



ประกาศสำนักงานพิพิธภัณฑ์เกษตร
เฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติ
พระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)
พ.ศ. ๒๕๖๖

โดยที่เป็นการสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) เพื่อให้การดำเนินการเกี่ยวกับการรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) ตลอดจนเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัย มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์เป็นที่ยอมรับในระดับสากล

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกอบมาตรา ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) พ.ศ. ๒๕๕๒ ผู้อำนวยการสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)

“ผู้อำนวยการ” หมายความว่า ผู้อำนวยการสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว

“รองผู้อำนวยการ” หมายความว่า รองผู้อำนวยการสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” (Chief Information Officer : CIO) หมายความว่า ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว

พระเจ้าอยู่หัว (องค์การมหาชน) ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

“ผู้อำนวยการสำนัก” หมายความว่า ผู้อำนวยการสำนักอำนาจการ ผู้อำนวยการสำนักพัฒนา พิพิธภัณฑสถานและองค์ความรู้ ผู้อำนวยการสำนักนวัตกรรมเกษตรเศรษฐกิจพอเพียง ผู้อำนวยการสำนักสารสนเทศ และการสื่อสาร และผู้อำนวยการสำนักพัฒนากิจการ

“หัวหน้าหน่วยงาน และหัวหน้ากลุ่มงาน” หมายความว่า หัวหน้าหน่วยงานตรวจสอบภายใน หัวหน้ากลุ่มงานกฎหมาย และหัวหน้ากลุ่มงานแผน ติดตามและประเมินผล

“ผู้บริหาร” หมายความว่า ผู้อำนวยการ รองผู้อำนวยการ ผู้อำนวยการสำนัก หัวหน้าหน่วยงาน และหัวหน้ากลุ่มงาน

“เจ้าหน้าที่” หมายความว่า เจ้าหน้าที่ตามมาตรา ๓๐ (๑) แห่งพระราชกฤษฎีกาจัดตั้ง สำนักงานพิพิธภัณฑสถานเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) พ.ศ. ๒๕๕๒

“ที่ปรึกษาหรือผู้เชี่ยวชาญ” หมายความว่า ที่ปรึกษาหรือผู้เชี่ยวชาญตามมาตรา ๓๐ (๒) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพิพิธภัณฑสถานเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) พ.ศ. ๒๕๕๒

“ผู้ดูแลระบบ (System Administrator)” หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมาย ให้ปฏิบัติหน้าที่จากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และ/หรือ ผู้อำนวยการสำนักสารสนเทศและการสื่อสาร

“ผู้ใช้งาน” หมายความว่า ผู้บริหาร เจ้าหน้าที่ ที่ปรึกษาหรือผู้เชี่ยวชาญ เจ้าหน้าที่จ้างเหมา บริการของสำนักงาน หรือบุคคลภายนอกที่ได้รับอนุญาต (Authorized user) ให้ใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

ข้อ ๔ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

หมวดที่ ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ มีแนวปฏิบัติ ดังนี้

- ๑) การเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)
- ๒) ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ
- ๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- ๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
- ๕) การควบคุมการเข้าถึงระบบเครือข่าย
- ๖) การควบคุมการเข้าถึงระบบปฏิบัติการ
- ๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
- ๘) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
- ๙) การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์
- ๑๐) การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย
- ๑๑) การบริหารจัดการสินทรัพย์
- ๑๒) การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

หมวดที่ ๒ นโยบายการจัดทำระบบสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

หมวดที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หมวดที่ ๔ หน้าที่และความรับผิดชอบ

ข้อ ๕ การกำหนดหน้าที่และความรับผิดชอบ

๕.๑ ระดับนโยบาย ได้แก่ ผู้อำนวยการ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) และผู้อำนวยการสำนักสารสนเทศและการสื่อสาร โดยมีหน้าที่และความรับผิดชอบ ดังนี้

๕.๑.๑ กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๕.๑.๒ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สำนักงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๒ ระดับบริหาร ได้แก่ ผู้อำนวยการสำนัก หัวหน้าหน่วยงาน หัวหน้ากลุ่มงาน โดยมีหน้าที่และความรับผิดชอบ ดังนี้

๕.๒.๑ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๕.๒.๒ ควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๕.๒.๓ วางแผน ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๕.๓ ระดับปฏิบัติ ได้แก่ เจ้าหน้าที่ฝ่ายสารสนเทศ สำนักสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบ ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และ/หรือ ผู้อำนวยการสำนักสารสนเทศและการสื่อสาร โดยมีหน้าที่และความรับผิดชอบ ดังนี้

๕.๓.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๓.๒ ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๕.๓.๓ ดำเนินการสำรองข้อมูลและเรียกคืนข้อมูล (backup and recovery) ตามรอบระยะเวลาที่กำหนด

๕.๓.๔ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูล จากบุคคลภายนอก (hacker) โดยไม่ได้รับอนุญาต

๕.๓.๕ การรักษาความปลอดภัย ระบบอินเทอร์เน็ต

๕.๓.๖ รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

๕.๓.๗ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๔ เพื่อให้การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน เป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้ฝ่ายสารสนเทศ เป็นผู้มีหน้าที่และความรับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ ๑ ครั้ง

โดยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ได้นำออกเผยแพร่ โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) ของสำนักงาน เผยแพร่เพื่อให้ ผู้ใช้งาน และได้เผยแพร่ทางเว็บไซต์ของสำนักงาน เพื่อให้ผู้ใช้งานได้ทราบและถือปฏิบัติตามนโยบายนี้ อย่างเคร่งครัด

ข้อ ๖ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดเป็นมาตรฐานด้านการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สำนักงาน เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง จึงให้ใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศตามเอกสารแนบท้ายประกาศนี้ ซึ่งผู้ใช้งานจะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑๓ เดือน เมษายน พ.ศ. ๒๕๖๖

พลอากาศเอก



(เสนาะ พรรณพิกุล)

ผู้อำนวยการสำนักงานพิพิธภัณฑ์เกษตร

เฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว