ระเบียบหน่วยราชการในพระองค์
ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล พ.ศ. ๒๕๖๗

เพื่อให้การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ของหน่วยราชการในพระองค์ เป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับกฎหมายที่แก้ไขเพิ่มเติมในปัจจุบัน และประกาศหน่วยราชการในพระองค์ เรื่อง นโยบายเทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ จึงเห็นสมควรปรับปรุง แก้ไขระเบียบที่เกี่ยวข้อง เพื่อให้การปฏิบัติงานด้านเทคโนโลยีดิจิทัลเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันและแก้ไขปัญหาจากการใช้งานระบบเทคโนโลยีดิจิทัล

อาศัยอำนาจตามมาตรา ๔ แห่งพระราชบัญญัติระเบียบบริหารราชการในพระองค์ พ.ศ. ๒๕๖๐ และมาตรา ๑๕ แห่งพระราชกฤษฎีกาจัดระเบียบราชการและการบริหารงานบุคคลของราชการในพระองค์ พ.ศ. ๒๕๖๐ ประกอบกับประกาศหน่วยราชการในพระองค์ เรื่อง นโยบายด้านเทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ประกาศ ณ วันที่ ๑๕ พฤษภาคม พ.ศ.๒๕๖๖ จึงออกระเบียบโดยได้รับพระบรมราชานุญาตไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบหน่วยราชการในพระองค์ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล พ.ศ. ๒๕๖๗”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ เมษายน ๒๕๖๗ เป็นต้นไป

ข้อ ๓ ให้ยกเลิก “ ระเบียบส่วนราชการในพระองค์ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ พ.ศ. ๒๕๖๐ ”

ข้อ ๔ ให้ประธานข้าราชบริพารในพระองค์ เป็นผู้รักษาการตามระเบียบนี้

หมวด ๑
บทนิยาม

ข้อ ๕ ในระเบียบนี้

หน่วยงาน หมายความว่า หน่วยงานระดับกองขึ้นไป หรือกองพันขึ้นไป ของหน่วยราชการในพระองค์

หน่วยงานภายนอก หมายความว่า หน่วยงานหรือองค์กร ที่ได้รับอนุญาตจากหน่วยราชการในพระองค์ ให้มีสิทธิในการเข้าถึงข้อมูล และใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้งาน ตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

บุคลากร (Peopleware) หมายความว่า ผู้ใช้งาน (User) และผู้ดูแลระบบ (Admin) ที่ปฏิบัติงานตามหน้าที่ของแต่ละหน่วยงาน

ผู้ดูแลระบบ (Admin) หมายความว่า ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษา ควบคุม เฝ้าระวัง และแจ้งเตือนที่เกี่ยวข้องกับระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของหน่วยราชการในพระองค์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลไม่ว่าส่วนหนึ่งส่วนใด

ผู้ใช้งาน (User) หมายความว่า หน่วยงานภายใต้หน่วยราชการในพระองค์ ข้าราชบริพารในพระองค์ หน่วยงานภายนอกและบุคคลภายนอก ที่ได้รับอนุญาต ให้ปฏิบัติงานให้กับหน่วยราชการในพระองค์ สามารถเข้าใช้งานเพื่อบริหารจัดการ ดูแลรักษาและแจ้งเตือนเหตุอันเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ของหน่วยราชการในพระองค์

ชื่อผู้ใช้งาน (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อเข้าสู่ระบบ (Login) สำหรับใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ที่มีการกำหนดสิทธิในการใช้งานไว้

บัญชีผู้ใช้บริการ (Account) หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์และบริการในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

สิทธิการเข้าถึง หมายความว่า การควบคุมการเข้าถึงข้อมูลของผู้ใช้งาน ผ่านการกำหนดรหัสผ่าน หรือการปิดสิทธิ์ไม่ให้ผู้ใช้งานเห็นข้อมูลนั้น ๆ

รหัสผ่าน (Password) หมายความว่า ตัวอักษร ตัวเลข และสัญลักษณ์ต่าง ๆ ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล (Authentication) และใช้ในการเข้าถึงระบบหรือข้อมูล (Authorization)

ทรัพย์สินดิจิทัล หมายความว่า อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่ายคอมพิวเตอร์ อุปกรณ์ต่อพ่วง Software ระบบฐานข้อมูล ข้อมูล และโดเมนเนม ที่ใช้ในการปฏิบัติงานของหน่วยราชการในพระองค์

โดเมนเนม (Domain Name) หมายความว่า ชื่อที่ตั้งขึ้นให้กับเว็บไซต์ เพื่อให้ง่ายต่อการจดจำและการนำไปใช้

ระบบคอมพิวเตอร์ (Computer System) หมายความว่า ระบบที่ประกอบด้วยอุปกรณ์คอมพิวเตอร์ (Hardware) ซอฟต์แวร์ (Software) และอุปกรณ์ต่อพ่วงที่ทำงานร่วมกันเพื่อให้เกิดการประมวลผลข้อมูล

เครื่องคอมพิวเตอร์ หมายความว่า เครื่องคอมพิวเตอร์ตั้งโต๊ะ เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์ส่วนบุคคลที่สามารถพกพาได้โดยใช้หน้าจอสัมผัสในการปฏิบัติหน้าที่ราชการ

อุปกรณ์คอมพิวเตอร์ (Hardware) หมายความว่า ส่วนของกลไกที่ทำให้คอมพิวเตอร์ทำงานได้

ซอฟต์แวร์ (Software) หมายความว่า ชุดคำสั่งที่มีขั้นตอน ตามลำดับ หรือตามเงื่อนไขที่กำหนด ที่สั่งให้เครื่องคอมพิวเตอร์ทำงาน เพื่อให้ได้ผลลัพธ์ตามที่ต้องการ หรือระบบปฏิบัติการที่ใช้งานบนคอมพิวเตอร์ เช่น ระบบปฏิบัติการ Windows/ macOS/ Linux โปรแกรมแอปพลิเคชันต่าง ๆ และโปรแกรมที่ใช้ในการควบคุมหรือจัดการฮาร์ดแวร์

