ประกาศจังหวัดพิษณุโลก

เรื่อง นโยบายด้านความปลอดภัยในระบบสารสนเทศ (IT Security)

ด้วย ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญในการดำเนินงานของส่วนราชการทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผล ระบบงานสำคัญต่าง ๆ โดยเฉพาะระบบงานที่เกี่ยวข้องกับการให้บริการประชาชน (front office system) และระบบปฏิบัติการ (back office system) เป็นต้น เทคโนโลยีสารสนเทศ ทำให้การดำเนินงานของส่วนราชการ มีความสะดวกรวดเร็ว มีประสิทธิภาพมากขึ้น อย่างไรก็ดี การใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการที่ควรคำนึงถึง โดยหากส่วนราชการไม่มีการบริหารจัดการและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารที่รัดกุมเพียงพอ ก็อาจส่งผลกระทบต่อการดำเนินงานหรือสร้างความเสียหายต่อส่วนราชการและประชาชนที่ติดต่องานได้ รวมทั้งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องต้องจัดให้มีนโยบายในการรักษาความปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ดังนั้น การควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงเป็นเรื่องที่ทุกส่วนราชการควรให้ความสำคัญ จังหวัดพิษณุโลก จึงมีนโยบายที่จะกำกับดูแลและตรวจสอบเกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของส่วนราชการอย่างจริงจัง เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติราชการให้เกิดประโยชน์สูงสุด และ เพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้นโดยให้ความสำคัญกับการบริหารจัดการและการควบคุมความเสี่ยงที่เกี่ยวข้อง ในเรื่องดังต่อไปนี้

๑. การควบคุมการใช้ข้อมูล และ ระบบงานคอมพิวเตอร์ และ การป้องกันการบุกรุกผ่านระบบเครือข่าย (Logical Security)

แนวทางการกำกับดูแล ส่วนราชการต้องให้ความสำคัญกับการจัดให้มีระบบการตรวจสอบผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (Authentication) และการกำหนดให้มีการใส่รหัสผ่าน (Password) ก่อนเข้าสู่ระบบคอมพิวเตอร์ โดยรหัสผ่านดังกล่าว ควรมีการกำหนดความยาวขั้นต่ำ อายุ จำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิด และควรกำหนดรหัสผ่านให้มีความยากแก่การคาดเดา นอกจากนี้ ส่วนราชการก็ควรมีการกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ และ สำหรับกรณีที่ส่วนราชการมีการเชื่อมต่อระบบเครือข่ายภายในกับภายนอก ส่วนราชการก็ควรมีระบบป้องกันการบุกรุกจากบุคคลภายนอกเช่นFirewallเป็นต้น และระบบป้องกันไวรัส (Anti virus) หรือ Malicious code อื่นๆ ทั้งนี้ ระบบต่าง ๆ ตามที่กล่าว รวมทั้งการใช้รหัสผ่าน และ สิทธิของผู้ใช้งานก็ควรมีการตรวจสอบอย่างสม่ำเสมอ

๒. การสำรองข้อมูล (Back up) และ ระบบงานคอมพิวเตอร์ และ การเตรียมพร้อมกรณีฉุกเฉิน (Contingency Plan) ในการปฏิบัติงานมีหลายกรณีที่อาจทำให้ข้อมูลหรือระบบงานคอมพิวเตอร์เสียหาย เช่น การติดไวรัส สภาวะแวดล้อม หรือ ภัยพิบัติต่างๆ หรือ อาจเกิดจากการปฏิบัติงานที่ผิดพลาดของผู้ใช้งาน เป็นต้น

/ ในการนี้ ๒

ในการนี้ ส่วนราชการต้องให้ความสำคัญกับการสำรองข้อมูล และ ระบบงานคอมพิวเตอร์ รวมทั้งการเตรียมพร้อมกรณีฉุกเฉินต่าง ๆ ดังนี้

