว็บไซต์อื่นที่เชื่อมโยงมายังเว็บไซต์ของกรมส่งเสริมการปกครองท้องถิ่น จะไม่รับผิดชอบ ต่อเนื้อหาใดๆ ที่แสดงบนเว็บไซต์ที่เชื่อมโยงมายังเว็บไซต์ของกรมส่งเสริมการปกครองท้องถิ่น หรือต่อความเสียหายใดๆ ที่เกิดขึ้นจากการใช้เว็บไซต์เหล่านั้น

7. การปฏิเสธความรับผิด

กรมส่งเสริมการปกครองท้องถิ่น จะไม่รับผิดชอบต่อความเสียหายใดๆ รวมถึง ความเสียหาย สูญเสียและค่าใช้จ่ายที่เกิดขึ้นไม่ว่าโดยตรงหรือโดยอ้อม ที่เป็นผลหรือสืบเนื่องจากการที่ผู้ใช้เข้าใช้เว็บไซต์นี้ หรือเว็บไซต์ที่เชื่อมโยงกับเว็บไซต์นี้ หรือต่อความเสียหาย สูญเสียหรือค่าใช้จ่ายที่เกิดจากความล้มเหลวในการใช้งานความผิดพลาด การละเว้น การหยุดชะงัก ข้อบกพร่องความไม่สมบูรณ์ คอมพิวเตอร์ไวรัส ถึงแม้ว่ากรมส่งเสริมการปกครองท้องถิ่น จะได้รับแจ้งว่าอาจจะเกิดความเสียหาย สูญเสียหรือค่าใช้จ่ายดังกล่าวขึ้น นอกจากนี้ กรมส่งเสริมการปกครองท้องถิ่นไม่รับผิดต่อผู้ใช้เว็บไซต์หรือบุคคลจากการเรียกร้องใดๆ ที่เกิดขึ้นจากบนเว็บไซต์ หรือเนื้อหาใดๆ ซึ่งรวมถึงการตัดสินใจหรือการกระทำใดๆ ไม่ว่าความเสียหายทางตรงหรือ

ทางอ้อม รวมถึงความเสียหายอื่นใด ที่อาจเกิดขึ้นได้ผู้ใช้บริการยอมรับและตระหนักดีว่า กรมส่งเสริมการปกครองท้องถิ่นจะไม่ต้องรับผิดชอบต่อการกระทำใดของผู้ใช้บริการทั้งสิ้น

8. กรรมสิทธิ์และสิทธิในทรัพย์สินทางปัญญา

กรมส่งเสริมการปกครองท้องถิ่นหรือผู้ให้อนุญาตแก่กรมส่งเสริมการปกครองท้องถิ่น เป็นผู้มีสิทธิ ตามกฎหมาย แต่เพียงผู้เดียวในกรรมสิทธิ์ ผลประโยชน์ทั้งหมด รวมถึงสิทธิในทรัพย์สินทางปัญญาใดๆ ที่มีอยู่ในบริการ ซึ่งกรมส่งเสริมการปกครองท้องถิ่นหรือผู้ให้อนุญาตแก่กรมส่งเสริมการปกครองท้องถิ่นเป็นผู้จัดทำขึ้น ไม่ว่าสิทธิเหล่านั้นจะได้รับการจดทะเบียนไว้หรือไม่ก็ตาม

ผู้ใช้บริการจะต้องไม่เปิดเผยข้อมูลที่กรมส่งเสริมการปกครองท้องถิ่นกำหนดให้เป็นความลับ โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรล่วงหน้าจากกรมส่งเสริมการปกครองท้องถิ่น

ผู้ใช้บริการจะต้องไม่ใช้ชื่อทางการค้า เครื่องหมายการค้า เครื่องหมายการบริการ ตราสัญลักษณ์ ชื่อโดเมนของกรมส่งเสริมการปกครองท้องถิ่น โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากกรมส่งเสริมการปกครองท้องถิ่น

9. กฎหมายที่ใช้บังคับ

การตีความ และการบังคับตามเงื่อนไขการให้บริการฉบับนี้ ให้เป็นไปตามกฎหมายไทย

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมส่งเสริมการปกครองท้องถิ่น พ.ศ. ๒๕๖๗

ด้วย กรมส่งเสริมการปกครองท้องถิ่นได้จัดให้มีระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศเพื่ออำนวยความสะดวกแก่เจ้าหน้าที่ในการปฏิบัติงาน ดังนั้น เพื่อให้การใช้งานระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดจากการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง กรมส่งเสริมการปกครองท้องถิ่น จึงกำหนดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีรายละเอียด ดังต่อไปนี้

วัตถุประสงค์

เพื่อให้ผู้ใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นได้ทราบถึงข้อปฏิบัติในการใช้งานระบบสารสนเทศให้เกิดความมั่นคงปลอดภัยไม่ละเมิดระเบียบ กฎหมายหรือทำให้เกิดความเสียหายอันเนื่องมาจากการใช้งานระบบสารสนเทศ

ขอบเขต

ผู้ใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นทุกคน ต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมส่งเสริมการปกครองท้องถิ่น

นิยามศัพท์

“หน่วยงาน” หมายถึง หน่วยงานภายในสังกัดกรมส่งเสริมการปกครองท้องถิ่น

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานราชการ และลูกจ้างของหน่วยงานภายในสังกัดกรมส่งเสริมการปกครองท้องถิ่นหรือผู้ที่กรมส่งเสริมการปกครองท้องถิ่นมอบหมายให้ปฏิบัติงานตามสัญญาข้อตกลงหรือใบสั่งซื้อ

“ผู้ดูแลระบบ (System Administrator)” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

“ผู้ใช้งาน (User)” หมายถึง ผู้ที่ได้รับอนุญาต (Authorized User) จากผู้ดูแลระบบให้สามารถเข้าใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

“สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือรูปภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ

/“ระบบเครือข่าย”...

“ระบบเครือข่าย (Network System)” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบเครือข่ายภายใน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ระบบอินทราเน็ต (Intranet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

“ระบบอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ (information Technology System)” หมายถึง ระบบงานของกรมส่งเสริมการปกครองท้องถิ่นที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากผู้ดูแลระบบให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลจะเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นสูญหาย

“ชื่อผู้ใช้ (Username)” รหัสที่ผู้ดูแลระบบเป็นผู้กำหนดให้ไว้สำหรับเข้าใช้งานระบบโดยสามารถระบุถึงตัวตนของผู้ใช้งานได้

“รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“ชุดคำสั่งไม่พึงประสงค์” หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิดการห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมส่งเสริมการปกครองท้องถิ่น พ.ศ. ๒๕๖๗ แบ่งนโยบายออกเป็น ๘ หมวดดังนี้

/หมวดที่ ๑...

หมวดที่ ๑
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ว่าด้วยการใช้งานระบบสารสนเทศอย่างถูกต้อง (Acceptable User Policy)

๑.๑ การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ข้อ ๑ ผู้ใช้งานต้องทำการลงทะเบียนเพื่อขอใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น และต้องป้องกัน ดูแล รักษาข้อมูลชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีชื่อผู้ใช้ (Username) ของตนเอง ห้ามใช้งานร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากชื่อผู้ใช้ (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๓ ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่าน (Password) ไม่น้อยกว่า ๖ ตัวอักษร ควรประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)

ข้อ ๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๖๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๕ ผู้ใช้งานต้องไม่นำรหัสผ่านที่เคยใช้มาแล้วกลับมาใช้งานใหม่

ข้อ ๖ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น โดยมีแนวทางในการปฏิบัติ ดังนี้

๑) กรณีที่ผู้ใช้งานมีเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น ควรมีการตั้งค่าชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ก่อนเข้าถึงระบบปฏิบัติการเพื่อพิสูจน์ตัวตนทุกครั้ง

๒) การใช้งานระบบเครือข่ายของกรมส่งเสริมการปกครองท้องถิ่น ทั้งระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนโดยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) สามารถระบุถึงตัวบุคคลได้

๓) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ จะต้องทำการออกจากระบบโดยใช้คำสั่ง Lock หน้าจอหรือ Log off ทุกครั้ง

๔) ผู้ใช้งานต้องตั้งเวลาพักหน้าจอ (Screen Saver) เครื่องคอมพิวเตอร์ทุกครั้ง อย่างน้อย ๑๕ นาที และต้องใส่รหัสผ่าน (Password) ให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

ข้อ ๗ หากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านหรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

ข้อ ๘ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

ข้อ ๙ ผู้ดูแลระบบ (System Administrator) ต้องการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศ และปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้างโดยปฏิบัติตามแนวทาง ดังนี้

/๑) พิมพ์รายชื่อ...

๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน

๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

๓) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

๔) ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง และทบทวนสำหรับผู้ที่มีสิทธิ์ในระดับสูงด้วยความถี่มากกว่าผู้ใช้งาน

๕) เมื่อเจ้าหน้าที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้ถอดถอนสิทธิ์ภายใน ๑ – ๒ วันทำการ

๑.๒ การบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ ๑ ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server Room) ของกรมส่งเสริมการปกครองท้องถิ่นซึ่งถูกกำหนดให้เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้แลระบบ

ข้อ ๒ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server Room) เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมต่อเข้ากับระบบเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๕ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

ข้อ ๖ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่กรมส่งเสริมการปกครองท้องถิ่นมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของตนเอง

ข้อ ๗ ในกรณีที่ต้องปฏิบัติงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่นที่ได้รับมอบหมาย

ข้อ ๘ ผู้ใช้งานต้องรับผิดชอบค่าเสียหายในกรณีที่ทรัพย์สินที่อยู่ในความรับผิดชอบนั้นชำรุดหรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๙ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของตน และหากมีการเปลี่ยนแปลงผู้ใช้งานเครื่องคอมพิวเตอร์นั้น จะต้องมีการบันทึกการเปลี่ยนแปลงไว้เป็นลายลักษณ์อักษร

ข้อ ๑๐ ทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่กรมส่งเสริมการปกครองท้องถิ่นจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้ในการปฏิบัติงานของกรมส่งเสริมการปกครองท้องถิ่นเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่กรมส่งเสริมการปกครองท้องถิ่นไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๑๑ ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๑๐ ให้ถือเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๑.๓ การบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๑ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของกรมส่งเสริมการปกครองท้องถิ่น หรือเป็นข้อมูลของบุคคลภายนอก

/ข้อ ๒ ข้อมูล...

ข้อ ๒ ข้อมูลที่อยู่ภายในระบบคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่น ถือเป็นทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น สามารถนำไปเผยแพร่ได้ ยกเว้นข้อมูลที่มีการจำกัดสิทธิการเข้าถึงข้อมูล ห้ามมิให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของกรมส่งเสริมการปกครองท้องถิ่น หรือข้อมูลของผู้รับบริการหากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิดหรือนำไปเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้น

ข้อ ๔ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๕ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กรมส่งเสริมการปกครองท้องถิ่นจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้น ในกรณีที่กรมส่งเสริมการปกครองท้องถิ่นต้องการตรวจสอบข้อมูลที่คาดว่าข้อมูลนั้นเกี่ยวข้องกับกรมส่งเสริมการปกครองท้องถิ่น ซึ่งผู้ดูแลระบบสามารถทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๑.๔ การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๑ ผู้ใช้งานมีสิทธิที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ แต่ต้องไม่ดำเนินการ ดังนี้

๑) การพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกการรักษาความปลอดภัยของระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือสุ่มรหัสผ่านของบุคคลอื่น

๒) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอน (Worm) หรือไวรัสคอมพิวเตอร์ (Virus)

๓) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้งาน (License) ซอฟต์แวร์

๔) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความหรือรูปภาพที่ไม่เหมาะสมขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย ในกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๒ ห้ามมิให้ผู้ใช้งานเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent) อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ห้ามมิให้ผู้ใช้งานเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ (Online) ทุกประเภท เพื่อความบันเทิง เช่น การห้ามดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาราชการ

ข้อ ๔ ห้ามมิให้ผู้ใช้งานใช้ทรัพยากร ระบบการสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกรมส่งเสริมการปกครองท้องถิ่นในการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรมความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรมส่งเสริมการปกครองท้องถิ่น

/ข้อ ๕ ห้ามมิให้...

ข้อ ๕ ห้ามมิให้ผู้ใช้งานใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกรมส่งเสริมการปกครองท้องถิ่น ในการรบกวน ก่อให้เกิดความเสียหายหรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๖ ห้ามมิให้ผู้ใช้งานใช้ทรัพยากรทุกประเภทที่เป็นของกรมส่งเสริมการปกครองท้องถิ่น เพื่อประโยชน์ทางการค้า

ข้อ ๗ ห้ามมิให้ผู้ใช้งานกระทำการใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๘ ห้ามมิให้ผู้ใช้งานกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น ต้องหยุดชะงัก

ข้อ ๙ ห้ามมิให้ผู้ใช้งานใช้ระบบสารสนเทศของกรมส่งเสรมการปกครองท้องถิ่น เพื่อควบคุมเครื่องคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๑๐ ห้ามผู้ใช้งานกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากร

ข้อ ๑๑ ห้ามมิให้ผู้ใช้งานติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อให้สามารถเข้าถึงระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๑.๕ การใช้งานซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual Property)

ข้อ ๑ กรมส่งเสริมการปกครองท้องถิ่นได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น กรมส่งเสริมการปกครองท้องถิ่นจะอนุญาตให้ใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

ข้อ ๒ หากผู้ใช้งานมีความประสงค์จะใช้ซอฟต์แวร์ประเภท Open Source สามารถรับการสนับสนุนทางเทคนิคได้จากศูนย์เทคโนโลยีสารสนเทศท้องถิ่น เพื่อใช้งานต่อไป

ข้อ ๓ ห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ กรมส่งเสริมการปกครองท้องถิ่นถือเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๔ ซอฟต์แวร์ (Software) ที่กรมส่งเสริมการปกครองท้องถิ่นได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

ข้อ ๕ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

/๖) ผู้พัฒนา...

๖) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ

๗) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมส่งเสริมการปกครองท้องถิ่น

๑.๖ การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Preventing Malware)

ข้อ ๑ เครื่องคอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่กรมส่งเสริมการปกครองท้องถิ่นได้กำหนดให้ใช้

ข้อ ๒ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๓ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่เกิดขึ้น

ข้อ ๔ ผู้ใช้งานต้องระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้ต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๕ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบทราบ

ข้อ ๖ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่นหรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๗ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้แต่ต้องไม่ดำเนินการ ดังนี้

๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความ รูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๑.๗ การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail)

ข้อปฏิบัติให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ว่าด้วยความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

๑.๘ บทลงโทษ

กรณีที่ผู้ใช้งานไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยดังกล่าว หรือก่อให้เกิดความเสียหายต่อบุคคลอื่น หรือต่อสมบัติของทางราชการ จะต้องรับโทษตามบทลงโทษต่อไปนี้

๑) ระงับสิทธิการใช้งานระบบเครือข่ายสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นตามระยะเวลาที่เหมาะสม

๒) หากการละเมิดฝ่าฝืนนั้นก่อให้เกิดความเสียหายต่อผู้อื่น หรือต่อทรัพย์สินของทางราชการอย่างร้ายแรง จะต้องรับโทษตามระเบียบและกฎหมายที่เกี่ยวข้อง

หมวดที่ ๒
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่การใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย Wireless LAN Client และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้งานระบบเครือข่ายไร้สายอย่างถูกต้อง

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งอุปกรณ์ไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายภายในและระบบเครือข่ายไร้สายของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และจัดทำรายงานผลการตรวจสอบทุกเดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บังคับบัญชาทราบทันที

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๘ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมส่งเสริมการปกครองท้องถิ่น จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อ ๙ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

/หมวดที่ ๓...

หมวดที่ ๓
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของระบบไฟร์วอลล์ (Firewall Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องเปิดใช้งานไฟร์วอลล์ (Firewall) ตลอดเวลา

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องบันทึกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเป็นการตรวจสอบผู้ใช้งานก่อนเข้าใช้งานระบบ และควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้หรือแก้ไขเปลี่ยนแปลงข้อมูลในระบบไฟร์วอลล์ (Firewall)

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดเส้นทางการเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตตามนโยบาย (Policy)

ข้อ ๔ การเปลี่ยนแปลงการกำหนดค่า (Configuration) ทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ หรือการปรับตั้งค่าต่าง ๆ จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๕ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องสามารถเข้าถึงได้เฉพาะผู้ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๖ ข้อมูลการจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องส่งค่าไฟร์วอลล์ไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๗ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์ (Firewall) เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๙ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๐ ผู้ดูแลระบบ (System Administrator) มีสิทธิที่จะระงับการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๑ การเชื่อมต่อในลักษณะของการเข้าถึงเครือข่ายระยะไกล (Remote Login) จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

ข้อ ๑๒ หากมีการละเมิดนโยบายความมั่นคงปลอดภัยของระบบไฟร์วอลล์ (Firewall Policy) ผู้ใช้งานจะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ข้อ ๑๓ หลังจากใช้งานระบบไฟร์วอลล์ (Firewall) เสร็จสิ้น ผู้ดูแลระบบ (System Administrator) จะต้องตัดการเชื่อมต่อกับระบบไฟร์วอลล์ (Firewall) โดยการ Log out ออกจากระบบทุกครั้ง

ข้อ ๑๔ การกำหนดค่าเริ่มต้นไฟร์วอลล์ (Firewall) ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๑๕ การเชื่อมต่อในลักษณะของการควบคุมระยะไกล (Remote Login) จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ต้องดำเนินการดังนี้

/๑) ขออนุญาต...

๑) ขออนุญาตการใช้งานเป็นลายลักษณ์อักษร

๒) เก็บข้อมูล Logfile ที่ Firewall

๓) เก็บ Logfile จากตัว Application

ข้อ ๑๖ ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

หมวดที่ ๔
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ (e-mail Policy)

ข้อ ๑ ในการลงทะเบียนผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้จะต้องทำการบันทึกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ผ่านเว็บไซต์ https://mailregislocal.dla.go.th เพื่อยื่นคำขอให้ผู้ดูแลระบบ

ข้อ ๒ เมื่อผู้ใช้งานได้รับรหัสผ่าน (Password) ของระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และมีการเข้าใช้งานระบบ ต้องเปลี่ยนรหัสผ่าน (Password) โดยทันที หลังจากการเข้าสู่ระบบในครั้งแรก

ข้อ ๓ ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๓ - ๖ เดือน

ข้อ ๕ ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

ข้อ ๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรออกจากระบบโดยการ Log out ทุกครั้ง

ข้อ ๗ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

ข้อ ๘ ผู้ใช้งานควรตรวจสอบ Spam Mail ในกล่องจดหมายทุกครั้งที่ระบบหรือผู้ดูแลระบบแจ้งเตือน

ข้อ ๙ ผู้ใช้งานต้องไม่ใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ในทางที่อาจก่อให้เกิดความเสียหายต่อบุคคลหรือหน่วยงาน

ข้อ ๑๐ ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้เช่น ไม่เกิน ๓ ครั้ง

ข้อ ๑๑ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๑๒ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๑๓ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ ๑๔ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๕ ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ (E-Mail) ทุกฉบับที่ส่งไป

ข้อ ๑๖ ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ (E-Mail) ตามความจำเป็นอย่างสม่ำเสมอ

/ข้อ ๑๗ ผู้ใช้งาน...

ข้อ ๑๗ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

ข้อ ๑๘ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๙ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๒๐ ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๒๑ ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ ๒๒ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลาง เพื่อการสื่อสารในภาครัฐ

หมวดที่ ๕
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของระบบอินเทอร์เน็ต (Internet Security Policy)

ข้อ ๑ ผู้ใช้งานไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของกรมส่งเสริมการปกครองท้องถิ่น เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล หรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมอดลิขสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ห้ามมิให้ผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมส่งเสริมการปกครองท้องถิ่นที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๓ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลด (Download) โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลดการอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๔ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ โปรแกรมสนทนาหรือโปรแกรมสนทนาออนไลน์ โปรแกรมหรือเว็บไซต์ประเภทเครือข่ายสังคมออนไลน์ (Social Network) หรือสื่อสังคมออนไลน์ (Social Media) ผู้ใช้งานไม่ควรเปิดเผยข้อมูลที่สำคัญและเป็นความลับของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ โปรแกรมสนทนาหรือโปรแกรมสนทนาออนไลน์ โปรแกรมหรือเว็บไซต์ประเภทเครือข่ายสังคมออนไลน์ (Social Network) หรือสื่อสังคมออนไลน์ (Social Media) ผู้ใช้งานไม่เสนอความคิดเห็นหรือใช้ข้อความ ภาพ ภาพเคลื่อนไหว และเสียงอันเป็นเท็จ ที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมส่งเสริมการปกครองท้องถิ่นหรือการทำลายความสัมพันธ์กับบุคคลของหน่วยงานอื่น ๆ

/ข้อ ๖ หลังจาก...

ข้อ ๖ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เรียบร้อยแล้ว ผู้ใช้งานต้องตัดการเชื่อมต่อระบบโดยการ Log out ออกจากระบบอินเทอร์เน็ตทุกครั้ง เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๗ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/หรือ กฎหมาย ระเบียบ วิธีปฏิบัติทางคอมพิวเตอร์ อื่นๆ ที่เกี่ยวข้อง อย่างเคร่งครัด

หมวดที่ ๖
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy)

๖.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ ๑ กรมส่งเสริมการปกครองท้องถิ่น กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นจะต้องขออนุญาตเป็นลายลักษณ์อักษร

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น และการตรวจสอบการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออก สถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๖.๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกรมส่งเสริมการปกครองท้องถิ่น ควรกำหนดให้มีขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก การพ้นจากตำแหน่งหรือการย้ายหน่วยงาน เป็นต้น

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศ ที่สำคัญ เช่น ระบบคอมพิวเตอร์ (Computer System) โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินทราเน็ต (Intranet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของผู้ใช้งานดังต่อไปนี้

๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย และควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

/๓) ควรกำหนด...

๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่ไม่มีการป้องกันการเข้าถึงข้อมูล

๕) การกำหนดชื่อผู้ใช้ (Username) ต้องไม่ซ้ำกัน

๖) ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับการพิจารณาจากผู้ดูแลระบบ โดยมีการกำหนดระยะเวลาในการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้ชื่อผู้ใช้งานแตกต่างกันจากชื่อผู้ใช้งานตามปกติ

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานต่าง ๆ

๒) ต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนที่แท้จริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูลได้

๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔) มาตรฐานการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๕) ควรกำหนดให้มีการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดและระดับความสำคัญของข้อมูล

๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรมส่งเสริมการปกครองท้องถิ่น เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่อยู่ในสื่อบันทึกที่ส่งไปตรวจซ่อม เป็นต้น

หมวดที่ ๗
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของการตรวจจับการบุกรุก
(Intrusion Detection System/Intrusion Prevention System Policy : IDS/IPS Policy)

ข้อ ๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในกรมส่งเสริมการปกครองท้องถิ่น ให้มีความมั่นคงปลอดภัยและเป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

ข้อ ๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกรมส่งเสริมการปกครองท้องถิ่น และข้อมูลในเครือข่ายทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

/ข้อ ๔ ระบบ...

ข้อ ๔ ระบบทั้งหมดใน DMZ (Demilitarized Zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๕ โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

ข้อ ๗ มีการตรวจสอบเหตุการณ์ ข้อมูลการจราจรคอมพิวเตอร์ พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ (Firewall) ที่ใช้ในการเข้าถึงระบบเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๙ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๐ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีรายงานให้ผู้ดูแลระบบทราบทันทีที่ตรวจพบ

ข้อ ๑๑ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบจะต้องมีการรายงานให้ผู้ดูแลระบบทราบภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๓ กรมส่งเสริมการปกครองท้องถิ่น มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

ข้อ ๑๔ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกรมส่งเสริมการปกครองท้องถิ่น การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ หรือเป็นการกระทำ ที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

หมวดที่ ๘
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ว่าด้วยการบริหารจัดการการใช้บริการจากหน่วยงานภายนอก (Outsourcing Policy)

ข้อ ๑ ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูลและระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

ข้อ ๒ การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอกต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

/ข้อ ๓ การบริการ...

