แผนการบริหารจัดการความเสี่ยง และแผนแก้ไขปัญหาจากภัยพิบัติ ด้านเทคโนโลยีสารสนเทศจังหวัดชัยนาท

(IT Contingency Plan)



สารบัญ

หน้า

ส่วนที่ ๑ บทนำ

๑.๑ หลักการและเหตุผล..... ๑
๑.๒ วัตถุประสงค์..... ๑
๑.๓ เป้าหมาย..... ๑
๑.๔ ขอบเขตการดำเนินงาน..... ๑
๑.๕ ประโยชน์ที่คาดว่าจะได้รับ..... ๑

ส่วนที่ ๒ ความเป็นมาของการบริหารความเสี่ยง

ความหมายของการบริหารความเสี่ยง..... ๒

ส่วนที่ ๓ การประเมินความเสี่ยง

๓.๑ การวิเคราะห์ความเสี่ยง..... ๓
๓.๒ ลักษณะความเสี่ยง..... ๓
๓.๓ การประเมินความเสี่ยง..... ๕
๓.๔ การประมาณความเสี่ยง..... ๖
๓.๕ การประเมินค่าความเสี่ยง..... ๗
๓.๖ แผนภูมิความเสี่ยง..... ๘
๓.๗ การรายงานผลการวิเคราะห์ความเสี่ยง..... ๙
๓.๘ การจัดการความเสี่ยง..... ๑๐

ส่วนที่ ๔ แผนรองรับสถานการณ์ฉุกเฉินภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๔.๑ วัตถุประสงค์..... ๑๒
๔.๒ กรอบแนวทางในการจัดทำแผน..... ๑๒
๔.๒.๑ การวิเคราะห์และประเมินความรุนแรงของสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ..... ๑๒
๔.๒.๒ แนวทางการป้องกัน และการเตรียมการเบื้องต้น..... ๑๓
๔.๓ การเตรียมความพร้อม..... ๑๕
๔.๓.๑ ภัยพิบัติจากภายนอก..... ๑๕
๔.๓.๒ ภัยพิบัติจากภายใน..... ๑๖
๔.๔ การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ..... ๑๗
๔.๔.๑ ระดับนโยบาย..... ๑๗
๔.๔.๒ ระดับอำนวยการ..... ๑๗
๔.๔.๓ ระดับปฏิบัติ..... ๑๘
๔.๕ มาตรการในการป้องกันและแก้ไขปัญหาสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ..... ๑๘
๔.๕.๑ กรณีเครื่องคอมพิวเตอร์ลูกข่าย (Client)..... ๑๘
๔.๕.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server)..... ๑๘

สารบัญ (ต่อ)

หน้า

๔.๖ มาตรการปฏิบัติในการสำรองระบบงาน (Backup) และการนำข้อมูลกลับมาใช้ (Recovery)..... ๑๘

๔.๖.๑ ขั้นตอนในการสำรองระบบงาน (Backup)..... ๑๘

๔.๖.๒ ขั้นตอนในการนำข้อมูลกลับมาใช้ (Recovery)..... ๑๙

๔.๗ แผนการกู้คืนระบบกลับสู่สภาพปกติ..... ๑๙

๔.๘ การติดตามและรายงานผล..... ๑๙

แผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
จังหวัดชัยนาท

ส่วนที่ ๑

บทนำ

๑.๑ หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลที่ดี โดยช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงานตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่จังหวัด โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานในจังหวัด ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่าง ๆ จึงจำเป็นต้องมีการจัดการความเสี่ยงอย่างเป็นระบบ ทั้งนี้ต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด และหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของจังหวัดชัยนาท ซึ่งการบริหารจัดการความเสี่ยงมีวัตถุประสงค์เพื่อเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริง และนำแนวทางจัดการความเสี่ยงนี้ไปใช้ดำเนินการต่อไป

๑.๒ วัตถุประสงค์

๑. เพื่อควบคุมความเสี่ยงและสร้างความปลอดภัยให้กับระบบสารสนเทศของจังหวัด

๒. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของจังหวัด

๑.๓ เป้าหมาย

พัฒนาศักยภาพการจัดการระบบเทคโนโลยีสารสนเทศเพื่อประโยชน์ในการบริหารจัดการพัฒนาจังหวัดแบบบูรณาการให้เกิดการพัฒนาบุคลากรของจังหวัด โดยใช้เทคโนโลยีสารสนเทศที่เหมาะสม ทันสมัย และมีประสิทธิภาพ

๑.๔ ขอบเขตการดำเนินงาน

๑. ศึกษาวิเคราะห์ออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศของจังหวัดให้มีความเหมาะสมตอบสนองต่อการพัฒนาจังหวัดแบบบูรณาการได้อย่างมีประสิทธิภาพ

๒. พัฒนาศักยภาพบุคลากรของจังหวัดให้มีความรู้ความสามารถในด้านการใช้เทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพในการจัดการระบบข้อมูลสารสนเทศของจังหวัด

๑.๕ ประโยชน์ที่คาดว่าจะได้รับ

๑. หน่วยงานมีความพร้อมในการรับรองสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของจังหวัด

๒. การเชื่อมโยงระบบข้อมูลสารสนเทศ การดูแลรักษาเทคโนโลยีสารสนเทศ ของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่าย สามารถใช้งานได้อย่างมีประสิทธิภาพ

๓. มีแนวทางในการดูแลบำรุงรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของจังหวัดให้มีเสถียรภาพและมีความพร้อมใช้งานอย่างต่อเนื่อง

ความเป็นมาของการบริหารความเสี่ยง

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และส่งผลกระทบหรือสร้างความเสียหาย หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสบรรลุวัตถุประสงค์/เป้าหมายของจังหวัด ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวก โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่ทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงได้อย่างถูกต้อง

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

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

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

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee๓ of Sponsoring Organization of the Tread way Commission) มีดังนี้

๑. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
๒. การระบุความเสี่ยงต่าง ๆ (Event Identification)
๓. การประเมินความเสี่ยง (Risk Assessment)
๔. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
๕. กิจกรรมการบริหารความเสี่ยง (Control Activites)
๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
๗. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

การประเมินความเสี่ยง (Risk Assessment)

