ประกาศศูนย์สัตว์ทดลองแห่งชาติ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

.....

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ประกอบกับตามมาตรา ๔๔ มาตรา ๔๕ ของพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

ดังนั้น เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์เป็นที่ยอมรับในระดับสากล ศูนย์สัตว์ทดลองแห่งชาติ จึงเห็นควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของศูนย์สัตว์ทดลองแห่งชาติ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศศูนย์สัตว์ทดลองแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

นโยบายที่ ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ มีแนวปฏิบัติ ดังนี้

๑) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒) การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์

๓) การเข้าถึงและควบคุมการใช้งานสารสนเทศ

- การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

- การควบคุมการเข้าถึงเครือข่าย
- การควบคุมการเข้าถึงระบบปฏิบัติการ
- การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ
- การรักษาชั้นความลับข้อมูลสารสนเทศ
- การควบคุมการใช้ลายเซ็นต์อิเล็กทรอนิกส์
- การควบคุมการเข้า-ออก ของผู้เกี่ยวข้องในพื้นที่ควบคุม

๔) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๕) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๖) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๗) การใช้งานอินเตอร์เน็ต และเครือข่ายสังคมออนไลน์

๘) การใช้งานจดหมายอิเล็กทรอนิกส์

๙) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑๐) การใช้งานระบบไฟร์วอลล์

๑๑) การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก

นโยบายที่ ๒ นโยบายการรักษาสภาพความพร้อมใช้งานของการให้บริการ มีแนวปฏิบัติ ดังนี้

๑) แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

นโยบายที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีแนวปฏิบัติ ดังนี้

๑) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒) การกำหนดหน้าที่และความรับผิดชอบด้านสารสนเทศ

ข้อ ๓ หน่วยงานต้องจัดทำ “แผนการรับมือภัยคุกคามทางไซเบอร์” ให้เป็นไปตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์ฯ

ข้อ ๔ การกำหนดความรับผิดชอบ

๔.๑ ผู้อำนวยการศูนย์สัตว์ทดลองแห่งชาติ ในฐานะผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) ของศูนย์ฯ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่ศูนย์ฯหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๒ ผู้อำนวยการศูนย์สัตว์ทดลองแห่งชาติ ในฐานะผู้บริหารระดับสูงสุด ของศูนย์ฯ เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบายให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๓ ผู้อำนวยการศูนย์สัตว์ทดลองแห่งชาติ เป็นผู้รับผิดชอบ ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะ วิธีการ และแนวทางแก้ไขปัญหาแก่เจ้าหน้าที่ระดับปฏิบัติหรือผู้ที่ได้รับมอบหมาย ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๔.๔ เพื่อให้การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์ฯ เป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้คณะกรรมการพัฒนาเทคโนโลยีสารสนเทศงานยุทธศาสตร์ หน่วยสารสนเทศ ผู้ดูแลระบบ ผู้รับผิดชอบระบบสารสนเทศ และผู้ที่ได้รับมอบหมาย เป็นผู้รับ ผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบาย และแนวปฏิบัติในการรัษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์ฯ ให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์ฯ ให้ประกาศให้เจ้าหน้าที่ทุกระดับของศูนย์ฯ รับทราบทุกครั้ง

ข้อ ๕ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดเป็นมาตรฐานด้านการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์ฯ เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง จึงให้ใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงและปลอดภัยด้านสารสนเทศตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่ของศูนย์ฯ และผู้เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ 1 ตุลาคม พ.ศ. ๒๕๖๗

นายสัตวแพทย์สุรชัย จันทร์ทิพย์
ผู้อำนวยการศูนย์สัตว์ทดลองแห่งชาติ