ข้อ ๓ การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๔ ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

ข้อ ๕ ต้องมีการทำสัญญาการรักษาความลับขององค์กร ระหว่างหน่วยงานและหน่วยงานภายนอกที่เข้ามาปฏิบัติงานก่อนเปิดให้ใช้บริการระบบเสมอ

ข้อ ๖ ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน และวิธีการดำเนินงาน เป็นอย่างน้อย เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการให้เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามขอบเขตที่ได้กำหนดไว้

ข้อ ๗ สัญญาระหว่างหน่วยงาน และ หน่วยงานภายนอก ในการให้บริการต้องระบุถึงหัวข้อต่าง ๆ ดังต่อไปนี้ เป็นอย่างน้อย

๑) รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ

๒) ระดับการให้บริการ (Service Level)

๓) หน้าที่และความรับผิดชอบขององค์การและหน่วยงานภายนอก ในการให้บริการในครั้งนี้

๔) ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้

๕) ราคา และเงื่อนไขการชำระเงิน

๖) ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)

๗) การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์การ

ประกาศ ณ วันที่ ๙ ธันวาคม พ.ศ. ๒๕๖๗

(นายเอกวิทย์ มีเพียร)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม
กรมส่งเสริมการปกครองท้องถิ่น

แผนบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ

กรมส่งเสริมการปกครองท้องถิ่น

ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

กรมส่งเสริมการปกครองท้องถิ่น

คำนำ

กรมส่งเสริมการปกครองท้องถิ่นตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น ไม่ว่าจะเป็นความเสี่ยงที่เกิดขึ้นจากธรรมชาติหรือการกระทำของมนุษย์ เช่น อัคคีภัย อุทกภัย ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ การบุกรุกหรือโจมตีจากภายนอก การก่อกวนจาก Hacker หรือการเจาะทำลายระบบจาก Cracker ไวรัสคอมพิวเตอร์ สถานการณ์ความไม่สงบ สถานการณ์โรคระบาด เป็นต้น ซึ่งสามารถสร้างความเสียหายให้กับฐานข้อมูล ระบบสารสนเทศ โปรแกรมซอฟต์แวร์ ตลอดทั้งอุปกรณ์คอมพิวเตอร์ ของกรมส่งเสริมการปกครองท้องถิ่น

กรมส่งเสริมการปกครองท้องถิ่น จึงจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมส่งเสริมการปกครองท้องถิ่น ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ เพื่อนำไปใช้เป็นกรอบแนวทางการบริหารจัดการความเสี่ยง เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ควบคุม แก้ไขความเสี่ยงและปัญหาจากภัยพิบัติด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น และเพิ่มประสิทธิภาพให้กับระบบสารสนเทศ ของกรมส่งเสริมการปกครองท้องถิ่น

คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
กรมส่งเสริมการปกครองท้องถิ่น
กันยายน ๒๕๖๗

สารบัญ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมส่งเสริมการปกครองท้องถิ่น ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

๑. หลักการและเหตุผล

กรมส่งเสริมการปกครองท้องถิ่นมีภารกิจในการส่งเสริมสนับสนุนองค์กรปกครองส่วนท้องถิ่นโดยการพัฒนาและให้คำปรึกษา แนะนำองค์กรปกครองส่วนท้องถิ่นในด้านการจัดทำแผนพัฒนาท้องถิ่น การบริหารงานบุคคล การเงินการคลัง การบริการสาธารณะ การบริหารจัดการต่าง ๆ และมีการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานด้านต่าง ๆ ขององค์กรปกครองส่วนท้องถิ่น เช่น ระบบข้อมูลกลางองค์กรปกครองส่วนท้องถิ่น (INFO) ระบบบัญชีคอมพิวเตอร์ขององค์กรปกครองส่วนท้องถิ่น (e-LAAS) ระบบสารสนเทศเพื่อการวางแผนและประเมินผลขององค์กรปกครองส่วนท้องถิ่น (e-Plan) ระบบสารสนเทศทางการศึกษาท้องถิ่น (LEC) ระบบศูนย์บริการข้อมูลบุคลากรท้องถิ่นแห่งชาติ (LHR) ระบบศูนย์ข้อมูลการเลือกตั้งท้องถิ่นแห่งชาติ (NLC) ระบบไปรษณีย์อิเล็กทรอนิกส์ (e-mail) เป็นต้น เพื่อเป็นมาตรฐานในการรักษาความปลอดภัยระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติในการบริหารจัดการความเสี่ยง การป้องกัน แก้ไขปัญหา และลดความเสียหาย อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น และเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริง และนำแนวทางจัดการความเสี่ยงไปดำเนินการแก้ไขปัญหา และเพื่อให้แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ จึงได้ปรับปรุงและทบทวนแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ ขึ้น

๒. วัตถุประสงค์

๑) เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศภายในกรมส่งเสริมการปกครองท้องถิ่น มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัว ลดโอกาสที่จะก่อให้เกิดความเสียหายต่อระบบสารสนเทศ

๒) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

๓) เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงและปัญหาจากภัยพิบัติด้านเทคโนโลยีสารสนเทศ

๔) เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

๓. ขอบเขตการดำเนินการ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมส่งเสริมการปกครองท้องถิ่น ดำเนินการภายในขอบเขตงาน ดังนี้

๑) ศึกษาขั้นตอนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒) วิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

๓) ระบุประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

๔) วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

๕) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

๖) จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

บทที่ ๑
ความหมายและกรอบการบริหารความเสี่ยง

๑. ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ หมายถึง ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้ หรือมีการเปลี่ยนแปลงเทคโนโลยีหรือนวัตกรรมต่าง ๆ อย่างเฉียบพลัน ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

๒. กรอบการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization) ประกอบด้วย ๘ ขั้นตอน ดังนี้

๒.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมขององค์การเป็นองค์ประกอบที่สำคัญในการกำหนดกรอบการบริหารความเสี่ยง และเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กร การวิเคราะห์สภาพแวดล้อมภายในองค์การจะสะท้อนการดำเนินงานชัดเจนขึ้น เมื่อพิจารณาให้ครอบคลุมถึงปัจจัยภายในและปัจจัยภายนอกที่อาจมีผลกระทบต่อองค์กร

- ปัจจัยภายใน เช่น โครงสร้างองค์การ กระบวนการและวิธีการปฏิบัติงาน วัฒนธรรมองค์การปรัชญาการบริหารความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ของผู้บริหาร
- ปัจจัยภายนอก เช่น ภาวะเศรษฐกิจ การเมืองทั้งในประเทศและต่างประเทศ ความก้าวหน้าทางเทคโนโลยี กฎเกณฑ์การกำกับดูแลของหน่วยงานที่เกี่ยวข้อง

๒.๒ การกำหนดวัตถุประสงค์ (Objective Setting)

องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยงให้มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม โดยการกำหนดวัตถุประสงค์ควรครอบคลุมวัตถุประสงค์ ด้านกลยุทธ์(Strategic Objectives) ด้านการปฏิบัติงาน (Operations Objectives) ด้านการรายงาน (Reporting Objectives) ด้านการปฏิบัติตามกฎระเบียบ (Compliance Objectives)

๒.๓ การบ่งชี้เหตุการณ์ (Event Identification)

เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร เช่น นโยบายการบริหารงาน บุคลากร ระบบสารสนเทศ ระเบียบข้อบังคับ เป็นต้น และเมื่อเกิดขึ้นแล้วส่งผลให้องค์การไม่บรรลุวัตถุประสงค์หรือเป้าหมาย ซึ่งความเสี่ยงของทุกองค์กรอาจแบ่งได้เป็น ๔ ประเภท ได้แก่

๑) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) เป็นความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ และการปฏิบัติตามแผนกลยุทธอย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมายกลยุทธ์ โครงสร้างองค์กร ทรัพยากรและสภาพแวดล้อมอันส่งผลกระทบต่อวัตถุประสงค์หรือเป้าหมายองค์กร

๒) ความเสี่ยงด้านการดำเนินงาน (Operational Risk) เป็นความเสี่ยงที่เกิดจากการปฏิบัติงานทุกๆ ขั้นตอน อันเนื่องมาจากขาดการกำกับดูแลที่ดีหรือขาดการควบคุมภายในที่ดี โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากร และความปลอดภัยของทรัพย์สิน

๓) ความเสี่ยงด้านการเงิน (Financial Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับทางด้านการเงิน สภาพคล่องทางการเงิน ความสามารถในการทำกำไรและการรายงานทางการเงิน

๔) ความเสี่ยงด้านกฎระเบียบ (Compliance Risk) เป็นความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับ

ทั้งนี้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้จัดทำคู่มือบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแบ่งประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ ๘ ประเภท ดังนี้

๑) ความเสี่ยงด้านข้อมูล (Information Risk) หมายถึง ความเสี่ยงที่เกิดจากข้อมูลต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาดโดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access Risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้เกิดการฟ้องร้องได้ หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ยังรวมไปถึงความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Backup) ที่สำคัญ คือ เพื่อไม่ให้ข้อมูล เกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูลสำรอง (Information Back-Up) การกู้คืนข้อมูล (Information Recovery)

๒) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากการเลือกใช้หรือความเสี่ยงจากการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ไม่หวังดีทำลายระบบ (Hacker) การควบคุมการ Reversion software ไม่เพียงพอ การที่ Software ที่ใช้อยู่ Out of date ความเสี่ยงที่เกิดจากการเลือกใช้ Software platforms ความเสี่ยงที่เกิดจากควบคุม การเปลี่ยนแปลง (Change control) ไม่เหมาะสมเพียงพอ ความเสี่ยงที่ไม่ได้กำหนดขั้นตอนการอนุมัติการใช้งาน Software การไม่ได้จัดทำ

ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Document operating procedures) ความเสี่ยงจากการไม่แยกระบบสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน (Separation of development, test and operation facilities) เป็นต้น

๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ความเสี่ยงในเรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงานและขององค์กร ที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการ และเหมาะสมกับงบประมาณ หรือความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงจากการที่อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุไปเอง ความเสี่ยงจากการไม่ได้กำหนด หรือกำหนดกระบวนการอนุมัติใช้อุปกรณ์เทคโนโลยีสารสนเทศไม่ชัดเจน

๔) ความเสี่ยงด้านบุคลากร (People Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศในเรื่องของการกำหนดโครงสร้าง การมอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ทั้งนี้ ยังรวมถึงการที่ขาดแผนการฝึกอบรมด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่ของหน่วยงานอย่างทั่วถึง ทั้งในส่วนของผู้ดูแลระบบ (Administration) ผู้พัฒนาระบบ (Developer/Programmer) และผู้ใช้งานทั่วไป (User) อย่างสม่ำเสมอ

๕) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่เกิดจากมนุษย์ เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย และการก่อการร้าย เป็นต้น

๖) ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบเครือข่ายสื่อสารขัดข้อง ไม่มีระบบเครือข่ายสื่อสารสำรอง ความเสี่ยงที่เกิดจากไม่ได้กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดในการบริหารจัดการสำหรับบริหารเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก การบำรุงรักษาอุปกรณ์เครือข่ายสื่อสารไม่สม่ำเสมอ การไม่มีรายชื่อและข้อมูลสำหรับติดต่อหน่วยงานอื่นกรณีมีความจำเป็น เช่น บมจ. ทศท. คอร์เปอเรชั่น บมจ. กสท. โทรคมนาคม ผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) ความเสี่ยงที่ผู้ดูแลระบบไม่มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่ายรวมทั้งสารสนเทศต่าง ๆ ที่ส่งผ่านทางเครือข่าย เป็นต้น

๗) ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้ เป็นต้น

๘) ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) หมายถึง ความเสี่ยงที่เกิดจากกระบวนการทางานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ซึ่งส่งผลให้ขาดการนำ Best Practice ที่ดีมาใช้งาน

๒.๔ การประเมินความเสี่ยง (Risk Assessment)

เป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๑) การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒) การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยง แต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

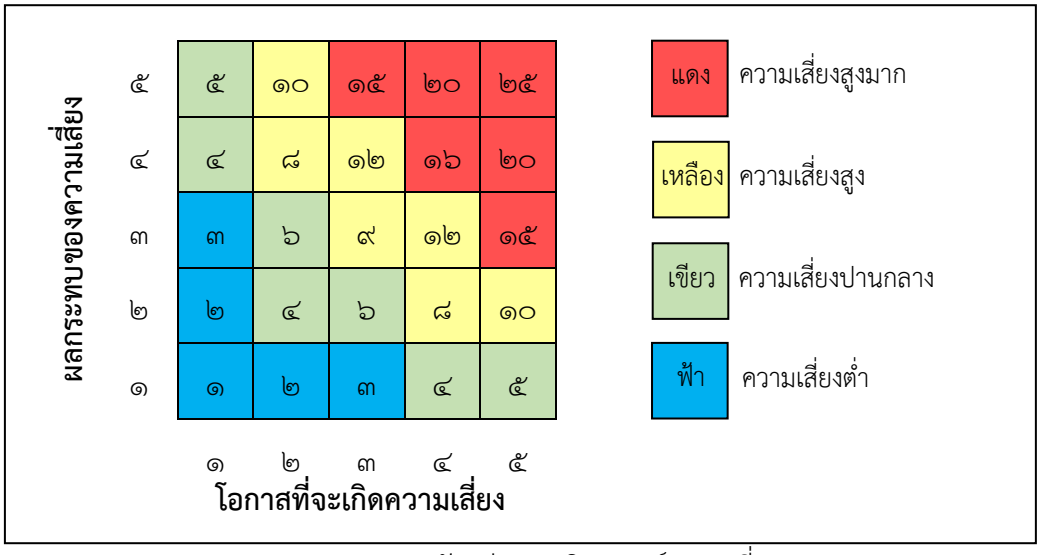
เกณฑ์การประเมินผลกระทบ เป็นดังนี้

ระดับ	การประเมิน
๑	น้อยมาก
๒	น้อย
๓	ปานกลาง
๔	สูง
๕	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง เป็นดังนี้

ระดับ	การประเมิน
๑	เกิดขึ้นน้อยมาก
๒	เกิดขึ้นน้อย
๓	เกิดขึ้นปานกลาง
๔	เกิดขึ้นสูง
๕	เกิดขึ้นสูงมาก

๓) การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน



ภาพตัวอย่างการวิเคราะห์ความเสี่ยง

๔) การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมากหรือสูง มาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๒.๕ การตอบสนองความเสี่ยง (Risk Response)

การควบคุมและบรรเทาความเสี่ยง จะขึ้นอยู่กับค่าระดับความเสี่ยงที่ประเมินได้ ทางเลือกในการควบคุมหรือบรรเทาความเสี่ยงจะมีด้วยกัน ๔ ทางเลือก ดังนี้

๑) การยอมรับความเสี่ยง (Acceptance) กรณีที่ค่าระดับความเสี่ยงอยู่ในบริเวณสีฟ้า ผู้ประเมินความเสี่ยงสามารถยอมรับความเสี่ยงได้ กรณีการยอมรับความเสี่ยงยังหมายรวมถึง

- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเขียว สีเหลือง หรือ สีแดง ก็ตาม แต่หน่วยงานยังไม่สามารถระบุมาตรการที่เหมาะสมได้ จึงอาจต้องยอมรับความเสี่ยงไว้ก่อน ในภายหลังเมื่อได้มาตรการที่เหมาะสมแล้ว จึงเสนอมาตรการเพื่อหาทางลดความเสี่ยงให้ลดลงมาอยู่ในระดับสีฟ้า เป็นต้น
- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเขียว สีเหลือง หรือ สีแดง แต่หน่วยงานพบว่าการจะจัดการกับความเสี่ยงนี้จะมีค่าใช้จ่ายที่ค่อนข้างสูงและไม่คุ้มค่าที่จะลงทุน จึงเห็นสมควรให้ยอมรับความเสี่ยงและไม่ดำเนินการใด ๆ

๒) การเลี่ยงความเสี่ยง (Avoidance) คือ การหาหนทางที่เหมาะสมเพื่อหลีกเลี่ยงความเสี่ยงที่พบนั้น เช่น หากพบว่าการนำทรัพย์สินไปตั้งไว้ในบริเวณที่มีความเสี่ยงต่อการสูญหาย ก็ควรจะหลีกเลี่ยงโดยการนำไปจัดเก็บไว้ในสถานที่ที่ปลอดภัย, การตัดสินใจที่จะแลกเปลี่ยนข้อมูลสำคัญกับองค์กรหนึ่งผ่านทางระบบออนไลน์ เมื่อพบว่าองค์กรนั้นยังไม่มีมาตรการความมั่นคงปลอดภัยที่ดีเพียงพอ ก็อาจยับยั้งการตัดสินใจนั้น โดยหลีกเลี่ยงความเสี่ยงไปใช้วิธีการแลกเปลี่ยนแบบ Manual แทน การหาหนทางที่เหมาะสมกว่า ควรพิจารณาว่าความเสี่ยงลดลงมาอยู่ในระดับที่ยอมรับได้หรือไม่ เช่น ตกอยู่ในบริเวณสีฟ้าหรือไม่

๓) การโอนย้ายความเสี่ยง (Transfer) คือ การให้หน่วยงานอื่นเป็นผู้รับความเสี่ยงหรือดำเนินการแทน เช่น การใช้ Outsource เรื่องการพัฒนาระบบให้หน่วยงานภายนอกโดยการทำสัญญาดูแลรักษาฮาร์ดแวร์ อุปกรณ์

เครือข่าย การซื้อประกันภัยจากหน่วยงานภายนอก การโอนย้ายความเสี่ยงควรพิจารณาว่า ผู้ดำเนินการสามารถจัดการความเสี่ยงนั้นได้เป็นอย่างดีหรือไม่ ระดับความเสี่ยงที่เกิดจากผู้ดำเนินการแทน ควรจะอยู่ในระดับที่หน่วยงานยอมรับได้ หากผู้ดำเนินการแทนไม่สามารถทำได้ดี ความเสี่ยงจะตกกลับมาที่หน่วยงานเอง

๔) การลดความเสี่ยง (Reduction) คือ การหาทางลดค่าความเสี่ยงที่อาจตกอยู่ในบริเวณสีเขียว สีเหลือง หรือ สีแดงก็ตาม ให้ลงมาอยู่ในระดับที่น้อยลง กรณีที่หน่วยงานสามารถลดความเสี่ยงลงมาอยู่ในบริเวณสีฟ้าได้ หน่วยงานสามารถยอมรับความเสี่ยงได้และไม่ต้องทำอะไรเพิ่มเติม แต่หากอยู่ในบริเวณสีเขียว หน่วยงานยังต้องคอยคุมความเสี่ยงไว้ (เพื่อป้องกันการเลื่อนระดับไปสู่ระดับที่สูงขึ้น) เมื่อมีการประเมินระดับความเสี่ยงในหัวข้อที่แล้ว หน่วยงานต้องพิจารณาค่าระดับความเสี่ยงนั้นและตัดสินใจว่าจะใช้ทางเลือกใด (จาก ๑ ใน ๔ ทางเลือก) เพื่อจัดการกับความเสี่ยงที่ประเมินนั้น

๒.๖ กิจกรรมการควบคุม (Control Activities)

การกำหนดกิจกรรมและการปฏิบัติต่าง ๆ เพื่อช่วยลดหรือควบคุมความเสี่ยง เพื่อสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้อง และทำให้การดำเนินงานบรรลุวัตถุประสงค์ และเป้าหมายองค์กร ป้องกันและลดระดับความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ

๒.๗ สารสนเทศและการสื่อสาร (Information and Communication)

องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงต่อไป ตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

๒.๘ การติดตามประเมินผล (Monitoring)

องค์กรจะต้องมีการติดตามผล เพื่อให้ทราบถึงผลการดำเนินงานว่าเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

บทที่ ๒
การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของกรมส่งเสริมการปกครองท้องถิ่น

๑. วิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

๑.๑ สภาพแวดล้อมภายใน

๑.๑.๑ อุปกรณ์คอมพิวเตอร์

๑.๑.๑.๑ อุปกรณ์คอมพิวเตอร์ในส่วนกลาง ได้แก่

๑) อุปกรณ์คอมพิวเตอร์ภายในห้องควบคุมระบบ (Server Room) และศูนย์ข้อมูล Data Center

ลำดับ	รายการ	ห้องควบคุมระบบ (Server Room) สถ. (เครื่อง)	ศูนย์ข้อมูล Data Center		รวม (เครื่อง)
			INET Data Center (เครื่อง)	UIH Data Center (เครื่อง)	
๑	เครื่องคอมพิวเตอร์แม่ข่าย	๕	๔๓	๙	๕๗
๒	อุปกรณ์ Web Application Firewall	-	๑	๒	๓
๓	อุปกรณ์ป้องกันการบุกรุก (Firewall)	๒	๑	๕	๘
๔	อุปกรณ์กระจายสัญญาณเครือข่าย (Switch)	๑๖	๑๓	๑๒	๔๑
๕	อุปกรณ์สำรองข้อมูลแบบ Virtual Tape	-	-	๑	๑
๖	อุปกรณ์สำรองข้อมูลแบบ Tape Library	๑	-	๑	๒
๗	อุปกรณ์จัดเก็บข้อมูลแบบภายนอก (External Storage)	๓	-	๕	๘
๘	อุปกรณ์จัดเก็บข้อมูลแบบเชื่อมต่อกับเครือข่าย (NAS)	-	๘	-	๘
๙	เครื่องสำรองไฟฟ้า (UPS)	๓	-	-	๓

๒) อุปกรณ์คอมพิวเตอร์สำนักงานและอุปกรณ์เครือข่าย (รายการที่ไม่ได้อยู่ในห้องควบคุมระบบ (Server Room) และศูนย์ข้อมูล Data Center)

ลำดับ	รายการ	รวม (เครื่อง)
๑	คอมพิวเตอร์ตั้งโต๊ะ	๗๔๒
๒	คอมพิวเตอร์โน้ตบุ๊ค	๒๑๕
๓	คอมพิวเตอร์แท็ปเล็ต	๓๐
๔	เครื่องสแกนเนอร์	๙๖
๕	เครื่องพิมพ์	๓๐๗
๖	เครื่องสำรองไฟฟ้า (UPS)	๑๐
๗	อุปกรณ์กระจายสัญญาณเครือข่าย (Switch)	๔๙

๑.๑.๑.๒ อุปกรณ์คอมพิวเตอร์ในส่วนภูมิภาค จำนวน ๗๖ จังหวัด ได้แก่

ลำดับ	รายการ	รวม (เครื่อง)
๑	คอมพิวเตอร์ตั้งโต๊ะ	๕,๕๒๕
๒	คอมพิวเตอร์โน้ตบุ๊ค	๗๑๖
๓	คอมพิวเตอร์แท็ปเล็ต	๖๓
๔	เครื่องสแกนเนอร์	๒๒๙
๕	เครื่องพิมพ์	๒,๙๒๖
๖	เครื่องสำรองไฟฟ้า (UPS)	๕๑๔
๗	อุปกรณ์กระจายสัญญาณเครือข่าย (Switch)	๗๖
๘	อุปกรณ์ป้องกันเครือข่าย (Firewall)	๗๖

*ข้อมูลอุปกรณ์คอมพิวเตอร์ ณ วันที่ ๓๐ มิถุนายน ๒๕๖๗

๑.๑.๒ ระบบสารสนเทศ / โปรแกรมซอฟต์แวร์

๑) ระบบเว็บไซต์กรมส่งเสริมการปกครองท้องถิ่น (www.dla.go.th) เป็นระบบบริหารจัดการเว็บไซต์ และแสดงเว็บไซต์ของกรมส่งเสริมการปกครองท้องถิ่น

๒) ระบบ Intranet กรมส่งเสริมการปกครองท้องถิ่น ประกอบด้วยระบบสารสนเทศ ได้แก่

-ระบบจองห้องประชุม เป็นระบบทำรายการจองใช้ห้องประชุมและตรวจสอบรายการใช้ห้องประชุมของกรมส่งเสริมการปกครองท้องถิ่น

-ระบบปฏิทินกิจกรรม เป็นระบบแจ้งกิจกรรมของกรมส่งเสริมการปกครองท้องถิ่น เช่น การประชุมประจำเดือนของกรมส่งเสริมการปกครองท้องถิ่น

-ระบบ e-Book เป็นระบบเผยแพร่และดาวน์โหลดหนังสืออิเล็กทรอนิกส์ของกรมส่งเสริมการปกครองท้องถิ่น

-ระบบ e-Library เป็นระบบเผยแพร่ แนะนำรายการหนังสือใหม่ของห้องสมุด กรมส่งเสริมการปกครองท้องถิ่น

-ระบบ KPI เป็นระบบแสดงข้อมูลตัวชี้วัดและผลการปฏิบัติราชการของกรมส่งเสริมการปกครองท้องถิ่น

-ระบบอินโฟกราฟฟิก เป็นระบบเผยแพร่ข้อมูลเกี่ยวกับภารกิจหน้าที่ และกระบวนงาน ตลอดทั้งข้อมูลที่น่าสนใจ ของกรมส่งเสริมการปกครองท้องถิ่น ในรูปแบบอินโฟกราฟฟิก (Info graphic)

-เว็บบอร์ด เป็นระบบเว็บบอร์ดสำหรับพูดคุย ตอบข้อซักถามของบุคลากรในสังกัดกรมส่งเสริมการปกครองท้องถิ่น

-ระบบเบิกจ่ายเงินค่าเช่าบ้านข้าราชการ เป็นระบบบันทึกสิทธิ์การเบิกค่าเช่าบ้าน บันทึกรายการเบิกจ่ายค่าเช่าบ้านของข้าราชการในสังกัดกรมส่งเสริมการปกครองท้องถิ่น

-ระบบพัสดุและครุภัณฑ์ เป็นระบบบันทึกข้อมูลพัสดุและครุภัณฑ์ของสำนัก/กอง ในสังกัดกรมส่งเสริมการปกครองท้องถิ่น

-ระบบเครื่องราชอิสริยาภรณ์ของบุคลากร เป็นระบบบันทึกประวัติการรับพระราชทานเครื่องราชอิสริยาภรณ์ของบุคลากรกรมส่งเสริมการปกครองท้องถิ่น

-ระบบสร้าง QR Code เป็นระบบสำหรับสร้าง QR Code สำหรับดาวน์โหลดไฟล์และเชื่อมโยงไปยังหน้าเว็บเพจที่กำหนด

๓) ระบบข้อมูลกลางองค์กรปกครองส่วนท้องถิ่น (info) เป็นระบบเผยแพร่ข้อมูลสำคัญของกรมส่งเสริมการปกครองท้องถิ่น และองค์กรปกครองส่วนท้องถิ่น เช่น ข้อมูลด้านการศึกษา (จำนวนสถานศึกษา ครู นักเรียน) ข้อมูลด้านโครงสร้างพื้นฐาน (จำนวนถนน) ข้อมูลด้านการบริหารจัดการน้ำ (จำนวนแหล่งน้ำ) เป็นต้น

๔) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นระบบงานสารบรรณของกรมส่งเสริมการปกครองท้องถิ่น สำหรับบันทึกรับ-ส่งหนังสือราชการ

๕) ระบบบริหารจัดการเอกสารแบบรวมศูนย์ (DMS) เป็นระบบบริหารจัดการข้อมูลเอกสาร จัดเก็บและเรียกดูข้อมูลในรูปแบบไฟล์ดิจิทัล

๖) ระบบไปรษณีย์อิเล็กทรอนิกส์ เป็นระบบไปรษณีย์อิเล็กทรอนิกส์ของกรมส่งเสริมการปกครองท้องถิ่น ที่ให้บริการแก่บุคลากรในสังกัด

๗) ระบบ Web Conference กรมส่งเสริมการปกครองท้องถิ่น เป็นระบบการประชุมทางไกลผ่านเครือข่ายอินเทอร์เน็ต

๘) ระบบจองห้องประชุม Conference กรมส่งเสริมการปกครองท้องถิ่น เป็นระบบสำหรับจองใช้ระบบ Web Conference ของกรมส่งเสริมการปกครองท้องถิ่น

๙) ระบบศูนย์ข้อมูล (Big Data) เพื่อสนับสนุนการตัดสินใจ และวิเคราะห์การบริหารจัดการท้องถิ่นแบบบูรณาการ เป็นระบบ Big Data ที่เชื่อมโยงข้อมูล วิเคราะห์ประมวลผลข้อมูล และแสดงรายงานเชิงบริหารสำหรับการบริหารจัดการท้องถิ่น

๑๐) ระบบช่วยตอบข้อความ ตอบคำถาม ให้ข้อมูล ในรูปแบบ Chat Bot เพื่อบริหารข้อมูลท้องถิ่นแบบอัตโนมัติ เป็นระบบตอบคำถามอัตโนมัติ แก่ประชาชนและผู้ติดต่อประสานงานกับกรมส่งเสริมการปกครองท้องถิ่น

๑๑) ระบบยืนยันตัวบุคคล DLA-SSO (Single Sign-On : SSO) เป็นการยืนยันตัวบุคคล (Authentication) ที่รองรับการให้ผู้ใช้งานลงชื่อใช้งานระบบ (Login) ครั้งเดียว แล้วสามารถใช้งานได้หลายๆ ระบบ เช่น ระบบ INFO ระบบ ELE ระบบ LHR ระบบ LPA เป็นต้น

๑๒) ระบบบริการข้อมูลกรมส่งเสริมการปกครองท้องถิ่น (WSG) เป็นระบบให้บริการเชื่อมโยงชุดข้อมูล (API) จากระบบข้อมูลกลางองค์กรปกครองส่วนท้องถิ่น (info)

๑๓) ระบบป้องกันไวรัสคอมพิวเตอร์ เป็นโปรแกรมสำหรับป้องกันการบุกรุกโจมตีคอมพิวเตอร์และเครือข่ายจากไวรัสคอมพิวเตอร์

๑๔) ระบบติดตาม (Monitor) ระบบเครือข่ายคอมพิวเตอร์ กรมส่งเสริมการปกครองท้องถิ่น เป็นระบบแสดงสถานะของเครือข่ายอินเทอร์เน็ต และอินทราเน็ต

๑๕) ระบบจัดเก็บข้อมูลอุปกรณ์เครือข่ายคอมพิวเตอร์ กรมส่งเสริมการปกครองท้องถิ่น เป็นระบบแสดงสถานะการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์

๑๖) ระบบสารสนเทศทรัพยากรบุคคลระดับกรม (DPIS) เป็นระบบบริหารจัดการเกี่ยวกับทะเบียนประวัติ ของข้าราชการ ลูกจ้างประจำ และพนักงานราชการ

๑๗) ระบบบัญชีคอมพิวเตอร์ขององค์กรปกครองส่วนท้องถิ่น (e-LAAS) เป็นระบบบริหารจัดการงบประมาณรายรับ รายจ่าย การบันทึกบัญชีและการจัดทำรายงานการเงินขององค์กรปกครองส่วนท้องถิ่น

๑๘) โปรแกรมแผนที่ภาษี (LTAXGIS ๒.๒) เป็นโปรแกรมสำหรับการจัดทำฐานข้อมูลแผนที่ภาษี สำหรับใช้ในการสำรวจข้อมูลภาคสนาม ใช้สำหรับการจัดเก็บภาษีที่ดินและสิ่งปลูกสร้าง และภาษีป้าย สำหรับองค์กรปกครองส่วนท้องถิ่น เป็นโปรแกรม Stand Alone ที่ติดตั้งในเครื่องใดก็สามารถใช้งานเฉพาะในเครื่องนั้นๆ

๑๙) โปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน (LTAX ๓๐๐๐ V๔) เป็นโปรแกรมสำหรับจัดทำฐานข้อมูลแผนที่ภาษีและทะเบียนทรัพย์สิน สำหรับใช้ในการจัดเก็บภาษีที่ดินและสิ่งปลูกสร้าง และภาษีป้าย สำหรับองค์กรปกครองส่วนท้องถิ่น เป็นโปรแกรม Stand Alone ที่ติดตั้งในเครื่องใดก็สามารถใช้งานเฉพาะในเครื่องนั้นๆ

๒๐) ระบบแผนที่ภาษีและทะเบียนทรัพย์สิน (LTAX Online) พัฒนาขึ้นมาเพื่อยกระดับโปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน (LATX ๓๐๐๐ V๔) ให้รองรับการทำงานผ่านระบบอินเทอร์เน็ตและอินทราเน็ต และให้สามารถรวบรวมข้อมูลการจัดเก็บภาษีที่ดินและสิ่งปลูกสร้างขององค์กรปกครองส่วนท้องถิ่นมาเก็บรวบรวมไว้ที่ส่วนกลางได้ เพื่อนำข้อมูลดังกล่าวมาวิเคราะห์เพื่อกำหนดนโยบายในการพัฒนารายได้ขององค์กรปกครองส่วนท้องถิ่น

๒๑) ระบบบูรณาการทะเบียนทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น (LTAX Online) พัฒนาขึ้นเพื่อยกระดับระบบแผนที่ภาษีและทะเบียนทรัพย์สิน (LTAX Online) ให้สามารถเชื่อมโยงฐานข้อมูลเกี่ยวกับที่ดินในความรับผิดชอบของกรมที่ดิน ฐานข้อมูลราคาประเมินทุนทรัพย์ของที่ดินและสิ่งปลูกสร้างในความรับผิดชอบของกรมธนารักษ์ สำหรับนำไปใช้ประโยชน์ในการจัดเก็บภาษีท้องที่ครบถ้วน ถูกต้อง และเป็นธรรม รวมถึงจัดทำโครงสร้างพื้นฐานที่จำเป็นเพื่ออำนวยความสะดวกแก่ประชาชนผู้มีหน้าที่เสียภาษีทั่วประเทศให้สามารถชำระภาษีท้องถิ่นผ่านระบบอิเล็กทรอนิกส์ (e-payment) ตามนโยบายของรัฐบาล

๒๒) ระบบศูนย์บริการข้อมูลบุคลากรท้องถิ่นแห่งชาติ (LHR) เป็นระบบฐานข้อมูลทะเบียนประวัติ ก.พ.๗ ของข้าราชการ พนักงาน ลูกจ้าง ขององค์กรปกครองส่วนท้องถิ่น สำหรับใช้วางแผนอัตรากำลัง คำนวณค่าใช้จ่ายด้านบุคลากร และการบริหารงานบุคคล

๒๓) ระบบการเรียนรู้ผ่านสื่ออิเล็กทรอนิกส์ (e-learning) กับการพัฒนาทรัพยากรบุคคลท้องถิ่น เป็นระบบที่เพิ่มโอกาศให้ทรัพยากรบุคคลได้รับการพัฒนาอย่างทั่วถึง ทันสถานการณ์ปัจจุบัน และพร้อมที่จะปรับตัวทันต่อการเปลี่ยนแปลงของโลกตลอดเวลา ส่งผลให้การปฏิบัติงานมีประสิทธิภาพและประสิทธิผลสูงสุด ตอบสนองความต้องการของประชาชนได้อย่างสะดวก รวดเร็ว และโปร่งใสผ่านระบบการเรียนแบบออนไลน์

๒๔) ระบบลงทะเบียนและบริหารจัดการหลักสูตรฝึกอบรมสถาบันพัฒนาบุคลากรท้องถิ่น เป็นระบบสำหรับลงทะเบียนเข้ารับการฝึกอบรมของข้าราชการหรือพนักงานส่วนท้องถิ่นทั่วประเทศ และบันทึกข้อมูลประวัติผู้เข้ารับการอบรม ตลอดจนประวัติการฝึกอบรม รวมไปถึงการคัดกรองของเจ้าหน้าที่ผู้ดูแลระบบในการคัดกรองผู้สมัครเข้ารับการอบรมหลักสูตรต่างๆ และยังอำนวยความสะดวกในการพิมพ์เอกสารการชำระเงินและการตรวจสอบการชำระเงินค่าลงทะเบียน

๒๕) ระบบการประเมินประสิทธิภาพองค์กรปกครองส่วนท้องถิ่น (LPA) เป็นระบบที่ใช้ในการรายงานข้อมูลการประเมินมาตรฐานการปฏิบัติราชการและนิเทศองค์กรปกครองส่วนท้องถิ่น ในมุมมองของจังหวัดและส่วนกลาง

๒๖) ระบบสารสนเทศในการการให้บริการประชาชน (Local Service) เป็นแพลตฟอร์มกลางสำหรับองค์กรปกครองส่วนท้องถิ่น (องค์การบริหารส่วนจังหวัด เทศบาล องค์การบริหารส่วนตำบล และเมืองพัทยา) สำหรับให้บริการประชาชนและสนับสนุนการปฏิบัติงานองค์กรปกครองปกครองส่วนท้องถิ่นในการอนุญาตการชำระค่าธรรมเนียม การชำระภาษี ใน ๔ กระบวนการ ได้แก่

- การยื่นแบบเพื่อชำระค่าธรรมเนียมบำรุงองค์การบริหารส่วนจังหวัดจากผู้พักโรงแรม (สำหรับองค์การบริหารส่วนจังหวัด)
- การยื่นแบบเพื่อชำระภาษีบำรุงองค์การบริหารส่วนจังหวัดจากการค้าน้ำมัน (สำหรับองค์การบริหารส่วนจังหวัด)
- การยื่นแบบเพื่อชำระภาษีบำรุงองค์การบริหารส่วนจังหวัดจาการค้ายาสูบ (สำหรับองค์การบริหารส่วนจังหวัด)

- การยื่นแบบการโฆษณาด้วยการปิด ทิ้ง หรือโปรยแผ่นประกาศในพื้นที่สารธารณะ (สำหรับเทศบาล องค์การบริหารส่วนตำบล และเมืองพัทยา)

๒๗) เว็บไซต์ศูนย์วิชาการกรมส่งเสริมการปกครองท้องถิ่น เป็นเว็บไซต์ระบบฐานข้อมูลทางวิชาการ สำหรับการเข้าถึงข้อมูลสถิติ นโยบายสำคัญของกระทรวงมหาดไทยผ่านสื่ออิเล็กทรอนิกส์

๒๘) โปรแกรมห้องสมุดอัตโนมัติ Alice for windows เป็นโปรแกรมฐานข้อมูลของห้องสมุดกรมส่งเสริมการปกครองท้องถิ่น

๒๙) ระบบสารสนเทศเพื่อขอรับการสนับสนุนงบประมาณเงินอุดหนุนขององค์กรปกครองส่วนท้องถิ่น (SOLA) เป็นระบบจัดทำคำของบประมาณเงินอุดหนุนขององค์กรปกครองส่วนท้องถิ่น

๓๐) ระบบสารสนเทศการจัดการฐานข้อมูลเบี้ยยังชีพขององค์กรปกครองส่วนท้องถิ่น (Welfare) เป็นระบบสารสนเทศในการบริหารจัดการ จัดเก็บข้อมูลผู้พิการ ผู้สูงอายุ และผู้ป่วยติดเชื้อเอดส์ เพื่อนำมาวิเคราะห์ตั้งงบประมาณสนับสนุนให้แก่องค์กรปกครองส่วนท้องถิ่น

๓๑) ระบบสารสนเทศทางการศึกษาท้องถิ่น (LEC) เป็นระบบจัดเก็บข้อมูลบุคลากรทางการศึกษา ข้อมูลนักเรียน ข้อมูลการเงิน ข้อมูลครุภัณฑ์ ข้อมูลกิจกรรมวิชาการ ข้อมูลพื้นฐานโรงเรียน/ศูนย์พัฒนาเด็กเล็ก เป็นต้น เพื่อนำไปประกอบการพิจารณาจัดสรรงบประมาณให้แก่องค์กรปกครองส่วนท้องถิ่น

๓๒) ระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น (CYCL) เป็นระบบเก็บรวบรวมข้อมูลสมาชิกสภาเด็กและเยาวชน

๓๓) ระบบฐานข้อมูล Smart Law (SLL) เป็นระบบงานเรื่องร้องทุกข์ ระบบงานสำนวนกฎหมาย และระบบสืบค้นกฎหมายของกรมส่งเสริมการปกครองท้องถิ่น

๓๔) ระบบศูนย์ข้อมูลการเลือกตั้งท้องถิ่นแห่งชาติ (NLC) เป็นระบบสำหรับจัดเก็บข้อมูลผู้บริหารท้องถิ่น คณะผู้บริหารท้องถิ่น และสมาชิกสภาท้องถิ่น รวมถึงข้อมูลอื่นๆ ที่เกี่ยวกับการเลือกตั้งขององค์กรปกครองส่วนท้องถิ่น จำนวน ๗,๘๔๙ แห่ง เพื่อเป็นข้อมูลในการบริหารงานภายใน การตรวจสอบคุณสมบัติและลักษณะต้องห้ามของผู้สมัครรับเลือกตั้งเป็นสมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่นขององค์กรปกครองส่วนท้องถิ่น การตรวจสอบลักษณะต้องห้ามสำหรับการเลือกหรือการคัดเลือกให้ดำรงตำแหน่งต่างๆ ในองค์กรอิสระ ตลอดจนให้บริการข้อมูลการดำรงตำแหน่งต่างๆ แก่หน่วยงานภาครัฐ และประชาชนทั่วไป

๓๕) ระบบสารสนเทศเพื่อการวางแผนและประเมินผลขององค์กรปกครองส่วนท้องถิ่น (e-Plan) เป็นระบบบริหารจัดการแผนพัฒนา เทศบัญญัติหรือข้อบัญญัติ ติดตามการใช้จ่ายงบประมาณ

๓๖) ระบบติดตามและประเมินผลของกรมส่งเสริมการปกครองท้องถิ่น (e-Dla Monitoring) เป็นระบบติดตามและประเมินผลขับเคลื่อนงานตามนโยบายรัฐบาล และข้อสั่งการของนายกรัฐมนตรี รัฐมนตรีว่าการกระทรวงมหาดไทย ตามอำนาจหน้าที่ที่กฎหมายกำหนด

๓๗) ระบบการเรียนรู้ออนไลน์ของกรมส่งเสริมการปกครองท้องถิ่นเพื่อพัฒนาท้องถิ่นอย่างยั่งยืน (Local MOOC) เป็นระบบที่ให้บุคลากรในสังกัดกรมส่งเสริมการปกครองท้องถิ่นทั้งส่วนกลางและส่วนภูมิภาค บุคลากรในสังกัดองค์กรปกครองส่วนท้องถิ่น ตลอดทั้งประชาชนทั่วไป สามารถเข้ามาศึกษาเรียนรู้ในรูปแบบออนไลน์ โดยมีเนื้อหาวิชาในด้านต่างๆ

๓๘) ระบบสารสนเทศด้านการจัดการขยะมูลฝอยขององค์กรปกครองส่วนท้องถิ่น (Waste) เป็นระบบสำหรับบันทึกข้อมูลการจัดการขยะขององค์กรปกครองส่วนท้องถิ่น วิธีการกำจัดขยะ สถานที่กำจัดและทิ้งขยะ และค่าใช้จ่ายในการจัดการขยะขององค์กรปกครองส่วนท้องถิ่น

๑.๑.๓ ระบบเครือข่ายอินเตอร์เน็ต

กรมส่งเสริมการปกครองท้องถิ่น มีการใช้งานระบบเครือข่ายอินเตอร์เน็ต ดังนี้

๑) ส่วนกลาง

๑.๑) เครือข่ายอินเตอร์เน็ตผ่านบริการ Leased Line Internet ซึ่งมีความเร็วในประเทศไม่น้อยกว่า ๕๐๐ Mbps และความเร็วต่างประเทศ ไม่น้อยกว่า ๒๕ เปอร์เซ็นต์ (ไม่น้อยกว่า ๑๒๕ Mbps) จำนวน ๑ วงจร

๑.๒) วงจร Internet (Fiber Optic) ขนาดไม่น้อยกว่า ๕๐ Mbps / ๒๐ Mbps (Download/Upload) แบบไม่จำกัดจำนวนผู้ใช้งานและปริมาณข้อมูล

๑.๓) ระบบเครือข่ายอินเตอร์เน็ตสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) มีความเร็วเฉลี่ย ๒ Mbps ในการ Download และ Upload

๑.๔) ระบบเครือข่ายอินเตอร์เน็ตของกระทรวงมหาดไทย สำหรับการใช้งานระบบ Web Conference ของกระทรวงมหาดไทย

๑.๕) ระบบเครือข่าย Metro Lan ขนาดความเร็วไม่น้อยกว่า ๑๐ Mbps สำหรับเชื่อมโยงข้อมูลสารสนเทศระหว่างกรมส่งเสริมการปกครองท้องถิ่น และ UIH Data Center

๑.๖) ระบบเครือข่าย KCS สำหรับเชื่อมโยงข้อมูลระบบ e-LAAS ระหว่างกรมส่งเสริมการปกครองท้องถิ่น และ UIH Data Center

๒) ส่วนภูมิภาค

๒.๑) เครือข่ายอินเตอร์เน็ตผ่านบริการ FTTx สำหรับสำนักงานท้องถิ่นจังหวัด ประกอบด้วย

- เครือข่ายอินเตอร์เน็ตความเร็วไม่น้อยกว่า ๘๐๐ Mbps / ๕๐๐ Mbps (Download/Upload)
- เครือข่ายอินเตอร์เน็ต พร้อม ๑ FixedIP ความเร็วไม่น้อยกว่า ๒๐๐ Mbps / ๒๐๐ Mbps (Download/Upload) สำหรับการใช้งานระบบ Web Conference ของกรมส่งเสริมการปกครองท้องถิ่น

๒.๒) เครือข่ายอินเตอร์เน็ตผ่านบริการ FTTx สำหรับสำนักงานท้องถิ่นอำเภอเมือง ความเร็วไม่น้อยกว่า ๕๐๐ Mbps / ๕๐๐ Mbps (Download/Upload)

๒.๓) เครือข่ายอินเตอร์เน็ตผ่านบริการ FTTx สำหรับสำนักงานท้องถิ่นอำเภอ ความเร็วไม่น้อยกว่า ๓๐๐ Mbps / ๓๐๐ Mbps (Download/Upload)

๑.๑.๓ ระบบเครือข่าย

ข้อมูลระบบเครือข่าย สำหรับเจ้าหน้าที่ผู้เกี่ยวข้องเท่านั้น

ข้อมูลระบบเครือข่าย สำหรับเจ้าหน้าที่ผู้เกี่ยวข้องเท่านั้น

๑.๑.๔ บุคลากร

กรมส่งเสริมการปกครองท้องถิ่นมีบุคลากรปฏิบัติงานประจำศูนย์เทคโนโลยีสารสนเทศท้องถิ่น ดังนี้

ตำแหน่ง	จำนวนบุคลากร	
	กรอบอัตรากำลัง	ที่มีอยู่จริง
๑. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศท้องถิ่น	๑	๑
๒. นักวิชาการคอมพิวเตอร์ ระดับชำนาญการพิเศษ	๓	๓
๓. นักวิชาการคอมพิวเตอร์ ระดับปฏิบัติการ/ชำนาญการ	๕	๔
๔. นักจัดการงานทั่วไป ระดับปฏิบัติการ/ชำนาญการ	๔	๓
๕. เจ้าพนักงานเครื่องคอมพิวเตอร์ ระดับปฏิบัติงาน/ชำนาญงาน	๑	-
๖. เจ้าพนักงานธุรการ ระดับปฏิบัติงาน/ชำนาญงาน	๕	๒
๗. พนักงานวิเคราะห์นโยบายและแผน	๓	๓
รวม	**๒๒**	**๑๖**

*ข้อมูลบุคลากร ณ วันที่ ๓๐ มิถุนายน ๒๕๖๗

๑.๒ สภาพแวดล้อมภายนอก

๑.๒.๑ ระบบสายสัญญาน

การใช้งานระบบสัญญาณอินเทอร์เน็ตของกรมส่งเสริมการปกครองท้องถิ่นใช้งานผ่าน ๒ เครือข่าย ได้แก่

๑) สัญญาณอินเทอร์เน็ตของบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (NT) เป็นเครือข่ายหลักสำหรับการใช้งานของกรมส่งเสริมการปกครองท้องถิ่นในส่วนกลางและส่วนภูมิภาค

๒) สัญญาณสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) มีการใช้งานในส่วนกลาง โดยใช้เชื่อมต่อกับสำนักทะเบียน กรมการปกครอง และกรมบัญชีกลาง

๑.๒.๒ ระบบไฟฟ้า

กรมส่งเสริมการปกครองท้องถิ่นมีการใช้ไฟฟ้าจากการไฟฟ้านครหลวง เมื่อเกิดเหตุไฟฟ้าขัดข้องอาจจะส่งผลกระทบต่ออุปกรณ์คอมพิวเตอร์และระบบสารสนเทศของกรมได้ ซึ่งได้มีการติดตั้งเครื่องสำรองไฟฟ้าเพื่อสำรองไฟฟ้าสำหรับอุปกรณ์คอมพิวเตอร์ ดังนี้

๑) ห้อง Server ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น จำนวน ๓ เครื่อง สามารถสำรองไฟฟ้าได้เป็นเวลาประมาณ ๒ ชั่วโมง

๒) คอมพิวเตอร์ตั้งโต๊ะที่ใช้ในงานสำนักงาน มีการใช้งานเครื่องสำรองไฟฟ้า จำนวน ๑๐ เครื่อง

๒. ปัจจัยความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ปัจจัยที่จะก่อให้เกิดความเสียหายด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น ได้แก่

๑) ปัจจัยภายนอก ได้แก่

๑.๑) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัย ความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

๑.๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์

๑.๓) ระบบการเชื่อมโยงเครือข่ายขัดข้อง

๑.๔) ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๑.๕) การบุกรุกหรือโจมตีจากภายนอก การก่อกวนจาก Hacker หรือการเจาะทำลายระบบจาก Cracker

๑.๖) ไวรัสคอมพิวเตอร์

๑.๗) ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

๑.๘) สถานการณ์โรคระบาด/โรคติดต่ออุบัติใหม่

๒) ปัจจัยภายใน ได้แก่

๒.๑) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๓. ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการศึกษาสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น สามารถจำแนกประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น ได้ดังนี้

๑) ความเสี่ยงด้านข้อมูล (Information Risk) เป็นความเสี่ยงที่ส่งผลให้ข้อมูลต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วน ไม่สามารถใช้ข้อมูลได้ตามปกติ และฐานข้อมูลสูญหาย ได้แก่

๑.๑) การบุกรุกหรือโจมตีจากภายนอก

๑.๒) ไวรัสคอมพิวเตอร์หรือ Malware ทำลายข้อมูล

๑.๓) การบันทึกข้อมูลไม่ถูกต้องครบถ้วน

๒) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) เป็นความเสี่ยงที่ส่งผลให้การทำงานของโปรแกรมต่าง ๆ ผิดปกติ ได้แก่

๒.๑) การบุกรุกหรือโจมตีจากภายนอก

๒.๒) ไวรัสคอมพิวเตอร์หรือ Malware บุกรุกและทำลายระบบ

๒.๓) การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง

๒.๔) ซอฟต์แวร์หมดอายุ

๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) ได้แก่

๓.๑) การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม

๓.๒) การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่มีมาตรฐาน

๔) ความเสี่ยงด้านบุคลากร (People Risk) ได้แก่

๔.๑) ขาดแคลนบุคลากรปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

๕) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) เป็นความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยจากมนุษย์ ได้แก่

๕.๑) อัคคีภัย

๕.๒) อุทกภัย/น้ำรั่วซึม

๕.๓) แผ่นดินไหว

๕.๔) ความชื้นและอุณหภูมิที่ไม่เหมาะสม

๕.๕) แมลงสัตว์กัดแทะอุปกรณ์

๕.๖) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๕.๗) ภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ

๕.๘) สถานการณ์โรคระบาด

๕.๙) การโจรกรรมอุปกรณ์คอมพิวเตอร์

๖) ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk) ได้แก่

๖.๑) การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต

๖.๒) การเชื่อมต่อระบบเครือข่ายอินทราเน็ตขัดข้อง

๗) ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) ได้แก่

๗.๑) การพัฒนา/บำรุงรักษาระบบไม่ทันกำหนด หรือไม่เป็นไปตามสัญญาจ้าง

๗.๒) การรักษาความลับของข้อมูล

๘) ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) เป็นความเสี่ยงที่เกิดจากกระบวนการทำงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ได้แก่

๘.๑) ระบบสารสนเทศไม่สอดคล้องกับระเบียบกฎหมายใหม่

๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นสามารถวิเคราะห์และประเมินระดับความเสี่ยง ได้ดังนี้

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส**X**ความรุนแรง)
IT๑	การบุกรุกหรือโจมตีจาก ภายนอก	ความเสี่ยงด้านข้อมูล และความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย	- Hacker - Cracker - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - การจัดหา พัฒนา และการบำรุงรักษาระบบสารสนเทศ ขาดความมั่นคงปลอดภัย	ฐานข้อมูล , ระบบสารสนเทศ และโปรแกรมซอฟแวร์ได้รับความเสียหายไม่สามารถใช้งานได้ตามปกติ	๒ X ๔ = ๘
IT๒	ไวรัสคอมพิวเตอร์หรือ Malware ทำลายข้อมูลและระบบ	ความเสี่ยงด้านข้อมูล และความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	ผู้ใช้งานภายในองค์กรนำอุปกรณ์ที่มีไวรัสหรือ Malware มาเชื่อมต่อกับคอมพิวเตอร์ หรือเปิดอ่านอีเมลล์ที่มีไวรัสหรือ Malware หรือดาวน์โหลดไฟล์ไวรัสมาจากเว็บไซต์	-ไวรัส/ Malware -ขาดความระมัดระวังในการเปิดใช้งานอุปกรณ์บันทึกข้อมูล การเปิดอ่านอีเมลล์ หรือการดาวน์โหลดไฟล์จากเว็บไซต์	ฐานข้อมูล , ระบบสารสนเทศ และโปรแกรมซอฟต์แวร์ได้รับความเสียหายไม่สามารถใช้งานได้ตามปกติ	๓ X ๔ = ๑๒
IT๓	การบันทึกข้อมูลไม่ถูกต้องครบถ้วน	ความเสี่ยงด้านข้อมูล	ผู้ใช้งานนำข้อมูลที่ไม่ถูกต้องหรือไม่ครบถ้วนเข้าสู่ระบบ ตลอดทั้งมีการเข้าใช้งานระบบโดยใช้ username/password ของบุคคลอื่น เพื่อเข้าถึงข้อมูลและเปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	- ขาดความระมัดระวังและความเข้าใจในการบันทึกข้อมูล - การอำพรางหรือสวมรอยผู้ใช้งาน - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ระบบฐานข้อมูลมีข้อมูลที่ไม่ครบถ้วนถูกต้อง ไม่สามารถนำข้อมูลมาใช้ประโยชน์ได้	๔ X ๒ = ๘

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส**X**ความรุนแรง)
IT๔	การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย เช่น MS Office	-การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย -ขาดงบประมาณ/ไม่มีการตั้งงบประมาณสำหรับจัดซื้อซอฟต์แวร์	หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	๑ X ๓ = ๓
IT๕	ซอฟต์แวร์หมดอายุ	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	ซอฟต์แวร์ที่ใช้อยู่หมดอายุ (Out of date) ทำให้ไม่สามารถใช้งานซอฟต์แวร์ได้	-ขาดงบประมาณ/ไม่มีการตั้งงบประมาณสำหรับจัดซื้อซอฟต์แวร์	ไม่สามารถใช้งานซอฟต์แวร์ได้	๑ X ๓ = ๓
IT๖	การติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศในพื้นที่ไม่เหมาะสม	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	การติดตั้งอุปกรณ์ในพื้นที่ที่เกิดความเสียหาย/ชำรุดได้ง่าย หรือติดตั้งในจุดที่ไม่สามารถใช้งานได้ หรือจุดอับสัญญาณ	-สภาพแวดล้อม แสงแดด น้ำฝน ทำให้อุปกรณ์ได้รับความเสียหาย -ฝาผนัง เสา กำแพง ปิดบังสัญญาณเครือข่าย	-อุปกรณ์เทคโนโลยีเสื่อมสภาพ/ชำรุด -ผู้ใช้งานไม่สามารถใช้งานอุปกรณ์ได้เต็มประสิทธิภาพ	๒ X ๓ = ๖
IT๗	เครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่มีมาตรฐาน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	ใช้งานอุปกรณ์ที่ไม่มีมาตรฐานเพียงพอ เกิดการชำรุดได้ง่าย และไม่มีความปลอดภัยเพียงพอ	-การนำเครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่มีมาตรฐานมาใช้งาน	เครื่องคอมพิวเตอร์และอุปกรณ์เกิดการชำรุดได้ง่าย และขาดความความมั่นคงปลอดภัย	๑ X ๓ = ๓
IT๘	ขาดแคลนบุคลากรปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	ความเสี่ยงด้านบุคลากร	การขาดแคลนบุคลากรด้านเทคโนโลยีสารสนเทศ อาจทำให้การทำงานหยุดชะงัก หากบุคลากร ผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน	-หน่วยงานขาดแคลนบุคลากร -การย้าย หรือออกจากราชการ โดยไม่มีบุคลากรมาทดแทน	การพัฒนาระบบ, ควบคุมดูแลระบบ และงานด้านเทคโนโลยีสารสนเทศเกิดความล่าช้า	๓ X ๒ = ๖

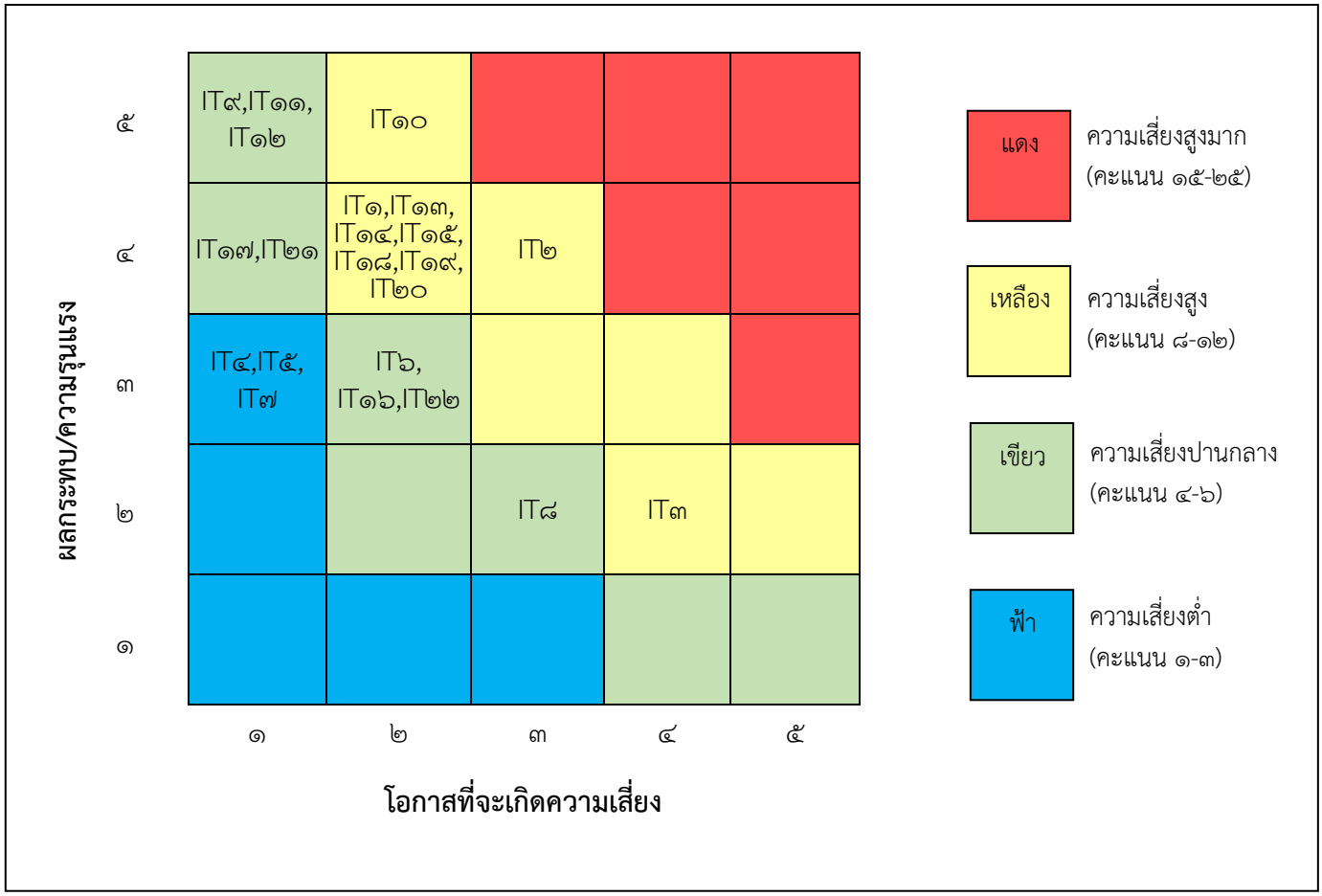
รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาสXความรุนแรง)
IT๙	อัคคีภัย	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดไฟไหม้อาคาร ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้	ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง	ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายทั้งหมดหรือบางส่วน	๑ X ๕ = ๕
IT ๑๐	อุทกภัย/น้ำรั่วซึม	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดน้ำท่วมจนต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้ หรือน้ำรั่วซึมเข้าสู่ห้องคอมพิวเตอร์แม่ข่าย	น้ำท่วมซึ่งเป็นภัยธรรมชาติ หรือน้ำรั่วซึมเข้าสู่ห้องคอมพิวเตอร์แม่ข่าย	-ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายทั้งหมดหรือบางส่วนจากน้ำท่วม -ไม่สามารถใช้งานระบบคอมพิวเตอร์ได้เนื่องจากการตัดกระแสไฟฟ้า	๒ X ๕ = ๑๐
IT ๑๑	แผ่นดินไหว	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดภัยธรรมชาติ แผ่นดินไหว อาคารได้รับความเสียหายและไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้	ภัยธรรมชาติ	ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายทั้งหมดหรือบางส่วน	๑ X ๕ = ๕
IT ๑๒	ความชื้นและอุณหภูมิที่ไม่เหมาะสม	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	ปัญหาความชื้น อุณหภูมิที่ไม่เหมาะสมภายในห้องคอมพิวเตอร์แม่ข่าย ส่งผลให้ระบบคอมพิวเตอร์ได้รับความเสียหายทั้งหมดหรือบางส่วน	ระบบควบคุมความชื้นภายในห้องคอมพิวเตอร์แม่ข่ายทำงานผิดปกติ/ชำรุด	ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายทั้งหมดหรือบางส่วน	๑ X ๕ = ๕
IT ๑๓	แมลงสัตว์กัดแทะอุปกรณ์	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	แมลงสัตว์กัดแทะอุปกรณ์ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์	สัตว์กัดแทะประเภทหนู หรือแมลง	เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ได้รับความเสียหาย	๒ X ๔ = ๘

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส**X**ความรุนแรง)
IT ๑๔	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	-เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ลูกข่าย ไม่สามารถเปิดใช้งานได้ และได้รับความเสียหาย/ชำรุด -ระบบฐานข้อมูล ระบบสารสนเทศ ไม่สามารถใช้งานได้ และอาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย	๒ X ๔ = ๘
IT ๑๕	ภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ หรือเกิดการบุกรุกและปิดล้อมหน่วยงาน	การชุมนุมประท้วง การจลาจล และการก่อการร้าย	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายได้รับความเสียหาย ไม่สามารถใช้งานได้ ซึ่งเป็นผลการทบมาจากการบุกรุกและปิดล้อมสถานที่ หรือการตัดไฟฟ้า เป็นต้น	๒ X ๔ = ๘
IT ๑๖	สถานการณ์โรคระบาด	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดสถานการณ์โรคระบาด จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	โรคระบาด โรคติดต่อที่ส่งผลกระทบต่อการเดินทางและการทำงานของบุคลากร	ผู้ใช้งานและผู้ดูแลระบบไม่สามารถปฏิบัติงานที่หน่วยงานได้ตามปกติ	๒ X ๓ = ๖

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส**X**ความรุนแรง)
IT ๑๗	การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงานได้	-การลักทรัพย์ -ขาดการดูแลรักษาความปลอดภัย	เครื่องคอมพิวเตอร์ และอุปกรณ์ไม่สามารถทำงานได้ตามปกติ	๑ X ๔ = ๔
IT ๑๘	การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง	ความเสี่ยงด้านเครือข่ายสื่อสาร	ไม่สามารถเชื่อมต่อเครือข่ายอินเทอร์เน็ตได้	-สายสัญญาณอินเทอร์เน็ตขาด/ชำรุด -สัญญาณอินเทอร์เน็ตจากผู้ให้บริการขัดข้อง	ไม่สามารถใช้งานระบบอินเทอร์เน็ตได้	๒ X ๔ = ๘
IT ๑๙	การเชื่อมต่อระบบเครือข่ายอินทราเน็ตขัดข้อง	ความเสี่ยงด้านเครือข่ายสื่อสาร	ไม่สามารถเข้าใช้ระบบงานในเครือข่ายอินทราเน็ตได้	-สายสัญญาณอินทราเน็ตชำรุด/ขัดข้อง -ระบบสารสนเทศ/ฐานข้อมูลที่ใช้งานในเครือข่ายอินทราเน็ตขัดข้อง	ผู้ใช้งานไม่สามารถใช้งานระบบอินทราเน็ตได้	๒ X ๔ = ๘
IT ๒๐	ผู้รับจ้าง (Outsource) พัฒนา/บำรุงรักษาระบบไม่ทันกำหนดหรือไม่เป็นไปตามสัญญาจ้าง	ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	ผู้รับจ้างพัฒนา/บำรุงรักษาระบบไม่ทันภายในระยะเวลาที่กำหนดหรือไม่เป็นไปตามข้อกำหนดการว่าจ้าง การปรับปรุงแก้ไขงานไม่ทันภายในระยะเวลาที่กำหนด ตลอดทั้งระบบสารสนเทศขาดความมั่นคงปลอดภัย	- Outsource ขาดบุคลากร - การเปลี่ยนตัวเจ้าหน้าที่ของ Outsource ทำให้งานไม่ต่อเนื่อง/เกิดข้อผิดพลาด - ความเข้าใจในงานไม่ตรงกัน	- การพัฒนา/บำรุงรักษาระบบไม่ทันกำหนดหรือไม่เป็นไปตามสัญญาจ้าง - ระบบสารสนเทศถูกเข้าถึงโดยผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูล	๒ X ๔ = ๘
IT ๒๑	ผู้รับจ้าง (Outsource) ไม่รักษาความลับของข้อมูล	ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	ผู้รับจ้างไม่รักษาความลับของข้อมูล เกิดการรั่วไหลของข้อมูลไปยังบุคคลภายนอก	- Outsource ไม่ดูแลรักษาข้อมูลให้เป็นความลับ - Outsource ที่หมดสัญญาเข้าใช้งานระบบสารสนเทศโดยไม่ได้รับอนุญาต	เกิดข้อมูลรั่วไหล เช่น ข้อมูลสารสนเทศ ข้อมูลระบบ ตลอดทั้งข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	๑ X ๔ = ๔
IT ๒๒	ระบบสารสนเทศไม่สอดคล้องทันสมัยกับระเบียบกฎหมาย	ความเสี่ยงด้านกระบวนการทำงาน	การปฏิบัติตามขั้นตอนใช้งานระบบสารสนเทศไม่ทันสมัยกับระเบียบกฎหมายในปัจจุบัน	-มีการพัฒนาระบบสารสนเทศ ก่อนประกาศหรือปรับปรุง ระเบียบกฎหมายที่ใช้ในปัจจุบัน	การใช้งานระบบสารสนเทศในบางขั้นตอนไม่สอดคล้อง/ทันสมัยกับระเบียบกฎหมาย	๒ X ๓ = ๖

จากการวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น สามารถนำมาอธิบายด้วยแผนภาพการวิเคราะห์ความเสี่ยง ซึ่งแสดงความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร โดยกำหนดระดับความเสี่ยงเป็น ๔ ระดับ ดังนี้

๑) ความเสี่ยงสูงมาก (คะแนน ๑๕-๒๕) มีจำนวน ๐ ข้อ
๒) ความเสี่ยงสูง (คะแนน ๘-๑๒) มีจำนวน ๑๐ ข้อ
๓) ความเสี่ยงปานกลาง (คะแนน ๔-๖) มีจำนวน ๙ ข้อ
๔) ความเสี่ยงต่ำ (คะแนน ๑-๓) มีจำนวน ๓ ข้อ



แผนภาพการวิเคราะห์ความเสี่ยง

๕. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เมื่อทำการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นแล้ว จึงจัดเรียงระดับความเสี่ยงจากความเสียงสูงไปความเสี่ยงต่ำ กำหนดกลยุทธ์การจัดการความเสี่ยงและแนวทางการดำเนินการจัดการความเสี่ยง ดังนี้

ลำดับ	ความเสี่ยง		ระดับความเสี่ยง		กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
			ระดับ	คะแนน		
๑	IT๒	ไวรัสคอมพิวเตอร์หรือ Malware ทำลายข้อมูลและระบบ	ความเสี่ยงสูง	๑๒	การลดความเสี่ยง	-ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ -ระมัดระวังการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ โดยการสแกนหาไวรัสก่อนเปิด และไม่เปิดไฟล์ที่นามสกุลแปลก -ระมัดระวังในการเปิด E-mail โดยไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา -ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต -ปิดการใช้งานฟังก์ชัน Autoplay เพื่อป้องกันไม่ให้ไวรัสที่แพร่ระบาดผ่านทางสื่อเก็บข้อมูลแบบพกพาใช้เป็นช่องทางในการรันไฟล์ไวรัสโดยอัตโนมัติ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๒	IT๑๐	อุทกภัย/น้ำรั่วซึม	ความเสี่ยงสูง	๑๐	การลดความเสี่ยง	-ติดตั้งระบบแจ้งเตือนน้ำรั่วซึมเข้าสู่ห้องคอมพิวเตอร์แม่ข่าย -มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site) -จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๓	IT๑	การบุกรุกหรือโจมตีจากภายนอก	ความเสี่ยงสูง	๘	การลดความเสี่ยง	-สแกนหาจุดอ่อนและอัพเดท Patch โดยใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่ -ติดตั้ง Firewall และตรวจสอบการตั้งค่า Policy , Log ของ Firewall อย่างสม่ำเสมอ -ติดตั้ง Proxy Server ซึ่งกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ -จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและ

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง		กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
		ระดับ	คะแนน		
					อินทราเน็ต เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป -ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอและปิดพอร์ตที่ไม่มีการใช้งาน -กำหนด password เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต -ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอก โดยการนำระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย -ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS -ประกาศใช้นโยบายการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ และการควบคุมการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๔	IT๓ การบันทึกข้อมูลไม่ถูกต้องครบถ้วน	ความเสี่ยงสูง	๘	การลดความเสี่ยง	-กำหนดให้มีการอบรมผู้ใช้งานระบบสารสนเทศ -จัดทำคู่มือการใช้งานระบบสารสนเทศ เพื่อให้ผู้ใช้งานระบบบันทึกข้อมูลได้ถูกต้องครบถ้วนตรงตามวัตถุประสงค์ของระบบสารสนเทศ -มีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศและฐานข้อมูล เพื่อให้การเข้าถึงข้อมูลเป็นไปตามสิทธิของผู้ใช้งาน -ผู้ใช้งานระบบเก็บรักษา username และ password ไว้เป็นความลับ/ไม่ให้ผู้อื่นทราบ -ประกาศใช้นโยบายการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ และการควบคุมการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ

ลำดับ	ความเสี่ยง		ระดับความเสี่ยง		กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
			ระดับ	คะแนน		
๕	IT๑๓	แมลงสัตว์กัดแทะอุปกรณ์	ความเสี่ยงสูง	๘	การลดความเสี่ยง	-ไม่นำอาหารหรือเครื่องดื่มมารับประทานหรือเก็บไว้ในบริเวณที่มีอุปกรณ์คอมพิวเตอร์ -ใช้ท่อห่อหุ้มสายไฟฟ้าหรือสายสัญญาณ เพื่อป้องกันการกัดแทะ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ(IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๖	IT๑๔	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	ความเสี่ยงสูง	๘	การลดความเสี่ยง	-ติดตั้งเครื่องสำรองไฟฟ้าให้กับเครื่องคอมพิวเตอร์แม่ข่าย -ติดตั้งเครื่องสำรองไฟฟ้าให้กับเครื่องคอมพิวเตอร์สำนักงาน และเมื่อเกิดกระแสไฟฟ้าดับ ให้รีบบันทึกข้อมูลและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ -บำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๗	IT๑๕	ภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ	ความเสี่ยงสูง	๘	การลดความเสี่ยง	-มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site) -จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๘	IT๑๘	การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง	ความเสี่ยงสูง	๘	การลดความเสี่ยง	-จัดให้มีเครือข่ายอินเทอร์เน็ตจำนวนไม่น้อยกว่า ๒ เครือข่าย ได้แก่ เครือข่ายหลัก และเครือข่ายสำรอง -บำรุงดูแลรักษาและตรวจสอบการทำงานอุปกรณ์เครือข่ายให้พร้อมใช้งานเสมอ -เมื่อเครือข่ายอินเทอร์เน็ตขัดข้อง ให้ทำการตรวจสอบอุปกรณ์และสายสัญญาณเครือข่ายอินเทอร์เน็ต/สอบถามผู้ให้บริการเครือข่ายอินเทอร์เน็ต เพื่อหาสาเหตุการขัดข้อง -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย

ลำดับ	ความเสี่ยง		ระดับความเสี่ยง		กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
			ระดับ	คะแนน		
๙	IT๑๙	การเชื่อมต่อระบบเครือข่ายอินทราเน็ตขัดข้อง	ความเสี่ยงสูง	๘	การลดความเสี่ยง	-บำรุงดูแลรักษาและตรวจสอบการทำงานอุปกรณ์เครือข่ายให้พร้อมใช้งานเสมอ -เมื่อเครือข่ายอินทราเน็ตขัดข้อง ให้ทำการตรวจสอบระบบสารสนเทศ อุปกรณ์เครือข่าย สายสัญญาณ และเครื่องคอมพิวเตอร์แม่ข่ายในระบบเครือข่ายอินทราเน็ต เพื่อหาสาเหตุการขัดข้อง -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๑๐	IT๒๐	ผู้รับจ้าง (Outsource) พัฒนา/บำรุงรักษาระบบไม่ทันกำหนดหรือไม่เป็นไปตามสัญญาจ้าง	ความเสี่ยงสูง	๘	การลดความเสี่ยง	-กำหนดเงื่อนไขสัญญาจ้างให้ชัดเจน ทั้งรายละเอียดงาน จำนวนและคุณสมบัติของบุคลากร และข้อกำหนดด้านความมั่นคงปลอดภัย -ตรวจงานจ้างตามข้อกำหนดของสัญญาจ้าง
๑๑	IT๖	การติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศในพื้นที่ไม่เหมาะสม	ความเสี่ยงปานกลาง	๖	การหลีกเลี่ยงความเสี่ยง	-มีการสำรวจความเหมาะสมจุดติดตั้งอุปกรณ์ก่อนการติดตั้ง -บำรุงดูแลรักษาอุปกรณ์ และตรวจสอบให้อยู่ในสภาพพร้อมใช้งานเสมอ
๑๒	IT๘	ขาดแคลนบุคลากรปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	ความเสี่ยงปานกลาง	๖	การโอนย้ายความเสี่ยง	-จัดหา Outsource ด้านเทคโนโลยีสารสนเทศมาช่วยปฏิบัติงาน
๑๓	IT๑๖	สถานการณ์โรคระบาด	ความเสี่ยงปานกลาง	๖	การลดความเสี่ยง	-เตรียมความพร้อม เครื่องมือและอุปกรณ์การทำงานให้เป็นอิเล็กทรอนิกส์ เพื่อรองรับนโยบาย Work From Home -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย

ลำดับ	ความเสี่ยง		ระดับความเสี่ยง		กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
			ระดับ	คะแนน		
๑๔	IT๒๒	ระบบสารสนเทศไม่สอดคล้องทันสมัยกับระเบียบกฎหมาย	ความเสี่ยงปานกลาง	๖	การลดความเสี่ยง	-ผู้ดูแลระบบมีการทบทวน/ปรับปรุงระบบสารสนเทศให้สอดคล้องทันสมัยกับระเบียบกฎหมายที่เกี่ยวข้องอย่างน้อย ๑ ครั้ง/ปี -เมื่อมีการจัดทำโครงการพัฒนา/ปรับปรุงระบบสารสนเทศ ให้เสนอโครงการ ให้คณะกรรมการพิจารณาและจัดหาระบบคอมพิวเตอร์ของ สถ. พิจารณาความเหมาะสมและให้ความเห็นชอบก่อนการจัดหาระบบสารสนเทศ -ประกาศใช้นโยบายการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ และการควบคุมการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ
๑๕	IT๙	อัคคีภัย	ความเสี่ยงปานกลาง	๕	การลดความเสี่ยง	-กำหนดเวรรักษาการณ์รักษาความปลอดภัย -ติดตั้งระบบตรวจจับควัน แจ้งเตือนเมื่อเกิดควัน/ไฟไหม้ -ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย -จัดทำเครื่องหมายระบุลำดับความสำคัญของอุปกรณ์คอมพิวเตอร์แม่ข่ายเพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน -มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site) -จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๑๖	IT๑๑	แผ่นดินไหว	ความเสี่ยงปานกลาง	๕	การลดความเสี่ยง	-มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site) -จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย

ลำดับ	ความเสี่ยง		ระดับความเสี่ยง		กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
			ระดับ	คะแนน		
๑๗	IT๑๒	ความชื้นและอุณหภูมิที่ไม่เหมาะสม	ความเสี่ยงปานกลาง	๕	การลดความเสี่ยง	-ติดตั้งระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย -ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศให้ใช้งานได้ตลอด ๒๔ ชม. -มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site) -จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๑๘	IT๑๗	การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงปานกลาง	๔	การลดความเสี่ยง	-กำหนดเวรรักษาการณ์รักษาความปลอดภัย -ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่าย -ติดตั้งระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตน (Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ -ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกพื้นที่ และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง -จัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน -มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site) -จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ -จัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นแนวทางปฏิบัติเมื่อเกิดภัย
๑๙	IT๒๑	ผู้รับจ้าง (Outsource) ไม่รักษาความลับของข้อมูล	ความเสี่ยงปานกลาง	๔	การเลี่ยงความเสี่ยง	-กำหนดเงื่อนไขสัญญาจ้างให้ชัดเจน ครอบคลุมข้อตกลงการรักษาความลับของข้อมูล และข้อกำหนดด้านความมั่นคงปลอดภัย -ทำการเปลี่ยน password การเข้าใช้ระบบ เมื่อเปลี่ยนตัวผู้รับจ้างหรือการว่าจ้างเสร็จสิ้น

ลำดับ	ความเสี่ยง		ระดับความเสี่ยง		กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
			ระดับ	คะแนน		
๒๐	IT๔	การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง	ความเสี่ยงต่ำ	๓	การเลี่ยงความเสี่ยง	-จัดหาซอฟต์แวร์ ตามคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์ของกระทรวงดิจิทัลฯ -เมื่อมีการจัดทำโครงการจัดหาซอฟต์แวร์ ให้เสนอโครงการ ให้คณะกรรมการพิจารณาและจัดหาระบบคอมพิวเตอร์ของ สถ. พิจารณาความเหมาะสมและให้ความเห็นชอบก่อนการจัดหาซอฟต์แวร์
๒๑	IT๕	ซอฟต์แวร์หมดอายุ	ความเสี่ยงต่ำ	๓	การเลี่ยงความเสี่ยง	-บำรุงรักษาระบบสารสนเทศ/ซอฟต์แวร์ และตรวจสอบอายุซอฟต์แวร์ หากพบว่าใกล้หมดอายุให้ทำการต่ออายุหรือจัดซื้อซอฟต์แวร์ใหม่ตามความเหมาะสม
๒๒	IT๗	เครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่มีมาตรฐาน	ความเสี่ยงต่ำ	๓	การเลี่ยงความเสี่ยง	-จัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ ตามคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์ของกระทรวงดิจิทัลฯ -เมื่อมีการจัดทำโครงการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ ให้เสนอโครงการให้คณะกรรมการพิจารณาและจัดหาระบบคอมพิวเตอร์ของ สถ. พิจารณาความเหมาะสมและให้ความเห็นชอบก่อนการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์

บทที่ ๓
แผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
กรมส่งเสริมการปกครองท้องถิ่น

แผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เป็นแผนในการแก้ไขความเสี่ยงจากพิบัติภัยที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ทั้งในส่วนของภัยที่มีสาเหตุมาจากธรรมชาติและภัยที่เกิดจากการกระทำของมนุษย์ เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินและลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ เป็นแนวทางในการดำเนินงานให้แก่บุคลากรให้สามารถบริหารจัดการความไม่แน่นอนที่จะเกิดขึ้นกับองค์กรได้อย่างเป็นระบบและมีประสิทธิภาพ

จากแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น นำมาจัดทำแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ โดยมีขั้นตอนการดำเนินการ ดังนี้

๑ การดำเนินการป้องกันภัยพิบัติ

๒. การเตรียมความพร้อม

๓. การกำหนดผู้รับผิดชอบ

๔. กระบวนการแก้ไขปัญหาภัยพิบัติ

๕. การกู้คืนระบบ

๖. การซ้อมแผนการแก้ไขความเสี่ยง

๗. การติดตามและรายงานผล

๑. การดำเนินการป้องกันภัยพิบัติ

จากการวิเคราะห์ความเสี่ยงในรูปแบบต่างๆ ที่อาจเกิดขึ้น เพื่อให้การบริหารที่มีการป้องกันและแก้ไขตลอดจนการจัดการกับระบบเทคโนโลยีสารสนเทศให้เป็นไปอย่างมีประสิทธิภาพ ในกรณีที่เกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติขึ้น จึงกำหนดแนวทางการดำเนินการเบื้องต้น ดังนี้

๑.๑) การตรวจสอบ วิเคราะห์ และสรุปสาเหตุเบื้องต้น การสังเกตอาการหรือเหตุอันผิดปกติ มี ๒ องค์ประกอบ คือ

(๑) ทางกายภาพ สภาพอันผิดปกติ เช่น กลิ่น อุณหภูมิ ไฟฟ้าดับ เสียง อาการสั่น

(๒) การทำงานของระบบ เช่น ไม่สามารถเข้าระบบงานได้ ระบบทำงานช้ากว่าปกติ โดยไม่มีสาเหตุ ระบบไม่ทำงานผิดพลาดแต่มีข้อความแจ้งเหตุอันผิดปกติ

๑.๒) การแจ้งเหตุ

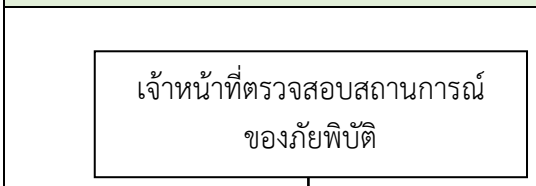
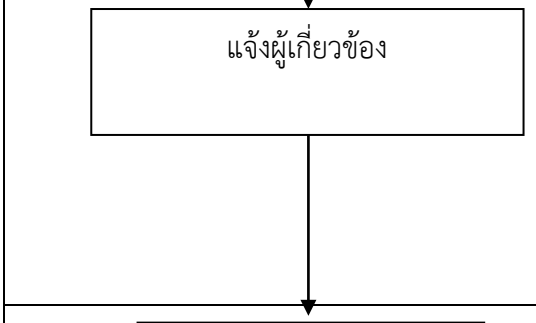
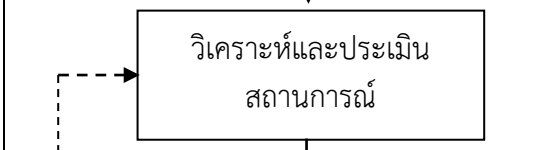
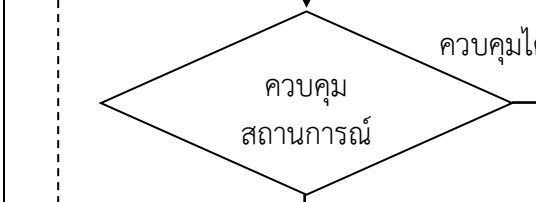
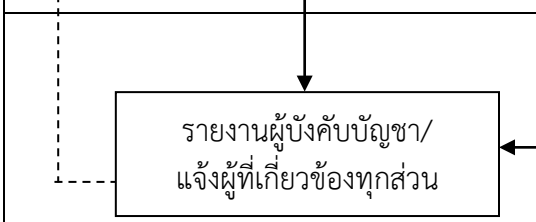
(๑) แจ้งเหตุกรณีเร่งด่วน ประสานแจ้งผู้ที่เกี่ยวข้องโดยตรง ได้แก่ เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น

(๒) แจ้งเหตุกรณีปกติ สรุปสาเหตุและจัดทำรายงานแจ้งไปยังผู้ที่เกี่ยวข้อง และเจ้าหน้าที่ผู้รับผิดชอบรายงานผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

๑.๓) การประเมินสถานการณ์ โดยการแจ้งผู้รับผิดชอบหรือเจ้าหน้าที่ที่ประจำ ณ จุดเกิดเหตุ

๑.๔) ปฏิบัติตามแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ

แนวทางการดำเนินการเบื้องต้น

กระบวนงาน	รายละเอียด
	เจ้าหน้าที่ผู้รับผิดชอบเข้าตรวจสอบสถานการณ์
	ประสานแจ้งผู้ที่เกี่ยวข้องให้รับทราบ ได้แก่ -เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น -เจ้าหน้าที่ผู้รับผิดชอบระบบสารสนเทศของสำนัก/กอง -เจ้าหน้าที่กองคลังกรณีเกิดความเสียหายต่อครุภัณฑ์คอมพิวเตอร์
	วิเคราะห์และประเมินสถานการณ์
	หากควบคุมได้สถานการณ์ ให้ปฏิบัติตามแผนป้องกันและแก้ไขปัญหาภัยพิบัติ และรายงานผู้บังคับบัญชาและแจ้งผู้เกี่ยวข้อง
	หากควบคุมไม่ได้สถานการณ์ ให้รายงานผู้บังคับบัญชาทราบและแจ้งผู้ที่เกี่ยวข้องทุกส่วนเตรียมพร้อมปฏิบัติงานตามคำสั่ง

กรมส่งเสริมการปกครองท้องถิ่นมีการดำเนินการบริหารจัดการความเสี่ยงและป้องกันภัยด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นและมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น ดังนี้

๑) การบุกรุกหรือโจมตีจากภายนอก

ภัยจากการบุกรุกหรือโจมตีจากภายนอกเพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายฐานข้อมูล หรือการก่อกวนจาก Hacker หรือการเจาะทำลายระบบจาก Cracker ดำเนินการ ดังนี้

๑.๑) สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๑.๒) ติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่นได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

๑.๓) ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตของกรมส่งเสริมการปกครองท้องถิ่นและ กลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

๑.๔) จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ตของกรมส่งเสริมการปกครองท้องถิ่น เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๑.๕) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน

๑.๖) ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอก โดยการนำระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย

๑.๗) ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS

๒) ไวรัสคอมพิวเตอร์หรือ Malware

๒.๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอและต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๒.๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

๒.๒.๑) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

๒.๒.๒) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

๒.๒.๓) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๒.๓) ใช้ความระมัดระวังในการเปิด E-mail

๒.๓.๑) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

๒.๓.๒) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๒.๔) ปิดการใช้งานฟังก์ชัน Autoplay เพื่อป้องกันไม่ให้ไวรัสที่แพร่ระบาดผ่านทางสื่อเก็บข้อมูลแบบพกพาใช้เป็นช่องทางในการรันไฟล์ไวรัสโดยอัตโนมัติ

๓) อัคคีภัย

๓.๑) กำหนดเวรรักษาการณ์รักษาความปลอดภัย

๓.๒) ติดตั้งระบบตรวจจับควัน แจ้งเตือนเมื่อเกิดควัน/ไฟไหม้

๓.๓) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย

๓.๔) จัดทำเครื่องหมายระบุลำดับความสำคัญของอุปกรณ์คอมพิวเตอร์แม่ข่ายเพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

๓.๕) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site)

๓.๖) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๔) อุทกภัย/น้ำรั่วซึม

๔.๑) เจ้าหน้าที่ที่เกี่ยวข้อง ติดตามข่าวสารภัยพิบัติตามสถานการณ์ที่เกิดขึ้น

๔.๒) ติดตั้งระบบแจ้งเตือนน้ำรั่วซึมเข้าสู่ห้องคอมพิวเตอร์แม่ข่าย

๔.๓) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site)

๔.๔) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๕) แผ่นดินไหว

๕.๑) เจ้าหน้าที่ที่เกี่ยวข้อง ติดตามข่าวสารภัยพิบัติตามสถานการณ์ที่เกิดขึ้น

๔.๒) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site)

๔.๓) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๖) ความชื้นและอุณหภูมิที่ไม่เหมาะสม

๖.๑) ติดตั้งระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย

๖.๒) ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศให้ใช้งานได้ตลอด ๒๔ ชม.

๖.๓) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site)

๖.๔) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๗) แมลงสัตว์กัดแทะอุปกรณ์

๗.๑) ไม่นำอาหารหรือเครื่องดื่มมารับประทานหรือเก็บไว้ในบริเวณที่มีอุปกรณ์คอมพิวเตอร์

๗.๒) ใช้ท่อห่อหุ้มสายไฟฟ้าหรือสายสัญญาณ เพื่อป้องกันการกัดแทะ

๘) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๘.๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์สำนักงาน

๘.๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ

๘.๓) เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้เครื่องคอมพิวเตอร์สำนักงานบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่าง ๆ

๘.๔) สำรองข้อมูลที่สำคัญบนสื่อที่สามารถจัดเก็บข้อมูลได้อย่างเหมาะสม (DVD , CD , External Harddisk , Handy drive ฯลฯ)

๙) ภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ

๙.๑) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site)

๙.๒) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๑๐) การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์

๑๐.๑) กำหนดเวรรักษาการณ์รักษาความปลอดภัย

๑๐.๒) ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่าย

๑๐.๓) ติดตั้งระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตน (Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

๑๐.๔) ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกพื้นที่ และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๑๐.๕) จัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน

๑๐.๖) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site)

๑๐.๗) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๑๑) การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง

๑๑.๑) จัดให้มีเครือข่ายอินเทอร์เน็ตจำนวนไม่น้อยกว่า ๒ เครือข่าย ได้แก่ เครือข่ายหลักและเครือข่ายสำรอง

๑๑.๒) บำรุงดูแลรักษาและตรวจสอบการทำงานอุปกรณ์เครือข่ายให้พร้อมใช้งานเสมอ

๑๑.๓) เมื่อเครือข่ายอินเทอร์เน็ตขัดข้อง ให้ทำการตรวจสอบอุปกรณ์และสายสัญญาณเครือข่ายอินเทอร์เน็ต/สอบถามผู้ให้บริการเครือข่ายอินเทอร์เน็ต เพื่อหาสาเหตุการขัดข้อง

๑๒) การเชื่อมต่อระบบเครือข่ายอินทราเน็ตขัดข้อง

๑๒.๑) บำรุงดูแลรักษาและตรวจสอบการทำงานอุปกรณ์เครือข่ายให้พร้อมใช้งานเสมอ

๑๒.๒) เมื่อเครือข่ายอินทราเน็ตขัดข้อง ให้ทำการตรวจสอบระบบสารสนเทศ อุปกรณ์เครือข่ายสายสัญญาณ และเครื่องคอมพิวเตอร์แม่ข่ายในระบบเครือข่ายอินทราเน็ต เพื่อหาสาเหตุการขัดข้อง

๑๓) สถานการณ์โรคระบาด

ปัจจุบันสถานการณ์การแพร่ระบาดอย่างรวดเร็วและต่อเนื่องของเชื้อไวรัส COVID-๑๙ มีแนวโน้มสร้างภาวะชะงักงันให้กับหน่วยงานและส่งผลกระทบเหมือนกับการบุกรุกทางด้านไซเบอร์หรือเป็นภัยพิบัติทางธรรมชาติ หน่วยงานต้องควบคุมสถานการณ์โดยสร้างความเชื่อมั่นในการควบคุมโรคให้กับบุคลากรและสามารถปฏิบัติงานได้อย่างต่อเนื่อง โดยการใช้เครื่องมือดิจิทัลเพื่อทำงานร่วมกันในการควบคุมความปลอดภัย และมีเครือข่ายรองรับมาตรการกักกันต่าง ๆ และข้อจำกัดการเดินทาง ในเบื้องต้นหน่วยงานที่ยังไม่มีความสามารถนำระบบทำงานแบบระยะไกลมาปรับใช้ได้นั้น อาจต้องแก้ไขโดยการการระบุข้อกำหนดกรณีการใช้งาน เช่น การส่งข้อความทันทีเพื่อสื่อสารทั่วไป การแชร์ไฟล์ หรือการประชุม และการเข้าถึงแอปพลิเคชั่นต่าง ๆ ขององค์กร เช่น ระบบสารสนเทศต่าง ๆ และเตรียมการด้านความปลอดภัยทั้งหมดเพื่อให้เข้าถึงแอปพลิเคชันและข้อมูลได้อย่างปลอดภัย ใช้ช่องทางดิจิทัลเป็นช่องทางหลักในการติดต่อสื่อสารกับบุคลากรและหน่วยงานอื่นที่เกี่ยวข้องนำแพลตฟอร์มดิจิทัลมาใช้ติดต่อสื่อสาร เช่น เว็บไซต์ หรือแอปพลิเคชั่นต่าง ๆ โซเชียลมีเดีย แต่การติดต่อแบบออฟไลน์ยังคงมีบทบาทสำคัญ การทำงานร่วมกันในสถานที่ทำงาน การประชุมผ่านวิดีโอและไลฟ์สตรีมมิ่ง สร้างแหล่งข้อมูลหลักที่เชื่อถือได้ให้แก่องค์กร และการเตรียมแผนรับมือตอนกลับเข้าสู่โหมดการดำเนินงานในภาวะปกติขององค์กร ซึ่งความวิตกกังวลดังกล่าวบรรเทาลงได้หากองค์กรสามารถใช้ประโยชน์จากข้อมูลมาช่วยในการตัดสินใจได้ดีขึ้น และสื่อสารความคืบหน้าของสถานการณ์อย่างมีประสิทธิภาพต่อพนักงาน องค์กรสามารถนำเสนอเนื้อหาที่คัดสรรมาจากแหล่งที่มาภายในและภายนอกองค์กร เพื่อให้คำแนะนำแก่พนักงานนำไปปรับใช้ได้ โดยแหล่งข้อมูลเหล่านี้จะรวมไปถึงข้อมูลข่าวสารของรัฐบาลท้องถิ่น หน่วยงานและองค์กรด้านสาธารณสุขระหว่างประเทศ เช่น องค์การอนามัยโลก (WHO) แจ้งขอความช่วยเหลือและขอรับการดูแลพิเศษในกรณีเกิดเหตุฉุกเฉินได้

๒. การเตรียมความพร้อม

๒.๑) การจัดเตรียมอุปกรณ์ที่จำเป็น

๒.๑.๑) แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

๒.๑.๒) สำรองข้อมูลและระบบงานที่สำคัญ

๒.๑.๓) แผ่นโปรแกรม antivirus/spyware

๒.๑.๔) แผ่น driver อุปกรณ์ต่างๆ

๒.๑.๕) ระบบสำรองไฟฉุกเฉิน

๒.๑.๖) อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๒.๒) การสำรองข้อมูล (Backup)

กรมส่งเสริมการปกครองท้องถิ่น มีการสำรองข้อมูลระบบสารสนเทศจากเครื่องคอมพิวเตอร์แม่ข่ายภายในห้อง Server ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น และศูนย์ข้อมูล (Data Center) โดยเครื่องคอมพิวเตอร์แม่ข่ายสำหรับสำรองข้อมูล (Backup Server) ทำการสำรองข้อมูลแบบอัตโนมัติ ดังนี้

๒.๒.๑) สำรองข้อมูลรายวัน ทำการสำรองข้อมูลแบบ Virtual Machine วันละ ๑ ครั้ง ในช่วงเวลา ๒๒.๐๐ – ๒๓.๐๐ น. หลังจากทำการสำรองข้อมูลแล้วจะตรวจสอบข้อมูลที่สำรองไว้ว่าสามารถใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้ดำเนินการแก้ไข และถ้าสามารถใช้งานได้จะดำเนินการจัดเก็บไฟล์ข้อมูลสำรองในสื่อบันทึกข้อมูล หลังจากนั้นการสำรองข้อมูลจะดำเนินการเฉพาะส่วนที่มีการเปลี่ยนแปลงจากการสำรองข้อมูลครั้งล่าสุดแบบ Incremental Backup

๒.๒.๒) สำรองข้อมูลรายสัปดาห์ ทำการสำรองข้อมูล สัปดาห์ละ ๑ ครั้ง ในทุกวันเสาร์ ช่วงเวลา ๐๑.๐๐ - ๐๓.๐๐ น. ซึ่งเป็นการสำรองข้อมูลทั้งหมดแบบ Full Backup หลังจากทำการสำรองข้อมูลแล้ว จะตรวจสอบข้อมูลที่สำรองไว้ว่าสามารถใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้ดำเนินการแก้ไข และถ้าสามารถใช้งานได้จะดำเนินการจัดเก็บไฟล์ข้อมูลสำรองในเทปแม่เหล็ก

๓. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

๓.๑) ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) กรมส่งเสริมการปกครองท้องถิ่น รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามการกำกับดูแล

๓.๒) ระดับอำนวยการ

การแก้ไขปัญหาจากภัยพิบัติ มีหน้าที่ในควบคุม ตรวจสอบ กำกับดูแลการประเมินสถานการณ์และตัดสินใจในกรณีที่ฝ่ายปฏิบัติงานประเมินสถานการณ์และรายงานการประเมินเบื้องต้นว่าอาจไม่สามารถควบคุมสถานการณ์ได้ จำเป็นจะต้องปฏิบัติงานนอกเหนือจากแผนป้องกันแก้ไขปัญหาจากภัยพิบัติที่กำหนดไว้ หรือสถานการณ์ยังไม่เกิดแต่มีสภาวการณ์หรือแนวโน้มที่อาจเกิดขึ้น รายงานผลต่อผู้บังคับบัญชา ประกอบด้วย

๓.๒.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศท้องถิ่น

๓.๒.๒) ผู้อำนวยการกลุ่มงานสารสนเทศ

๓.๒.๓) ผู้อำนวยการกลุ่มงานระบบงานคอมพิวเตอร์

๓.๒.๔) ผู้อำนวยการกลุ่มงานวิชาการคอมพิวเตอร์

๓.๓) ระดับปฏิบัติ

ดำเนินการตามแผนป้องกันและแก้ไขปัญหาเกี่ยวกับภัยพิบัติรายงานผลการดำเนินการตามแผนฯ ทบทวนแผนฯ ประเมินสถานการณ์ ติดต่อประสานงานฝ่ายต่างๆ ที่เกี่ยวข้อง รวมทั้งขอรับการสนับสนุนจากหน่วยงานภายนอกหรือบริษัทคู่สัญญา ดังนี้

๓.๓.๑) ด้านฐานข้อมูล ระบบสารสนเทศ ประกอบด้วย

- ผู้อำนวยการกลุ่มงานสารสนเทศ
- เจ้าหน้าที่กลุ่มงานสารสนเทศ

๓.๓.๒) ด้านระบบงานคอมพิวเตอร์ ประกอบด้วย

- ผู้อำนวยการกลุ่มงานระบบงานคอมพิวเตอร์
- เจ้าหน้าที่กลุ่มงานระบบงานคอมพิวเตอร์

๓.๓.๓) ด้านสนับสนุนการแก้ไขปัญหาจากภัยพิบัติ มีหน้าที่ในการสนับสนุนการแก้ไขปัญหาจากภัยพิบัติตามที่ฝ่ายปฏิบัติงานแก้ไขปัญหาจากภัยพิบัติร้องขอ ประกอบด้วย

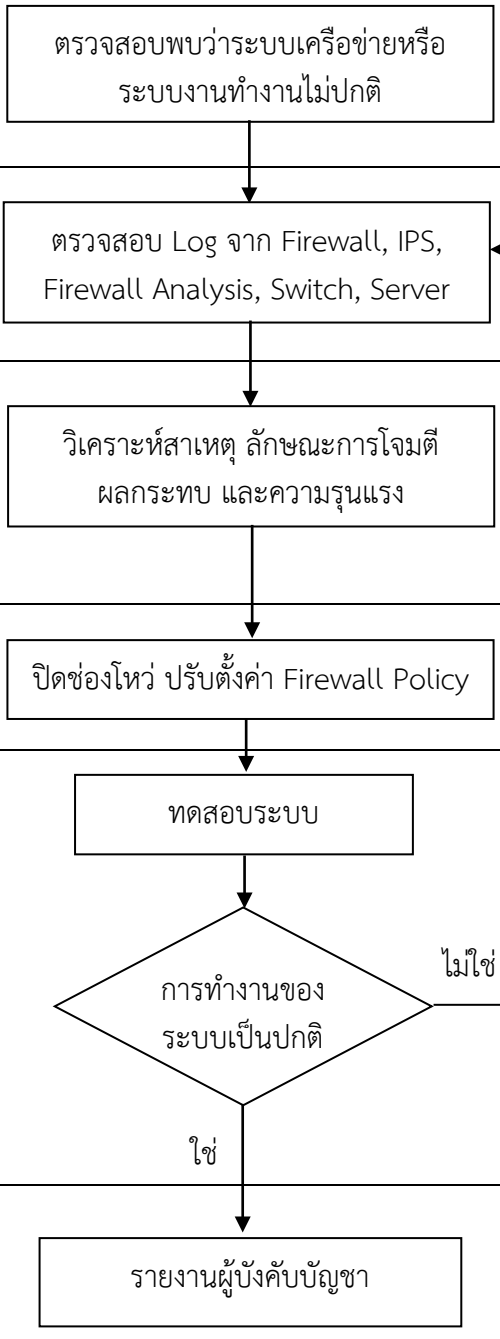
- ผู้อำนวยการกลุ่มงานวิชาการคอมพิวเตอร์
- เจ้าหน้าที่กลุ่มงานวิชาการคอมพิวเตอร์