๓.๑ การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของจังหวัด โดยคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) สามารถแยกประเภทความเสี่ยงในด้านต่าง ๆ ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่เกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ ซึ่งอาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒. ความเสี่ยงจากอุปกรณ์ เป็นความเสี่ยงที่เกิดความเสื่อมสภาพของอุปกรณ์ต่าง ๆ ที่ส่งผลกระทบการดำเนินงานด้านดิจิทัล

๓. ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่เกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้เข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของจังหวัดเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการวางแนวนโยบายในการบริหารจัดการที่ส่งผลกระทบต่อการดำเนินการด้านดิจิทัล และความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก เพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้ได้

๕. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่เกิดขึ้นจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศของจังหวัด เช่น ไฟฟ้าขัดข้อง อุทกภัย อัคคีภัย แผ่นดินไหว อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓.๒ ลักษณะความเสี่ยง (Description of Risk)

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง / สิ่งคุกคาม	ผลกระทบ / ผู้ได้รับผลกระทบ
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้งานระบบ	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต	- ผู้ใช้งานระบบสารสนเทศ
๒. ความเสี่ยงจากการนำอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาต่อเชื่อม	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้งานระบบเครือข่าย เช่น การนำ Wireless router หรือ Switch/Hub มาเชื่อมต่อกับระบบเครือข่ายของจังหวัด โดยไม่ได้รับอนุญาต และไม่ได้ตั้งค่าเครื่องที่ถูกต้อง	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง / สิ่งคุกคาม	ผลกระทบ / ผู้ได้รับผลกระทบ
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากอุปกรณ์ / ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย	- แหล่งกำเนิดไฟฟ้าขัดข้อง หรือแรงดันไฟฟ้าไม่คงที่	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศและการสื่อสาร
๔. ความเสี่ยงจากภัยคุกคามทางไซเบอร์	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีทางไซเบอร์ เช่น Hacker, Malware, Phishing Mail และ Cross-site scripting (XSS) เป็นต้น	- แฮ็คเกอร์ / แคร็กเกอร์ - การโจมตีการให้บริการ (Denial of services/DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส / มัลแวร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศและการสื่อสาร
๕. ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะทางด้านดิจิทัล	ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยงด้านการบริหารจัดการ	บุคลากรขาดทักษะด้านดิจิทัล ทำให้การปฏิบัติงานไม่ต่อเนื่องและไม่มีประสิทธิภาพ	- นโยบายจากรัฐบาล	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศและการสื่อสาร
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	- นโยบายจากผู้บริหาร	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศและการสื่อสาร
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	- งบประมาณ - ทักษะบุคลากร	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง / สิ่งคุกคาม	ผลกระทบ / ผู้ได้รับผลกระทบ
๘. ความเสี่ยงจากการเกิดอัคคีภัย อุทกภัย แผ่นดินไหว	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศและการสื่อสาร - อุปกรณ์เครือข่าย
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงจากอุปกรณ์	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค ความเสื่อมสภาพ/ความสึกกร่อนของอุปกรณ์ หรือความเสียหายจากสัตว์กัดทำลาย	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยงด้านการบริหารจัดการ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงานหรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย
๑๒. ความเสี่ยงจากผู้รับจ้างหรือจัดจ้าง	ความเสี่ยงด้านการบริหารจัดการ	ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ	- ผู้รับจ้างไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้ได้	- ผู้ใช้งาน - ผู้ดูแลระบบ

๓.๓ การประเมินความเสี่ยง (Risk Estimation)

เป็นการประเมินความเสี่ยงในโอกาสของการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีความถี่มากน้อยเพียงใด และผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด ดังนี้

ระดับความถี่ในการเกิดเหตุการณ์/ระดับความรุนแรงของผลกระทบ

ระดับ	โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้น	ผลกระทบต่อองค์กร
๕	สูงมาก	๕ ครั้ง/ปี	มากกว่า ๑๐ ล้านบาท
๔	สูง	๔ ครั้ง/ปี	๕ แสนบาท – ๑๐ ล้านบาท
๓	ปานกลาง	๓ ครั้ง/ปี	๑ – ๕ แสนบาท
๒	น้อย	๒ ครั้ง/ปี	๑ หมื่นบาท – ๑ แสนบาท
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง/ปี	น้อยกว่า ๑ หมื่นบาท

๓.๔ การประมาณความเสี่ยง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ความถี่	ความรุนแรง
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	R๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความรอบคอบในการเข้าใช้ระบบสารสนเทศ เช่น มอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเข้าใช้งานระบบฯ	- การสวมรอยเป็นผู้ใช้ - การเข้าถึง ข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งานระบบสารสนเทศ ระบบฐานข้อมูล	๕	๔
๒. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ	R๐๒	ความเสี่ยงจากอุปกรณ์/สถานการณ์ฉุกเฉิน	กระแสไฟฟ้าขัดข้อง เครื่องคอมพิวเตอร์และอุปกรณ์อาจเสียหาย	แหล่งกำเนิดไฟฟ้าขัดข้อง/แรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน/ผู้ดูแลระบบ	๕	๒
๓. ความเสี่ยงจากภัยคุกคามทางไซเบอร์	R๐๓	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การโจมตีทางไซเบอร์ ได้แก่ Hacker, Malware, Phishing Mail, Cross-site scripting (XSS)	- Hacker - โจมตีการให้บริการ - ดักจับข้อมูล - ไวรัส/เวิร์ม	ผู้ใช้งาน/ผู้ดูแลระบบ	๓	๔
๔. ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะด้านดิจิทัล	R๐๔	ความเสี่ยงจากผู้ปฏิบัติงาน/ด้านการบริหารจัดการ	บุคลากรขาดทักษะด้านดิจิทัล ทำให้ปฏิบัติไม่ต่อเนื่อง/ไม่มีประสิทธิภาพ	นโยบายจากรัฐบาล	ผู้ใช้งาน/ผู้ดูแลระบบ	๕	๔
๕. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	R๐๕	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลง ส่งผลกระทบต่อโครงการต่างๆ		ผู้ใช้งาน/ผู้ดูแลระบบ	๑	๑
๖. ความเสี่ยงต่อการได้รับงบประมาณ	R๐๖	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณทำให้ระบบสารสนเทศไม่สามารถดำเนินการได้อย่างต่อเนื่อง		ผู้ใช้งาน/ผู้ดูแลระบบ	๕	๔

