

นโยบายและแนวทางปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศและการสื่อสาร จังหวัดชัยนาท



ประกาศจังหวัดชัยนาท
เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ ข้อ ๒ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ประกอบกับมาตรา ๔๔ มาตรา ๔๕ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ดังนั้น เพื่อให้การดำเนินการใด ๆ ที่เกี่ยวข้องกับวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือหน่วยงานของรัฐมีความมั่นคงปลอดภัย มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์เป็นที่ยอมรับในระดับสากล จังหวัดชัยนาท โดยคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) ได้ประชุมคณะกรรมการฯ เมื่อวันที่ ๒๐ เมษายน ๒๕๖๙ มีมติที่ประชุมเห็นชอบให้พิจารณาทบทวนแนวนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัดชัยนาท จึงได้ดำเนินการทบทวนและกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร เพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงานและผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของจังหวัดชัยนาท จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศจังหวัดชัยนาท เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร”

ข้อ ๒ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

นโยบายที่ ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศและการสื่อสาร

มีแนวปฏิบัติ ดังนี้

หมวด ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศและการสื่อสาร

หมวด ๒ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

/หมวด ๓ ...

หมวด ๓ การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
หมวด ๔ การใช้งานจดหมายอิเล็กทรอนิกส์
หมวด ๕ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
หมวด ๖ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
หมวด ๗ การควบคุมการเข้าออกห้องเครื่องมือสื่อสารของสถานีสื่อสารจังหวัดชัยนาท
หมวด ๘ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

นโยบายที่ ๒ นโยบายการป้องกัน รับมือภัยคุกคามงานสารสนเทศและการสื่อสาร มีแนวปฏิบัติดังนี้

หมวด ๙ การใช้งานระบบไฟร์วอลล์
หมวด ๑๐ การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก
หมวด ๑๑ แนวทางปฏิบัติในการสำรวจข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน
หมวด ๑๒ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

นโยบายที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและการสื่อสาร มีแนวปฏิบัติ ดังนี้

หมวด ๑๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและการสื่อสาร
หมวด ๑๔ การกำหนดหน้าที่และความรับผิดชอบด้านสารสนเทศและการสื่อสาร

ข้อ ๓ หน่วยงานต้องจัดทำ “แผนการรับมือภัยคุกคามทางไซเบอร์” ให้เป็นไปตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของจังหวัดชัยนาท

ข้อ ๔ การกำหนดความรับผิดชอบ

๔.๑ ผู้ว่าราชการจังหวัดชัยนาท ในฐานะผู้บริหารระดับสูง (Chief Executive Officer : CEO) ของจังหวัดชัยนาท เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่จังหวัดชัยนาทหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร

๔.๒ รองผู้ว่าราชการจังหวัดชัยนาท ที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Provincial Chief Information Officer Committee : PCIO) ของจังหวัดชัยนาท เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบายให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร

๔.๓ หัวหน้าสำนักงานจังหวัดชัยนาท เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ วิธีการ และแนวทางแก้ไขปัญหาแก่เจ้าหน้าที่ระดับผู้ปฏิบัติหรือผู้ที่ได้รับมอบหมาย ให้เป็นไปตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร

๔.๔ เพื่อให้การปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัดชัยนาทเป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้สำนักงานจังหวัดชัยนาท ซึ่งเป็นหน่วยงานที่มีภารกิจและอำนาจหน้าที่ผู้ดูแลระบบ ผู้รับผิดชอบระบบสารสนเทศ และผู้ที่ได้รับมอบหมายที่เกี่ยวข้อง

/กับเทคโนโลยี...

กับเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัดชัยนาท เป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบาย และแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัดชัยนาทให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลงนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของจังหวัดชัยนาทให้ประกาศให้เจ้าหน้าที่ทุกระดับของจังหวัดชัยนาทรับทราบทุกครั้ง

ข้อ ๕ นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร จัดเป็นมาตรฐานด้านการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัดชัยนาท เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง จึงให้ใช้นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่ของจังหวัดชัยนาทและผู้ที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๕ พฤษภาคม พ.ศ. ๒๕๖๙

(นายภูมิวัชร์ อุดมทรัพย์)
ผู้ว่าราชการจังหวัดชัยนาท

เอกสารแนบท้ายประกาศ

นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศและการสื่อสาร
จังหวัดชัยนาท
พ.ศ. ๒๕๖๙

คำนำ

ระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับจังหวัดในปัจจุบัน เพื่อช่วยอำนวยความสะดวกในการดำเนินงานทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และประหยัดต้นทุนในการดำเนินงานด้านต่าง ๆ ของจังหวัด ในขณะเดียวกันจังหวัดมีความเสี่ยงจากภัยคุกคามของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งสร้างความเสียหายต่อการปฏิบัติราชการได้ เนื่องจากระบบเทคโนโลยีสารสนเทศมีการเชื่อมโยงข้อมูลไปยังสำนักงานต่าง ๆ ส่งผลให้ช่องทางการติดต่อสื่อสารเสี่ยงในการถูกบุกรุก และอาจก่อให้เกิดเหตุอาชญากรรมทางคอมพิวเตอร์กับจังหวัดได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการส่งผลให้จังหวัดสูญเสียชื่อเสียงหรือภาพพจน์ได้ ดังนั้น ผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความเป็นต้องตระหนักถึงการดูแลบำรุงรักษา และควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ จังหวัดชัยนาท โดยคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) ได้ประชุมคณะกรรมการฯ เมื่อวันที่ ๒๐ เมษายน ๒๕๖๙ มีมติที่ประชุมเห็นชอบให้พิจารณาทบทวนแนวนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัดชัยนาท จึงได้ดำเนินการทบทวนและกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัด เพื่อให้มีมาตรการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของหน่วยงานภายในจังหวัดชัยนาทเป็นไปในทิศทางเดียวกัน สอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัดชัยนาท ฉบับนี้ เป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัดชัยนาททุกคน ให้นำปฏิบัติตามอย่างเคร่งครัดและต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วต่อไป

สารบัญ

หน้า

คำนำ ๒
สารบัญ ๓
๑. วัตถุประสงค์และขอบเขต ๖
๒. องค์ประกอบของนโยบายและแนวปฏิบัติ ๗
๓. คำยาม ๘
ส่วนที่ ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศและการสื่อสาร ๑๓
หมวด ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศและการสื่อสาร ๑๓
๑. วัตถุประสงค์ ๑๓
๒. คำจำกัดความของผู้เกี่ยวข้อง ๑๓
๓. บทบาทและความรับผิดชอบ ๑๓
๔. กระบวนการควบคุมการเข้าออกห้องเครื่องมือสื่อสารของสถานีสื่อสารจังหวัดชัยนาท ๑๓
หมวด ๒ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ๑๕
๑. วัตถุประสงค์ ๑๕
๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ๑๕
หมวด ๓ การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์ ๑๖
๑. วัตถุประสงค์ ๑๖
๒. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต ๑๖
๓. แนวทางปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์ ๑๗
หมวด ๔ การใช้งานจดหมายอิเล็กทรอนิกส์ ๑๘
๑. วัตถุประสงค์ ๑๘
๒. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์ ๑๘
หมวด ๕ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล ๒๐
๑. วัตถุประสงค์ ๒๐
๒. การใช้งานทั่วไป ๒๐
๓. การควบคุมการเข้าถึงระบบปฏิบัติการ ๒๑
๔. แนวทางปฏิบัติในการใช้รหัสผ่าน ๒๑
๕. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ๒๑
๖. การสำรองข้อมูลและการกู้คืน ๒๑
หมวด ๖ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา ๒๒
๑. วัตถุประสงค์ ๒๒
๒. การใช้งานทั่วไป ๒๒
๓. ความปลอดภัยทางด้านกายภาพ ๒๓
๔. การควบคุมการเข้าถึงระบบปฏิบัติการ ๒๓

หน้า

๕. แนวทางปฏิบัติในการใช้รหัสผ่าน ๒๓
๖. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ๒๓
๗. การสำรองข้อมูลและการกู้คืน ๒๔
หมวด ๗ การควบคุมการเข้าออกห้องเครื่องมือสื่อสาร ๒๕
๑. วัตถุประสงค์ ๒๕
๒. คำจำกัดความของผู้เกี่ยวข้อง ๒๕
๓. บทบาทและความรับผิดชอบ ๒๕
๔. กระบวนการควบคุมการเข้าออกห้องเครื่องมือสื่อสาร ๒๕
หมวด ๘ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ๒๗
๑. วัตถุประสงค์ ๒๗
๒. แนวทางปฏิบัติ ๒๗
ส่วนที่ ๒ นโยบายการป้องกัน รับมือภัยคุกคามงานสารสนเทศและการสื่อสาร ๓๐
หมวด ๙ การใช้งานระบบไฟร์วอลล์ ๓๐
๑. วัตถุประสงค์ ๓๐
๒. แนวทางปฏิบัติในการรักษาความปลอดภัยไฟร์วอลล์ ๓๐
หมวด ๑๐ การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก ๓๒
๑. วัตถุประสงค์ ๓๒
๒. แนวทางปฏิบัติในการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก ๓๒
หมวด ๑๑ การรักษาสภาพความพร้อมใช้งานของการให้บริการ ๓๓
๑. วัตถุประสงค์ ๓๓
๒. แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน ๓๓
หมวด ๑๒ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ๓๔
๑. วัตถุประสงค์ ๓๔
๒. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย ๓๔
๓. การควบคุมการเข้าออก อาคาร สถานที่ ๓๔
๔. ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ ๓๕
๕. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ๓๕
๖. การบำรุงรักษาอุปกรณ์ ๓๖
๗. การนำทรัพย์สินของจังหวัดออกนอกจังหวัด ๓๖
๘. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกจังหวัด ๓๖
๙. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง ๓๖
๑๐. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ๓๗

หน้า

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและการสื่อสาร ๓๘
หมวด ๑๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและการสื่อสาร ๓๘
๑. วัตถุประสงค์ ๓๘
๒. แนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ๓๘
หมวด ๑๔ การกำหนดหน้าที่และความรับผิดชอบด้านสารสนเทศและการสื่อสาร ๓๙
๑. วัตถุประสงค์ ๓๙
๒. แนวทางปฏิบัติ ๓๙
ส่วนที่ ๑ ระดับนโยบาย ๓๙
ส่วนที่ ๒ ระดับปฏิบัติงาน ๓๙
ภาคผนวก ๔๑
การรักษาความมั่นคงปลอดภัยด้านการสื่อสาร ๔๒
๑. ขั้นตอนปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๔๒
๒. แผนและวิธีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัย ๔๒
๓. การระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๔๒
๔. การประเมินความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ ๔๓
๕. แผนและขั้นตอนการรับมือเหตุคุกคามทางไซเบอร์ ๔๓
๖. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ๔๔
๗. ขั้นตอนการรับมือ ๔๖
๘. วิธีการปฏิบัติด้านการรักษาความมั่นคงและปลอดภัยระบบกล้องโทรทัศน์วงจรปิด (CCTV) ของจังหวัดชัยนาท ๔๘
การรักษาความมั่นคงปลอดภัยด้านโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร ๕๐
๑. ระบบเครือข่าย ๕๐
๒. ระบบโทรศัพท์ IP Phone ๕๒
๓. ระบบ Call Center 1567 ของศูนย์ดำรงธรรม ๕๔
๔. ป้ายประชาสัมพันธ์อัจฉริยะ ๕๕

นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร
จังหวัดชัยนาท

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัดชัยนาท หรือต่อไปนี้เรียกว่า “จังหวัด” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ จังหวัดจึงกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑.๑ การจัดทำนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของจังหวัด ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ

๑.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๐ ที่มีการปรับปรุงอย่างต่อเนื่อง

๑.๓ นโยบายและแนวทางปฏิบัตินี้ได้ดำเนินการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในจังหวัดได้รับทราบและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับจังหวัดตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕ นโยบายนี้มีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้งต่อปี หรือตามที่ระบุไว้ในเอกสาร “การตรวจสอบประเมินนโยบาย”

๒. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร

ส่วนที่ ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศและการสื่อสาร

แนวปฏิบัติที่เกี่ยวข้อง มีดังนี้

๑) การเข้าถึงและควบคุมการใช้งานสารสนเทศและการสื่อสาร

๒) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๓) การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์

๔) การใช้งานจดหมายอิเล็กทรอนิกส์

๕) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๖) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๗) การควบคุมการเข้าออกห้องเครื่องมือสื่อสารของสถานีสื่อสารจังหวัดชัยนาท

๘) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๒ นโยบายการป้องกัน รับมือภัยคุกคามงานสารสนเทศและการสื่อสาร

แนวปฏิบัติที่เกี่ยวข้อง มีดังนี้

๑) การใช้งานระบบไฟร์วอลล์

๒) การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก

๓) แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

๔) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและการสื่อสาร

แนวปฏิบัติที่เกี่ยวข้อง มีดังนี้

๑) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและการสื่อสาร

๒) การกำหนดหน้าที่และความรับผิดชอบด้านสารสนเทศและการสื่อสาร

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัด ดังกล่าวข้างต้น ประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด เพื่อทำให้จังหวัดมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สินและบุคลากรของจังหวัด ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัดนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด ซึ่งเจ้าหน้าที่ของจังหวัด หน่วยงานภายนอก และผู้ที่เกี่ยวข้องต้องปฏิบัติตามอย่างเคร่งครัด

๓. คำนิยาม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารของจังหวัด ประกอบด้วยคำนิยาม ดังนี้

จังหวัด หมายความว่า จังหวัดชัยนาท

หน่วยงานภายใน หมายความว่า สำนักงานจังหวัดชัยนาท กลุ่มงาน ศูนย์ และหน่วยงานอื่นภายในจังหวัดชัยนาท

ห้องเครื่องมือสื่อสาร หมายความว่า ห้องเครื่องมือสื่อสารของสถานีสื่อสารจังหวัดชัยนาท เป็นห้องจัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ติดตั้งวางระบบเครื่องแม่ข่าย อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่ายของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ

ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) หมายความว่า ผู้ว่าราชการจังหวัดชัยนาท

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) หมายความว่า รองผู้ว่าราชการจังหวัดชัยนาท (ด้านเศรษฐกิจและสังคม) ที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด

ผู้บังคับบัญชา หมายความว่า ผู้บังคับบัญชาของหน่วยงานภายใน หรือผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของจังหวัด

ผู้ใช้งาน หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหารจัดการ หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของจังหวัด โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดในการเข้าถึงสารสนเทศและการสื่อสารของจังหวัด ดังนี้

- **ผู้บริหาร** หมายความว่า ผู้ว่าราชการจังหวัดชัยนาท รองผู้ว่าราชการจังหวัดชัยนาท หัวหน้าสำนักงานจังหวัดชัยนาท ผู้อำนวยการกลุ่มงาน/ศูนย์ หัวหน้า

- **ผู้ดูแลระบบ** (System Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์ และระบบเครือข่าย ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

- **ผู้ดูแลครุภัณฑ์** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ควบคุมดูแลพัสดุหรือทรัพย์สินของจังหวัดที่อยู่ในความครอบครองของหน่วยงานภายใน ให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา โดยมิให้เกิดการสูญหาย

- **เจ้าหน้าที่** หมายความว่า ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานจ้างเหมาบริการ หรือบุคคลอื่นใดของสำนักงานจังหวัด

- **บุคคลภายนอก** หมายความว่า บุคคลจากหน่วยงานภายนอกที่เข้ามาประชุมหรือปฏิบัติงานร่วมกับจังหวัด

หน่วยงานภายนอก หมายความว่า หน่วยงานภายนอกที่สำนักงานจังหวัดอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของจังหวัด โดยได้รับสิทธิในการใช้งานตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานจังหวัด เพื่อการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึงการป้องกัน

ทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลายหรือล่วงรู้โดยมิชอบ

มาตรฐาน (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

วิธีการปฏิบัติ (Procedure) หมายความว่า รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

เจ้าของข้อมูล หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบดูแลข้อมูลโดยตรง โดยเจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล และได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูล นำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหารจัดการ การวางแผน การตัดสินใจ และอื่น ๆ

ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์คอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่เป็นแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ชื่อเครื่องคอมพิวเตอร์ (Computer Name) หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่าย โดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

ระบบเครือข่าย (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสำนักงานจังหวัดได้ เช่น ระบบแลน ระบบอินทราเน็ต ระบบอินเทอร์เน็ต เป็นต้น

- **ระบบแลน** (Local Area Network : LAN) และ**ระบบอินทราเน็ต** (Intranet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในสำนักงานจังหวัดเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงานจังหวัด

- **ระบบอินเทอร์เน็ต** (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของจังหวัด เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

SSID (Service Set Identifier) หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า ค่าเดียวกัน

WPA (Wi-Fi Protected Access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย

VPN (Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงทำการเข้ารหัสเฉพาะแล้วรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

ไฟร์วอลล์ (Firewall) หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

MAC Address (Media Access Control Address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้มากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดมีหมายเลขที่ไม่ซ้ำกันตัวเลขอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้มีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

เลขที่อยู่ไอพี (IP Address) หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขที่อยู่ไอพีของแต่ละเครื่องต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน หรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของจังหวัด

อุปกรณ์จัดเส้นทาง (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ทำหน้าที่จัดเส้นทางและค้นหาเส้นทาง เพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

ชุดคำสั่งไม่พึงประสงค์ หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม นำมาซึ่งการขัดแย้งหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานของจังหวัดที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่จังหวัดสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายความว่า พื้นที่ที่จังหวัดอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

- **พื้นที่ทำงานทั่วไป** (General working area) หมายความว่า พื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
- **พื้นที่ทำงานของผู้ดูแลระบบ** (System administrator area)
- **พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย** (IT equipment or network area) หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
- **พื้นที่ควบคุมพิเศษ** หมายความว่า ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) หรือพื้นที่ติดตั้งละจัดวางระบบเครื่องแม่ข่าย อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่ายของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ
- **พื้นที่ใช้งานระบบเครือข่ายไร้สาย** (Wireless LAN coverage area)

สินทรัพย์ หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตน ที่มีคุณค่าสำหรับจังหวัด ได้แก่ ข้อมูล ระบบข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล อุปกรณ์ต่อพ่วง เป็นต้น

สื่อบันทึกพกพา (Portable Media) หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ CD, DVD, Flash Drive หรือ Thumb Drive หรือ External Hard disk เป็นต้น

จดหมายอิเล็กทรอนิกส์ (e-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อมูลระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปให้ผู้รับคนเดียวหรือหลายคนได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3, IMAP และ Exchange เป็นต้น

บัญชีรายชื่อผู้ใช้งาน (User account) หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศในระบบเครือข่ายของจังหวัด

บัญชีชื่อผู้ใช้งาน (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

รหัสผ่าน (Password) หมายความว่า ชุดของตัวอักษรหรืออักขระหรือตัวเลข ที่ถูกกำหนดขึ้นเพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลที่มีการกำหนดสิทธิการใช้งานไว้เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้งานระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

ลงบันทึกเข้า (Login) หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้ เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย โดยกรอกบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

ลงบันทึกออก (Logout) หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

การเข้ารหัสลับ (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสลับ เพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้ต้องมีโปรแกรมถอดรหัสลับ เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของจังหวัด

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของจังหวัดถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

ภัยคุกคามทางไซเบอร์ หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ไซเบอร์ หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกนเป็นการทั่วไป

ประมวลแนวทางปฏิบัติ หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบ ซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคง ปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตน ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หน่วยงานควบคุมหรือกำกับดูแล หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคล ซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ส่วนที่ ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศและการสื่อสาร

หมวด ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศและการสื่อสาร (Computer Center Entry Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกัน มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของจังหวัด โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องเครื่องมือสื่อสารของสถานีสื่อสารจังหวัดชัยนาท

๒. คำจำกัดความของผู้เกี่ยวข้อง

๒.๑ ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ที่ปฏิบัติงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในห้องเครื่องมือสื่อสาร

๒.๒ เจ้าหน้าที่ห้องเครื่องมือสื่อสาร หมายความว่า เจ้าหน้าที่ของจังหวัดที่ปฏิบัติงานภายในห้องเครื่องมือสื่อสาร

๒.๓ เจ้าหน้าที่ หมายความว่า เจ้าหน้าที่ของจังหวัดที่มีสิทธิในการเข้าออกสถานที่/อาคาร/ห้องภายในศาลากลางจังหวัดชัยนาท

๒.๔ ผู้ติดต่อหรือบุคคลภายนอก หมายความว่า บุคคลจากหน่วยงานภายนอกที่มาติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของห้องเครื่องมือสื่อสาร หรือผู้รับจ้างที่เข้ามาซ่อมบำรุงอุปกรณ์ภายในห้องเครื่องมือสื่อสาร

๓. บทบาทและความรับผิดชอบ

๓.๑ หัวหน้าสำนักงานจังหวัด

๓.๑.๑ อนุมัติสิทธิการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๑.๒ อนุมัติกระบวนการควบคุมการเข้าออกห้องเครื่องมือสื่อสาร

๓.๒ ผู้ดูแลระบบ

๓.๒.๑ ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องเครื่องมือสื่อสารให้ปฏิบัติตามระเบียบและกฎเกณฑ์อย่างเคร่งครัด

๓.๒.๒ ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกห้องเครื่องมือสื่อสารต้องลงชื่อในสมุดควบคุม พร้อมทั้งแสดงบัตรประจำตัวประชาชน หรือแสดงตนผ่านระบบ ThaiD

๔. กระบวนการควบคุมการเข้าออกห้องเครื่องมือสื่อสารของสถานีสื่อสารจังหวัดชัยนาท

๔.๑ ผู้ดูแลระบบ เจ้าหน้าที่ห้องเครื่องมือสื่อสาร และเจ้าหน้าที่ของจังหวัด มีแนวทางปฏิบัติ ดังนี้

๔.๑.๑ ผู้ดูแลระบบ ต้องจัดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นสัดส่วนที่ชัดเจน เช่น พื้นที่ควบคุมส่วนระบบเครือข่าย (Network Zone) พื้นที่ควบคุมพิเศษส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๔.๑.๒ หัวหน้าสำนักงานจังหวัด ต้องอนุมัติสิทธิในการเข้าออกพื้นที่ห้องเครื่องมือสื่อสาร และการเข้าถึงพื้นที่ควบคุมพิเศษ เจ้าหน้าที่ที่ปฏิบัติหน้าที่ภายในห้องเครื่องมือสื่อสาร และมีการบันทึกในสมุดควบคุม เช่น ผู้ดูแลระบบ เจ้าหน้าที่ห้องเครื่องมือสื่อสาร เป็นต้น

๔.๑.๓ เจ้าหน้าที่ห้องเครื่องมือสื่อสารทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกห้องเครื่องมือสื่อสารทุกคนต้องลงชื่อในสมุดควบคุมดังกล่าว

๔.๒ ผู้ติดต่อหรือบุคคลภายนอก มีแนวทางปฏิบัติ ดังนี้

๔.๒.๑ ผู้ติดต่อหรือบุคคลภายนอกทุกคนต้องทำการแสดงบัตรประจำตัวประชาชน หรือแสดงตัวผ่านระบบ ThaiD ให้กับเจ้าหน้าที่ห้องเครื่องมือสื่อสาร

๔.๒.๒ ผู้ติดต่อหรือบุคคลภายนอกที่เข้าปฏิบัติงาน หรือนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในห้องเครื่องมือสื่อสารต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกให้ถูกต้องชัดเจน

๔.๒.๓ ผู้ติดต่อหรือบุคคลภายนอก สามารถเข้าออกห้องเครื่องมือสื่อสารได้ต้องมีเจ้าหน้าที่ห้องเครื่องมือสื่อสารเป็นผู้เปิดประตูให้

๔.๒.๔ ผู้ติดต่อหรือบุคคลภายนอก สามารถนำผู้ติดตามเข้ามาช่วยงานได้ไม่เกินครั้งละ ๒ คน

๔.๒.๕ เจ้าหน้าที่ห้องเครื่องมือสื่อสารต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในการเข้าออกพื้นที่ และตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

๔.๒.๖ เจ้าหน้าที่ห้องเครื่องมือสื่อสารควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกการเข้าออกพื้นที่เป็นประจำทุกเดือน

๔.๒.๗ เจ้าหน้าที่ห้องเครื่องมือสื่อสารต้องทำการทบทวนสิทธิของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การย้าย โอน ลาออก หรือสิ้นสุดสัญญาจ้าง

หมวด ๒ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุม ป้องกัน และการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของสำนักงานจังหวัด เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของจังหวัด

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๒.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของจังหวัด ต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ก่อนเท่านั้น

๒.๒ ผู้ดูแลระบบ กำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่และความผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๒.๔ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access Point : AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

๒.๕ ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ ทั้งนี้ การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

๒.๖ ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

๒.๗ ผู้ดูแลระบบต้องเปลี่ยนค่า ชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๒.๘ ผู้ดูแลระบบต้องกำหนดค่าใช้มาตรฐานความปลอดภัยแบบ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ เพื่อให้ยากต่อการดักจับ ช่วยให้ปลอดภัยมากขึ้น

๒.๙ ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address ร่วมกับบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address บัญชีชื่อผู้ใช้งาน และรหัสผ่านตามที่กำหนดไว้เท่านั้น ในการเชื่อมต่อกับเครือข่ายไร้สายตาม SSID ที่กำหนดไว้ สำหรับบุคคลภายนอกกำหนดให้ใช้งานเครือข่ายไร้สายโดยไม่ควบคุม MAC Address แต่ให้ใช้งานได้ตาม SSID ที่ผู้ดูแลระบบกำหนดแยกเฉพาะสำหรับบุคคลภายนอกเท่านั้น

๒.๑๐ ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในสำนักงาน

๒.๑๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สาย ติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๒.๑๒ ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

หมวด ๓ การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
(Use of the Internet and Social Network)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์อย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำเกี่ยวกับคอมพิวเตอร์ ได้แก่ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันก่อให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของจังหวัดถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๒.๑ ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่จังหวัดจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากหัวหน้าสำนักงานจังหวัดเป็นลายลักษณ์อักษรแล้ว

๒.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

๒.๓ การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต ต้องมีการตรวจสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

๒.๔ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของจังหวัดนอกเหนือจากเพื่อประโยชน์ของทางราชการ หรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม เว้นแต่เป็นการดำเนินงานตามภารกิจของจังหวัด

๒.๕ ผู้ใช้งานถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของจังหวัด

๒.๖ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับจังหวัด

๒.๗ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของจังหวัด ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๒.๘ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๒.๙ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด อันทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๒.๑๐ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๒.๑๑ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๒.๑๒ การใช้งานเว็บบอร์ด (Web Board) ของจังหวัด ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของจังหวัด

๒.๑๓ ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่ทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของจังหวัด การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

๒.๑๔ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๓. แนวทางปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์

๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่จังหวัดได้กำหนดไว้เท่านั้น เช่น Facebook, Line, Twitter เป็นต้น

๓.๒ หากต้องการใช้งานเครือข่ายสังคมออนไลน์ในลักษณะอื่นใดนอกเหนือจากที่จังหวัดกำหนดให้ขออนุญาตจากสำนักงานจังหวัดก่อนใช้งาน

๓.๓ ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของจังหวัด

๓.๔ ผู้ใช้งานพึงตระหนักว่าข้อความหรือความเห็นที่เผยแพร่บนเครือข่ายสังคมออนไลน์เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุ ให้ร้าย ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

๓.๕ ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้เป็นการแสดงความคิดเห็นในนามบัญชีชื่อผู้ใช้ส่วนตัว แต่อาจส่งผลกระทบกับจังหวัดได้ และพึงระมัดระวังเรื่องผลประโยชน์ในเชิงพาณิชย์

๓.๖ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อจังหวัด ผู้ใช้งานต้องแจ้งต่อหัวหน้าสำนักงานจังหวัดโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๓.๗ ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

หมวด ๔ การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

๑. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของจังหวัด ซึ่งผู้ใช้งานต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้น จากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่สร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด อันทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของจังหวัด ให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

๒.๒ ผู้ดูแลระบบต้องมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง การโอน ย้าย ลาออก หรือสิ้นสุดสัญญาจ้าง

๒.๓ ผู้ดูแลระบบกำหนดบัญชีชื่อผู้ใช้งาน E-Mail (username) และรหัสผ่าน (password) สำหรับการใช้งานครั้งแรก ให้แก่ผู้ใช้งาน โดยส่งมอบให้ผู้ใช้งานเป็นเอกสารปิดผนึกที่เป็นความลับ หรือทางอีเมลส่วนบุคคลของผู้ใช้งาน

๒.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อได้รับรหัสผ่านครั้งแรก (Default Password) หรือเมื่อเข้าระบบครั้งแรก ระบบต้องบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ และควรเปลี่ยนรหัสผ่านใหม่ทุก ๖ เดือน

๒.๕ การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

๒.๖ ระบบต้องไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งาน ระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านต้องแสดงด้วยรูปแบบของสัญลักษณ์แทนตัวอักษร เช่น ‘x’ หรือ ‘*’ ในการพิมพ์แต่ละตัวอักษร

๒.๗ ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน ๓ ครั้ง หากเกินกว่าที่กำหนดระบบทำการล็อคสิทธิการเข้าถึงของผู้ใช้งานทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อคให้

๒.๘ ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ออกจากระบบโดยอัตโนมัติ (Time out) เพื่อตัดการใช้งานระบบ เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลา ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

๒.๙ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๒.๑๐ ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อจังหวัด หรือละเมิดสิทธิ์สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของจังหวัด

๒.๑๑ ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่น เพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของแล้วเท่านั้น และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๒.๑๒ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของจังหวัด เพื่อการทำงานของจังหวัดเท่านั้น

๒.๑๓ หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Logout ออกจากระบบ และปิดเว็บเบราว์เซอร์ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

๒.๑๔ ผู้ใช้ต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดด้วยโปรแกรมป้องกันไวรัส เป็นการป้องกันการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

๒.๑๕ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้จากผู้ส่งที่ไม่รู้จัก

๒.๑๖ ผู้ใช้งานต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์และใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง และระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป รวมทั้งจำกัดกลุ่มผู้รับจดหมายอิเล็กทรอนิกส์เท่าที่มีความจำเป็นต้องรับรู้รับทราบ

๒.๑๗ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๑๘ ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวัน และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์ให้เหลือจำนวนน้อยที่สุด

๒.๑๙ ผู้ใช้งานควรทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ที่สำคัญตามความจำเป็นอย่างสม่ำเสมอ

๒.๒๐ ข้อควรระวัง ผู้ใช้งานไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้น ไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๒.๒๑ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบในการเก็บรักษาบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) เป็นความลับไม่ให้บุคคลอื่นล่วงรู้

หมวด ๕ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Use of Personal Computer)

๑. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้จัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้งานควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของจังหวัดให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. การใช้งานทั่วไป

๒.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลที่จังหวัดอนุญาตให้เจ้าหน้าที่ใช้งาน เป็นทรัพย์สินของจังหวัด เพื่อใช้ในงานราชการ ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่อประโยชน์ของจังหวัด

๒.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลของจังหวัด ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยอยู่ในความรับผิดชอบของหน่วยงานภายใน ผู้ใช้งานต้องได้รับอนุญาตจากผู้บังคับบัญชาของหน่วยงานภายในก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลครุภัณฑ์ของหน่วยงานภายในต้องระบุว่าผู้ใดเป็นผู้ครอบครองเครื่องคอมพิวเตอร์นั้น

๒.๓ เจ้าหน้าที่ห้องเครื่องมือสื่อสารเป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล ทั้งนี้ ต้องเป็นผู้ที่หัวหน้าสำนักงานจังหวัดมอบหมายให้ทำหน้าที่เป็นผู้ติดตั้งโปรแกรมและระบบปฏิบัติการเท่านั้น

๒.๔ โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของจังหวัด ต้องเป็นโปรแกรมที่สำนักงานจังหวัดซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๕ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของจังหวัด หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๒.๖ การเคลื่อนย้ายเครื่องคอมพิวเตอร์ส่วนบุคคลออกนอกพื้นที่ปฏิบัติงานของหน่วยงานภายในจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา และแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำออกนอกสถานที่

๒.๗ การนำเครื่องคอมพิวเตอร์ส่วนบุคคลของจังหวัดส่งซ่อมภายนอก ต้องผ่านการตรวจประเมินจากเจ้าหน้าที่ห้องเครื่องมือสื่อสารที่หัวหน้าสำนักงานจังหวัดมอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากหัวหน้าสำนักงานจังหวัด โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องดำเนินการโดยเจ้าหน้าที่ห้องเครื่องมือสื่อสาร หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางจังหวัดเท่านั้น

๒.๘ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบหาไวรัส โดยโปรแกรมป้องกันไวรัส

๒.๙ ไม่ควรเก็บข้อมูลสำคัญของจังหวัดไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๒.๑๐ ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของจังหวัด

๒.๑๑ ผู้ใช้งานมีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยหลีกเลี่ยงการวางอาหารหรือเครื่องดื่มบริเวณเครื่องคอมพิวเตอร์และไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

๓. การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑ ผู้ใช้งานต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของจังหวัด

๓.๒ ผู้ใช้งานควรกำหนดรหัสผ่านที่มีคุณภาพตามคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

๓.๓ ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๑๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

๓.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๓.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) จากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๔. แนวทางปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

๕. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๕.๑ ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๕.๒ เจ้าหน้าที่ห้องเครื่องมือสื่อสาร มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์เป็นโปรแกรมพื้นฐาน

๕.๓ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๕.๔ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๕.๕ ผู้ใช้งานต้องตรวจสอบว่าข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๖. การสำรองข้อมูลและการกู้คืน

๖.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เพื่อป้องกันการสูญหายของข้อมูล

๖.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖.๓ ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

หมวด ๖ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer)

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพา และการนำไปปฏิบัติงานภายนอกสำนักงาน และเป็นการป้องกันทรัพยากรและข้อมูลที่มีค่าของจังหวัดให้เกิดความปลอดภัย ผู้ใช้งานจึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยงในการใช้งานเครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๒. การใช้งานทั่วไป

๒.๑ เครื่องคอมพิวเตอร์แบบพกพาที่จังหวัดอนุญาตให้เจ้าหน้าที่ใช้งาน เป็นทรัพย์สินของจังหวัด เพื่อใช้ในงานราชการ ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่อประโยชน์ของจังหวัด

๒.๒ เครื่องคอมพิวเตอร์แบบพกพาของจังหวัด ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยอยู่ในความรับผิดชอบของหน่วยงานภายใน ผู้ใช้งานต้องได้รับอนุญาตจากผู้บังคับบัญชาของหน่วยงานภายในก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลครุภัณฑ์ของหน่วยงานภายในต้องระบุว่าผู้ใดเป็นผู้ครอบครองหรือนำไปใช้งาน

๒.๓ เจ้าหน้าที่ห้องเครื่องมือสื่อสารเป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพา ทั้งนี้ ต้องเป็นผู้ที่หัวหน้าสำนักงานจังหวัดมอบหมายให้ทำหน้าที่เป็นผู้ติดตั้งโปรแกรมและระบบปฏิบัติการเท่านั้น

๒.๔ โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของจังหวัด ต้องเป็นโปรแกรมที่สำนักงานจังหวัดซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๕ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบพกพาของจังหวัด หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๒.๖ การนำเครื่องคอมพิวเตอร์แบบพกพาของจังหวัดไปใช้งานภายนอกพื้นที่ปฏิบัติงานของหน่วยงานภายในจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา และแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำออกนอกสถานที่

๒.๗ การนำเครื่องคอมพิวเตอร์แบบพกพาของจังหวัดส่งซ่อมภายนอก ต้องผ่านการตรวจประเมินจากเจ้าหน้าที่ห้องเครื่องมือสื่อสารที่หัวหน้าสำนักงานจังหวัดมอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากหัวหน้าสำนักงานจังหวัด โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องดำเนินการโดยเจ้าหน้าที่ห้องเครื่องมือสื่อสาร หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางจังหวัดเท่านั้น

๒.๘ การเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ใส่ในกระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาให้เรียบร้อย เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน การหลงลืมอุปกรณ์ และไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

๒.๙ กรณีที่ต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้นโดยเด็ดขาด

๒.๑๐ ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่ และควรรักษาสภาพคอมพิวเตอร์ให้มีสภาพพร้อมใช้งานตลอดเวลา

๒.๑๑ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๒.๑๒ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาเสียหายได้

๒.๑๓ ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

๒.๑๔ การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะทำให้หน้าจอมีรอยขีดข่วนได้

๓. ความปลอดภัยทางด้านกายภาพ

๓.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ดังนั้น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๓.๒ การใช้เครื่องคอมพิวเตอร์แบบพกพาเครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๓.๓ ผู้ใช้งานไม่เก็บหรือใช้งานเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๓.๔ ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

๓.๕ ไม่ควรติดตั้งหรือวางเครื่องคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน

๓.๖ ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ

๔.๑ ผู้ใช้งานต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพาของจังหวัด

๔.๒ ผู้ใช้งานควรกำหนดรหัสผ่านที่มีคุณภาพตามคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

๔.๓ ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๑๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

๔.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๔.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) จากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๕. แนวทางปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

๖. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๖.๑ ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๖.๒ เจ้าหน้าที่ห้องเครื่องมือสื่อสาร มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์เป็นโปรแกรมพื้นฐาน

๖.๓ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา และผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๖.๔ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๖.๕ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

๗. การสำรองข้อมูลและการกู้คืน

๗.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกอื่น ๆ เพื่อป้องกันการสูญหายของข้อมูล

๗.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗.๓ ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

๗.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

หมวด ๗ การควบคุมการเข้าออกห้องเครื่องมือสื่อสาร
(Communication equipment rooms Entry Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกัน มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของจังหวัด โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องเครื่องมือสื่อสาร

๒. คำจำกัดความของผู้เกี่ยวข้อง

๒.๑ ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ที่ปฏิบัติงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในห้องเครื่องมือสื่อสาร

๒.๒ เจ้าหน้าที่ห้องเครื่องมือสื่อสาร หมายความว่า เจ้าหน้าที่ของสำนักงานจังหวัดที่ปฏิบัติงานภายในห้องเครื่องมือสื่อสาร

๒.๓ เจ้าหน้าที่ หมายความว่า เจ้าหน้าที่ของจังหวัดที่มีสิทธิในการเข้าออกสถานที่/อาคาร/ห้องภายในสำนักงาน

๒.๔ ผู้ติดต่อหรือบุคคลภายนอก หมายความว่า บุคคลจากหน่วยงานภายนอกที่มาติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของห้องเครื่องมือสื่อสาร หรือผู้รับจ้างที่เข้ามาซ่อมบำรุงอุปกรณ์ภายในห้องเครื่องมือสื่อสาร

๓. บทบาทและความรับผิดชอบ

๓.๑ หัวหน้าสำนักงานจังหวัด

๓.๑.๑ อนุมัติสิทธิการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๑.๒ อนุมัติกระบวนการควบคุมการเข้าออกห้องเครื่องมือสื่อสาร

๓.๒ ผู้ดูแลระบบ

ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องเครื่องมือสื่อสารให้ปฏิบัติตามระเบียบและกฎเกณฑ์อย่างเคร่งครัด

๔. กระบวนการควบคุมการเข้าออกห้องเครื่องมือสื่อสาร

๔.๑ ผู้ดูแลระบบ เจ้าหน้าที่ห้องเครื่องมือสื่อสาร และเจ้าหน้าที่ของจังหวัด มีแนวทางปฏิบัติ ดังนี้

๔.๑.๑ ผู้ดูแลระบบ ต้องจัดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นสัดส่วนชัดเจน เช่น พื้นที่ควบคุมส่วนระบบเครือข่าย (Network Zone) พื้นที่ควบคุมพิเศษส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึง หรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๔.๑.๒ หัวหน้าสำนักงานจังหวัด ต้องอนุมัติสิทธิในการเข้าออกพื้นที่ห้องเครื่องมือสื่อสาร และการเข้าถึงพื้นที่ควบคุมพิเศษ เจ้าหน้าที่ที่ปฏิบัติหน้าที่ภายในห้องเครื่องมือสื่อสาร และมีการบันทึกในสมุดควบคุมการเข้าออก

๔.๑.๓ สิทธิในการเข้าออกห้องเครื่องมือสื่อสารของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากหัวหน้าสำนักงานจังหวัด

๔.๑.๔ การเข้าถึงพื้นที่ห้องเครื่องมือสื่อสาร และพื้นที่ควบคุมพิเศษ ต้องมีการลงบันทึกในสมุดควบคุมการเข้าออก

๔.๒ ผู้ติดต่อหรือบุคคลภายนอก มีแนวทางปฏิบัติ ดังนี้

๔.๒.๑ ผู้ติดต่อหรือบุคคลภายนอกทุกคนต้องแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้กับเจ้าหน้าที่ และทำการลงบันทึกในสมุดควบคุมการเข้าออก

๔.๒.๒ ผู้ติดต่อหรือบุคคลภายนอกที่เข้าปฏิบัติงาน หรือนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในจังหวัด ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ให้ถูกต้องชัดเจน

๔.๒.๓ ผู้ติดต่อหรือบุคคลภายนอก จะสามารถเข้าออกห้องเครื่องมือสื่อสารได้ต้องมีเจ้าหน้าที่ห้องเครื่องมือสื่อสารเป็นผู้ดูแลควบคุม

๔.๒.๔ ผู้ติดต่อหรือบุคคลภายนอก สามารถนำผู้ติดตามเข้ามาช่วยงานได้ไม่เกินครั้งละ ๒ คน

๔.๒.๕ เจ้าหน้าที่ห้องเครื่องมือสื่อสาร ต้องตรวจสอบรายการอุปกรณ์ที่ผู้ติดต่อหรือบุคคลภายนอกนำเข้าออกห้องเครื่องมือสื่อสารให้ถูกต้องตามแบบฟอร์ม

๔.๒.๖ เจ้าหน้าที่ห้องเครื่องมือสื่อสารต้องทำการทบทวนสิทธิของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การย้าย โอนลาออก หรือสิ้นสุดสัญญาจ้าง

หมวด ๘ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Third Party Access Control)

๑. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก

๒. แนวทางปฏิบัติ

๒.๑ ต้องมีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผล โดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

๒.๒ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๒.๒.๑ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัดต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้าสำนักงานจังหวัด

๒.๒.๒ จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก เพื่อระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

๑) เหตุผลในการขอใช้

๒) ระยะเวลาในการใช้

๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๔) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๒.๒.๓ หน่วยงานภายนอกที่ปฏิบัติงานให้กับจังหวัด ทั้งภายในและภายนอกจังหวัดจำเป็นต้องลงนามในสัญญาไม่เปิดเผยข้อมูลของจังหวัด โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศของจังหวัด

๒.๒.๔ จังหวัดควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

๒.๒.๕ เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๒.๒.๖ สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของจังหวัด ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๒.๒.๗ จังหวัดมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจว่าจังหวัดสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๒.๒.๘ ควรดำเนินการให้ผู้ให้บริการภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๒.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๒.๓.๑ กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

๒.๓.๒ ระบุผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

๒.๓.๓ กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่มีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับ โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๒.๓.๔ กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ก่อนการติดตั้ง

๒.๓.๕ การทดสอบซอฟต์แวร์ห้ามทดสอบบนระบบและฐานข้อมูลที่ใช้งานต้องสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

๒.๔ มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

๒.๔.๑ ผู้ให้บริการภายนอกที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของจังหวัดต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากหัวหน้าสำนักงานจังหวัด

๒.๔.๒ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

๒.๔.๓ กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น ทั้งนี้ หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๒.๔.๔ การอนุญาตให้ผู้ให้บริการภายนอกเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากหัวหน้าสำนักงานจังหวัดก่อนทุกครั้ง

๒.๕ มาตรการควบคุมช่องโหว่ทางเทคนิค

๒.๕.๑ การบริหารจัดการช่องโหว่ของระบบ ควรมีการบันทึก ดังต่อไปนี้

๑) ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน

๒) สถานที่ที่ติดตั้ง

๓) เครื่องแม่ข่ายที่ติดตั้ง

๔) ผู้ผลิตซอฟต์แวร์

๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๒.๕.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๒.๕.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการดังนี้

๑) มีการเฝ้าระวังและติดตามประเมินความเสี่ยง สำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

๒) ให้กำหนดแหล่งข้อมูลข่าวสาร เพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของจังหวัด

๓) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยง เมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๒.๕.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๒.๖ การบริหารจัดการบุคลากรที่เกี่ยวข้อง

การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ทำให้บทบาทหน้าที่ รวมถึงความรู้ ความเชี่ยวชาญในการปฏิบัติงานเปลี่ยนแปลงจากที่หน่วยงานเคยดำเนินการ หน่วยงานควรจัดสรรบุคลากรสร้างความเข้าใจและความตระหนักก่อนการเปลี่ยนแปลง รวมถึงพัฒนาความรู้ ความเชี่ยวชาญของบุคลากรที่เกี่ยวข้อง ให้เพียงพอในการปฏิบัติงานอย่างมีประสิทธิภาพ เช่น จัดให้มีการพัฒนาทักษะความรู้ของเจ้าหน้าที่ที่เกี่ยวข้องครอบคลุมการบริหารจัดการความเสี่ยงจากบุคคลภายนอก การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรณีการใช้ Cloud Computing ควรเสริมสร้างทักษะความรู้ให้แก่ผู้บริหารและเจ้าหน้าที่ที่เกี่ยวข้องให้สามารถปฏิบัติงานได้ตามมาตรฐานและแนวปฏิบัติที่ดีของผู้ให้บริการ Cloud Computing เป็นต้น

ส่วนที่ ๒ นโยบายการป้องกัน รับมือภัยคุกคามงานสารสนเทศและการสื่อสาร

หมวด ๙ การใช้งานระบบไฟร์วอลล์
(Firewall Policy)

๑. วัตถุประสงค์

เพื่อป้องกันการบุกรุกจากบุคคลภายนอกในการเข้าถึงระบบเครือข่ายภายในของจังหวัด และทำการตรวจสอบติดตามแพ็คเก็ต (Packet) โดยอนุญาตให้ผู้มีสิทธิเข้าออกระบบ เพื่อควบคุมการเชื่อมต่อจากภายนอกสู่ภายในจังหวัด และจากภายในจังหวัดสู่ภายนอกจังหวัด

๒. แนวทางปฏิบัติในการรักษาความปลอดภัยไฟร์วอลล์ (Firewall)

๒.๑ ผู้ดูแลระบบต้องเฝ้าระวังและบริหารจัดการระบบรักษาความปลอดภัย (Firewall)

๒.๒ ผู้ดูแลระบบต้องกำหนดนโยบาย (Policy) การใช้งานไฟร์วอลล์

๒.๓ ผู้ดูแลระบบต้องจัดให้มีระบบตรวจสอบยืนยันตัวตนและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ

๒.๔ ผู้ดูแลระบบต้องกำหนดค่า (Configuration) หรือกำหนดนโยบาย (Policy) เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ป้องกันผู้บุกรุก ไวรัส รวมทั้ง Malicious Code ต่าง ๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

๒.๕ ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติต้องดำเนินการแก้ไข รวมทั้งมีการรายงานหัวหน้าสำนักงานจังหวัดโดยทันที

๒.๖ การเปิดใช้บริการ (Service) ต้องได้รับอนุญาตจากหัวหน้าสำนักงานจังหวัด ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม

๒.๗ ผู้ดูแลระบบต้องบริหารจัดการให้ไฟร์วอลล์สามารถเปิดใช้งานได้ตลอดเวลา และในกรณีที่พบปัญหาหรือการทำงานในลักษณะที่ผิดปกติต้องดำเนินการแก้ไข รวมทั้งมีการรายงานหัวหน้าสำนักงานจังหวัดโดยทันที

๒.๘ ผู้ดูแลระบบต้องออกจากระบบ (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์

๒.๙ ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งาน โดยบริหารจัดการบัญชีรายชื่อผู้ใช้งาน

๒.๑๐ ผู้ดูแลระบบต้องบันทึกบัญชีรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อยืนยันตัวตนผู้ใช้งานก่อนเข้าใช้งานระบบ (Authentication) และควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่ที่เกี่ยวข้อง

๒.๑๑ ผู้ดูแลระบบต้องติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของซอฟต์แวร์ระบบ (System Software)

๒.๑๒ ผู้ดูแลระบบต้องทดสอบซอฟต์แวร์ระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังการแก้ไข หรือบำรุงรักษา

๒.๑๓ หัวหน้าสำนักงานจังหวัดต้องกำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ อย่างชัดเจน

๒.๑๔ ผู้ขอใช้งานต้องยอมรับและปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

๒.๑๕ ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของจังหวัด หรือกฎหมาย หรืออาจทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศหรือทำให้เกิดความเสียหายต่อระบบสารสนเทศ ต้องยกเลิกการให้บริการทันที

หมวด ๑๐ การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก
(Intrusion Detection System (IDS) and Intrusion Prevention System (IPS))

๑. วัตถุประสงค์

เพื่อป้องกันการบุกรุกจากบุคคลที่ไม่พึงประสงค์ โดยมีรายงานที่สามารถตรวจสอบการดำเนินกิจกรรมของผู้ใช้งานได้ตลอดจนติดตามสืบค้นหาช่องโหว่ของระบบ และค้นหาที่มาของผู้บุกรุกได้อย่างมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก

๒.๑ ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ (IDS/IPS) เหตุการณ์ผิดปกติและการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ ต้องถูกทำการวิเคราะห์และหาสาเหตุของการบุกรุกในระบบเทคโนโลยีสารสนเทศของจังหวัด เพื่อเป็นเครื่องมือสำหรับการสืบสวนหาบุคคลที่โจมตีบุกรุก หรือใช้ระบบในทางที่ผิด และเป็นการป้องกันก่อนที่จะเกิดการโจมตี

๒.๒ ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามบุกรุกหรือโจมตีจังหวัด เป็นเครื่องมือวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟร์วอลล์ เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตรายที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือรวมทั้งไวรัสประเภทต่าง ๆ

๒.๓ ผู้ดูแลระบบต้องมีการบริหารจัดการเหตุการณ์บุกรุกระบบ (Incident Management) เป็นการตอบสนองต่อเหตุการณ์บุกรุกทางเครือข่าย สามารถช่วยวิเคราะห์ลักษณะการบุกรุกทางเครือข่ายและทำให้สามารถแก้ไขสถานการณ์ได้อย่างถูกต้อง ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการบุกรุก โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับจังหวัด และจัดทำวิธีปฏิบัติที่ถูกต้องให้กับจังหวัดเพื่อป้องกันเหตุการณ์เกิดซ้ำการตอบสนองต่อเหตุการณ์การบุกรุกแบ่งเป็น ๔ ขั้นตอน คือ

๒.๓.๑ จำกัดขอบเขต (Containment) จำกัดพื้นที่ที่เสี่ยงต่อการบุกรุกและจำกัดความรุนแรงของการบุกรุก

๒.๓.๒ กำจัดต้นเหตุ (Eradication) กำจัดต้นเหตุของการบุกรุก รวมถึงปิดกั้นช่องทางของการบุกรุก

๒.๓.๓ กู้คืนระบบ (Recovery) แก้ไขระบบที่ถูกบุกรุกให้สามารถกลับมาทำงานได้ตามปกติ

๒.๓.๔ ติดตามผล (Follow-Up) บันทึกผลกระทบของเหตุการณ์และแนะนำวิธีปฏิบัติเพื่อป้องกันเหตุการณ์เกิดซ้ำ

๒.๔ หัวหน้าสำนักงานจังหวัดต้องกำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่าย และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

๒.๕ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบ

๒.๖ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ต้องได้รับการอนุมัติจากหัวหน้าสำนักงานจังหวัด และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๗ ผู้ดูแลระบบต้องทำการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ และต้องประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง

หมวด ๑๑ การรักษาสภาพความพร้อมใช้งานของการให้บริการ
(IT Service Continuity)

๑. วัตถุประสงค์

เพื่อมั่นใจได้ว่าระบบสารสนเทศที่ให้บริการและข้อมูลสำคัญของจังหวัด มีความพร้อมใช้งานอยู่ตลอดและสามารถดำเนินการต่อไปได้ในขณะที่จังหวัดเผชิญกับภาวะวิกฤตหรือภัยพิบัติเพื่อลดผลกระทบที่อาจเกิดขึ้นกับจังหวัด โดยมีการลำดับความสำคัญจากผลกระทบจากความเสียหายของทรัพย์สิน และผลการวิเคราะห์ความเสี่ยงเพื่อใช้ในการพิจารณาวิธีการสร้างความต่อเนื่อง

๒. แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

๒.๑ เครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่มีความสำคัญต้องมีการสำรองข้อมูลให้อยู่สภาพพร้อมใช้งาน

๒.๒ ผู้ดูแลระบบต้องสำรองข้อมูลและซอฟต์แวร์เก็บไว้ โดยคัดเลือกและจัดเรียงลำดับตามผลกระทบจากความสูญเสียของระบบที่มีผลต่อภารกิจหลักของจังหวัด

๒.๓ ต้องมีขั้นตอนการปฏิบัติการสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๒.๔ ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองในสื่อบันทึกข้อมูลสำรอง โดยมีการแสดงชื่อระบบที่สำรอง วัน เดือน ปีและเวลาในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองต้องจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ในสถานที่จัดทำระบบสำรอง (ห้องเครื่องมือสื่อสาร) และต้องมีการทดสอบสื่อบันทึกข้อมูลสำรองอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

