

ประกาศจังหวัดสระแก้ว

เรื่อง นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

ด้วยในปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทและเป็นเครื่องมือสำคัญในการสนับสนุนการดำเนินงานของส่วนราชการ ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญต่าง ๆ โดยเฉพาะระบบงานที่เกี่ยวข้องกับการให้บริการประชาชน (front office system) และระบบปฏิบัติการ (back office system) เพื่อให้การดำเนินงานของส่วนราชการมีความสะดวกรวดเร็ว มีประสิทธิภาพมากขึ้น แต่อย่างไรก็ตาม การใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการ หากส่วนราชการไม่มีการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ ก็อาจส่งผลกระทบต่อการดำเนินงานหรือสร้างความเสียหายต่อส่วนราชการและประชาชนได้เช่นกัน

จังหวัดสระแก้ว ได้เล็งเห็นความสำคัญของการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงมีนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศจังหวัดสระแก้ว เพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น โดยได้กำหนดแนวทางปฏิบัติให้ส่วนราชการในจังหวัดสระแก้วดำเนินการกำกับ ดูแล และตรวจสอบเกี่ยวกับการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

๑. การควบคุมการใช้ข้อมูลและระบบคอมพิวเตอร์

๑.๑ กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ (Access Right)

๑.๒ กำหนดให้มีการใส่รหัสผ่าน (Password) ก่อนเข้าสู่ระบบคอมพิวเตอร์

๑.๓ มีการตรวจสอบสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานอย่างสม่ำเสมอ รวมถึงการเปลี่ยนแปลงหรือยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก พ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒. การป้องกันการบุกรุกผ่านระบบเครือข่าย (Logical Security)

๒.๑ มีระบบการตรวจสอบผู้ใช้งานก่อนเข้าสู่ระบบเครือข่ายอินเทอร์เน็ต (Authentication)

๒.๒ มีระบบป้องกันการบุกรุกจากบุคคลภายนอก เช่น Firewall, Proxy, IDS/IPS เป็นต้น

๒.๓ มีระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล ที่เป็นไปตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เช่น Log Server ระบบ Block Website ระบบตรวจสอบ IP Address เครื่องคอมพิวเตอร์ เป็นต้น

๓. การสำรองข้อมูลและระบบงานคอมพิวเตอร์ (Back up)

๓.๑ ให้ความสำคัญกับความครบถ้วนของการสำรองข้อมูลและระบบงานคอมพิวเตอร์ วิธีการเก็บรักษาสื่อที่ใช้บันทึกข้อมูลและระบบงานคอมพิวเตอร์

๓.๒ มีการทดสอบความถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบงานคอมพิวเตอร์ที่ได้สำรองไว้

/๔. การเตรียม....

๔. การเตรียมความพร้อมกรณีฉุกเฉิน (Contingency Plan)

๔.๑ มีแผนรองรับเหตุการณ์ฉุกเฉินต่าง ๆ เช่น กรณีไฟไหม้, ไฟดับ, ไวรัสคอมพิวเตอร์ เป็นต้น ซึ่งแผนดังกล่าวควรมีรายละเอียดที่ชัดเจนเกี่ยวกับขั้นตอนปฏิบัติและผู้รับผิดชอบ ควรมีการสื่อสารให้ผู้เกี่ยวข้องเข้าใจและรับทราบหน้าที่ความรับผิดชอบ

๔.๒ มีการทดสอบ/ซักซ้อมแผนรองรับเหตุการณ์ฉุกเฉินต่างๆเพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ

ประกาศจังหวัดสระแก้วฉบับนี้ จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อให้ส่วนราชการในจังหวัดสระแก้ว ถือเป็นแนวทางปฏิบัติในการกำกับ ดูแล ตรวจสอบเกี่ยวกับการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของส่วนราชการ เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติราชการให้เกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น

ประกาศ ณ วันที่ เดือน พฤษภาคม พ.ศ. ๒๕๖๐

(นายสมชัย ธมรวัฒนสวัสดิ์)
รองผู้ว่าราชการจังหวัด ปฏิบัติราชการแทน
ผู้ว่าราชการจังหวัดสระแก้ว