DIGITAL GOVERNMENT DEVELOPMENT AGENCY

ด่วนที่สุด

ที่ สพร ๒๕๖๘/๑๕๙๐

กวค. 71.1
วันที่ 28 พ.ค. 68
เวลา 10.30 น.

๒๗ พฤษภาคม ๒๕๖๘

เรื่อง ตอบกลับกรอบแนวทางการดำเนินการความปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

สลค. (eMail)
ส่ง : กวค.
รับที่ : ธ5720/68
28 พ.ค. 2568 เวลา 10.30 น.

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามที่อ้างถึง สำนักงานคณะกรรมการรักษาความปลอดภัยไซเบอร์แห่งชาติได้เสนอเรื่องกรอบแนวทางดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล โดยกองวิเคราะห์เรื่องเสนอคณะรัฐมนตรี มีการสอบถามความเห็นในส่วนรายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๓/๒๕๖๗ วาระที่ ๔.๓ เรื่อง แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับป้องกันข้อมูลส่วนบุคคลรั่วไหล สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้ข้อมูลรั่วไหล มีรายละเอียดการป้องกัน ๘ รายการ ดังนี้

๑. การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทาง มาตรฐาน ISO/IEC 27001 หรือ NIST ในการออกแบบ พัฒนา และบำรุงรักษาระบบ งดใช้ข้อมูลจริงในขั้นตอนการพัฒนาระบบ หรือกำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน รวมทั้ง กำหนดเกณฑ์สำหรับการเลือกบริษัทพัฒนาซอฟต์แวร์ที่มีประสบการณ์และมาตรฐานที่ผ่านการรับรองทางความปลอดภัยตลอดจนกำหนดให้มีการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วงการพัฒนาและก่อนการใช้งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที

๒. หน่วยงานควรจัดการอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่อง การออกแบบและพัฒนาระบบให้ปลอดภัย พร้อมสร้างความรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

๓. จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ รวมถึงการตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด

๔. กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้นความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา

๕. สร้างระบบเฝ้าระวังเพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่ เกิดขึ้นอย่างรวดเร็ว รวมถึงการมีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์

๖. สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์ และแพตช์ด้านความปลอดภัยเมื่อมีช่องโหว่ถูกค้นพบ

๗. หากมีระบบงานที่ไม่ได้ใช้งาน ควรมีการปิดระบบเพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลได้

๘. ให้หน่วยงานยึดหลักตาม Cloud Security Standards และสอดคล้องกับนโยบาย Cloud First Policy เพื่อเสริมสร้างความมั่นคงปลอดภัยทางดิจิทัล

ในการนี้ สำนักงาน...

ในการนี้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) มีความเห็นในข้อ ๑ ดังนี้

๑. "การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทาง มาตรฐาน ISO/IEC 27001 หรือ NIST ในการออกแบบ พัฒนา และบำรุงรักษาระบบ" สำนักงานเห็นว่าควรให้ความชัดเจนในประเด็นนี้ ในส่วนของงานที่มีการจ้างพัฒนาจากภายนอกหรือหน่วยงานรัฐจำเป็นต้องผ่านการรับรองมาตรฐาน ISO/IEC 27001 ในงานที่เกี่ยวข้องในการพัฒนาออกแบบหรือไม่ เพราะจะมีผลต่อการขอใบรับรองและเกิดค่าใช้จ่ายของหน่วยงานรัฐ หรือหน่วยงานภายนอกที่ต้องดำเนินการ

๒. "กำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน" สำนักงานเห็นว่า ควรมีการระบุความชัดเจนของข้อความที่ครอบคลุมถึงวิธีการลบ หรือทำลายที่ปลอดภัย พร้อมระบุให้ทวนสอบการลบข้อมูลหรือทำลาย ว่าข้อมูลไม่สามารถนำกลับมาใช้งานได้

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการ รักษาการแทน
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ฝ่ายความมั่นคงปลอดภัยไซเบอร์
ส่วนแผนงานและที่ปรึกษาความมั่นคงปลอดภัยไซเบอร์
มือถือ ๐๘ ๐๐๔๕ ๓๑๖๓ (ศรีสุดา)
ไปรษณีย์อิเล็กทรอนิกส์ cbp_division@dga.or.th
ไปรษณีย์อิเล็กทรอนิกส์สารบรรณกลาง saraban@dga.or.th