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ความถี่	ความรุนแรง
๗. ความเสี่ยงจากอัคคีภัย/อุทกภัย/แผ่นดินไหว	R๐๗	ความเสี่ยงจากภัย/สถานการณ์ฉุกเฉิน	การเกิดไฟไหม้/แผ่นดินไหว/น้ำท่วม อาจทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหาย	- อัคคีภัย - อุทกภัย - แผ่นดินไหว	ผู้ใช้งาน/ผู้ดูแลระบบ	๑	๕
๘. ความเสี่ยงจากเครื่องคอมพิวเตอร์/อุปกรณ์ไม่สามารถทำงานได้ตามปกติ	R๐๘	ความเสี่ยงจากอุปกรณ์	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุด/เสื่อมสภาพ/สัตว์กัดแทะ	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะ	ผู้ใช้งาน/ผู้ดูแลระบบ	๓	๔
๙. ความเสี่ยงจากการลักทรัพย์เครื่องคอมพิวเตอร์/อุปกรณ์	R๐๙	ความเสี่ยงจากผู้ปฏิบัติงาน/ด้านการบริหารจัดการ	การลักทรัพย์เครื่องคอมพิวเตอร์/อุปกรณ์/ชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงานได้	- การลักทรัพย์	ผู้ใช้งาน/ผู้ดูแลระบบ	๓	๑
๑๐. ความเสี่ยงจากผู้รับจ้างว่าจ้าง/จัดจ้าง	R๑๐	ความเสี่ยงด้านการบริหารจัดการ	เกิดจากการว่าจ้าง/จัดจ้างผู้ให้บริการภายนอกจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่างๆ	- ผู้รับจ้างไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดได้	ผู้ใช้งาน/ผู้ดูแลระบบ	๕	๔

๓.๕ การประเมินค่าความเสี่ยง

พิจารณาจากปัจจัยในขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้น ทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยที่มีผลต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ (ระดับความเสี่ยง = โอกาสในการเกิดเหตุ X ความรุนแรงของเหตุ) ซึ่งแบ่งเกณฑ์ ดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	พื้นที่สี
๑ – ๘	ต่ำ	ยอมรับความเสี่ยง	ขาว
๙ – ๑๖	ปานกลาง	ยอมรับความเสี่ยง (มาตรการติดตาม)	เหลือง
๑๗ – ๒๔	สูง	ควบคุมความเสี่ยง (แผนควบคุมความเสี่ยง)	ฟ้า
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

๓.๖ แผนภูมิความเสี่ยง

การวัดระดับความเสี่ยง

มาก

ความรุนแรง

ความเสี่ยงปานกลาง - ผลกระทบรุนแรงมาก - โอกาสเกิดน้อย	**ความเสี่ยงสูง** - ผลกระทบรุนแรงมาก - โอกาสเกิดมาก
ความเสี่ยงต่ำ - ผลกระทบน้อย - โอกาสเกิดน้อย	**ความเสี่ยงปานกลาง** - ผลกระทบน้อย - โอกาสเกิดมาก

น้อย ——— ความถี่ ———→ มาก

การประเมินความเสี่ยง

ความรุนแรง

๕	๕	๑๐	๑๕	๒๐	๒๕	สีแดง	ความเสี่ยงสูงมาก
๔	๔	๘	๑๒	๑๖	๒๐	สีฟ้า	ความเสี่ยงสูง
๓	๓	๖	๙	๑๒	๑๕	สีเหลือง	ความเสี่ยงปานกลาง
๒	๒	๔	๖	๘	๑๐		
๑	๑	๒	๓	๔	๕	สีขาว	ความเสี่ยงต่ำ (สามารถยอมรับได้)
	๑	๒	๓	๔	๕		

ความถี่

จากแผนภูมิความเสี่ยงสามารถประเมินค่าความเสี่ยงได้ ดังนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	R๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความรอบคอบในการเข้าใช้ระบบสารสนเทศ เช่น มอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเข้าใช้งานระบบฯ	๕	๔	๒๐
๒. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ	R๐๒	ความเสี่ยงจากอุปกรณ์/สถานการณ์ฉุกเฉิน	กระแสไฟฟ้าขัดข้อง เครื่องคอมพิวเตอร์และอุปกรณ์อาจเสียหาย	๕	๒	๑๐
๓. ความเสี่ยงจากภัยคุกคามทางไซเบอร์	R๐๓	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การโจมตีทางไซเบอร์ ได้แก่ Hacker, Malware, Phishing Mail, Cross-site scripting (XSS)	๓	๔	๑๒
๔. ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะด้านดิจิทัล	R๐๔	ความเสี่ยงจากผู้ปฏิบัติงาน/ด้านการบริหารจัดการ	บุคลากรขาดทักษะด้านดิจิทัล ทำให้ปฏิบัติไม่ต่อเนื่อง/ไม่มีประสิทธิภาพ	๕	๔	๒๐

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๕. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	R๐๕	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงส่งผลกระทบต่อโครงการต่างๆ	๑	๑	๑
๖. ความเสี่ยงต่อการได้รับงบประมาณ	R๐๖	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณทำให้ระบบสารสนเทศไม่สามารถดำเนินการได้อย่างต่อเนื่อง	๕	๔	๒๐
๗. ความเสี่ยงจากอัคคีภัย/อุทกภัย/แผ่นดินไหว	R๐๗	ความเสี่ยงจากภัย/สถานการณ์ฉุกเฉิน	การเกิดไฟไหม้/ แผ่นดินไหว/น้ำท่วม อาจทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหาย	๑	๕	๕
๘. ความเสี่ยงจากเครื่องคอมพิวเตอร์/อุปกรณ์ไม่สามารถทำงานได้ตามปกติ	R๐๘	ความเสี่ยงจากอุปกรณ์	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุด/เสื่อมสภาพ/สัตว์กัดแทะ	๓	๔	๑๒
๙. ความเสี่ยงจากการลักทรัพย์เครื่องคอมพิวเตอร์/อุปกรณ์	R๐๙	ความเสี่ยงจากผู้ปฏิบัติงาน/ด้านการบริหารจัดการ	การลักทรัพย์เครื่องคอมพิวเตอร์/อุปกรณ์/ชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงานได้	๓	๑	๓
๑๐. ความเสี่ยงจากผู้รับจ้างว่าจ้าง/จัดจ้าง	R๑๐	ความเสี่ยงด้านการบริหารจัดการ	เกิดจากการว่าจ้าง/จัดจ้างผู้ให้บริการภายนอกจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่างๆ	๕	๔	๒๐

๓.๗ การรายงานผลการวิเคราะห์ความเสี่ยง

สามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศในการบริหารจัดการได้ ดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	R๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความรอบคอบในการเข้าใช้ระบบสารสนเทศ เช่น มอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเข้าใช้งานระบบฯ	๒๐
๒	R๐๔ ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะด้านดิจิทัล	ความเสี่ยงจากผู้ปฏิบัติงาน/ด้านการบริหารจัดการ	บุคลากรขาดทักษะด้านดิจิทัล ทำให้ปฏิบัติไม่ต่อเนื่อง/ไม่มีประสิทธิภาพ	๒๐
๓	R๐๖ ความเสี่ยงต่อการได้รับงบประมาณ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณทำให้ระบบสารสนเทศไม่สามารถดำเนินการได้อย่างต่อเนื่อง	๒๐

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๔	R๑๐ ความเสี่ยงจากผู้รับจ้างว่าจ้าง/จัดจ้าง	ความเสี่ยงด้านการบริหารจัดการ	เกิดจากการว่าจ้าง/จัดจ้างผู้ให้บริการภายนอกจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่างๆ	๒๐
๕	R๐๓ ความเสี่ยงจากภัยคุกคามทางไซเบอร์	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การโจมตีทางไซเบอร์ ได้แก่ Hacker, Malware, Phishing Mail, Cross-site scripting (XSS)	๑๒
๖	R๐๘ ความเสี่ยงจากเครื่องคอมพิวเตอร์/อุปกรณ์ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงจากอุปกรณ์	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุด/เสื่อมสภาพ/สัตว์กัดแทะ	๑๒
๗	R๐๒ ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับ	ความเสี่ยงจากอุปกรณ์/สถานการณ์ฉุกเฉิน	กระแสไฟฟ้าขัดข้อง เครื่องคอมพิวเตอร์และอุปกรณ์อาจเสียหาย	๑๐
๘	R๐๗ ความเสี่ยงจากอัคคีภัย/อุทกภัย/แผ่นดินไหว	ความเสี่ยงจากภัย/สถานการณ์ฉุกเฉิน	การเกิดไฟไหม้/ แผ่นดินไหว/น้ำท่วม อาจทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหาย	๕
๙	R๐๙ ความเสี่ยงจากการลักทรัพย์เครื่องคอมพิวเตอร์/อุปกรณ์	ความเสี่ยงจากผู้ปฏิบัติงาน/ด้านการบริหารจัดการ	การลักทรัพย์เครื่องคอมพิวเตอร์/อุปกรณ์/ชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงานได้	๓
๑๐	R๐๕ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงส่งผลกระทบต่อโครงการต่างๆ	๑

๓.๘ การจัดการความเสี่ยง

นโยบายของจังหวัดชัยนาท ระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤๙ ซึ่งสำนักงาน ก.พ.ร. กำหนดให้ความเสี่ยงจำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยง ดังนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑	R๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๒๐	- ควบคุมความเสี่ยง (แผนควบคุมความเสี่ยง)	- สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการรักษาสิทธิ์ของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติรักษาความมั่นคงปลอดภัยสารสนเทศ
๒	R๐๔ ความเสี่ยงจากการขาดแคลนบุคลากรที่มีทักษะด้านดิจิทัล	๒๐	- ควบคุมความเสี่ยง (แผนควบคุมความเสี่ยง)	- ส่งเสริมให้บุคลากรเข้ารับการอบรมด้านดิจิทัล
๓	R๐๖ ความเสี่ยงต่อการได้รับงบประมาณ	๒๐	- ควบคุมความเสี่ยง (แผนควบคุมความเสี่ยง)	

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๔	R๑๐ ความเสี่ยงจากผู้รับจ้างว่าจ้าง/จัดจ้าง	๒๐	- ควบคุมความเสี่ยง (แผนควบคุมความเสี่ยง)	- จัดหาเครื่องคอมพิวเตอร์/อุปกรณ์สำรองให้ใช้งานทดแทน - ทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องคอมพิวเตอร์/อุปกรณ์เป็นประจำ
๕	R๐๓ ความเสี่ยงจากภัยคุกคามทางไซเบอร์	๑๒	- ยอมรับความเสี่ยง (มาตรการติดตาม)	- ตรวจสอบ Firewall อย่างสม่ำเสมอ - ติดตั้งระบบรักษาความมั่นคงปลอดภัยไซเบอร์
๖	R๐๘ ความเสี่ยงจากเครื่องคอมพิวเตอร์/อุปกรณ์ไม่สามารถทำงานได้ตามปกติ	๑๒	- ยอมรับความเสี่ยง (มาตรการติดตาม)	- ตรวจสอบ บำรุง ซ่อมแซมอุปกรณ์คอมพิวเตอร์เป็นประจำ - จัดหาอุปกรณ์สำรองเพื่อใช้ทดแทนอุปกรณ์ที่ชำรุด
๗	R๐๒ ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับ	๑๐	- ยอมรับความเสี่ยง (มาตรการติดตาม)	- จัดทำแผนรับสถานการณ์เพื่อให้ปฏิบัติงานได้อย่างต่อเนื่อง - สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่ที่เหมาะสม
๘	R๐๗ ความเสี่ยงจากอัคคีภัย/อุทกภัย/แผ่นดินไหว	๕	- ยอมรับความเสี่ยง	- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันแรงดันไฟฟ้าไม่คงที่ - จัดทำแผนรับสถานการณ์เพื่อให้ปฏิบัติงานได้อย่างต่อเนื่อง
๙	R๐๙ ความเสี่ยงจากการลักทรัพย์เครื่องคอมพิวเตอร์/อุปกรณ์	๓	- ยอมรับความเสี่ยง	- รักษาความปลอดภัยอาคารสถานที่คัดกรองคนจากภายนอกที่เข้ามาติดต่อราชการ - ปลูกฝังคุณธรรมจริยธรรมแก่บุคลากรภายใน
๑๐	R๐๕ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๑	- ยอมรับความเสี่ยง	