๔. กระบวนการแก้ไขปัญหาภัยพิบัติ

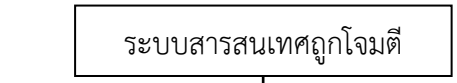
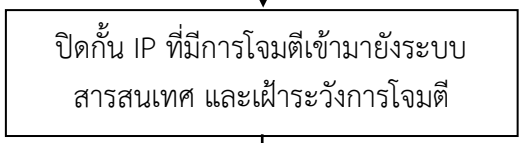
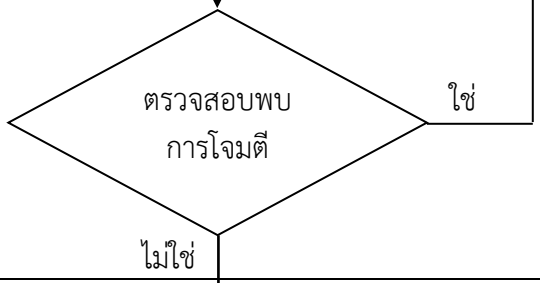
๔.๑) ข้อปฏิบัติกรณีเกิดการบุกรุกหรือโจมตีจากภายนอก

การบุกรุกหรือโจมตีจากภายนอก เป็นการสร้างความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศซึ่งอาจเป็นการเจาะระบบเครือข่าย หรือการโจมตีระบบสารสนเทศ จึงมีข้อปฏิบัติ ดังนี้

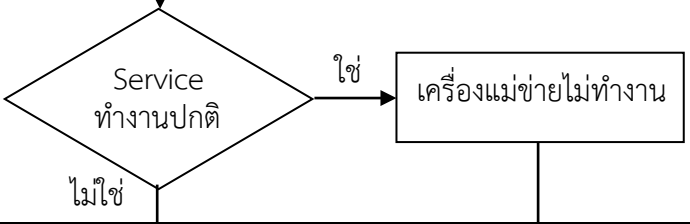
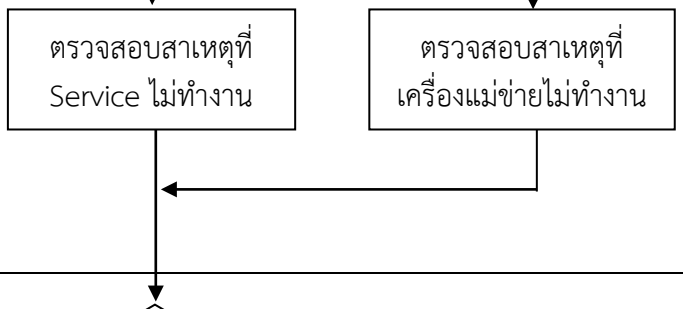
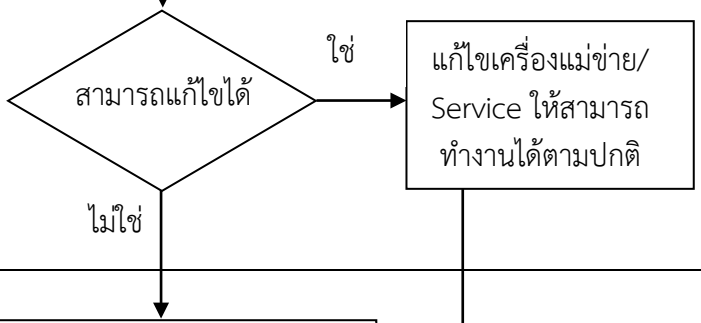
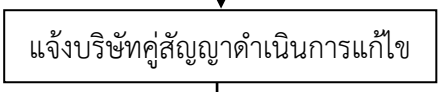
๔.๑.๑) กรณีโดนเจาะระบบเครือข่าย

กระบวนงาน	รายละเอียด
	- ตรวจสอบพบว่าระบบเครือข่ายหรือระบบงานทำงานไม่ปกติ - ฝ่ายปฏิบัติตรวจสอบ Log File จากอุปกรณ์ Firewall IPS, Firewall Analysis, Switch - วิเคราะห์สาเหตุที่ทำให้ระบบเครือข่ายหรือระบบงานไม่ปกติ ลักษณะ การโจมตี ประเภทการโจมตี ผลกระทบ และความรุนแรง - ปิดช่องโหว่ที่เป็นช่องทางเข้าโจมตี โดยการปรับตั้งค่า Firewall Policy - ทดสอบระบบเครือข่ายหรือระบบงานว่าทำงานเป็นปกติหรือไม่ - หากพบว่าระบบมีการทำงานปกติแล้ว ให้รวมรวบข้อมูลรายงานให้ฝ่ายบริหารทราบ

๔.๑.๒) กรณีโดนโจมตีระบบสารสนเทศ

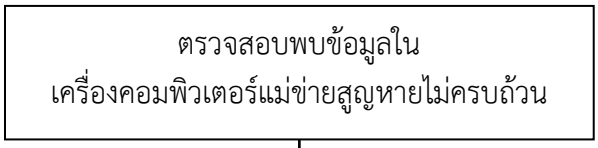
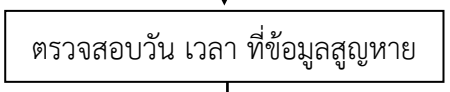
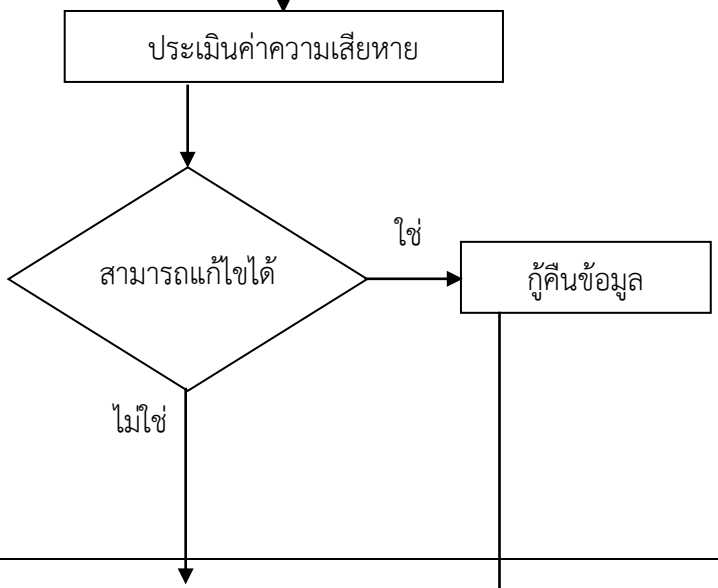
กระบวนงาน	รายละเอียด
	- ตรวจสอบจากอุปกรณ์ Firewall พบว่าระบบสารสนเทศมีการเข้าใช้งานสูงผิดปกติ
	- ฝ่ายปฏิบัติตรวจสอบ Log File จากอุปกรณ์ Firewall เพื่อตรวจสอบ IP ต้นทางที่โจมตี และวิเคราะห์ลักษณะการโจมตี
	- ปรับตั้ง Policy เพื่อปิดกั้น IP ที่มีการโจมตีเข้ามายังระบบสารสนเทศ และเฝ้าระวังว่ามี IP เพิ่มเติมหรือไม่ - ปิดช่องโหว่ที่เป็นช่องทางเข้าโจมตี โดยการปรับตั้งค่า Firewall Policy
	- ตรวจสอบว่ายังมีการโจมตีอยู่หรือไม่
	- ปรับตั้งค่า Policy ให้ตรวจจับพฤติกรรมและ IP ที่มาจากต้นทางเดียวกันเป็นพิเศษ
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๒) ข้อปฏิบัติกรณีเครื่องแม่ข่ายหรืออุปกรณ์ขัดข้อง

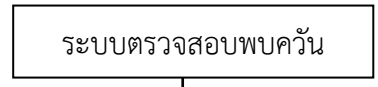
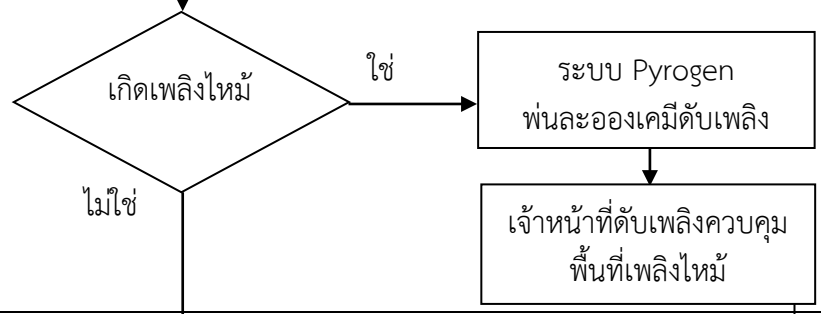
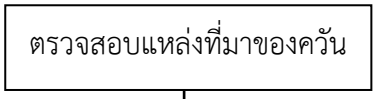
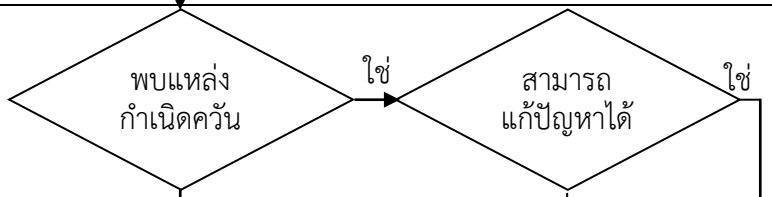
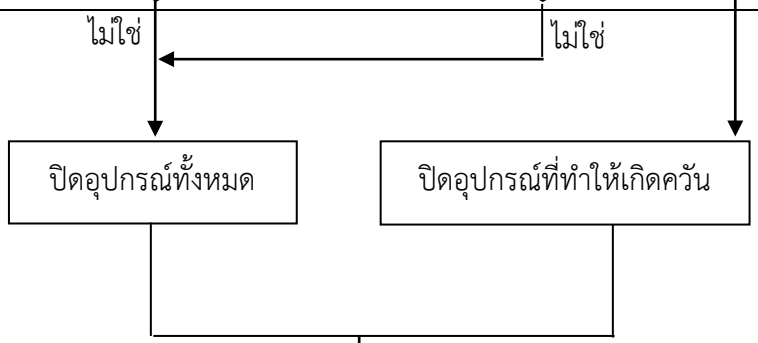
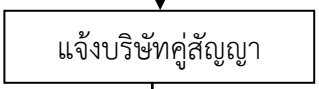
กระบวนงาน	รายละเอียด
	- ตรวจสอบในโปรแกรม Monitoring พบว่าเครื่องแม่ข่ายไม่ทำงาน (ขึ้นสัญลักษณ์สีแดง)
	- ตรวจสอบ Service ทำงานเป็นปกติหรือไม่ - หาก Service ทำงานปกติ แสดงว่าเครื่องแม่ข่ายไม่ทำงาน
	- หาก Service ไม่ทำงานให้ตรวจสอบสาเหตุที่ Service ไม่ทำงาน - หากเครื่องแม่ข่ายไม่ทำงานให้ตรวจสอบสาเหตุที่เครื่องแม่ข่ายไม่ทำงาน
	- ประเมินสถานการณ์ว่าสามารถแก้ไขปัญหาได้หรือไม่ - หากแก้ไขได้ให้ดำเนินการแก้ไขให้เครื่องแม่ข่ายหรือ Service สามารถทำงานได้ตามปกติ
	- หากไม่สามารถแก้ไขได้ ให้แจ้งบริษัทคู่สัญญาดำเนินการเปลี่ยนอุปกรณ์/แก้ไข
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๓) ข้อปฏิบัติกรณีข้อมูลได้รับความเสียหาย

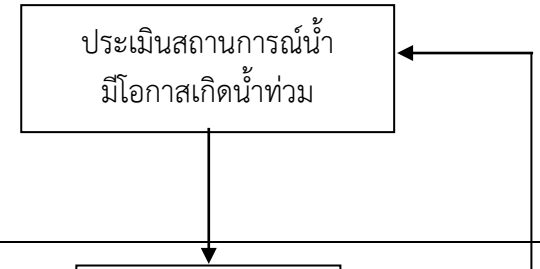
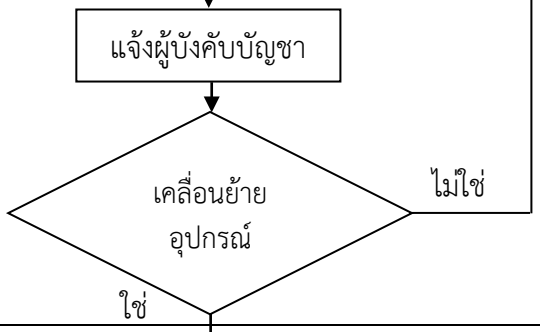
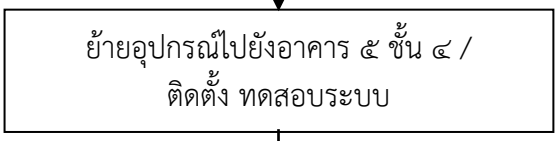
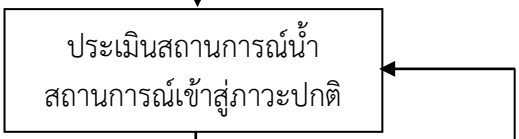
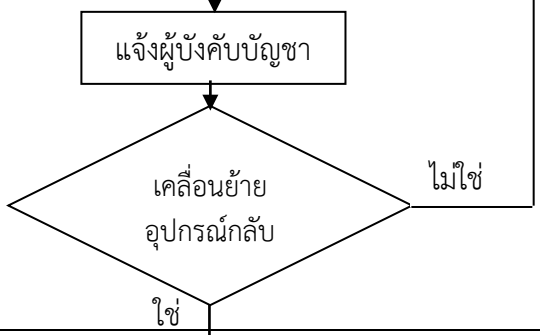
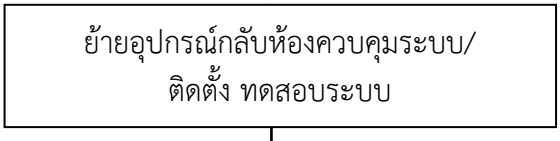
กรณีตรวจพบข้อมูลในเครื่องคอมพิวเตอร์แม่ข่ายได้รับความเสียหาย ข้อมูลสูญหาย ไม่ครบถ้วน มีข้อปฏิบัติ ดังนี้

กระบวนงาน	รายละเอียด
	- ตรวจสอบพบข้อมูลในเครื่องคอมพิวเตอร์แม่ข่ายสูญหายไม่ครบถ้วน
	- ตรวจสอบวัน เวลา ที่ข้อมูลสูญหาย และระบบที่มีข้อมูลสูญหาย
	- ประเมินสถานการณ์ว่าสามารถแก้ไขได้หรือไม่ - หากแก้ไขได้ ให้นำข้อมูลที่สำรองไว้มา Restore ในเครื่องทดสอบ - ทำการกู้คืนข้อมูลไปยังระบบที่ตรวจสอบพบว่าข้อมูลสูญหาย
	- หากไม่สามารถแก้ไขได้ ให้แจ้งบริษัทคู่สัญญาดำเนินการแก้ไขข้อมูล
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๔) ข้อปฏิบัติกรณีเกิดอัคคีภัย

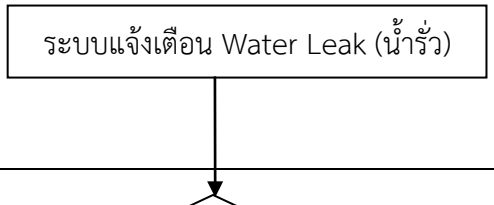
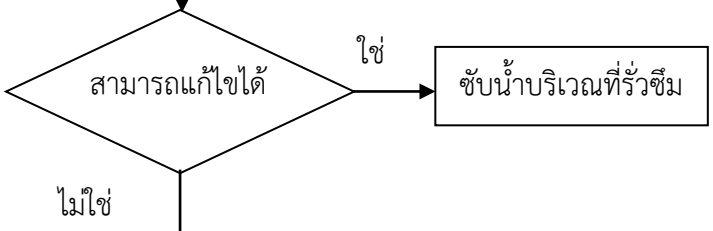
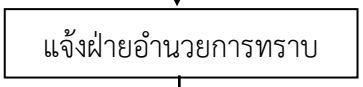
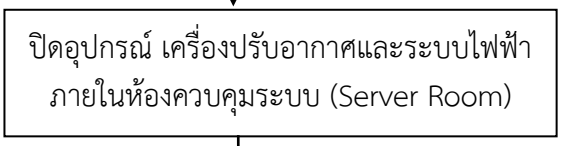
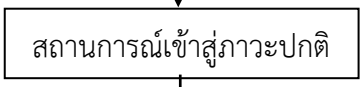
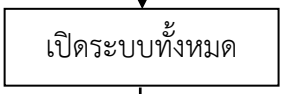
กระบวนงาน	รายละเอียด
	- ระบบไฟฟ้าดับ ระบบ Tale Alarm แจ้งว่าตรวจพบควัน (SMOKE DETECTER)
	- ฝ่ายปฏิบัติตรวจสอบประเมินเหตุการณ์ว่าเกิดเพลิงไหม้หรือไม่ แจ้งฝ่ายอำนวยการฝ่ายสนับสนุน ทราบให้บุคลากรออกจากพื้นที่ แจ้งสถานีดับเพลิงดุสิต - หากเกิดเพลิงไหม้ระบบ Pyrogen จะทำงานอัตโนมัติ
	- หากไม่เกิดเพลิงไหม้ ให้ฝ่ายปฏิบัติตรวจสอบแหล่งที่มาของควันและประเมินสถานการณ์และแจ้งให้ฝ่ายอำนวยการทราบ
	- หากตรวจสอบพบแหล่งที่มาของควัน ให้ประเมินสถานการณ์ว่าสามารถควบคุมและแก้ไขได้หรือไม่
	- หากตรวจสอบไม่พบแหล่งที่มาของควันให้ทำการให้ปิดอุปกรณ์ทั้งหมด ปิดเครื่องปรับอากาศและระบบไฟฟ้า - หากตรวจพบแหล่งกำเนิดควันแต่ไม่สามารถแก้ไขปัญหาได้ ให้ปิดอุปกรณ์ทั้งหมด ปิดเครื่องปรับอากาศ และระบบไฟฟ้า - หากตรวจพบแหล่งกำเนิดควันและสามารถแก้ไขปัญหาได้ให้ปิดอุปกรณ์ที่ทำให้เกิดควัน
	- แจ้งบริษัทคู่สัญญาให้มาตรวจสอบความเสียหายของอุปกรณ์และซ่อมแซม
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๕) ข้อปฏิบัติกรณีเกิดอุทกภัย (น้ำท่วม)

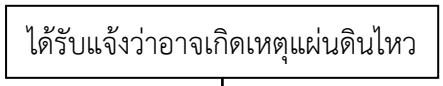
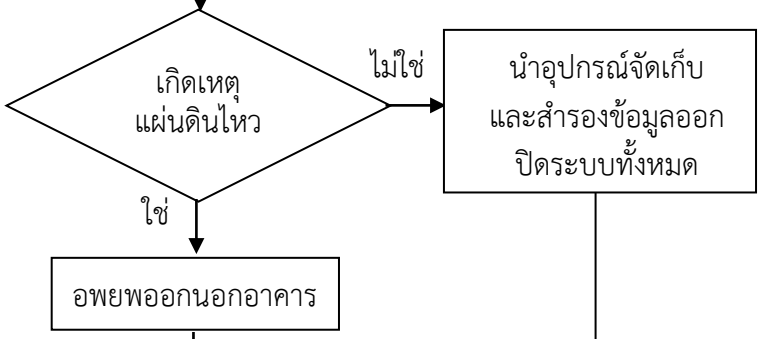
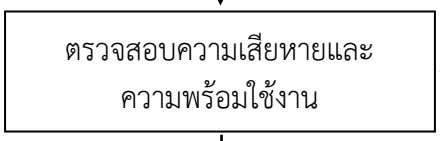
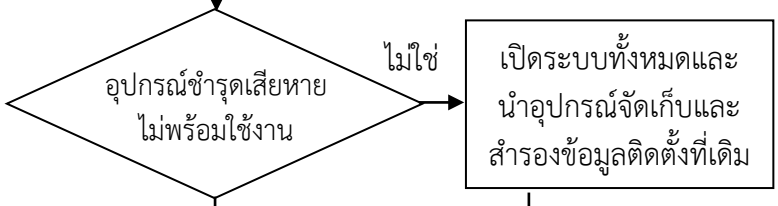
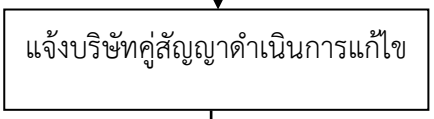
กระบวนงาน	รายละเอียด
	- ฝ่ายปฏิบัติงานติดตามข่าวสารและประกาศจากศูนย์ป้องกันและแก้ไขปัญหาภัยพิบัติแห่งชาติ - ฝ่ายปฏิบัติประเมินสถานการณ์และวิเคราะห์ความน่าจะเป็นที่อาจจะเกิดน้ำท่วมบริเวณห้องควบคุมระบบ
	- รวมรวบข้อมูล สถานการณ์น้ำท่วม และแนวโน้มที่อาจเกิดน้ำท่วมให้ฝ่ายบริหารทราบ - ขอความเห็นชอบในการย้ายอุปกรณ์ไปยังห้องควบคุมสำรอง
	- แจ้งบริษัทคู่สัญญา (MA) ดำเนินการย้ายอุปกรณ์ - ปิดระบบ/ปิดอุปกรณ์ทั้งหมด - ดำเนินการย้าย ติดตั้ง ทดสอบระบบ
	- ฝ่ายปฏิบัติงาน ติดตามข่าวสารและประเมินสถานการณ์ว่าสถานการณ์เข้าสู่ภาวะปกติ
	- รวมรวบข้อมูล สถานการณ์น้ำท่วมให้ฝ่ายบริหารทราบ - ขอความเห็นชอบในการย้ายอุปกรณ์กลับห้องควบคุมระบบ (Server Room)
	- แจ้งบริษัทคู่สัญญา (MA) ดำเนินการย้ายอุปกรณ์ - ปิดระบบ/ปิดอุปกรณ์ทั้งหมด - ดำเนินการย้าย ติดตั้ง ทดสอบระบบ
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

หมายเหตุ : กำหนดให้ใช้อาคาร ๕ ชั้น ๔ ของ สถ. เป็นห้องแม่ข่ายสำรอง

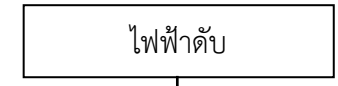
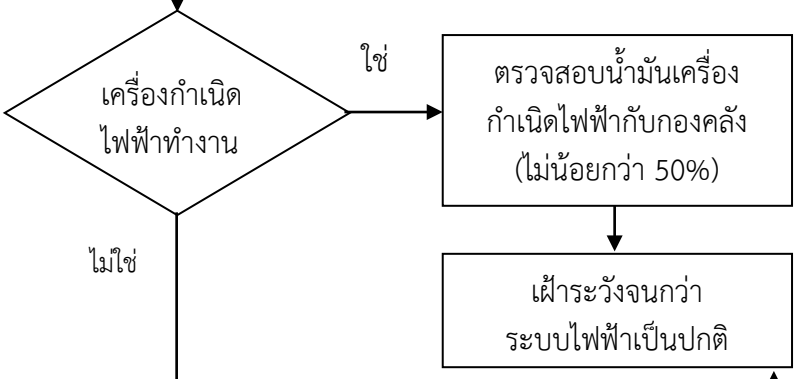
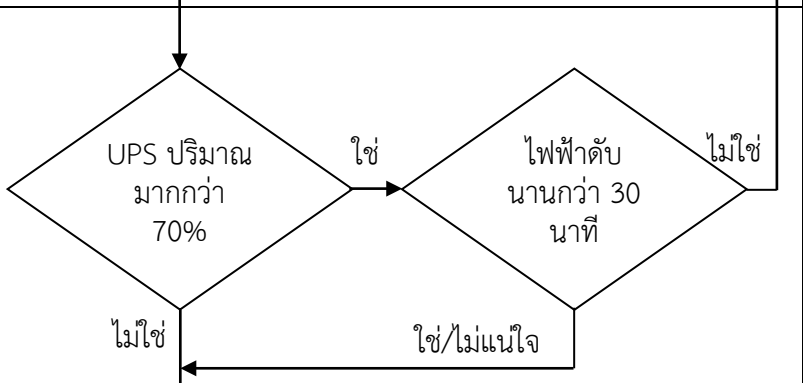
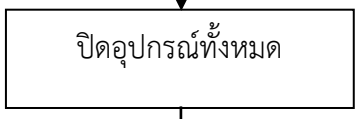
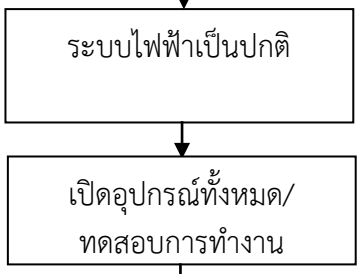
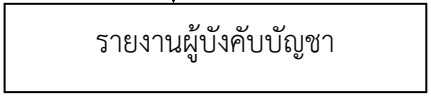
๔.๖) ข้อปฏิบัติกรณีเกิดน้ำรั่วซึม

