ประกาศกรมการปกครอง
เรื่อง แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมการปกครอง
พ.ศ. ๒๕๖๕

เพื่อให้การใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมการปกครอง มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเชื่อถือได้ ตลอดจนดำเนินการให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมการปกครองจึงกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้ ดังต่อไปนี้

ข้อ ๑. คำนิยาม คำนิยามที่ใช้ในแนวทางปฏิบัตินี้ประกอบด้วย

(๑) **ส่วนราชการ** หมายถึง ส่วนราชการภายในของกรมการปกครอง ที่มีฐานะเป็น สำนัก กอง ศูนย์หรือหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่ากอง

(๒) **เทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง เทคโนโลยีที่เกี่ยวข้องกับข่าวสาร ข้อมูล และการสื่อสารนับตั้งแต่การสร้าง การนำมาวิเคราะห์หรือประมวลผลการรับและส่งข้อมูล การจัดเก็บ และการนำไปใช้งานใหม่ เทคโนโลยีเหล่านี้มักจะหมายถึงคอมพิวเตอร์ซึ่งประกอบด้วยส่วนอุปกรณ์ (hardware) ส่วนคำสั่ง (software) และส่วนข้อมูล (data) และระบบการสื่อสารต่าง ๆ ไม่ว่าจะเป็นโทรศัพท์ระบบสื่อสารข้อมูล ดาวเทียม หรือเครื่องมือสื่อสารใด ๆ ทั้งมีสายและไร้สาย

(๓) **ผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนราชการ

(๔) **ผู้ใช้บริการ** หมายถึง ข้าราชการ พนักงานของรัฐ พนักงานราชการ หรือผู้ที่ส่วนราชการอนุญาตให้ใช้ระบบคอมพิวเตอร์ได้

(๕) **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๖) **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของกรมได้

(๗) **ระบบสารสนเทศ** หมายถึง กระบวนการจัดเก็บรวบรวมข้อมูลซึ่งทำให้เป็นสารสนเทศการจัดเก็บและการนำเสนอสารสนเทศให้เป็นปัจจุบัน

/(๘) **ไฟร์วอลล์...**

(๘) **ไฟร์วอลล์ (Firewall)** หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

(๙) **VPN (Virtual Private Network)** หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัวโดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเตอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

(๑๐) **WEP (Wired Equivalent Privacy)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

(๑๑) **WPA (Wi-Fi Protected Access)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

(๑๒) **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้บริการ และรหัสผ่าน

(๑๓) **ลงบันทึกเข้า (Login)** หมายถึง กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้บริการ และรหัสผ่าน ให้ถูกต้อง

(๑๔) **ลงบันทึกออก (Logout)** หมายถึง กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

(๑๕) **ช่องโหว่ (Vulnerability)** หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๑๖) **การเข้ารหัส (Encryption)** หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

(๑๗) **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

(๑๘) **โปรแกรมประสงค์ร้าย (Malware)** หมายถึง โปรแกรมคอมพิวเตอร์ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอนคอมพิวเตอร์ (Worm) หรือม้าโทรจัน (Trojan Horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

/**ข้อ ๒.** นโยบาย...

ข้อ ๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการปกครอง

(๑) ข้อมูลทั้งหมดในการดำเนินงานของหน่วยงานที่เป็นระบบอิเล็กทรอนิกส์ นับตั้งแต่กระบวนการสร้าง จัดเก็บ การเข้าใช้งาน รวมถึงการทำลาย ต้องมีขั้นตอน และการดำเนินการรักษาความลับอย่างเหมาะสม

(๒) ข้อมูลทั้งหมดในการดำเนินงานของหน่วยงาน ต้องมีความถูกต้อง ครบถ้วนสมบูรณ์ และเป็นปัจจุบัน

(๓) การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ มีนโยบายให้บริการระบบสารสนเทศแก่ผู้ดูแลระบบ ผู้ใช้งาน โดยสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย ภายใต้บทบัญญัติของกฎหมาย

(๔) ต้องจัดให้มีการบริหารความเสี่ยงของความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานอย่างเหมาะสม

(๕) ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินทางอิเล็กทรอนิกส์ที่มีประสิทธิภาพเพื่อความมั่นคงปลอดภัยด้านสารสนเทศ

(๖) การเข้าถึงระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์ของหน่วยงาน

(๗) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือการใช้งาน และการจัดการฝึกอบรมหรือเผยแพร่การใช้งานระบบสารสนเทศทางเว็บไซต์ภายใน (Intranet) และเว็บไซต์ภายนอก (Internet) ของหน่วยงานแก่ผู้ดูแลระบบ และผู้ใช้งาน

(๘) ให้มีการติดตามประมวลผล และทบทวน การปฏิบัติตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ตามระยะเวลา ๑ ครั้งต่อปี

ข้อ ๓. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศกรมการปกครอง ประกอบด้วยแนวทางปฏิบัติในด้านต่าง ๆ ดังนี้

(๑) แนวทางปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๒) แนวทางปฏิบัติการกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๓) แนวทางปฏิบัติการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๔) แนวทางปฏิบัติการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

(๕) แนวทางปฏิบัติการบริหารจัดการระบบเครือข่าย กรมการปกครอง

(๖) แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

(๗) แนวทางปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ

(๘) แนวทางปฏิบัติการควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ

(๙) แนวทางปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้บริการ

(๑๐) แนวทางปฏิบัติการสำรอง และกู้คืนข้อมูล

/(๑๑) แนวทาง...

(๑๑) แนวทางปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(๑๒) แนวทางปฏิบัติของผู้ใช้บริการ

กรมการปกครอง มอบหมายศูนย์สารสนเทศเพื่อการบริหารงานปกครอง เป็นหน่วยงานหลักในการรับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ตามข้อ ๓

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๙ เดือน ธันวาคม พ.ศ. ๒๕๖๕

(นายแมนรัตน์ รัตนสุคนธ์)
อธิบดีกรมการปกครอง