แผนรองรับสถานการณ์ฉุกเฉินภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

เพื่อให้การจัดการฐานข้อมูล การจัดเก็บดูแลรักษาข้อมูลสารสนเทศ และการเฝ้าระวัง เกิดความมั่นคงปลอดภัย และพร้อมใช้งานอย่างเต็มประสิทธิภาพ การนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการองค์กร การเลือกใช้วิธีการบริหารจัดการความเสี่ยงอย่างเหมาะสมทั้งภายนอกและภายใน ให้อยู่ในระดับที่สามารถยอมรับได้ จังหวัดชัยนาท จึงมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ ระบบเครือข่าย เพื่อแก้ไขปัญหาจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ซึ่งเป็นแนวทางการดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และมาตรการควบคุมเพื่อป้องกัน ลดความเสี่ยงที่สร้างความเสียหายได้ทั้งทางตรงและทางอ้อมของระบบเทคโนโลยีสารสนเทศ

๔.๑ วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดำเนินการ กำกับดูแล ตรวจสอบการบริหารจัดการ และดูแลรักษาระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งาน และเฝ้าระวังความเสี่ยงใหม่ ๆ ที่อาจเกิดขึ้นได้ตลอดเวลา พร้อมสร้างความเข้าใจให้แก่บุคลากรเพื่อให้สามารถบริหารจัดการได้อย่างเป็นระบบและมีประสิทธิภาพ

๒. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น ลดความเสี่ยงจากภัยคุกคามในการโจมตีระบบเทคโนโลยีสารสนเทศของจังหวัดชัยนาท

๓. เพื่อเป็นแนวทางการบริหารจัดการภัยคุกคามระบบสารสนเทศของจังหวัดชัยนาทให้สามารถดำเนินการได้อย่างต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้ทันที

๔.๒ กรอบแนวทางในการจัดทำแผน

การจัดทำแผนรองรับสถานการณ์ฉุกเฉินภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) มีแนวทางในการดูแลรักษาและแก้ไขปัญหาที่ส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของจังหวัด ดังนี้

๑. การวิเคราะห์และประเมินความรุนแรงของสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ
๒. แนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ
๕. มาตรการในการป้องกันและแก้ไขปัญหาสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ
๖. กระบวนการในการป้องกันและแก้ไขปัญหาสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ
๗. แผนกู้คืนระบบกลับสู่สภาพปกติ
๘. การติดตามและรายงานผล

๔.๒.๑ การวิเคราะห์และประเมินความรุนแรงของสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ

จากการวิเคราะห์และตรวจสอบความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศ มีดังนี้

๑. สถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติจากภายนอก
   ๑.๑ การเชื่อมโยงระบบเครือข่ายขัดข้อง
   ๑.๒ ระบบกระแสไฟฟ้าขัดข้อง/อัคคีภัย/อุทกภัย/แผ่นดินไหว

๑.๓ การลักทรัพย์เครื่องคอมพิวเตอร์/อุปกรณ์ที่เกี่ยวข้อง

๑.๔ การบุกรุก/โจมตีจากภายนอกเพื่อควบคุมระบบเทคโนโลยีสารสนเทศ เพื่อสร้างความเสียหาย/ทำลายข้อมูล ไวรัสคอมพิวเตอร์ การก่อกวนจาก Hacker การเจาะระบบข้อมูล รวมถึงการนำอุปกรณ์อื่น ๆ มาเชื่อมต่อกับระบบภายในองค์กร

๑.๕ การจ้างผู้รับจ้าง

๒. สถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติจากภายใน

๒.๑ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๒.๒ ภัยจากผู้ใช้งานระบบ

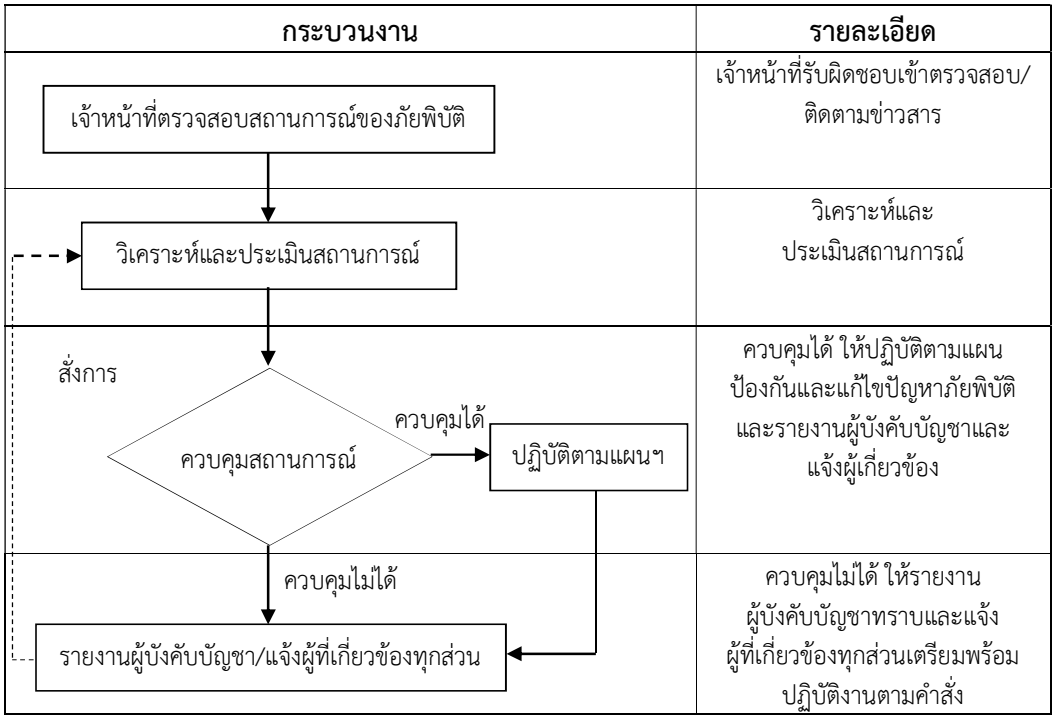
๒.๓ การเปลี่ยนแปลงนโยบายของผู้บริหาร

๒.๔ การได้รับงบประมาณไม่เพียงพอ

๒.๕ ระบบคอมพิวเตอร์/อุปกรณ์ต่าง ๆ เสียหาย

๔.๒.๒ แนวทางการป้องกัน และการเตรียมการเบื้องต้น

๑. แนวทางการดำเนินการเบื้องต้น



๒. แนวทางการป้องกันและเตรียมการเบื้องต้น

๑) การประกาศแผน

ประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทราบและปฏิบัติตามอย่างเคร่งครัด เพื่อเป็นแนวทางในการปฏิบัติตามแผนเมื่อเกิดเหตุการณ์ฉุกเฉิน