๒.๕ ห้องเครื่องมือสื่อสารต้องกำหนดสถานที่และเตรียมพื้นที่ให้อยู่ในสภาพพร้อมใช้งานระบบสำรอง

๒.๖ หัวหน้าสำนักงานจังหวัดต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมฉุกเฉิน

๒.๗ ห้องเครื่องมือสื่อสารต้องดำเนินการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมฉุกเฉินปีละ ๑ ครั้ง

๒.๘ ผู้ดูแลระบบต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยระบบสารสนเทศได้ตามปกติ โดยต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวอย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๒.๙ ห้องเครื่องมือสื่อสาร และหน่วยงานภายในที่เกี่ยวข้อง ต้องทดสอบปฏิบัติตามคู่มือแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

หมวด ๑๒ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ อีกทั้งเพื่อป้องกันทรัพย์สินของจังหวัดจากการสูญหาย เสียหาย ถูกขโมย หรือโจรกรรม หรือสารสนเทศถูกเปิดเผยโดยมิได้รับอนุญาต โดยมาตรการนี้มีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด

๒. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๒.๑ จังหวัดต้องมีการจำแนกและกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒.๒ ผู้บริหารต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่ควบคุมพิเศษ และพื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

๒.๓ ผู้บริหารต้องกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

๒.๓.๑ จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓.๒ ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

๒.๓.๓ จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน

๒.๓.๔ ต้องมีการทบทวนปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับสิทธิการเข้าออกพื้นที่ เช่น การโอนโยกย้าย ลาออก หรือสิ้นสุดการจ้าง

๓. การควบคุมการเข้าออก อาคาร สถานที่

๓.๑ หน่วยงานภายในที่รับผิดชอบด้านความปลอดภัยอาคารและสถานที่ หรือผู้บังคับบัญชาที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีเจ้าหน้าที่หรือวิธีการรักษาความปลอดภัยเพื่อควบคุมให้เข้าสถานที่ทำงานได้เฉพาะบุคคลที่ได้รับอนุญาตจากเจ้าของพื้นที่เท่านั้น

๓.๒ จัดทำเอกสารระบุสิทธิของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ดังนี้

๓.๒.๑ จังหวัดต้องกำหนดสิทธิผู้ใช้งานที่มีสิทธิผ่านเข้าออก และช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละ “พื้นที่งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” อย่างชัดเจน

๓.๒.๒ การเข้าถึงอาคารของจังหวัดของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย ต้องแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการบันทึกลงสมุดควบคุมการเข้าออกสถานที่

๓.๒.๓ กรณีที่บุคคลภายนอกหรือผู้ติดต่อต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์แบบพกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยต้องลงบันทึกในแบบฟอร์มการเข้าออกพื้นที่ในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้องและชัดเจน

๓.๒.๔ เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ ต้องลงชื่ออนุญาตเข้าออกในแบบฟอร์มการเข้าออกพื้นที่ให้ถูกต้องและชัดเจน

๓.๒.๕ เจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบบุคคลภายนอกหรือผู้ติดต่อ อุปกรณ์พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้องและชัดเจน

๓.๓ ผู้ใช้งานได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่กำหนดเพื่อใช้สำหรับปฏิบัติงานเท่านั้น

๓.๔ หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานภายในเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้ ต้องแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้ โดยหน่วยงานภายในเจ้าของพื้นที่ต้องจดบันทึกการขอเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๔. ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

จัดให้มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของจังหวัดที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งาน ดังนี้

๔.๑ ติดตั้งเครื่องกำหนดกระแสไฟฟ้าสำรอง

๔.๒ ติดตั้งระบบระงับเพลิง

๔.๓ ติดตั้งระบบปรับอากาศและควบคุมความชื้น

๔.๔ ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องแม่ข่ายทำงานผิดปกติหรือหยุดการทำงาน

๔.๕ วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของจังหวัดอย่างสม่ำเสมอ ให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ปกติ

๕. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

๕.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของจังหวัดในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงต้องติดตั้งระบบป้องกันที่ปลอดภัย

๕.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ หรือมีการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อป้องกันการตัดสายสัญญาณทำให้เกิดความเสียหาย หรือการดักรับข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต

๕.๓ สายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสม เพื่อป้องกันการรบกวนของสัญญาณ

๕.๔ ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๕.๕ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๕.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๕.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณแบบ Coaxial Cable สำหรับระบบสารสนเทศที่สำคัญ

๕.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี ๓ เดือน / ๖ เดือน สำหรับสายไฟเบอร์ออฟติก

๖. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๖.๑ วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา และต้องมีการซ่อมบำรุงอย่างทันท่วงทีตามความสำคัญของระบบ

๖.๒ บันทึกประวัติการบำรุงรักษาและซ่อมบำรุงอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง โดยมีรายละเอียด ได้แก่ วันที่บำรุงรักษาและซ่อมบำรุง รายการอุปกรณ์ สถานะของอุปกรณ์ ปัญหาที่พบและการแก้ไข ผู้ดำเนินการบำรุงรักษาและซ่อมบำรุงพร้อมลงลายมือชื่อ

๖.๓ ถ้ามีการจัดจ้างหน่วยงานหรือผู้ให้บริการภายนอก เพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์หน่วยงานภายในที่จัดจ้างต้องจัดให้มีสัญญาหรือข้อตกลงการจ้าง โดยต้องกำหนดระยะเวลาขอบเขต และระดับการให้บริการอย่างชัดเจน

๖.๔ ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในสำนักงานในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบหรือผู้รับผิดชอบการซ่อมบำรุงอุปกรณ์จะต้องอยู่ในพื้นที่ทุกครั้ง

๖.๕ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างหรือผู้ให้บริการภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๗. การนำทรัพย์สินของจังหวัดออกจากจังหวัด (Removal Of Property)

๗.๑ หน่วยงานภายในต้องมอบหมายเจ้าหน้าที่เป็น “ผู้ดูแลครุภัณฑ์” มีหน้าที่ควบคุมดูแลพัสดุหรือทรัพย์สินของจังหวัดที่อยู่ในความครอบครอง ให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลาโดยมิให้เกิดการสูญหาย และจัดทำ “ทะเบียนครุภัณฑ์” ของหน่วยงานภายใน บันทึกว่าถูกใช้ประจำอยู่ที่ใคร และสถานภาพและการเคลื่อนย้ายของครุภัณฑ์ ทั้งนี้ ต้องตรวจสอบสถานภาพของครุภัณฑ์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง การเคลื่อนย้าย เช่น ได้รับมอบครุภัณฑ์เพิ่มเติม การตัดจำหน่าย การเปลี่ยนผู้ครอบครอง การยืม การโอน หรือการส่งซ่อม

๗.๒ ต้องขออนุญาตจากผู้บังคับบัญชาของหน่วยงานภายในและแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอกสำนักงาน หรือนำไปซ่อมบำรุงที่ห้องเครื่องมือสื่อสาร

๗.๓ ต้องได้รับความเห็นชอบจากหัวหน้าสำนักงานจังหวัดก่อนนำครุภัณฑ์คอมพิวเตอร์ส่งซ่อมภายนอกสำนักงาน

๗.๔ การให้ยืมอุปกรณ์หรือทรัพย์สิน ผู้ดูแลครุภัณฑ์ต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวนำกลับมาตามช่วงเวลาที่กำหนด และอยู่ในสภาพดี หรือไม่ต่างจากตอนที่ถูกยืม และต้องบันทึกข้อมูลการนำอุปกรณ์ของสำนักงานออกไปใช้งานนอกสำนักงาน และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

๘. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกจังหวัด (Security of Equipment off Premises)

๘.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของสำนักงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๘.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของจังหวัดไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

๘.๓ เจ้าหน้าที่ผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๙. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use Equipment)

๙.๑ การจำหน่ายครุภัณฑ์คอมพิวเตอร์ อุปกรณ์เครือข่าย หน่วยงานภายในที่เป็นเจ้าของทรัพย์สินต้องจัดให้มีการทำลายข้อมูลและซอฟต์แวร์ลิขสิทธิ์ในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ก่อนการจำหน่ายเพื่อให้มั่นใจว่าข้อมูลและซอฟต์แวร์ลิขสิทธิ์จะไม่สามารถนำกลับมาใช้ได้อีก (non-retrievable)

๙.๒ หัวหน้าสำนักงานจังหวัดเป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ ต้องยื่นเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

๙.๓ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวไม่สามารถนำกลับมาใช้ได้อีก

๑๐. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

หน่วยงานควรดูแลให้มั่นใจว่าการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นไปตามกรอบหลักการที่สำคัญ ๓ ประการ คือ การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (Availability) หรือ CIA สอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และมาตรฐานสากลด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เช่น ISO/IEC 27001, ISO/IEC 27017 เป็นต้น ทั้งนี้ ในกรณีที่มีการใช้บริการ Cloud Computing หน่วยงานควรนำแนวปฏิบัติที่ดีของผู้ให้บริการ Cloud Computing มาเป็นแนวทางในการปฏิบัติงานและควบคุมดูแลเพื่อให้ระบบที่ใช้บริการ Cloud Computing มีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หมวด ๑๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและการสื่อสาร (IT Risk Management)

๑. วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์การตรวจสอบและประเมินความเสี่ยงของระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของจังหวัด ให้มั่นใจได้ว่าความเสี่ยงของระบบสารสนเทศของจังหวัด ได้ถูกพิจารณาและได้มีการจัดเตรียมมาตรการในการควบคุมความเสี่ยงที่เหมาะสม เพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้นกับจังหวัดได้

๒. แนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒.๑ การระบุความเสี่ยงให้สอดคล้องกับความเสี่ยงที่อาจจะเกิดขึ้นจริงกับการทำงาน ดังนี้

๒.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการ เพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๒.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๒.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือสารสนเทศหรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๒.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้าใช้งาน (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายที่มีบัญชีชื่อผู้ใช้งาน (Username) เดียวกันในเวลาเดียวกันมากกว่าหนึ่งจุด

๒.๑๕ ความเสี่ยงอื่นที่เกี่ยวข้องกับระบบสารสนเทศจังหวัด ซึ่งอาจจะส่งผลกระทบกับการปฏิบัติงานของจังหวัดในอนาคต

๒.๒ การตรวจสอบและประเมินความเสี่ยง ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๒.๒.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุทำการประเมินในแต่ละด้านของผลกระทบ โดยให้พิจารณาถึงมาตรการควบคุมที่มีอยู่ในปัจจุบันด้วย

๒.๒.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ รวมถึงความเป็นไปได้ที่เกิดขึ้นโดยต้องพิจารณา ๒ ปัจจัยหลัก ได้แก่ แนวโน้มการเกิดขึ้นของเหตุการณ์ความเสี่ยงพิจารณาจากความน่าจะเป็นหรือค่าทางสถิติที่มีการบันทึกไว้ เช่น เหตุการณ์ความเสี่ยงประเภทภัยธรรมชาติต่าง ๆ น่าจะมีแนวโน้มการเกิดต่ำ เมื่อดูจากสถิติที่เคยเกิดขึ้นความยากง่ายที่จะถูกกระทำ พิจารณาจากจุดอ่อนหรือข้อบกพร่องที่มีอยู่ และตัวควบคุมในปัจจุบัน หากมีจุดอ่อนหรือข้อบกพร่องมากและไม่มีตัวควบคุมเลย โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงจะสูงกว่าในกรณีที่มีตัวควบคุมอยู่

๒.๒.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ พิจารณาข้อบกพร่องของระบบหรือข้อบกพร่องของการควบคุมที่ปัจจุบันอาจจะไม่มีอยู่ และส่งผลให้ระบบไม่มีความมั่นคงปลอดภัยที่ดี

๒.๒.๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศของจังหวัดอย่างน้อยปีละ ๑ ครั้ง

๒.๒.๕ การตรวจสอบต้องดำเนินการโดยผู้ตรวจสอบสารสนเทศของจังหวัด (Internet IT Auditor) อย่างน้อยปีละ ๑ ครั้ง

หมวด ๑๔ การกำหนดหน้าที่และความรับผิดชอบด้านสารสนเทศและการสื่อสาร

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง (CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (PCIO) หัวหน้าสำนักงานจังหวัด ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน

๒. แนวทางปฏิบัติ

ส่วนที่ ๑ ระดับนโยบาย

๑.๑ ผู้ว่าราชการจังหวัดชัยนาท ในฐานะผู้บริหารระดับสูง (Chief Executive Officer : CEO) ของจังหวัด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่จังหวัดหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ผู้บริหารที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) ของจังหวัด เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ หัวหน้าสำนักงานจังหวัด เป็นผู้รับผิดชอบ ดังนี้

๑.๓.๑ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๑.๓.๒ ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

๑.๓.๓ วางแผน จัดทำ ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ส่วนที่ ๒ ระดับปฏิบัติงาน

ระดับผู้ปฏิบัติงาน ประกอบด้วย ผู้ดูแลระบบ ผู้ทีได้รับมอบหมายให้ปฏิบัติหน้าที่ และผู้ใช้งานเป็นผู้รับผิดชอบตามภารกิจ ดังนี้

๒.๑ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เป็นผู้รับผิดชอบ ดังนี้

๒.๑.๑ ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๑.๓ ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ระบบเครือข่าย ระบบสารสนเทศ ห้องควบคุมระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๒.๑.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๑.๖ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๒ ผู้ใช้งานเป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด

ภาคผนวก

การรักษาความมั่นคงปลอดภัยด้านการสื่อสาร

๑. ขั้นตอนปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

จังหวัดชัยนาท โดยคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) ได้ดำเนินการตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ กำหนดให้หน่วยงานของรัฐจัดทำกรอบการดำเนินงาน ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) โดยรายละเอียดแบ่งเป็น ๒ ส่วนหลัก คือ

๑.๑ ประมวลแนวทางปฏิบัติ มีองค์ประกอบ ๓ เรื่อง ดังนี้

๑) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓) แผนการรับมือภัยคุกคามทางไซเบอร์

๑.๒ การกำหนดกรอบมาตรฐาน ประกอบไปด้วย ๕ หัวข้อหลัก ดังนี้

๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่เครื่องคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๒. แผนและวิธีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัย

จังหวัดชัยนาท โดยคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) ได้จัดทำแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบภายในอย่างน้อย ปีละ ๑ ครั้ง และจัดให้มีการรายงานผลการเฝ้าระวังภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ตาม SLA ของระดับความรุนแรงตามที่กำหนด และสรุปรายงานผลการเฝ้าระวังให้กับผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัดชัยนาท อย่างน้อยเดือนละ ๑ ครั้ง โดยจังหวัดชัยนาทมีกระบวนการและขั้นตอนการตรวจสอบภายหลังจากการประชุมคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) และมอบหมายหน้าที่รับผิดชอบให้ดำเนินการตามขั้นตอนปฏิบัติการรักษาความปลอดภัยทางไซเบอร์

๓. การระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ขอบเขตของงานและสโคป (Scope) ของงานที่อยู่ในความรับผิดชอบของจังหวัดชัยนาทที่เกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ดังนี้

๓.๑ ระบบกล้องโทรทัศน์วงจรปิด (CCTV) ของจังหวัดชัยนาท จากการตรวจสอบเบื้องต้นไม่พบความเสี่ยงเนื่องจากเป็นระบบปิด มีผู้เข้าระบบเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องชัดเจน ไม่ปล่อยให้เปิดดูในระบบออนไลน์

๓.๒ ระบบการประชุมออนไลน์ทางไกล (VCS) อุปกรณ์ดังกล่าวเป็นระบบปิดที่มีผู้ที่เกี่ยวข้องหรือผู้รับผิดชอบชัดเจนในการเข้ารหัสใช้งาน

๓.๓ ระบบวิทยุสื่อสารและดาวเทียม อุปกรณ์ส่วนใหญ่เป็นฮาร์ดแวร์ ส่วนที่เป็นโปรแกรมหรือซอฟต์แวร์ เป็นระบบปิดที่ป้องกันบุคคลที่ไม่เกี่ยวข้องมาใช้งานหรือ Login เข้าระบบได้ต้องเป็นผู้ที่ได้รับอนุญาตเท่านั้น

๓.๔ เครื่องคอมพิวเตอร์เพื่อการใช้งานประจำวันสำหรับเข้าใช้บริการออนไลน์ ใช้อินเทอร์เน็ตหรือใช้พิมพ์งานต่าง ๆ เป็นอุปกรณ์ชนิดเดียวที่สำนักงานจังหวัดชัยนาทมีความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งการใช้งานผ่านระบบรักษาความปลอดภัย (Firewall) ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ที่มีอุปกรณ์ต่าง ๆ ปิดกั้นและป้องกันที่ปลอดภัยจากระบบอยู่แล้วชั้นหนึ่ง

๔. การประเมินความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์

จังหวัดชัยนาท โดยคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) ได้กำหนดกระบวนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

๕. แผนและขั้นตอนการรับมือเหตุคุกคามทางไซเบอร์

๕.๑ หลักการและเหตุผล

แผนและขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ของจังหวัดชัยนาทฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน อย่างน้อยปีละ ๑ ครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อเห็นเป็นไปตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดชัยนาทด้วย

๕.๒ วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในจังหวัดชัยนาท โดยเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใต้คณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) ในการกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้องการรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของจังหวัดชัยนาท

๕.๓ ขอบเขต

แผนและขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศและข้อมูลดิจิทัลของจังหวัดชัยนาท รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๕.๔ หน้าที่การทบทวนแผน

คณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee : PCIO) จังหวัดชัยนาท มีหน้าที่ทบทวนและขออนุมัติแผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ถึงผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัดต่อไป

๕.๕ หน้าที่การดำเนินการตามแผน

สำนักงานจังหวัดชัยนาท มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้

๕.๖ ความเกี่ยวข้องกับเอกสารอื่น

(๑) นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

(๒) นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จังหวัดชัยนาท

(๓) นโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลจังหวัดชัยนาท

(๔) นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารจังหวัดชัยนาท

๕.๗ นิยาม

(๑) เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบได้

(๒) เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

(๓) ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้เครื่องคอมพิวเตอร์และระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

(๔) เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๖. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT)

จังหวัดชัยนาท ใช้โมเดล (Model) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ประกอบด้วย

ที่	ชื่อ-นามสกุล	ตำแหน่ง	หน้าที่/ความรับผิดชอบ
๑	นายคณิต คงเมือง	หัวหน้าทีมรับมือฯ (Team Manager)	ทำหน้าที่สื่อสารกับผู้บริหาร/หน่วยงานที่เกี่ยวข้อง
๒	นางสาวปาริชาติ พิมปาน	รองหัวหน้าทีมรับมือฯ (Deputy Team Manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	นายอานนท์ อยู่ยอด	เจ้าหน้าที่รับมือฯ (Incident Lead)	ทำหน้าที่สนับสนุนช่วยเหลือให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
๔	นายนิทัศน์ จาตุรัตน์	เจ้าหน้าที่รับมือฯ (Incident Lead)	ทำหน้าที่สนับสนุนช่วยเหลือให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
๕	นายทนงศักดิ์ เอกกัณหา	เจ้าหน้าที่รับมือฯ (Technical Lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

นอกจากทีมรับมือฯ ดังกล่าวข้างต้น บุคคลต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ ดังนี้

ที่	ชื่อ-นามสกุล	ตำแหน่ง	หน้าที่/ความรับผิดชอบ
๑	นายพิชิต ธาดาวงษา	ผู้ดูแลระบบเครือข่ายการติดต่อสื่อสารระบบสารสนเทศ กสส.	ทำหน้าที่ควบคุม ดูแล ป้องกันผลกระทบจากภัยคุกคามทางไซเบอร์ และรายงานผล
๒	นายยศพร มาสะระ	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ด้านกฎหมายที่เกี่ยวข้องและตามคำสั่งแต่คณะทำงานส่วนกลาง
๓	นายจีระศักดิ์ ลำเทียน	ผู้ทดสอบและเจาะระบบ	ทำหน้าที่ตามนโยบายและแนวทางปฏิบัติด้านการรักษาความปลอดภัยทางไซเบอร์
๔	นายนิธิ หวังเจริญรุ่ง	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามนโยบายและแนวทางปฏิบัติด้านการรักษาความปลอดภัยทางไซเบอร์
๕	นางสาวกุลธิดา ตันเจริญ	ผู้ช่วยด้านบริหารจัดการความเสี่ยง	ทำหน้าที่ตามนโยบายและแนวทางปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล
๖	นางสาวสุภาวดี มีเย็น	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย	ทำหน้าที่ตามนโยบายและแนวทางปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

ที่	ชื่อ-นามสกุล	ตำแหน่ง	หน้าที่/ความรับผิดชอบ
๗	นางกาญจนา ลำลึก	ผู้ดูแลเว็บไซต์จังหวัดชัยนาท	ทำหน้าที่ควบคุม ดูแล ป้องกันผลกระทบจากภัยคุกคามทางไซเบอร์ และรายงานผล
๘	นายประมนต์ อินมงคล	ผู้ดูแลระบบเครือข่ายการติดต่อสื่อสาร ระบบสารสนเทศ จังหวัดชัยนาท	ทำหน้าที่ควบคุม ดูแล ป้องกันผลกระทบจากภัยคุกคามทางไซเบอร์ และรายงานผล
๙	นายรุ่ง รวมผล	ผู้ช่วยรับผิดชอบระบบเครือข่ายการติดต่อสื่อสาร ระบบสารสนเทศ จังหวัดชัยนาท	ทำหน้าที่ตามนโยบายและแนวทางปฏิบัติด้านความปลอดภัยสารสนเทศ

๗. ขั้นตอนการรับมือ

แผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดชัยนาท ดังนี้

๗.๑ ขั้นการเตรียมการ เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่ต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย/แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT)

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๗.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) ซึ่งเป็นสิ่งจำเป็นที่ช่วยให้หน่วยงานสามารถ

บรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๗.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยการดำเนินการดังกล่าวควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น เพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ เช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี

(๖) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๗.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ เป็นการดำเนินการที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident activity) นั้น หน่วยงานควรกำหนดขั้นตอน วิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าวช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้ หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญาหรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๒) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๔ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๘. วิธีการปฏิบัติด้านการรักษาความมั่นคงและปลอดภัย ระบบกล้องโทรทัศน์วงจรปิด (CCTV) ของจังหวัดชัยนาท

จังหวัดชัยนาท มีระบบกล้องโทรทัศน์วงจรปิด (CCTV) ภายในศาลากลางจังหวัดชัยนาท เป็นระบบปิดใช้การแบบโยงเครือข่ายเป็นระบบภายใน (LAN : Local Area Network) ไม่มีการเชื่อมโยงเครือข่ายที่สามารถออกสู่อินเทอร์เน็ต (Internet Network) จึงไม่มีอุปกรณ์ป้องกันการโจมตีทางเครือข่าย (Firewall) ซึ่งมีเพียงอุปกรณ์ที่เกี่ยวข้องทางด้านรักษาความมั่นคงและปลอดภัยทางไซเบอร์ ได้แก่ กล้องโทรทัศน์วงจรปิด เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย สายสัญญาณ เครื่องบันทึกภาพ และอุปกรณ์อื่น ดังนี้

๘.๑ รายการอุปกรณ์ที่ศาลากลางจังหวัดชัยนาท ประกอบด้วย

(๑) กล้องโทรทัศน์วงจรปิด (ภายนอก ๑๒ กล้อง และภายใน ๒๐ กล้อง) จำนวน ๓๒ กล้อง

(๒) อุปกรณ์บันทึกภาพแบบเครือข่าย (DVR : Digital Video Recorder) จำนวน ๓ ชุด

(๓) อุปกรณ์บันทึกข้อมูล ขนาด ๒ TB จำนวน ๒ ลูก

(๔) เครื่องคอมพิวเตอร์สำหรับจัดการระบบกล้องโทรทัศน์วงจรปิด จำนวน ๑ ชุด

(๕) เครื่องคอมพิวเตอร์สำหรับงานประมวลผล (Server) จำนวน ๑ ชุด

๘.๒ ขั้นตอนการปฏิบัติงาน

(๑) ขั้นตอนการขอดูภาพหรือขอสำเนาภาพจากกล้องโทรทัศน์วงจรปิด

- กรอกแบบคำขอร้องขอดูภาพหรือขอสำเนาภาพจากกล้องโทรทัศน์วงจรปิด
- ผู้ขอแจ้งรายละเอียด เช่น วัน เวลา และสถานที่เกิดเหตุ พร้อมระบุเหตุผลการนำไปใช้งาน
- แนบสำเนาบัตรประชาชน สำเนาบันทึกแจ้งความ หรือเอกสารอื่นที่ทางราชการออกให้
- นายช่างไฟฟ้าชำนาญงาน สำนักงานจังหวัดชัยนาท เซ็นรับรอง
- เสนอขอความเห็นชอบต่อหัวหน้าสำนักงานจังหวัดชัยนาท

(๒) การใช้งานคอมพิวเตอร์ในหน่วยงานสิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้

- มีการแยกผู้ใช้งานกันของแต่ละบุคคล
- มีการ Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ
- มีการ Update Patchระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่จดรหัสผ่าน (Password) และติดรหัสผ่านไว้ที่หน้าจอ
- มีการใช้รหัสผ่าน (Password) ที่ดี และไม่บอกรหัสผ่านแก่ผู้อื่น

(๓) การใช้เกี่ยวกับรหัสผ่าน (Password) การใช้รหัสผ่านที่ดี ดังนี้

- มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)
- มีความของรหัสผ่าน (Password) อย่างน้อย ๘ ตัวอักษร
- หลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์
- มีการเปลี่ยนรหัสผ่าน (Password) อย่างสม่ำเสมอ
- ไม่ใช้รหัสผ่าน (Password) ซ้ำกันในแต่ละระบบ
- ไม่บอกรหัสผ่าน (Password) แก่ผู้อื่น

(๔) การใช้อีเมล (E-mail) สิ่งที่ปฏิบัติเพื่อความปลอดภัย ดังนี้

- ไม่เปิดอีเมล์ (E-mail) ที่น่าสงสัย หรือผู้ส่งที่ไม่ชัดเจน
- ไม่เปิดไฟล์แนบจากอีเมล (E-mail) ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- ไม่คลิกลิงก์ Link ในอีเมล (E-mail) โดยไม่มีการตรวจเช็ค
- เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ มีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

(๕) การใช้เว็บไซต์ (Website) สิ่งที่ปฏิบัติเพื่อความปลอดภัย ดังนี้

- ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ
- ไม่ทำการบันทึกรหัสผ่าน (Password) ต่าง ๆ บนเว็บเบราว์เซอร์ (Browser)
- เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
- ใช้เว็บเบราว์เซอร์ (Browser) ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome Mozilla Firefox เป็นต้น
- มีการ Update Versionของเว็บเบราว์เซอร์ (Browser) อย่างสม่ำเสมอ
- กรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งานเบราว์เซอร์ (Browser) ในโหมด Sage Web Browsing
- ติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ

การรักษาความมั่นคงปลอดภัยด้านโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร

๑. ระบบเครือข่าย (Network)

๑.๑ ขั้นตอนการปฏิบัติงาน การเข้าถึงอุปกรณ์เครือข่าย เพื่อควบคุมระบบ หรือการกำหนดค่าต่าง ๆ ให้แก่อุปกรณ์เครือข่าย

(๑) เข้าวงเครือข่าย Network Management โดยเป็นวงอินทราเน็ต (Intranet) ไม่เชื่อมต่อออก อินเทอร์เน็ต (Internet) หรือเข้าวงเครือข่าย โดยการเข้าทางระบบ VPN สำหรับการเข้าถึงอุปกรณ์เครือข่าย ผ่านอุปกรณ์ Fortinet Firewall, Cisco Any Connect

(๒) เมื่ออยู่ในวงเครือข่าย Network Management แล้ว มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์เครือข่ายต่าง ๆ เช่น Router, Switch โดย User Password ที่ Radius Server แบ่งสิทธิ์การเข้าถึงอุปกรณ์สำหรับการควบคุม หรือการกำหนดค่าต่าง ๆ ของอุปกรณ์

(๓) มีระบบเก็บ Log การเข้าระบบ การเปลี่ยนแปลงค่า Configuration อุปกรณ์เครือข่าย โดยระบบที่มีใช้ Radius Server, SolarWinds, Network Device Log

(๔) มีระบบ Network Monitor สำหรับดูการทำงานของ Router, Switch ว่ามีการทำงานผิดปกติหรือไม่ เช่น CPU หรือ RAM ทำงานหนักผิดปกติ ดู Traffic Network ว่าสูงหรือไม่ โดยระบบ SolarWinds

(๕) มีระบบแจ้งเตือนอุปกรณ์ Network Down หรือทำงานผิดปกติผ่าน Line Alert ด้วย Zabbix

(๖) มีระบบแจ้งเตือน Link Down (SMS) ของผู้ให้บริการวงจรเช่า

(๗) มีการตรวจสอบอุปกรณ์เครือข่าย ตรวจสอบวงจรเชื่อมโยงอุปกรณ์เครือข่ายประจำวัน

(๘) ในระบบเครือข่ายทำการแบ่ง Virtual Router และ Vlan สำหรับแต่ละระบบงาน เช่น ระบบ VCS, ระบบ Internet, ระบบ IP Phone, ระบบ Network Management ให้อยู่คนละวงเครือข่าย Network เพื่อไม่ให้เกิดการรบกวนหากระบบใดระบบหนึ่งมีปัญหา

(๙) สำรองข้อมูล Backup Configuration ของอุปกรณ์ Router, Switch L3, Switch L2 เก็บในคอมพิวเตอร์, USB และ CD กรณีถูกโจมตี โดนแฮค หรืออุปกรณ์เสีย

๑.๒ วิธีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) ตรวจสอบอุปกรณ์เครือข่าย ตรวจสอบวงจรเชื่อมโยงอุปกณ์เครือข่ายประจำวัน

(๒) มีระบบ Network Monitor สำหรับดูการทำงานของ Router, Switch ว่ามีการทำงานผิดปกติหรือไม่ เช่น CPU หรือ RAM ทำงานหนักผิดปกติ ดู Traffic Network ว่าสูงหรือไม่ โดยระบบ SolarWinds และระบบ Alert การทำงานผิดปกติไปยัง Line ด้วย Zabbix

(๓) ตรวจสอบ Log การเข้าระบบว่ามีการ Login หรือพยายาม Login เข้าสู่ระบบโดยผิดปกติหรือไม่ เช่น ผู้ใช้ (User) ที่ไม่มีในระบบ Radius Server หรือการใส่รหัสผิดซ้ำ ๆ กันหลาย ๆ ครั้งของผู้ใช้ (User) บางผู้ใช้ (User)

(๔) ดูการทำงานที่ผิดปกติของตัวอุปกรณ์ด้วย Network Device Log

๑.๓ การระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) เสี่ยงจากการโดน Hack User Password

(๒) เสี่ยงจากการ User Password รั่วไหล เช่น การ Login เข้าอุปกรณ์ Network หรือ Login เข้าระบบงานผ่านเว็บเบราว์เซอร์ (Browser) แล้วให้เว็บเบราว์เซอร์ (Browser) จดจำ User Password

(๓) เสี่ยงจากการโดนล้างค่า Configuration เนื่องจากโดน Hack User Password

(๔) เสี่ยงจากการโดนยิง Packet สูง รบกวนในระบบเครือข่าย

๑.๔ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) รุนแรงมาก ระบบเครือข่ายใช้งานไม่ได้ ระบบล่ม (CPU cpu peak 100%)

(๒) รุนแรงปานกลาง ระบบเครือข่ายยังใช้งานได้บางระบบ เช่น ระบบอินเทอร์เน็ต (Internet) ไม่สามารถใช้งานได้ แต่ระบบ IP Phone, ระบบ Network Management ยังสามารถใช้งานได้ มีการรบกวนระบบทำให้เครือข่ายช้าการใช้งานไม่เสถียร บางอุปกรณ์อาจใช้งานไม่ได้

(๓) รุนแรงน้อย ระบบเครือข่ายยังใช้งานได้มีการรบกวนระบบทำให้ Traffic สูง เครือข่ายช้าการใช้งานไม่เสถียร

๑.๕ ขั้นตอนการรับเหตุภัยคุกคามทางไซเบอร์

เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์และผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของระบบเครือข่ายของจังหวัดชัยนาท ทำงานผิดพลาดหรือล่าช้าลง หรือส่งผลให้ระบบเครือข่ายไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้น บุคลากรของสำนักงานจังหวัดชัยนาท ต้องแจ้งให้กลุ่มงานเทคโนโลยีการสื่อสาร (กสส.) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ดำเนินการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ในเบื้องต้นสำนักงานจังหวัดชัยนาทต้องสำรองข้อมูลของจังหวัดชัยนาท และกู้คืนข้อมูล (Backup and Recovery) ของระบบเครือข่าย, Back-up Server VM เก็บในคอมพิวเตอร์ USB และ CD กรณีถูกโจมตี โดนแฮค หรืออุปกรณ์เสีย

ภัยคุกคาม	แผนการรับมือ				ผู้รับผิดชอบ
	แผนการป้องกัน		แผนการแก้ไข		
	แผน/ การควบคุม	ผลการ ดำเนินการ	แผน/การแก้ไข	ผลการ ดำเนินการ	
๑. รหัสผ่านอุปกรณ์เครือข่ายรั่วไหล โดนแฮค หรือรหัสผ่านผู้ดูแลระบบถูกเปลี่ยน	เปลี่ยนรหัสผ่าน / ไม่จดจำรหัสผ่านผู้ใช้จากเว็บเบราว์เซอร์	รหัสผ่านไม่รั่วไหลหรือไม่โดนแฮค	ทำการเปลี่ยนรหัสผ่านอุปกรณ์ทุก ๆ เดือน/ลบหรือบล็อกรหัสผ่านผู้ใช้ที่ต้องสงสัย เช่น ดูจาก Log ว่ามีการ Login Password ผิด ซ้ำ ๆ กันหลายครั้ง	รหัสผ่านของอุปกรณ์เครือข่ายมีความปลอดภัย	กสส. สป.มท.
๒. อุปกรณ์เครือข่าย เช่น Router โดนล้างค่า Configuration ไม่สามารถใช้งานระบบเครือข่ายได้	Backup Configuration ของอุปกรณ์เครือข่ายเก็บไว้หลาย ๆ ที่	มี Configuration ของอุปกรณ์เครือข่ายต่าง ๆ เก็บไว้หลาย ๆ ที่ ในคอมพิวเตอร์ ใน USB ใน CD	หากอุปกรณ์เครือข่ายโดนล้างค่า Configuration จนไม่สามารถใช้งานได้ ต้อง recovery configuration ที่ Backup กลับคืน และเปลี่ยน User Password ใหม่ทั้งหมด	อุปกรณ์ระบบเครือข่ายสามารถใช้งานได้	กสส. สป.มท.

ภัยคุกคาม	แผนการรับมือ				ผู้รับผิดชอบ
	แผนการป้องกัน		แผนการแก้ไข		
	แผน/ การควบคุม	ผลการ ดำเนินการ	แผน/การแก้ไข	ผลการ ดำเนินการ	
๓. การโดนยิง Packet สูง รบกวนในระบบเครือข่าย	กำหนด Policy ที่ Port Switch ของเครือข่าย/กำหนดแบนวิธ Port Switch หากมีการใช้งาน Packet ที่สูงผิดปกติ	มีการกำหนด Policy ที่ Port Switch และ Package ไม่สูงเกินแบนวิธที่กำหนดไว้	ดูว่า Packet สูงผิดปกติที่ Port ไหนหาเครื่องที่ต่อกับ Port นั้น นำออกจากระบบเครือข่ายก่อนแล้วทำการตรวจสอบเครื่อง	ไม่เกิดการรบกวนในระบบเครือข่าย	กสส. สป.มท.

๒. ระบบโทรศัพท์ IP Phone

๒.๑ ขั้นตอนการปฏิบัติงาน การเข้าถึงอุปกรณ์ระบบโทรศัพท์ IP Phone เพื่อควบคุมระบบ หรือการกำหนดค่าต่าง ๆ ของระบบ

(๑) เข้าวง Management ระบบโทรศัพท์ IP Phone โดยเป็นวงอินทราเน็ต (Intranet) ไม่เชื่อมต่อออกอินเทอร์เน็ต (Internet) หรือเข้าวง Management อุปกรณ์ โดยการเข้าทางระบบ VPN สำหรับการเข้าถึงอุปกรณ์ระบบโทรศัพท์ IP Phone ผ่านอุปกรณ์ Cisco AnyConnect

(๒) เมื่ออยู่ในวงระบบโทรศัพท์ IP Phone แล้วมีการกำหนดสิทธิ์การเข้าถึงระบบหรืออุปกรณ์ระบบต่าง ๆ เช่น Server IP Phone, Router, Switch โดย User Password ที่แบ่งสิทธิ์การเข้าถึงอุปกรณ์สำหรับการ Monitor หรือการ Configuration ระบบหรืออุปกรณ์

(๓) มีระบบเก็บ Log การเข้าระบบ การเปลี่ยนแปลงค่า Configuration ระบบหรืออุปกรณ์ด้วย Server, SolarWinds, Network Device Log

(๔) มีระบบ Network Monitor สำหรับดูการทำงานของ Router, Switch ว่ามีการทำงานผิดปกติหรือไม่ เช่น CPU หรือ RAM ทำงานหนักผิดปกติ ดู Traffic Network ว่าสูงหรือไม่ โดยระบบ SolarWinds

(๕) การตรวจสอบอุปกรณ์ Network ตรวจสอบ Server ระบบโทรศัพท์ IP Phone ประจำวัน

(๖) Server ของระบบมีการแบ่งแยกการทำงานของ Server ต่าง ๆ ด้วยระบบ VM

(๗) สำรองข้อมูล Backup Configuration ของ Server ระบบ, อุปกรณ์ Router, Switch L3, Switch L2 เก็บในคอมพิวเตอร์ USB และ CD กรณีถูกโจมตี โดนแฮค หรืออุปกรณ์เสีย (Telnet, Ssh)

๒.๒ วิธีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) ตรวจสอบอุปกรณ์ ระบบโทรศัพท์ IP Phone ประจำวัน

(๒) มีระบบ Monitor สำหรับดูการทำงานของ Router, Switch ว่ามีการทำงานผิดปกติหรือไม่ เช่น CPU หรือ RAM ทำงานหนักผิดปกติ ดู Traffic Network ว่าสูงหรือไม่ โดยระบบ SolarWinds

(๓) ตรวจสอบ Log การเข้าระบบว่ามีการ Login หรือพยายาม Login เข้าสู่ระบบโดยผิดปกติหรือไม่ เช่น ผู้ใช้ (User) ที่ไม่มีในระบบ Radius Server หรือการใส่รหัสผิดซ้ำ ๆ กันหลาย ๆ ครั้งของผู้ใช้ (User) บางผู้ใช้ (User)

(๔) ดูการทำงานที่ผิดปกติของตัวอุปกรณ์ด้วย Network Device Log

๒.๓ การระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) เสี่ยงจากการโดน Hack User Password

(๒) เสี่ยงจากการ User Password รั่วไหล เช่น การ Login เข้าอุปกรณ์ Network หรือ Login เข้าระบบงานผ่านเว็บเบราว์เซอร์ (Browser) แล้วให้เว็บเบราว์เซอร์ (Browser) จดจำ User Password

(๓) เสี่ยงจากการโดนล้างค่า Configuration เนื่องจากโดน Hack User Password

(๔) เสี่ยงจากการโดนยิง Packet สูง รบกวนในระบบเครือข่าย

๒.๔ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) รุนแรงมาก ระบบโทรศัพท์ IP Phone ไม่สามารถใช้งานได้ ระบบล่ม (CPU cpu peak 100%)

(๒) รุนแรงปานกลาง ระบบโทรศัพท์ IP Phone ยังใช้งานได้ภายในจังหวัด มีการรบกวนระบบทำให้ระบบโทรศัพท์ใช้งานไม่เสถียร โทรออกเบอร์องค์การโทรศัพท์ไม่ได้

(๓) รุนแรงน้อย ระบบโทรศัพท์ IP Phone ยังใช้งานได้มีการรบกวนระบบโทรศัพท์ใช้งานไม่เสถียร