กระบวนงาน	รายละเอียด
	- ระบบ Tale Alarm แจ้งว่าตรวจสอบพบน้ำ (Water Leak) ในพื้นห้องควบคุมระบบ (Server Room)
	- ฝ่ายปฏิบัติงานแก้ไขปัญหาจากภัยพิบัติ ดำเนินการเปิดพื้น และซับน้ำให้แห้ง
	- ฝ่ายปฏิบัติงานแจ้งฝ่ายอำนวยการทราบปัญหาและขออนุญาตปิดอุปกรณ์ทั้งหมด
	- ฝ่ายปฏิบัติงานดำเนินการปิดอุปกรณ์ทั้งหมด ปิดระบบไฟฟ้าและเครื่องปรับอากาศ
	- แจ้งบริษัทคู่สัญญา MA ระบบดำเนินการแก้ไข
	- ตรวจสอบสถานการณ์ หากเข้าสู่ภาวะปกติ แจ้งฝ่ายอำนวยการทราบและขอเปิดระบบ
	- เปิดระบบไฟฟ้า ระบบเครื่องปรับอากาศ รอให้อุณหภูมิอยู่ที่ ๒๕°C แล้วเปิดอุปกรณ์ทั้งหมด
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๗) ข้อปฏิบัติกรณีเกิดแผ่นดินไหว

กระบวนงาน	รายละเอียด
	- ได้รับแจ้งจากหน่วยงานที่เกี่ยวข้อง แจ้งว่าจะเกิดเหตุแผ่นดินไหว
	- ประเมินสถานการณ์หากเกิดเหตุแผ่นดินไหวขึ้นแล้วให้อพยพออกนอกอาคาร - หากยังไม่เกิดขึ้นแต่ได้รับการแจ้งเตือนให้นำอุปกรณ์สำรองข้อมูลออกจากห้องควบคุมระบบและปิดระบบทั้งหมด
	- รอเหตุการณ์สงบหรือพ้นระยะเวลาที่ได้รับแจ้งว่าอาจเกิดแผ่นดินไหวให้ดำเนินการตรวจสอบความเสียหายและความพร้อมใช้งานของ อุปกรณ์
	- ตรวจสอบอุปกรณ์ทั้งหมดว่าได้รับความเสียหายหรือไม่ หากไม่ได้รับความเสียหายให้ประเมินความพร้อมใช้งาน หากมีความพร้อมใช้งานให้เปิดระบบทั้งหมดดังเดิม
	- กรณีอุปกรณ์ได้รับความเสียหายให้แจ้งบริษัทคู่สัญญาบำรุงรักษาระบบมาตรวจสอบดำเนินการแก้ไขหรือจัดหาอุปกรณ์มาทดแทน
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๘) ข้อปฏิบัติกรณีไฟฟ้าดับ

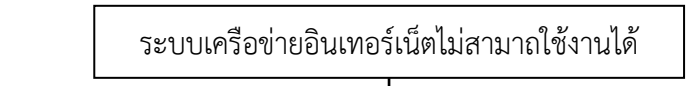
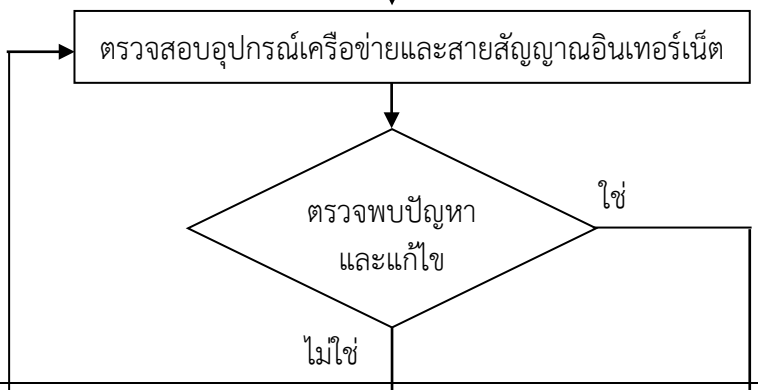
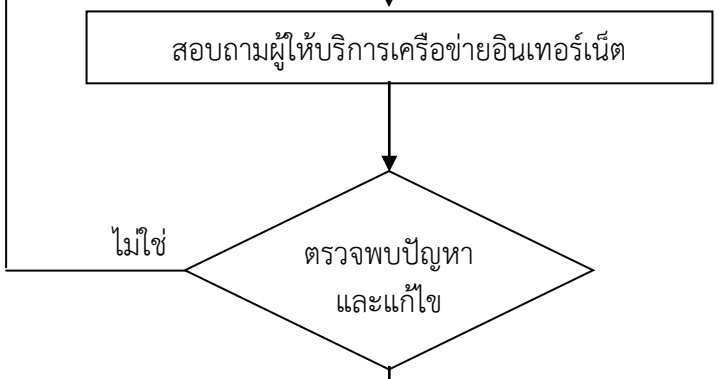
กระบวนงาน	รายละเอียด
	- ระบบไฟฟ้าดับ ระบบ Tale Alarm แจ้งว่าไฟฟ้าดับ (Main Power FAIL)
	- ตรวจสอบเครื่องกำเนิดไฟฟ้าว่าทำงานหรือไม่ - กรณีที่เครื่องกำเนิดไฟฟ้าทำงานให้ฝ่ายปฏิบัติตรวจสอบปริมาณน้ำมันและแจ้งกองคลัง สำรองน้ำมันหากมีน้ำมันน้อยกว่า ๕๐% และเฝ้าระวังจนกว่าระบบไฟฟ้าจะเป็นปกติ
	- กรณีเครื่องกำเนิดไฟฟ้าไม่ทำงาน ฝ่ายปฏิบัติตรวจสอบ UPS ว่าปริมาณไฟฟ้าสำรองมากกว่า ๗๐% และให้สอบถาม การไฟฟ้านครหลวงถึงระยะเวลาที่ไฟฟ้าจะกลับเป็นปกติ - หากไฟฟ้าดับน้อยกว่า ๓๐ นาทีให้เฝ้าระวังจนกว่าระบบไฟฟ้าจะเป็นปกติ
	- ปิดอุปกรณ์หากปริมาณไฟฟ้าสำรองของ UPS น้อยกว่า ๗๐% หรือไฟฟ้าดับนานกว่า ๓๐ นาที หรือไม่แน่ใจสถานการณ์
	- เมื่อระบบไฟฟ้าเป็นปกติ ให้เปิดระบบไฟฟ้าเครื่องปรับอากาศ และให้อุณหภูมิอยู่ที่ ๒๕°C - แล้วเปิดอุปกรณ์ทั้งหมดและทดสอบการทำงานให้เป็นปกติ
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๙) ข้อปฏิบัติกรณีเกิดภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ

กรณีเกิดภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ และได้มีการปิดล้อมสถานที่ปฏิบัติงาน มีข้อปฏิบัติ ดังนี้

กระบวนงาน	รายละเอียด
ได้รับข่าวว่าอาจถูกปิดล้อมสถานที่ปฏิบัติงาน	- ได้รับแจ้งจากหน่วยงานที่เกี่ยวข้อง แจ้งว่าจะเกิดเหตุปิดล้อมสถานที่ปฏิบัติงาน
ติดตามข่าว เฝ้าระวังและเตรียมความพร้อม	- ประสานหน่วยงานที่เกี่ยวข้องจัดเตรียมสถานที่ปฏิบัติงานสำรอง
เกิดเหตุปิดล้อมสถานที่ปฏิบัติงาน (ไม่ใช่ / ใช่)	- ประเมินสถานการณ์ รอคำสั่งจากฝ่ายบริหารให้ย้ายสถานที่ปฏิบัติงาน
ย้ายสถานที่ปฏิบัติงาน/ ย้ายเครื่องแม่ข่ายระบบ Intranet ไปยัง Data Center	- ดำเนินการติดตั้งอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงสำหรับปฏิบัติงาน ณ สถานที่ปฏิบัติงานสำรอง - ย้ายเครื่องแม่ข่าย Intranet ที่ห้องควบคุมไป Data Center
ประเมินสถานการณ์ เหตุการณ์ปกติ (ไม่ใช่ / ใช่)	- ประเมินสถานการณ์ว่าเข้าสู่ภาวะปกติหรือไม่ - รอคำสั่งจากฝ่ายบริหารให้ย้ายสถานที่ปฏิบัติงาน
ย้ายสถานที่ปฏิบัติงานกลับมายัง สถ./ ย้ายเครื่องแม่ข่ายระบบ Intranet กลับมายังห้องควบคุม	- หากเหตุการณ์เข้าสู่ภาวะปกติ ให้ดำเนินการย้ายสถานที่ปฏิบัติงานกลับมายัง สถ. ตรวจสอบอุปกรณ์ให้สามารถใช้งานตามปกติ - ย้ายเครื่องแม่ข่าย Intranet กลับมายังห้องควบคุม
รายงานผู้บังคับบัญชา	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

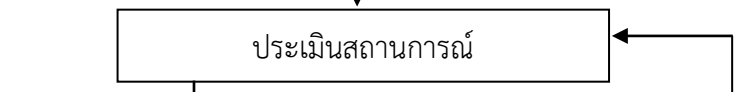
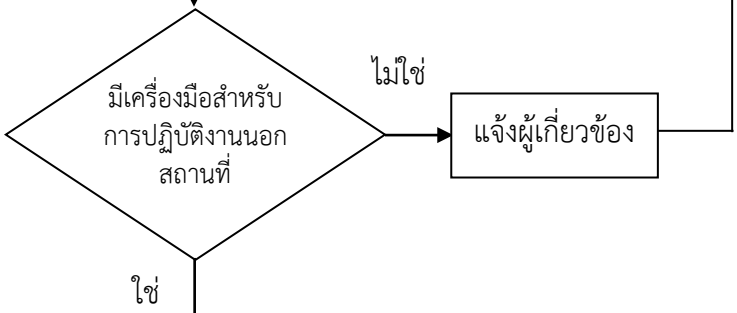
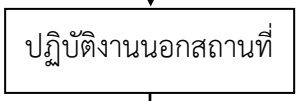
๔.๑๐) ข้อปฏิบัติกรณีเกิดการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง

กระบวนงาน	รายละเอียด
	- ตรวจพบระบบเครือข่ายอินเทอร์เน็ตขัดข้อง ไม่สามารถใช้งานได้
	- ตรวจสอบอุปกรณ์เครือข่ายและสายสัญญาณอินเทอร์เน็ต หากพบปัญหาให้ดำเนินการแก้ไข
	- หากไม่พบปัญหา ว่าเกิดจากอุปกรณ์เครือข่ายและสายสัญญาณอินเทอร์เน็ตภายใน สถ. ให้สอบถามผู้ให้บริการเครือข่ายอินเทอร์เน็ต - หากพบปัญหา ว่าเกิดจากผู้ให้บริการเครือข่ายอินเทอร์เน็ต ให้ผู้ให้บริการเครือข่ายอินเทอร์เน็ตดำเนินการแก้ไขปรับปรุงให้แล้วเสร็จโดยไว
	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๑๑) ข้อปฏิบัติกรณีเกิดการเชื่อมต่อระบบเครือข่ายอินทราเน็ตขัดข้อง

กระบวนงาน	รายละเอียด
ระบบเครือข่ายอินทราเน็ตไม่สามาถใช้งานได้	- ตรวจพบระบบเครือข่ายอินทราเน็ตขัดข้อง ไม่สามารถใช้งานได้
ตรวจสอบอุปกรณ์เครือข่ายและสายสัญญาณอินทราเน็ต ตรวจพบปัญหาและแก้ไข ใช่ ไม่ใช่	- ตรวจสอบอุปกรณ์เครือข่ายและสายสัญญาณอินทราเน็ต หากพบปัญหาให้ดำเนินการแก้ไข
ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายในระบบเครือข่ายอินทราเน็ต ไม่ใช่ ตรวจพบปัญหาและแก้ไข ใช่	- หากไม่พบปัญหา ว่าเกิดจากอุปกรณ์เครือข่ายและสายสัญญาณอินทราเน็ต ให้ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายในระบบเครือข่ายอินทราเน็ต - หากพบปัญหา ว่าเกิดจากเครื่องคอมพิวเตอร์แม่ข่ายในระบบเครือข่ายอินทราเน็ตอินเทอร์เน็ตขัดข้อง ให้ดำเนินการแก้ไข ตามกรณีเครื่องแม่ข่ายหรืออุปกรณ์ขัดข้อง
รายงานผู้บังคับบัญชา	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๑๒) ข้อปฏิบัติกรณีเกิดสถานการณ์โรคระบาดในสถานที่ปฏิบัติงาน

กระบวนงาน	รายละเอียด
	- ได้รับแจ้งจากหน่วยงานที่เกี่ยวข้อง เกี่ยวกับสถานการณ์โรคระบาด
	- ประเมินสถานการณ์เตรียมสถานที่ปฏิบัติงานสำรอง/การทำงานที่บ้าน (WFH) และรอคำสั่งจากฝ่ายบริหารประกาศห้ามเข้าพื้นที่เขตโรคระบาด ฯลฯ
	- จัดเตรียมเครื่องมือสำหรับการปฏิบัติงานนอกสถานที่ อาทิ โปรแกรมการประชุมทางไกล - หากขาดความพร้อมในส่วนของเครื่องมือสำหรับการปฏิบัติงานนอกสถานที่ ให้ผู้เกี่ยวข้องจัดเตรียมเครื่องมือสำหรับใช้ในการปฏิบัติงาน
	- หากมีความพร้อมในส่วนของเครื่องมือสำหรับการปฏิบัติงานนอกสถานที่ ให้ปฏิบัติงานนอกสถานที่
	- รายงานการทำงานที่บ้าน (WFH) ให้ฝ่ายบริหารทราบ

๕. การกู้คืนระบบ

การกู้คืนระบบเมื่อเกิดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วย การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และการกู้คืนระบบสารสนเทศและฐานข้อมูล ซึ่งมีขั้นตอน ดังนี้

๑) การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑.๑) จัดหาอุปกรณ์/ชิ้นส่วนเพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๑.๒) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้แล้วเสร็จภายใน ๒๔ ชั่วโมง

๑.๓) จัดหาอุปกรณ์คอมพิวเตอร์ทดแทนจากหน่วยงานอื่นมาใช้เป็นการชั่วคราว

๑.๔) นำสื่อที่ได้จัดเก็บข้อมูลที่สำรองไว้กลับมา Restore

๑.๕) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

กระบวนงาน	รายละเอียด
ระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย เสียหายหรือหยุดทำงาน	- เกิดภัยด้านเทคโนโลยีสารสนเทศส่งผลให้ระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายได้รับความเสียหายหรือหยุดทำงาน
จัดหาอุปกรณ์/ชิ้นส่วนเพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย ซ่อมบำรุงอุปกรณ์	- เมื่อพบความเสียหาย ให้จัดหาอุปกรณ์/ชิ้นส่วนเพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย โดยซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้แล้วเสร็จภายใน ๒๔ ชั่วโมง - หรือจัดหาอุปกรณ์คอมพิวเตอร์ทดแทนจากหน่วยงานอื่นมาใช้เป็นการชั่วคราว
นำข้อมูลที่สำรองไว้มา Restore	- นำสื่อที่ได้จัดเก็บข้อมูลที่สำรองไว้กลับมา Restore
ตรวจสอบระบบ	- ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่น ๆ ที่เกี่ยวข้อง

๒) การกู้คืนระบบสารสนเทศและฐานข้อมูลให้สู่สภาวะปกติ ดังนี้

๒.๑) ตรวจสอบวันเวลาที่ข้อมูลสูญหาย

๒.๒) คัดลอกไฟล์สำรองข้อมูล ที่ทำการ Backup ไว้ในแต่ละวันเพื่อใช้ในการ Restore ข้อมูล

๒.๓) ปิดระบบสารสนเทศที่ต้องการกู้คืนข้อมูล

๒.๔) ทำการกู้คืนข้อมูล Restore

๒.๕) เปิดใช้งานระบบสารสนเทศ

๒.๖) ตรวจสอบข้อมูลที่ได้ทำการกู้คืนโดยผู้ดูแลระบบ

๒.๗) แจ้งผู้ใช้งานให้ดำเนินการตรวจสอบข้อมูลหลังจาก Restore

กระบวนงาน	รายละเอียด
ระบบสารสนเทศและฐานข้อมูลเสียหายหรือหยุดทำงาน	- เกิดภัยด้านเทคโนโลยีสารสนเทศส่งผลให้ระบบสารสนเทศและฐานข้อมูล ได้รับความเสียหายหรือหยุดทำงาน
ตรวจสอบวันเวลาที่ข้อมูลสูญหาย	- ตรวจสอบวันเวลาที่ข้อมูลสูญหาย
คัดลอกไฟล์สำรองข้อมูล	- ทำการคัดลอกไฟล์สำรองข้อมูล
ปิดระบบสารสนเทศที่ต้องการกู้คืนข้อมูล	- ปิดระบบสารสนเทศที่ต้องการกู้คืนข้อมูล
นำข้อมูลที่สำรองไว้มา Restore	- เตรียมไฟล์ Database ที่ทำการ Backup ไว้ในแต่ละวันเพื่อใช้ในการ Restore ข้อมูล - ทำการกู้คืนข้อมูล Restore
เปิดระบบสารสนเทศ	- เปิดใช้งานระบบสารสนเทศ
ตรวจสอบข้อมูลที่ทำการกู้คืน	- ตรวจสอบข้อมูลที่ได้ทำการกู้คืนโดยผู้ดูแลระบบ
แจ้งผู้ใช้งานตรวจสอบข้อมูล	- แจ้งผู้ใช้งานให้ดำเนินการตรวจสอบข้อมูลหลังจาก Restore
รายงานผู้บังคับบัญชา	- รวมรวบข้อมูล รายงานให้ฝ่ายบริหารทราบ

ในส่วนของระยะเวลาการกู้คืนข้อมูลของระบบสารสนเทศและระบบเครือข่าย (Network) คำนึงถึงความสำคัญ ความจำเป็นและความเหมาะสมในแต่ละภารกิจของกรมส่งเสริมการปกครองท้องถิ่น ดังนี้

๑) ระบบเว็บไซต์กรมส่งเสริมการปกครองท้องถิ่น (www.dla.go.th) กำหนดระยะเวลากู้คืนข้อมูลภายในเวลา ๒๔ ชั่วโมง

๒) ระบบสารสนเทศสำหรับสนับสนุนการปฏิบัติงานของกรมส่งเสริมการปกครองท้องถิ่น ที่มีความสำคัญต่อการปฏิบัติงานประจำวันค่อนข้างมาก เช่น ระบบ Intranet ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น กำหนดระยะเวลากู้คืนข้อมูลภายในเวลา ๒๔ ชั่วโมง

๓) ระบบสารสนเทศสำหรับสนับสนุนการปฏิบัติงานของกรมส่งเสริมการปกครองท้องถิ่น ที่ไม่ได้มีลักษณะในการปฏิบัติงานประจำวัน (Not Routine) เช่น การประเมินประสิทธิภาพองค์กรปกครองส่วนท้องถิ่น (LPA) กำหนดระยะเวลากู้คืนข้อมูลภายในเวลา ๔๘ ชั่วโมง

๔) ระบบสารสนเทศเพื่อการบริหารจัดการภายในกรมส่งเสริมการปกครองท้องถิ่น (ERP) เช่น ระบบเบิกจ่ายเงินค่าเช่าบ้านข้าราชการ ระบบพัสดุและครุภัณฑ์ เป็นต้น กำหนดระยะเวลากู้คืนข้อมูลภายในเวลา ๔๘ ชั่วโมง

๕) ระบบสารสนเทศสำหรับสนับสนุนการปฏิบัติงานขององค์กรปกครองส่วนท้องถิ่น เช่น ระบบ INFO ระบบ ELE ระบบ LEC เป็นต้น กำหนดระยะเวลากู้คืนข้อมูลภายในเวลา ๔๘ ชั่วโมง

๖) ระบบ Network เมื่อเกิดความขัดข้องไม่สามารถทำงานได้ตามปกติ จะดำเนินการแก้ไขให้สามารถใช้งานได้ตามปกติภายในเวลา ๔ ชั่วโมง และหากต้องมีการเปลี่ยนหรือซ่อมแซมอุปกรณ์จะดำเนินการให้แล้วเสร็จเพื่อให้ระบบสามารถใช้งานได้ตามปกติภายในเวลา ๒๔ ชั่วโมง

ทั้งนี้ สามารถแสดงระยะเวลาเป้าหมายในการกู้คืนข้อมูลของระบบสารสนเทศ กรมส่งเสริมการปกครองท้องถิ่น ได้ดังนี้

ลำดับ	ระบบสารสนเทศ	ระยะเวลาเป้าหมายในการกู้คืนข้อมูล (ชั่วโมง)	
		๒๔	๔๘
๑	ระบบเว็บไซต์กรมส่งเสริมการปกครองท้องถิ่น (www.dla.go.th)	/	
๒	ระบบ Intranet	/	
๓	ระบบ ERP เช่น ระบบค่าเช่าบ้าน ระบบบริหารพัสดุ ระบบเครื่องราชอิสริยาภรณ์ของบุคลากร ฯลฯ		/
๔	ระบบข้อมูลกลางองค์กรปกครองส่วนท้องถิ่น (INFO)		/
๕	ระบบสารบรรณอิเล็กทรอนิกส์	/	
๖	ระบบบริหารจัดการเอกสารแบบรวมศูนย์ (DMS)		/
๗	ระบบไปรษณีย์อิเล็กทรอนิกส์	/	
๘	ระบบ Web Conference กรมส่งเสริมการปกครองท้องถิ่น	/	
๙	ระบบจองห้องประชุม Conference กรมส่งเสริมการปกครองท้องถิ่น		/
๑๐	ระบบศูนย์ข้อมูล (Big Data)		/
๑๑	ระบบช่วยตอบข้อความ ตอบคำถาม ให้ข้อมูลในรูปแบบ Chat Bot		/
๑๒	ระบบยืนยันตัวบุคคล DLA-SSO (Single Sign-On : SSO)	/	
๑๓	ระบบบริการข้อมูลกรมส่งเสริมการปกครองท้องถิ่น (WSG)		/

ลำดับ	ระบบสารสนเทศ	ระยะเวลาเป้าหมายในการกู้คืนข้อมูล (ชั่วโมง)	
		๒๔	๔๘
๑๔	ระบบป้องกันไวรัสคอมพิวเตอร์	/	
๑๕	ระบบติดตาม (Monitor) ระบบเครือข่ายคอมพิวเตอร์ กรมส่งเสริมการปกครองท้องถิ่น	/	
๑๖	ระบบจัดเก็บข้อมูลอุปกรณ์เครือข่ายคอมพิวเตอร์ กรมส่งเสริมการปกครองท้องถิ่น	/	
๑๗	ระบบสารสนเทศทรัพยากรบุคคลระดับกรม (DPIS)		/
๑๘	ระบบบัญชีคอมพิวเตอร์ขององค์กรปกครองส่วนท้องถิ่น (e-LAAS)		/
๑๙	โปรแกรมแผนที่ภาษี (LTAXGIS ๒.๒)		/
๒๐	โปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน (LTAX ๓๐๐๐ V๔)		/
๒๑	ระบบแผนที่ภาษีและทะเบียนทรัพย์สิน (LTAX Online)		/
๒๑	ระบบบูรณาการทะเบียนทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น (LTAX Online)		/
๒๓	ระบบศูนย์บริการข้อมูลบุคลากรท้องถิ่นแห่งชาติ (LHR)		/
๒๔	ระบบการเรียนรู้ผ่านสื่ออิเล็กทรอนิกส์ (e-learning)		/
๒๕	ระบบลงทะเบียนและบริหารจัดการหลักสูตรฝึกอบรมสถาบันพัฒนาบุคลากรท้องถิ่น		/
๒๖	การประเมินประสิทธิภาพองค์กรปกครองส่วนท้องถิ่น (LPA)		/
๒๗	ระบบสารสนเทศในการการให้บริการประชาชน (Local Service)		/
๒๘	เว็บไซต์ศูนย์วิชาการกรมส่งเสริมการปกครองท้องถิ่น		/
๒๙	โปรแกรมห้องสมุดอัตโนมัติ Alice for windows		/
๓๐	ระบบสารสนเทศเพื่อขอรับการสนับสนุนงบประมาณเงินอุดหนุนขององค์กรปกครองส่วนท้องถิ่น (SOLA)		/
๓๑	ระบบสารสนเทศการจัดการฐานข้อมูลเบี้ยยังชีพขององค์กรปกครองส่วนท้องถิ่น (Welfare)		/
๓๒	ระบบสารสนเทศทางการศึกษาท้องถิ่น (LEC)		/
๓๓	ระบบการลงทะเบียนและฐานข้อมูลกิจการสภาเด็กและเยาวชนขององค์กรปกครองส่วนท้องถิ่น (CYCL)		/
๓๔	ระบบฐานข้อมูล Smart Law (SLL)		/
๓๕	ระบบศูนย์ข้อมูลการเลือกตั้งท้องถิ่นแห่งชาติ (NLC)		/
๓๖	ระบบสารสนเทศเพื่อการวางแผนและประเมินผลขององค์กรปกครองส่วนท้องถิ่น (e-Plan)		/
๓๗	ระบบติดตามและประเมินผลของกรมส่งเสริมการปกครองท้องถิ่น (e-Dla Monitoring)		/