๒) กระบวนการดำเนินงาน

จังหวัดชัยนาทได้จัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดในองค์กรเมื่อเกิดเหตุการณ์ฉุกเฉินโดยเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น พร้อมรวบรวมเหตุการณ์ที่เกิดขึ้นเพื่อยุติเหตุการณ์ได้อย่างถูกต้อง

๓) การติดต่อสื่อสาร

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอกเพื่อใช้ในการติดต่อทางด้านความมั่นคงปลอดภัย ได้แก่ การไฟฟ้าส่วนภูมิภาคจังหวัดชัยนาท สถานีดับเพลิงของเทศบาลเมืองชัยนาท และสถานีตำรวจภูธรเมืองชัยนาท

๔) การจัดเตรียมอุปกรณ์ที่จำเป็น

มีการเตรียมพร้อมรับภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ได้แก่ แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/ระบบงานที่สำคัญ/อุปกรณ์สำรองข้อมูล/แผ่นโปรแกรม Antivirus หรือ Spyware/ระบบสำรองไฟฉุกเฉิน

๕) การสำรองข้อมูล

เพื่อป้องกันการเสียหายที่เกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัส/ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล ซึ่งสามารถนำข้อมูลที่เสียหายกลับมาใช้งานได้ทันที

๖) การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยองค์กรมีนโยบายป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี

๗) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เพื่อป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าที่สร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

- ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายกับอุปกรณ์คอมพิวเตอร์
- เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้สามารถใช้งานได้อยู่เสมอ
- เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้รีบบันทึกข้อมูลที่ค้างทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ
- ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมใช้งานอยู่เสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๘) การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

- มีการดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์
- มีมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่เกี่ยวข้องเข้าในห้องควบคุมระบบเครือข่าย
- มีการติดตั้ง Firewall ป้องกันการบุกรุกโดยเปิดใช้งาน Firewall ตลอดเวลา
- มีการติดตั้ง Proxy Server เพิ่มประสิทธิภาพบริการอินเตอร์เน็ตขององค์กร รวมถึงกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์
- มีเจ้าหน้าที่ดูแลระบบเครือข่าย เพื่อตรวจสอบความผิดปกติของระบบสารสนเทศและระบบเครือข่ายขององค์กร

๙) การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

- เตรียมอุปกรณ์ยังชีพ เช่น ยารักษาโรค ไฟฉาย และแจ้งให้ทุกทราบถึงที่เก็บ
- ซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน
- ทราบตำแหน่งวาล์วน้ำประปา/สะพานไฟฟ้า และถังก๊าซ (ถ้ามี)

- ผูก/ยึดเครื่องใช้ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง
- ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๔.๓ การเตรียมความพร้อม

๔.๓.๑ ภัยพิบัติจากภายนอก

๑. ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของระบบเครือข่ายและระบบสารสนเทศ ได้แก่ อัคคีภัย อุทกภัย แผ่นดินไหว ความชื้น อุณหภูมิที่ผิดปกติ และสัตว์กัดแทะ

๑.๑ การดำเนินการและการป้องกันด้านอัคคีภัย ดังนี้

- กำหนดเวรรักษาความปลอดภัย
- มีการซ้อมแผนอัคคีภัย
- ติดตั้งถังดับเพลิงในห้องระบบสารสนเทศ/เครือข่าย และในอาคาร
- มีเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์ที่ต้องเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

๑.๒ การดำเนินการและการป้องกันด้านอุทกภัย ความชื้น และอุณหภูมิที่ผิดปกติ

- เปิดเครื่องปรับอากาศสำหรับระบบสารสนเทศและเครือข่ายตลอด ๒๔ ชั่วโมง พร้อมทั้งตรวจสอบการทำงานให้ใช้งานได้ตลอดเวลา
- ติดตามข่าวภัยพิบัติตามสถานการณ์ที่เกิดขึ้น

๑.๓ การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็นกรณีเกิดแผ่นดินไหว

- เตรียมอุปกรณ์ยังชีพ เช่น ยารักษาโรค ไฟฉาย และแจ้งให้ทุกทราบถึงที่เก็บ
- ซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน
- ทราบตำแหน่งวาล์วน้ำประปา/สะพานไฟฟ้า และถังก๊าซ (ถ้ามี)
- ผูก/ยึดเครื่องใช้ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง
- ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๒. การลักทรัพย์อุปกรณ์คอมพิวเตอร์แม่ข่ายสำหรับจัดเก็บข้อมูล

ควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่เกี่ยวข้องเข้าในห้องควบคุมระบบเครือข่าย

- มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย พร้อมทั้งตรวจสอบการทำงานของระบบอย่างสม่ำเสมอ
- ติดตั้งระบบกล้องโทรทัศน์วงจรปิด

๓. ระบบการเชื่อมโยงเครือข่ายขัดข้อง

๓.๑ ตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา

๓.๒ จัดให้มีเครือข่ายสำรอง สำหรับกรณีที่เครือข่ายหลักไม่สามารถใช้งานได้

๓.๓ ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อแก้ไขปัญหา

๔. ระบบกระแสไฟฟ้าขัดข้อง

๔.๑ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์

๔.๒ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาที่ใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่สภาพพร้อมใช้งานตลอดเวลา

๔.๓ เมื่อกระแสไฟฟ้าขัดข้องให้ผู้ใช้งานบันทึกข้อมูลที่ดำเนินการค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์พร้อมอุปกรณ์ต่าง ๆ

๔.๔ สำรองข้อมูลที่สำคัญบนสื่อตามความเหมาะสม เช่น External Hard disk, Handy drive เป็นต้น

๕. ภัยการบุกรุกหรือโจมตีจากภายนอกเพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายฐานข้อมูล ไวรัสคอมพิวเตอร์ หรือการก่อกวนจาก Hacker หรือการเจาะทำลายระบบจาก Cracker