๒.๕ ขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์

(๑) มี Link วงจรสำรอง (ผ่านระบบเครือข่าย MPLS)

(๒) มีระบบไฟฟ้าสำรอง UPS

(๓) การสำรองและกู้คืนข้อมูล (Backup and Recovery) ของอุปกรณ์ Router, Switch L3, Switch L2 เก็บในคอมพิวเตอร์, USB และ CD กรณีถูกโจมตี โดนแฮค หรืออุปกรณ์เสีย

ภัยคุกคาม	แผนการรับมือ				ผู้รับผิดชอบ
	แผนการป้องกัน		แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินการ	แผน/การแก้ไข	ผลการดำเนินการ	
๑. รหัสผ่านของระบบโทรศัพท์ IP Phone รั่วไหล โดนแฮค หรือรหัสผ่านผู้ดูแลระบบถูกเปลี่ยน	เปลี่ยนรหัสผ่าน / ไม่จดจำรหัสผ่านผู้ใช้จากเว็บเบราว์เซอร์	รหัสผ่านไม่รั่วไหลหรือไม่โดนแฮค	ทำการเปลี่ยนรหัสผ่านอุปกรณ์ทุก ๆ เดือน/ลบหรือบล็อกรหัสผ่านผู้ใช้ที่ต้องสงสัย เช่น ดูจาก Log ว่ามีการ Login Password ผิด ซ้ำ ๆ กันหลายครั้ง	รหัสผ่านของระบบโทรศัพท์ IP Phone มีความปลอดภัย	กสส. สป.มท.
๒. การโดนล้างค่า Configuration เนื่องจากโดน Hack User Password	Backup Configuration ของระบบโทรศัพท์ IP Phone เก็บไว้หลาย ๆ ที่/Backup VM แต่ละระบบแยกเก็บไว้	มี Configuration ของระบบโทรศัพท์ IP Phone และข้อมูล Backup VM แต่ละระบบเก็บไว้แยกในคอมพิวเตอร์ ใน USB ใน CD	หากระบบโทรศัพท์ IP Phone โดนล้างค่า Configuration จนไม่สามารถใช้งานได้ ต้อง recovery configuration ที่ Backup กลับคืนและเปลี่ยน User Password ใหม่ทั้งหมด	ระบบโทรศัพท์ IP Phone สามารถใช้งานได้	กสส. สป.มท.

๓. ระบบ Call Center 1567 ของศูนย์ดำรงธรรม

๓.๑ ขั้นตอนการปฏิบัติงาน การเข้าถึงอุปกรณ์ระบบ Call Center ๑๕๖๗ เพื่อควบคุมระบบ หรือการกำหนดค่าต่าง ๆ ของระบบ

(๑) เข้าวง Management ระบบ Call Center 1567 โดยเป็นวงอินทราเน็ต (Intranet) ไม่เชื่อมต่อออกอินเทอร์เน็ต (Internet) หรือเข้าวง Management อุปกรณ์

(๒) เมื่ออยู่ในวงเครือข่ายของระบบ Call Center 1567 แล้วมีการกำหนดสิทธิ์การเข้าถึงระบบหรืออุปกรณ์ ระบบแบ่งสิทธิ์การเข้าถึงอุปกรณ์สำหรับการ Monitor หรือการ Configuration ระบบ

(๓) มีระบบ Monitor และ Management (ผ่าน Web Browser)

(๔) ตรวจสอบอุปกรณ์ระบบ Call Center และเครือข่ายของ Call Center 1567 ประจำวัน

๓.๒ วิธีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) ตรวจสอบอุปกรณ์ระบบ Call Center และเครือข่ายของ Call Center 1567 ประจำวัน

(๒) มีระบบ Monitor สำหรับดูการทำงานของ Server

๓.๓ การระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) เสี่ยงจากการโดน Hack User Password

(๒) เสี่ยงจากการ User Password รั่วไหล เช่น การ Login เข้าอุปกรณ์ Network หรือ Login เข้าระบบงานผ่านเว็บเบราว์เซอร์ (Browser) แล้วให้เว็บเบราว์เซอร์ (Browser) จดจำ User Password

(๓) เสี่ยงจากการโดนล้างค่า Configuration เนื่องจากโดน Hack User Password

๓.๔ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) รุนแรงมาก ระบบ Call Center 1567 ไม่สามารถใช้งานได้ ระบบล่ม (CPU cpu peak 100%) ไม่สามารถรับสายจากประชาชนได้

(๒) รุนแรงปานกลาง ระบบ Call Center 1567 ยังใช้งานได้อาจจะมีบางจังหวัดที่ใช้งานไม่ได้ มีการรบกวนระบบทำให้ไม่สามารถรับสายจากประชาชนได้ในบางครั้ง

(๓) รุนแรงน้อย ระบบ Call Center 1567 ยังใช้งานได้มีการรบกวนระบบโทรศัพท์ใช้งานไม่เสถียร

๓.๕ ขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์

เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์และผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของระบบ Call Center 1567 ทำงานผิดพลาดหรือล่าช้า ส่งผลให้ระบบ Call Center 1567 ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้น บุคลากรของสำนักงานจังหวัดชัยนาท ต้องแจ้งให้กลุ่มงานเทคโนโลยีการสื่อสาร (กสส.) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ดำเนินการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery) ของ Server ระบบ Call Center 1567, Back-up Server VM เก็บในคอมพิวเตอร์ USB และ CD กรณีถูกโจมตี โดนแฮค หรืออุปกรณ์เสีย

ภัยคุกคาม	แผนการรับมือ				ผู้รับผิดชอบ
	แผนการป้องกัน		แผนการแก้ไข		
	แผน/ การควบคุม	ผลการ ดำเนินการ	แผน/การแก้ไข	ผลการ ดำเนินการ	
๑. รหัสผ่านของระบบ Call Center 1567 ของศูนย์ดำรงธรรม รั่วไหล โดนแฮค หรือรหัสผ่านผู้ดูแลระบบถูกเปลี่ยน	เปลี่ยนรหัสผ่าน / ไม่จดจำรหัสผ่านผู้ใช้จากเว็บเบราว์เซอร์	รหัสผ่านไม่รั่วไหลหรือไม่โดนแฮค	ทำการเปลี่ยนรหัสผ่านอุปกรณ์ทุก ๆ เดือน/ลบหรือบล็อกรหัสผ่านผู้ใช้ที่ต้องสงสัย เช่น ดูจาก Log ว่ามีการ Login Password ผิด ซ้ำ ๆ กันหลายครั้ง	รหัสผ่านของระบบ Call Center 1567 ของศูนย์ดำรงธรรม มีความปลอดภัย	กสส. สป.มท.
๒. การโดนล้างค่า Configuration เนื่องจากโดน Hack User Password	Backup Configuration ของระบบ Call Center 1567 ของศูนย์ดำรงธรรมเก็บไว้หลาย ๆ ที่/Backup VM แต่ละระบบแยกเก็บไว้	มี Configuration ของระบบ Call Center 1567 ของศูนย์ดำรงธรรม และข้อมูล Backup VM แต่ละระบบเก็บไว้แยกในคอมพิวเตอร์ ใน USB ใน CD	หากระบบ Call Center 1567 ของศูนย์ดำรงธรรม โดนล้างค่า Configuration จนไม่สามารถใช้งานได้ ต้อง recovery configuration ที่ Backup กลับคืน และเปลี่ยน User Password ใหม่ทั้งหมด	ระบบ Call Center 1567 ของศูนย์ดำรงธรรม สามารถใช้งานได้	กสส. สป.มท.

๔. ป้ายประชาสัมพันธ์อัจฉริยะ

๔.๑ ขั้นตอนการปฏิบัติงาน การเข้าถึงระบบเครือข่ายของป้ายประชาสัมพันธ์อัจฉริยะ เพื่อควบคุมระบบ หรือการกำหนดค่าต่าง ๆ ของระบบ หรืออัพเดทคอนเทนต์ (Content)

(๑) มีการกำหนดสิทธิ์ผู้ใช้ (User) ในการอัพเดทคอนเทนต์ (Content) โดยผู้ใช้ (User Password, Web Browser)

(๒) มี Any Desk ไว้รีโมทในการอัพเดทคอนเทนต์ (Content)

(๓) มีระบบ Firewall สำหรับป้องกันการใช้งานอินเทอร์เน็ต (Sophos Firewall)

(๔) มีระบบ Monitor ป้ายประชาสัมพันธ์อัจฉริยะ (ผ่าน Web Browser)

(๕)มีระบบกล้องโทรทัศน์วงจรปิด (CCTV) ไว้ดูป้ายว่ากำลังแสดงคอนเทนต์ (Content) อะไรอยู่แบบเรียลไทม (Real time) และบันทึกดูย้อนหลัง

(๖)มีการตรวจสอบอุปกรณ์ระบบป้ายประชาสัมพันธ์อัจฉริยะประจำวัน

๔.๒ วิธีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) ตรวจสอบการทำงานของ Server ป้ายประชาสัมพันธ์อัจฉริยะ

(๒) ตรวจสอบการทำงานของระบบ Firewall ป้ายประชาสัมพันธ์อัจฉริยะ

(๓) ตรวจสอบการทำงานของระบบกล้องโทรทัศน์วงจรปิด (CCTV) ป้ายประชาสัมพันธ์อัจฉริยะ

๔.๓ การระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) เสี่ยงจากการโดน Hack User Password

(๒) เสี่ยงจากการ User Password รั่วไหล เช่น การ Login เข้าอุปกรณ์ Network หรือ Login เข้าระบบงานผ่านเว็บเบราว์เซอร์ (Browser) แล้วให้เว็บเบราว์เซอร์ (Browser) จดจำ User Password

(๓) เสี่ยงจากการโดนล้างค่า Configuration เนื่องจากโดน Hack User Password

(๔) เสี่ยงจากการโดน Hack User Password แล้วโดนอัพเดทคอนเทนต์ (Content) ที่ไม่เหมาะสม

๔.๔ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) รุนแรงมาก ระบบป้ายประชาสัมพันธ์อัจฉริยะ โดน Hack User Password แล้วโดนอัพเดทคอนเทนต์ (Content) ที่ไม่เหมาะสม ไม่สามารถใช้งานได้ ระบบล่ม (CPU cpu peak 100%)

(๒) รุนแรงปานกลาง ระบบป้ายประชาสัมพันธ์อัจฉริยะ ยังใช้งานได้บางส่วน แต่ไม่สามารถเปลี่ยนคอนเทนต์ (Content) ได้

(๓) รุนแรงน้อย ระบบป้ายประชาสัมพันธ์อัจฉริยะ ยังใช้งานได้มีการรบกวนระบบให้ใช้งานได้ไม่เสถียร

๔.๕ ขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์

เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์และผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของระบบป้ายประชาสัมพันธ์อัจฉริยะ ทำงานผิดพลาดหรือล่าช้า ส่งผลให้ระบบไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้น บุคลากรของสำนักงานจังหวัดชัยนาท ต้องแจ้งให้กลุ่มงานเทคโนโลยีการสื่อสาร (กสส.) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ดำเนินการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery) ของ Server ระบบป้ายประชาสัมพันธ์อัจฉริยะ, Back-up Server VM เก็บในคอมพิวเตอร์ USB และ CD กรณีถูกโจมตี โดนแฮค หรืออุปกรณ์เสีย

ภัยคุกคาม	แผนการรับมือ				ผู้รับผิดชอบ
	แผนการป้องกัน		แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินการ	แผน/การแก้ไข	ผลการดำเนินการ	
๑. รหัสผ่านของระบบป้ายประชาสัมพันธ์อัจฉริยะ รั่วไหล โดนแฮค หรือรหัสผ่านผู้ดูแลระบบถูกเปลี่ยน	เปลี่ยนรหัสผ่าน / ไม่จดจำรหัสผ่านผู้ใช้จากเว็บเบราว์เซอร์	รหัสผ่านไม่รั่วไหลหรือไม่โดนแฮค	ทำการเปลี่ยนรหัสผ่านอุปกรณ์ทุก ๆ เดือน/ลบหรือบล็อกรหัสผ่านผู้ใช้ที่ต้องสงสัย เช่น ดูจาก Log ว่ามีการ Login Password ผิด ซ้ำ ๆ กันหลายครั้ง	รหัสผ่านของระบบป้ายประชาสัมพันธ์อัจฉริยะ มีความปลอดภัย	กสส. สป.มท.

ภัยคุกคาม	แผนการรับมือ				ผู้รับผิดชอบ
	แผนการป้องกัน		แผนการแก้ไข		
	แผน/ การควบคุม	ผลการ ดำเนินการ	แผน/การแก้ไข	ผลการ ดำเนินการ	
๒. การโดนล้างค่า Configuration เนื่องจากโดน Hack User Password	Backup Configuration ของระบบป้าย ประชาสัมพันธ์ อัจฉริยะ เก็บไว้หลาย ๆ ที่/Backup VM แต่ละระบบแยกเก็บไว้	มี Configuration ของระบบป้าย ประชาสัมพันธ์ อัจฉริยะ และข้อมูล Backup VM แต่ละระบบเก็บไว้แยกในคอมพิวเตอร์ ใน USB ใน CD	หากระบบป้าย ประชาสัมพันธ์ อัจฉริยะ โดนล้างค่า Configuration จนไม่สามารถใช้งานได้ ต้อง recovery configuration ที่ Backup กลับคืน และเปลี่ยน User Password ใหม่ทั้งหมด	ระบบป้าย ประชาสัมพันธ์ อัจฉริยะ สามารถใช้งานได้	กสส. สป.มท.

สำนักงานจังหวัดชัยนาท
กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
โทร.๐-๕๖๔๑-๑๒๐๔