ลำดับ	ระบบสารสนเทศ	ระยะเวลาเป้าหมายในการกู้คืนข้อมูล (ชั่วโมง)	
		๒๔	๔๘
๓๘	ระบบการเรียนรู้ออนไลน์ของกรมส่งเสริมการปกครองท้องถิ่นเพื่อพัฒนาท้องถิ่นอย่างยั่งยืน (Local MOOC)		/
๓๙	ระบบสารสนเทศด้านการจัดการขยะมูลฝอยขององค์กรปกครองส่วนท้องถิ่น (Waste)		/

๖. การซ้อมแผนการแก้ไขความเสี่ยง

เพื่อเป็นการเตรียมความพร้อมรับมือกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงกำหนดแผนการซ้อมการแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ จากสถานการณ์ฉุกเฉิน/พิบัติภัย โดยกำหนดให้มีการซ้อมจำนวนไม่น้อยกว่า ๑ ครั้งต่อปี ซึ่งมีขั้นตอน ดังนี้

๑) เตรียมการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ

๑.๑) เลือกประเภทของภัยพิบัติที่จะดำเนินการซ้อมแผน ซึ่งเป็นภัยพิบัติที่ปรากฏตาม แผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ได้แก่ กรณีอัคคีภัย กรณีแผ่นดินไหว กรณีน้ำท่วม กรณีน้ำรั่ว กรณีเครื่องแม่ข่ายหรืออุปกรณ์ขัดข้อง กรณีไฟฟ้าดับ กรณีโดนเจาะระบบเครือข่าย กรณีโดนโจมตีระบบสารสนเทศ กรณีโดนปิดล้อมสถานที่ปฏิบัติงาน กรณีข้อมูลได้รับความเสียหาย กรณีเกิดโรคระบาดในสถานที่ปฏิบัติงาน

๑.๒) กำหนดวัน เวลา ในการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ

๑.๓) ประชุมเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อเตรียมการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ

๒) ดำเนินการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ ตามกรณีที่เกิดภัย

กรมส่งเสริมการปกครองท้องถิ่น ได้กำหนดขั้นตอนการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติใน ๒ กรณี ได้แก่ กรณีอัคคีภัยและกรณีน้ำรั่ว ดังนี้

๒.๑) กรณีเกิดน้ำรั่ว ดำเนินการ ดังนี้

๒.๑.๑) ตรวจสอบการทำงานของระบบตรวจสอบและแจ้งเตือนภายในห้อง ควบคุมทั้งหมด

๒.๑.๒) เปิดพื้นห้องเพื่อดูแนวสายตรวจจับน้ำรั่ว

๒.๑.๓) จำลองเหตุการณ์การเกิดน้ำรั่วซึม โดยการนำน้ำมาหยดลงบนสายตรวจจับน้ำรั่ว

๒.๑.๔) อุปกรณ์ตรวจจับน้ำรั่ว จะแสดงพิกัดที่ตรวจสอบพบน้ำรั่ว

๒.๑.๕) ระบบตรวจจับน้ำรั่ว จะส่งข้อความเตือน Water Leak Alarm

๒.๑.๖) ทำการตรวจสอบ วิเคราะห์และประเมินว่าสามารถแก้ไขปัญหาได้หรือไม่ กรณีที่แก้ไขได้ให้นำผ้าไปซับน้ำบริเวณที่มีน้ำรั่ว รอจนกว่าระบบจะแจ้งเตือนว่า Water Leak back to normal และกรณีที่ไม่สามารถแก้ไขได้ให้ดำเนินการตามแนวทางปฏิบัติการแก้ไขปัญหาน้ำรั่ว ตามแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๒.๒) กรณีเกิดอัคคีภัย จะดำเนินการซ้อมแผนในส่วนที่ตรวจจับพบควันเท่านั้น เพื่อให้เกิดความปลอดภัยกับระบบมากที่สุด และเกิดผลกระทบกับส่วนอื่น ๆ น้อยที่สุด ซึ่งดำเนินการ ดังนี้

๒.๒.๑) ตรวจสอบการทำงานของระบบตรวจสอบและแจ้งเตือนภายในห้อง ควบคุมทั้งหมด

๒.๒.๒) จำลองเหตุการณ์การเกิดอัคคีภัย โดยการนำสเปรย์ควันมาฉีดที่บริเวณท่อตรวจจับควัน

๒.๒.๓) ระบบตรวจจับควัน จะตรวจสอบพบควัน

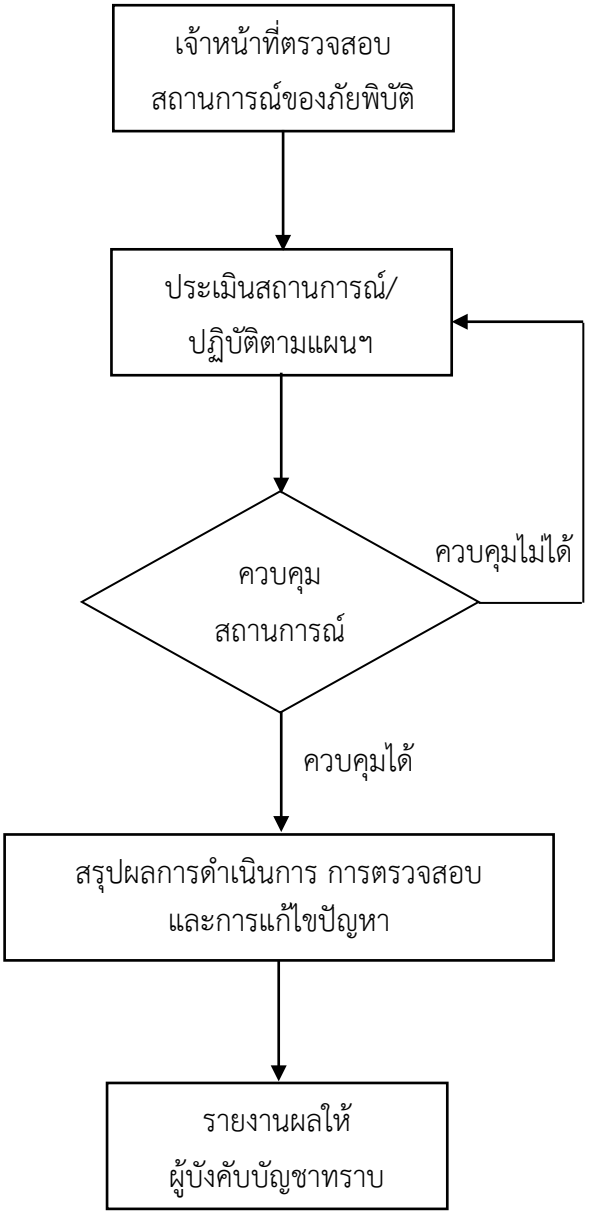
๒.๒.๔) ระบบตรวจจับควัน จะส่งข้อความเตือน SMOKE DETECTOR

๒.๒.๕) ทำการตรวจสอบ วิเคราะห์และประเมินสถานการณ์ว่าสามารถแก้ไขปัญหาได้หรือไม่ กรณีแก้ไขไม่ได้ให้แจ้งบุคลากรภายในศูนย์เทคโนโลยีสารสนเทศท้องถิ่นออกจากพื้นที่และปฏิบัติตามแนวทางปฏิบัติการแก้ไขปัญหาจากอัคคีภัย ตามแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๗. การติดตามและรายงานผล

เมื่อเกิดภัยพิบัติด้านระบบเทคโนโลยีสารสนเทศ ให้เจ้าหน้าที่ผู้รับผิดชอบรายงานการเกิดปัญหา และผลการแก้ไขให้ทราบในทันที ตามกระบวนการในการป้องกันและแก้ไขปัญหาภัยพิบัติ ตามแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) พร้อมทั้งสรุปรายงานผลการดำเนินการ การตรวจสอบและการแก้ไขปัญหาต่าง ๆ ให้ผู้บังคับบัญชาทราบ

ขั้นตอนการติดตามและรายงานผล



บรรณานุกรม

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570). **ราชกิจจานุเบกษา.** เล่ม ๑๓๙ ตอนพิเศษ ๒๘๘ ง. หน้า ๗.

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔. **ราชกิจจานุเบกษา.** เล่ม ๑๓๘ ตอนพิเศษ ๒๐๘ ง. หน้า ๙-๑๐.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕. **ราชกิจจานุเบกษา.** เล่ม ๑๒๙ ตอนพิเศษ ๑๙๑ ง. หน้า ๔๒.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (๒๕๖๕). *หลักการพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ*. เอกสารประกอบการสอนหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน, ออนไลน์.

สำนักงานตรวจสอบภายใน มหาวิทยาลัยราชภัฏเชียงใหม่. (๒๕๖๔). *คู่มือแผนการบริหารความเสี่ยง บริหารจัดการความเสี่ยง*. สืบค้น ๒๐ พฤษภาคม ๒๕๖๗, จาก https://internalaudit.cmru.ac.th/main/assets/files/document/20211213152421_doc.pdf

สำนักงานพัฒนารัฐบาลดิจิทัล. (๒๕๖๒). *นโยบายและคู่มือบริหารความเสี่ยง*. สืบค้น ๒๒ พฤษภาคม ๒๕๖๗, จาก https://www.dga.or.th/wp-content/uploads/2021/02/file_c0682ec125623dd091c945274a90dd99.pdf

ภาคผนวก

แบบรายงานการแก้ไขปัญหา/ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
กรมส่งเสริมการปกครองท้องถิ่น

๑.ชื่อความเสี่ยง/ภัย/ปัญหาที่พบ.....

๒.วันที่เกิดภัย.....เวลา.....

๓.สถานที่เกิดภัย.....

๔.ลักษณะการเกิดภัย/ความเสียหาย/ผลกระทบ.....
.....
.....
.....
.....

๕.ผู้รับผิดชอบ ชื่อ-สกุล.....ตำแหน่ง.....
สำนัก/กอง/กลุ่ม.....

๖.การดำเนินการแก้ไข

วิธีการแก้ไข	ผลการแก้ไข

๗.ปัญหา/อุปสรรค.....
.....
.....

๘.ผลการดำเนินการ

☐ แก้ไขความเสี่ยงได้
ระบุวัน/เวลาที่แก้ไขเสร็จ วันที่.....เวลา.....

☐ ไม่สามารถแก้ไขความเสี่ยงได้ เห็นควรดำเนินการ (ระบุ).....
.....
.....

ลงชื่อ
(.....)
ตำแหน่ง.....

แบบรายงานการซ้อมแผนแก้ไขปัญหา/ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
กรมส่งเสริมการปกครองท้องถิ่น

๑.ชื่อความเสี่ยง/ภัย/ปัญหา.....

๒.วัน/เดือน/ปี ที่ทำการซ้อมแผน.....เวลา.....

๓.สถานที่ ที่ทำการซ้อมแผน.....

๔.หน่วยงานผู้ดำเนินการ(ระบุชื่อสำนัก/กอง และกลุ่มงาน).....

๕.ผู้เข้าร่วมการซ้อมแผน

๑).....๔).....

๒).....๕).....

๓).....๖).....

๖.วิธีการ/ขั้นตอนการซ้อมแผน

ลำดับที่	วิธีการ/ขั้นตอนการซ้อมแผน
๑.	
๒.	
๓.	
๔.	
๕.	
๖.	
๗.	
๘.	
๙.	
๑๐.	

๗.ผลการซ้อมแผน

☐ แก้ไขปัญหาได้

☐ ไม่สามารถแก้ไขปัญหาได้

๘.ระบุผลการซ้อมแผนเพิ่มเติม (ถ้ามี).....

.....

.....

ลงชื่อ

(.....)

ตำแหน่ง.....

ประกาศกรมส่งเสริมการปกครองท้องถิ่น
เรื่อง นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk Management Policy)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ - ๒๕๖๘

.....

ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ได้กำหนดแนวปฏิบัติในการตรวจสอบประเมินความเสี่ยง และรับมือภัยคุกคามทางไซเบอร์ ประกอบกับประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ได้กำหนดนโยบายและกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศเพื่อให้หน่วยงานภาครัฐใช้เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ได้กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์เป็นวิธีการที่เชื่อถือได้ กรมส่งเสริมการปกครองท้องถิ่นตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตามกรอบแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ จึงออกประกาศนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management Policy) ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ – ๒๕๖๘ ดังนี้

ข้อ ๑ เพื่อให้การบริหารงานด้านเทคโนโลยีสารสนสนเทศเป็นไปตามหลักธรรมาภิบาล สามารถปฏิบัติงานบรรลุตามวิสัยทัศน์ พันธกิจ และเป้าหมายของกรมส่งเสริมการปกครองท้องถิ่นจึงกำหนดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ดีและเหมาะสม เพื่อสร้างความมั่นใจในการปฏิบัติงานของกรมส่งเสริมการปกครองท้องถิ่นได้อย่างมีประสิทธิภาพและประสิทธิผล

ข้อ ๒ มุ่งเน้นการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของกรมส่งเสริมการปกครองท้องถิ่นอยู่ในระดับที่ยอมรับได้ และไม่กระทบต่อทิศทางการบริหารงานตามแผนปฏิบัติราชการของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๓ กำหนดระดับความเสี่ยงที่ยอมรับได้ด้านเทคโนโลยีสารสนเทศในระดับต่ำ (Low Appetite) เพื่อให้สามารถสร้างความต่อเนื่องในการให้บริการและการบริหารจัดการที่มีคุณภาพ เนื่องจากกรมส่งเสริมการปกครองท้องถิ่นเป็นหน่วยงานที่ให้บริการและส่งเสริม สนับสนุนการปฏิบัติงานด้วยระบบเทคโนโลยีสารสนเทศให้กับหน่วยงานในสังกัดและองค์กรปกครองส่วนท้องถิ่น ผ่านระบบข้อมูลและเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัยสูง และมีศักยภาพในการให้บริการหน่วยงานที่เกี่ยวข้องอย่างต่อเนื่อง

/ข้อ ๔ ให้มีการ...

ข้อ ๔ ให้มีการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับกรม เพื่อให้หน่วยงานและบุคลากรในสังกัดใช้เป็นแนวทางปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ข้อ ๕ ให้มีการทบทวนนโยบายและแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมส่งเสริมการปกครองท้องถิ่น อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญ

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ เดือน สิงหาคม พ.ศ. ๒๕๖๗

(นายขจร ศรีชวโนทัย)
อธิบดีกรมส่งเสริมการปกครองท้องถิ่น

คำสั่งกรมส่งเสริมการปกครองท้องถิ่น
ที่ ๒๐๔ / ๒๕๖๕
เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
กรมส่งเสริมการปกครองท้องถิ่น

ตามคำสั่งกรมส่งเสริมการปกครองท้องถิ่น ที่ ๒๘๗/๒๕๖๒ ลงวันที่ ๒๖ มีนาคม ๒๕๖๒ ได้แต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมส่งเสริมการปกครองท้องถิ่น เพื่อกำหนดนโยบาย แนวทางการบริหารจัดการความเสี่ยงและดูแลรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น กำหนดแนวทางในการบริหารจัดการ ควบคุม แก้ไขปัญหาความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น และกำหนดแนวทางการดำเนินการกำกับดูแล ตรวจสอบเกี่ยวกับการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศกรมส่งเสริมการปกครองท้องถิ่น นั้น

เนื่องจากกรมส่งเสริมการปกครองท้องถิ่นได้ยกเลิกคำสั่งกรมส่งเสริมการปกครองท้องถิ่น ที่ ๖๔๖/๒๕๖๑ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๑ เรื่อง แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ของกรมส่งเสริมการปกครองท้องถิ่น และมีคำสั่ง ที่ ๘๕/๒๕๖๕ ลงวันที่ ๑๐ กุมภาพันธ์ ๒๕๖๕ เรื่อง แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) กรมส่งเสริมการปกครองท้องถิ่น ดังนั้น เพื่อให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นมีความพร้อมรองรับสถานการณ์ฉุกเฉิน ป้องกัน บรรเทาความรุนแรง ความเสียหายที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของ สถ. และมีความสอดคล้องกับสถานการณ์ปัจจุบัน จึงยกเลิกคำสั่งกรมส่งเสริมการปกครองท้องถิ่น ที่ ๒๘๗/๒๕๖๒ ลงวันที่ ๒๖ มีนาคม ๒๕๖๒ และแต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมส่งเสริมการปกครองท้องถิ่น ดังนี้

๑. รองอธิบดีกรมส่งเสริมการปกครองท้องถิ่น ผู้ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) กรมส่งเสริมการปกครองท้องถิ่น	ประธานกรรมการ
๒. ผู้อำนวยการสถาบันพัฒนาบุคลากรท้องถิ่น	กรรมการ
๓. ผู้อำนวยการสำนักพัฒนาระบบบริหารงานบุคคลส่วนท้องถิ่น	กรรมการ
๔. ผู้อำนวยการสำนักบริหารการคลังท้องถิ่น	กรรมการ
๕. ผู้อำนวยการกองพัฒนาและส่งเสริมการบริหารงานท้องถิ่น	กรรมการ
๖. ผู้อำนวยการกองส่งเสริมและพัฒนาการจัดการศึกษาท้องถิ่น	กรรมการ
๗. ผู้อำนวยการกองยุทธศาสตร์และแผนงาน	กรรมการ
๘. ผู้อำนวยการกองการเลือกตั้งท้องถิ่น	กรรมการ
๙. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศท้องถิ่น	กรรมการและเลขานุการ
๑๐. ผู้อำนวยการกลุ่มงานสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น	กรรมการและ ผู้ช่วยเลขานุการ
๑๑. ผู้อำนวยการกลุ่มงานระบบงานคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น	กรรมการและ ผู้ช่วยเลขานุการ

/๑๒. ผู้อำนวยการ...

๑๒. ผู้อำนวยการกลุ่มงานวิชาการคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น	กรรมการและ ผู้ช่วยเลขานุการ
๑๓. นักวิชาการคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น	กรรมการและ ผู้ช่วยเลขานุการ

โดยให้คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมส่งเสริมการปกครองท้องถิ่น มีอำนาจหน้าที่ดังนี้

๑) กำหนดนโยบาย แนวทางการบริหารจัดการความเสี่ยงและดูแลรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

๒) กำหนดแนวทางการกำกับดูแลตรวจสอบการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศกรมส่งเสริมการปกครองท้องถิ่น

๓) แต่งตั้งคณะอนุกรรมการหรือคณะทำงาน เพื่อพิจารณาหรือช่วยเหลือในการปฏิบัติงานของคณะกรรมการฯ ตามความจำเป็น

๔) ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๐ เมษายน พ.ศ. ๒๕๖๕

(นายประยูร รัตนเสนีย์)
อธิบดีกรมส่งเสริมการปกครองท้องถิ่น

คำสั่งศูนย์เทคโนโลยีสารสนเทศท้องถิ่น
ที่ ๔ / ๒๕๖๗
เรื่อง แต่งตั้งคณะทำงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น

ตามที่กรมส่งเสริมการปกครองท้องถิ่นได้คำนึงถึงความสำคัญของการใช้ข้อมูลสารสนเทศ การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ซึ่งอาจมีสภาวะความไม่แน่นอนที่ส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร และศูนย์เทคโนโลยีสารสนเทศท้องถิ่นได้มีคำสั่ง ที่ ๓/๒๕๖๒ ลงวันที่ ๒๗ มีนาคม ๒๕๖๒ แต่งตั้งคณะทำงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น นั้น

เนื่องจากกรมส่งเสริมการปกครองท้องถิ่นมีการปรับเปลี่ยนโยกย้ายบุคลากรของศูนย์เทคโนโลยีสารสนเทศท้องถิ่น ดังนั้น เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศท้องถิ่น มีการดำเนินการอย่างเป็นรูปธรรมมีความสอดคล้องตรงตามเป้าหมายของกรมส่งเสริมการปกครองท้องถิ่น มีความต่อเนื่องในการดำเนินการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงยกเลิกคำสั่งศูนย์เทคโนโลยีสารสนเทศท้องถิ่น ที่ ๓/๒๕๖๒ ลงวันที่ ๒๗ มีนาคม ๒๕๖๒ และแต่งตั้งคณะทำงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น โดยมีองค์ประกอบ ดังนี้

๑. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศท้องถิ่น	ประธานคณะทำงาน
๒. ผู้อำนวยการกลุ่มงานระบบงานคอมพิวเตอร์	คณะทำงาน
๓. ผู้อำนวยการกลุ่มงานสารสนเทศ	คณะทำงาน
๔. หัวหน้าฝ่ายบริหารทั่วไป	คณะทำงาน
๕. นักวิชาการคอมพิวเตอร์	คณะทำงาน
๖. ผู้อำนวยการกลุ่มงานวิชาการคอมพิวเตอร์	คณะทำงานและเลขานุการ
๗. บุคลากรสังกัดกลุ่มงานวิชาการคอมพิวเตอร์ ที่ได้รับมอบหมาย	คณะทำงานและผู้ช่วยเลขานุการ

ให้คณะทำงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น มีอำนาจหน้าที่ ดังนี้

๑. กำหนดแนวทางการบริหารจัดการความเสี่ยงและดูแลรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศท้องถิ่น

๒. กำหนดแนวทางในการบริหารจัดการควบคุมและแก้ไขปัญหาความเสี่ยงด้านเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศท้องถิ่น

๓. กำหนดแนวทางการกำกับดูแลตรวจสอบเกี่ยวกับการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศท้องถิ่น

๔. ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๓ กันยายน พ.ศ. ๒๕๖๗

(นายธีร์ พัฒนากูล)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศท้องถิ่น

ประกาศกรมส่งเสริมการปกครองท้องถิ่น
เรื่อง นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk Management Policy)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

.....

ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ได้กำหนดแนวปฏิบัติในการตรวจสอบประเมินความเสี่ยง และรับมือภัยคุกคามทางไซเบอร์ ประกอบกับประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ได้กำหนดนโยบายและกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศเพื่อให้หน่วยงานภาครัฐใช้เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ได้กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์เป็นวิธีการที่เชื่อถือได้ กรมส่งเสริมการปกครองท้องถิ่นตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตามกรอบแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๕ และที่แก้ไขเพิ่มเติม จึงออกประกาศนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management Policy) ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ดังนี้

ข้อ ๑ เพื่อให้การบริหารงานด้านเทคโนโลยีสารสนสนเทศเป็นไปตามหลักธรรมาภิบาล สามารถปฏิบัติงานบรรลุตามวิสัยทัศน์ พันธกิจ และเป้าหมายของกรมส่งเสริมการปกครองท้องถิ่นจึงกำหนดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ดีและเหมาะสม เพื่อสร้างความมั่นใจในการปฏิบัติงานของกรมส่งเสริมการปกครองท้องถิ่นได้อย่างมีประสิทธิภาพและประสิทธิผล

ข้อ ๒ มุ่งเน้นการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของกรมส่งเสริมการปกครองท้องถิ่นอยู่ในระดับที่ยอมรับได้ และไม่กระทบต่อทิศทางการบริหารงานตามแผนปฏิบัติราชการของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๓ กำหนดระดับความเสี่ยงที่ยอมรับได้ด้านเทคโนโลยีสารสนเทศในระดับต่ำ (Low Appetite) เพื่อให้สามารถสร้างความต่อเนื่องในการให้บริการและการบริหารจัดการที่มีคุณภาพ เนื่องจากกรมส่งเสริมการปกครองท้องถิ่นเป็นหน่วยงานที่ให้บริการและส่งเสริม สนับสนุนการปฏิบัติงานด้วยระบบเทคโนโลยีสารสนเทศให้กับหน่วยงานในสังกัดและองค์กรปกครองส่วนท้องถิ่น ผ่านระบบข้อมูลและเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัยสูง และมีศักยภาพในการให้บริการหน่วยงานที่เกี่ยวข้องอย่างต่อเนื่อง

/ข้อ ๔ ให้มีการ...

ข้อ ๔ ให้มีการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับกรม เพื่อให้หน่วยงานและบุคลากรในสังกัดใช้เป็นแนวทางปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ข้อ ๕ ให้มีการทบทวนนโยบายและแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมส่งเสริมการปกครองท้องถิ่น อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญ

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่๑๕ เดือน กันยายน พ.ศ. ๒๕๖๘

ร้อยตำรวจโท

(ภพชนก ชลานุเคราะห์)
อธิบดีกรมส่งเสริมการปกครองท้องถิ่น