๒.๑ การสำรองข้อมูล (Back up) และ ระบบงานคอมพิวเตอร์ หากมิได้มีการสำรองข้อมูลและระบบงานคอมพิวเตอร์ที่เพียงพอในกรณีที่เกิดเหตุการณ์ที่ทำให้ข้อมูลหรือระบบงานคอมพิวเตอร์เสียหาย ส่วนราชการก็อาจไม่มีข้อมูล หรือ ระบบงานคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของส่วนราชการ และ อาจก่อให้เกิดความเสียหายต่อประชาชนที่มารับบริการได้

แนวทางการกำกับดูแล ส่วนราชการต้องให้ความสำคัญกับความครบถ้วนของการสำรองข้อมูลและระบบงานคอมพิวเตอร์ วิธีการเก็บรักษาสื่อที่ใช้บันทึกข้อมูลและระบบงานคอมพิวเตอร์ และการทดสอบความถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบงานคอมพิวเตอร์ที่ได้สำรองไว้

๒.๒ การเตรียมพร้อมกรณีฉุกเฉิน การสำรองข้อมูล และ ระบบงานคอมพิวเตอร์เพียงอย่างเดียวนั้นอาจไม่เพียงพอแก่การป้องกันการหยุดชะงักของการปฏิบัติงาน ดังนั้น การจัดให้มีแผนฉุกเฉินเพื่อรองรับในกรณีที่อาจเกิดเหตุการณ์ฉุกเฉิน (Contingency Plan) จะทำให้การควบคุมความเสี่ยงด้าน availability risk มีประสิทธิภาพมากขึ้น

แนวทางการกำกับดูแล ส่วนราชการต้องให้ความสำคัญกับการจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉินต่าง ๆ ซึ่งแผนดังกล่าวควรมีรายละเอียดที่ชัดเจนเกี่ยวกับขั้นตอนปฏิบัติและผู้รับผิดชอบ ควรมีการสื่อสารให้ผู้เกี่ยวข้องเข้าใจและรับทราบหน้าที่ความรับผิดชอบ รวมทั้งควรมีการทดสอบแผนดังกล่าวเพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ

๓. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ การปฏิบัติงานประจำด้านคอมพิวเตอร์ที่สำคัญ คือ การควบคุมการประมวลผลข้อมูล ซึ่งการประมวลผลข้อมูลที่ถูกต้องและครบถ้วนมีความสำคัญต่อการปฏิบัติงานของส่วนราชการ โดยหากไม่มีวิธีการปฏิบัติและการควบคุมที่ชัดเจนและรัดกุมเพียงพอ ทำให้ข้อมูลไม่ถูกต้องหรือไม่ครบถ้วน (integrity risk) ซึ่งอาจก่อให้เกิดความเสียหายต่อส่วนราชการและประชาชนที่ติดต่อได้

แนวทางการกำกับดูแล ส่วนราชการต้องให้ความสำคัญกับการกำกับดูแลและควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์อย่างใกล้ชิดของผู้บังคับบัญชา การปฏิบัติงานที่มีขั้นตอนที่ชัดเจนและสามารถตรวจสอบได้ รวมทั้งควรจัดให้มีระบบการรายงานและการตรวจสอบการปฏิบัติงานประจำดังกล่าวอย่างสม่ำเสมอ

ประกาศจังหวัดพิษณุโลกฉบับนี้ จัดทำขึ้นโดยมีวัตถุประสงค์ เพื่อให้ส่วนราชการต่าง ๆ ถือเป็นแนวทางปฏิบัติในการกำกับ ดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และ การควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของส่วนราชการอย่างจริงจัง เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติราชการให้เกิดประโยชน์สูงสุด และ เพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้นโดยให้ความสำคัญกับการบริหารจัดการและการควบคุมความเสี่ยงที่เกี่ยวข้อง

ประกาศ ณ วันที่ ๗ กุมภาพันธ์ พ.ศ. ๒๕๕๖

(นายปรีชา เรืองจันทร์)
ผู้ว่าราชการจังหวัดพิษณุโลก