๕.๑ กำหนดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่าย เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีสิ่งใดผิดปกติหรือไม่ เพื่อเตรียมการป้องกันต่อไป

๕.๒ ใช้เครื่องมือในการค้นหาช่องโหว่และอัพเดท Patch เพื่อปิดกั้นช่องโหว่นั้น

๕.๓ ติดตั้ง Firewall ป้องกันผู้บุกรุกจากระบบเครือข่ายโดยเปิดระบบ Firewall ตลอดเวลา

๕.๔ ติดตั้ง Proxy Server เพิ่มประสิทธิภาพการให้บริการอินเตอร์เน็ต และกลั่นกรองข้อมูลทางเว็บไซต์

๕.๕ ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้อัพเดทอย่างสม่ำเสมอ และปิดพอร์ทที่ไม่มีการใช้งาน

๕.๖ กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้อนุญาต ให้ยากต่อการคาดเดา มีความยาวอย่างน้อย ๘ อักขระ ไม่ใช้รหัสร่วมกับผู้อื่น หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานอื่น ๆ

๕.๗ นำระบบ DMZ มาป้องกันการปลอมแปลง IP Address โดยการกรอง Packet ที่มาจากภายนอก

๕.๘ ติดตั้งระบบเครือข่ายให้สามารถป้องกันการโจมตีแบบ DOS/DDOS ได้

๖. ไวรัสคอมพิวเตอร์

๖.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทโปรแกรมป้องกันไวรัสอยู่เสมอ โดยสแกนตรวจหาไวรัสอย่างน้อย ๑ ครั้ง/สัปดาห์

๖.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกต่าง ๆ โดยการสแกนตรวจหาไวรัสก่อนใช้งานทุกครั้ง ไม่เปิดไฟล์นามสกุลที่น่าสงสัย ไม่ใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

๖.๓ ใช้ความระมัดระวังในการเปิด E-mail ที่ไม่ทราบที่มา และลบ E-mail ที่น่าสงสัยทิ้งทันที

๖.๔ ระวังการดาวน์โหลดไฟล์ต่าง ๆ จากอินเตอร์เน็ต

๖.๕ ปิดการใช้งานฟังก์ชัน Autoplay ป้องกันไวรัสผ่านทางสื่อเก็บข้อมูลแบบพกพาที่ใช้การรันไฟล์ไวรัสโดยอัตโนมัติ

๔.๓.๒ ภัยพิบัติจากภายใน

๑. ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๑.๑ กำหนดให้เจ้าหน้าที่สำรองข้อมูลด้วยระบบ Manual ตามระยะเวลาที่กำหนดทุกสัปดาห์ลงในสื่อบันทึก

๑.๒ สำรองข้อมูลโดยอัตโนมัติลงในสื่อบันทึกทุกวัน

๑.๓ กำหนดเจ้าหน้าที่บำรุงรักษาสื่อบันทึกข้อมูลเพื่อลดความเสียหายของข้อมูล

๑.๔ ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้สำรองไว้ในสื่อบันทึก

๒. ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๒.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๒.๒ สร้างความรู้ความเข้าใจเบื้องต้นในการป้องกันและแก้ไขปัญหาจากไวรัสคอมพิวเตอร์

๓. การจัดเตรียมอุปกรณ์ที่จำเป็น

๓.๑ แผ่น Driver อุปกรณ์ต่าง ๆ รวมถึงแผ่นติดตั้งระบบปฏิบัติการระบบงานที่สำคัญ

๓.๒ สื่อบันทึกที่สำรองข้อมูลและระบบงานที่สำคัญ

๓.๓ แผ่นโปรแกรม Antivirus/Spyware รวมถึงระบบสำรองไฟฟ้าฉุกเฉิน

๓.๔ สำรองอุปกรณ์ต่าง ๆ ของเครื่องคอมพิวเตอร์ที่สำคัญ

๔. การสำรองข้อมูล (Back Up)

๔.๑ สำรองข้อมูลโดยอัตโนมัติลงในสื่อบันทึก จำนวน ๑ ชุด

๔.๒ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ โดยมีไฟฟ้าสำรองใช้ได้ประมาณ ๓๐-๖๐ นาที

๔.๓ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาที่ใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่สภาพพร้อมใช้งานตลอดเวลา

๔.๔ กำหนดให้เจ้าหน้าที่สำรองข้อมูลด้วยระบบ Manual ตามระยะเวลาที่กำหนดทุกสัปดาห์ลงในสื่อบันทึก ได้แก่ โครงสร้างข้อมูล และ Source Code

๕. การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

๕.๑ มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและป้องกันความเสียหายโดยห้ามบุคคลที่ไม่เกี่ยวข้องเข้าในห้องควบคุมระบบเครือข่าย

๕.๒ ติดตั้ง Firewall ป้องกันผู้บุกรุกจากระบบเครือข่ายโดยเปิดระบบ Firewall ตลอดเวลา

๕.๓ ติดตั้ง Proxy Server เพิ่มประสิทธิภาพการให้บริการอินเตอร์เน็ต และกลั่นกรองข้อมูลทางเว็บไซต์

๕.๔ กำหนดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่าย เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีสิ่งใดผิดปกติหรือไม่ เพื่อเตรียมการป้องกันต่อไป

๕.๕ ดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์

๔.๔ การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ

๔.๔.๑ ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามการกำกับ ดูแล ควบคุม และตรวจสอบ

๔.๔.๒ ระดับอำนวยการ

หัวหน้าส่วนราชการในพื้นที่จังหวัดชัยนาท มีหน้าที่แก้ไขปัญหาจากภัยพิบัติ ควบคุม ตรวจสอบ กำกับดูแลการประเมินสถานการณ์ และตัดสินใจในกรณีที่ฝ่ายปฏิบัติงานประเมินสถานการณ์และรายงานการประเมินเบื้องต้นว่าอาจไม่สามารถควบคุมสถานการณ์ได้ ต้องปฏิบัติงานนอกเหนือจากแผนป้องกันปัญหาจากภัยพิบัติที่กำหนดไว้ หรือสถานการณ์ยังไม่เกิดหรือมีแนวโน้มอาจจะเกิดขึ้น รายงานผลต่อผู้บังคับบัญชา

๔.๔.๓ ระดับปฏิบัติ

เจ้าหน้าที่ที่รับผิดมอบหมายของส่วนราชการในพื้นที่จังหวัดชัยนาท มีหน้าที่ดำเนินการตามแผนป้องกันและแก้ไขปัญหาเกี่ยวกับภัยพิบัติรายงานผลการดำเนินการตามแผน ทบทวนแผน ประเมินสถานการณ์ ติดต่อประสานงานฝ่ายต่าง ๆ ที่เกี่ยวข้อง รวมทั้งขอรับการสนับสนุนจากหน่วยงานภายนอกหรือบริษัทคู่สัญญาตรวจสอบและประเมินผล รวมทั้งด้าน Hardware และ Software พร้อมจัดทำรายงานความเสียหาย เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน มี ๔ ด้าน ดังนี้

๑. ด้านฐานข้อมูลและระบบสารสนเทศ มีหน้าที่ในการจัดการแก้ไขปัญหาที่เกิดภัยต่าง ๆ ประสานงาน กู้คืนข้อมูลระบบงาน ประเมินสถานการณ์ต่าง ๆ ตลอดจนติดตั้งระบบงาน และฐานข้อมูลให้พร้อมใช้งาน

๒. ด้านโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร มีหน้าที่แก้ไขปัญหาสถานที่สำหรับเว็บไซต์สำรองและระบบไฟฟ้าให้พร้อมใช้งาน

๓. ด้านระบบสื่อสารและเครือข่าย มีหน้าที่จัดการเตรียมอุปกรณ์/ระบบสื่อสารให้พร้อมใช้งาน รวมถึงตรวจสอบและประเมินความเสียหาย

๔. ด้านสนับสนุนการแก้ไขปัญหาจากภัยพิบัติ มีหน้าที่สนับสนุนแก้ไขปัญหาจากภัยพิบัติตามที่ฝ่ายปฏิบัติงานร้องขอ

๔.๕ มาตรการในการป้องกันและแก้ไขปัญหาสถานการณ์ฉุกเฉิน/เหตุการณ์ภัยพิบัติ

๔.๕.๑ กรณีเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๑. กรณีเครื่องคอมพิวเตอร์ไม่สามารถใช้งานระบบสารสนเทศได้ตามปกติให้เจ้าหน้าที่แจ้งเหตุให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศของหน่วยงานทราบ

๒. กรณีถูกไวรัสคอมพิวเตอร์เพื่อป้องกันความเสียหายให้ดึงสายเชื่อมโยงระบบเครือข่ายออกจากเครื่องโดยเร็ว

๔.๕.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑. ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว และปิดอุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒. กรณีไฟฟ้าตก/ดับ ให้ปิดเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย ตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่เกิดเหตุ ประสิทธิภาพของเครื่องสำรองไฟฟ้าและเครื่องกำเนิดไฟฟ้า

๓. ตัดระบบจ่ายไฟ

๔. ตรวจสอบปัญหาที่เกิดขึ้น กรณีที่ไม่ปลอดภัยให้ขนย้ายไปไว้ในที่ปลอดภัย

๕. กรณีเกิดอัคคีภัยให้ดับเพลิงด้วยระบบดับเพลิงอัตโนมัติ

๖. ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๗. กรณีอุปกรณ์ฮาร์ดแวร์เสีย ให้หาอุปกรณ์สำรองมาทดแทน หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๘. ผู้ดูแลระบบต้องรีบแจ้งให้หัวหน้าส่วนราชการนั้น ๆ ทราบโดยเร็ว

๔.๖ มาตรการปฏิบัติในการสำรองระบบงาน (Backup) และการนำข้อมูลกลับมาใช้ (Recovery)

๔.๖.๑ ขั้นตอนในการสำรองระบบงาน (Backup)

๑. ทำการสำรองฐานข้อมูลเป็น Database ลงดิสก์ (Disk) เก็บไว้ที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) ศาลากลางจังหวัดชัยนาท ชั้น ๓ เวลา ๒๒.๐๐ น. ทุกวัน

๒. ทำการสำรองโปรแกรมประยุกต์ (Application) โดยการสำรองลงเทป (Tape) เก็บไว้ที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) ศาลากลางจังหวัดชัยนาท ชั้น ๓ เวลา ๒๐ น. ของทุกวันที่ ๒๘ ของเดือน และทำการคัดลอก (Copy) เก็บไว้อีกชุดที่สำนักงานจังหวัดชัยนาท ชั้น ๒ ศาลากลางจังหวัดชัยนาท

๔.๖.๒ ขั้นตอนในการนำข้อมูลกลับมาใช้ (Recovery)

๑. ดำเนินการกู้คืนระบบงานเพื่อเริ่มต้นการทำงานของเครื่องแม่ข่ายเสมือนที่ศูนย์สำรองข้อมูลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.มท.

๒. นำแผ่นระบบปฏิบัติการมาติดตั้งใหม่ เพื่อติดตั้งโปรแกรมพื้นฐานตามการใช้งาน โดยการนำเทป (Tape) มากู้คืนระบบ (Recovery)

๔.๗ แผนการกู้คืนระบบกลับสู่สภาพปกติ

ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ โดยปกติต้องอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆ ได้ ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุด เนื่องจากเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณต้องทำงานด้านบริการ (Service) แก่เครื่องลูกข่ายให้สามารถใช้งานได้ปกติ การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณจำเป็นต้องทำอย่างรวดเร็ว เพื่อให้ใช้งานได้อย่างรวดเร็วที่สุด แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และแฟ้มข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๑. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
๒. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง
๔. นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา restore ใช้
๕. ทีมกู้ระบบ (ผู้ดูแลระบบ นักวิชาการคอมพิวเตอร์ และบริษัทที่ปรึกษา) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง
๖. ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

๔.๘ การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ เมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉิน ให้หัวหน้าสำนักงานจังหวัดทราบ เพื่อนำเสนอรายงานสรุปการเกิดปัญหา และผลการแก้ไขให้ผู้บังคับบัญชาทราบในทันทีตามแผนกระบวนการในการป้องกันและแก้ไขปัญหาภัยพิบัติในทุกกรณี พร้อมทั้งสรุปรายงานผลการดำเนินการ การตรวจสอบ และการแก้ไขปัญหาต่าง ๆ ให้ผู้บังคับบัญชาทราบ