ระบบเครือข่ายคอมพิวเตอร์ หมายความว่า อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อถึงกันตั้งแต่ ๒ เครื่องขึ้นไปสามารถแลกเปลี่ยนข้อมูลและแบ่งปันทรัพยากรระหว่างกันได้

คอมพิวเตอร์แม่ข่าย (Server) หมายความว่า เครื่องคอมพิวเตอร์ตัวหลักในเครือข่ายที่จะทำหน้าที่ให้บริการระบบสารสนเทศที่เป็นส่วนกลางในเครือข่ายทั้งหมดนั้น ๆ เป็นทั้งที่เก็บโปรแกรมและข้อมูลพื้นฐาน

แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผังที่แสดงการเชื่อมต่อของอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ และระบบสารสนเทศของหน่วยงานต่าง ๆ

ระบบเครือข่ายภายใน (Intranet) หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ภายในขององค์กร ซึ่งใช้ได้เฉพาะคนในองค์กรเท่านั้น

ระบบสารสนเทศ (Information System) หมายความว่า เป็นระบบพื้นฐานของการทำงานต่าง ๆ ในรูปแบบของการนำเข้า (input) การประมวลผล (processing) แสดงผล (output) และมีส่วนจัดเก็บข้อมูล (storage)

การเก็บข้อมูล (Log File) หมายความว่า ข้อมูลเส้นทางการใช้งานอินเทอร์เน็ต หรือการเชื่อมต่อสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ หรืออื่น ๆ ที่เกี่ยวข้อง

การควบคุมการเข้าถึง (Access Control) หมายความว่า การควบคุมการเข้าออกพื้นที่ต่าง ๆ และการเข้าถึงทางระบบจากระยะไกล (Remote Access) โดยกำหนดสิทธิให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

VPN (Virtual Private Network) หมายความว่า เครือข่ายเสมือนจริง สำหรับใช้ในการเข้าถึงระบบเครือข่ายภายในองค์กร

การเข้าถึงจากระยะไกล (Remote Access) หมายความว่า วิธีการเข้าถึงระบบเครือข่ายคอมพิวเตอร์จากระยะทางไกล ที่สามารถควบคุมเครื่องคอมพิวเตอร์ได้

BYOD (Bring Your Own Device) หมายความว่า การนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้ในสำนักงาน โดยอุปกรณ์ดังกล่าวมีความสามารถในการเชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงาน

Two-Factor Authentication หมายความว่า การที่ผู้ใช้งานทำการยืนยันว่าตนเองเป็นผู้ใช้งานจริง โดยการแสดงสิ่งที่ใช้ยืนยันตัวตนเพิ่มเติมจากรหัสผ่าน

ความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ

ภัยคุกคามทางไซเบอร์ หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ๒
คณะกรรมการการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล หน่วยราชการในพระองค์

ข้อ ๖ ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการอำนวยการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล” ประกอบด้วย

(๑) ประธานข้าราชบริพารในพระองค์	ประธานกรรมการอำนวยการ
(๒) รองเลขาธิการพระราชวัง	รองประธานกรรมการอำนวยการ
(๓) ผู้ช่วยราชเลขานุการในพระองค์ พระบาทสมเด็จพระเจ้าอยู่หัว	รองประธานกรรมการอำนวยการ
(๔) เลขาธิการองคมนตรี	กรรมการอำนวยการ
(๕) ผู้บัญชาการสำนักงานราชองครักษ์ประจำพระองค์	กรรมการอำนวยการ
(๖) ผู้บัญชาการกองบัญชาการทหารมหาดเล็กราชวัลลภรักษาพระองค์	กรรมการอำนวยการ
(๗) ผู้บัญชาการกองบัญชาการนายตำรวจราชองครักษ์ประจำพระองค์	กรรมการอำนวยการ
(๘) ผู้อำนวยการศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	กรรมการอำนวยการและเลขานุการ
(๙) ผู้อำนวยการกองระบบเครือข่ายสารสนเทศและความปลอดภัย ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	ผู้ช่วยเลขานุการ

ข้อ ๗ ให้คณะกรรมการอำนวยการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล มีอำนาจ และหน้าที่ ดังต่อไปนี้

(๑) กำหนดนโยบายการบริหารงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลของหน่วยราชการในพระองค์

(๒) ให้คำแนะนำ และคำปรึกษา เกี่ยวกับการดำเนินงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลต่อคณะกรรมการดำเนินการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล

(๓) ติดตามการดำเนินการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลของหน่วยราชการในพระองค์

(๔) ให้อำนาจคณะกรรมการดำเนินการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ติดตาม ตรวจสอบ สอบสวน และเร่งรัดการดำเนินการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลของหน่วยราชการในพระองค์

(๕) พิจารณา แก้ไข นโยบาย ระเบียบ ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลของหน่วยราชการในพระองค์

ข้อ ๘ ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการดำเนินการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล” ประกอบด้วย

(๑)	ผู้อำนวยการศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	ประธานกรรมการ
(๒)	รองผู้อำนวยการศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	รองประธานกรรมการ
(๓)	ผู้อำนวยการกองบังคับการศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	กรรมการ
(๔)	ผู้อำนวยการกองสนับสนุนสารสนเทศและการสื่อสาร ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	กรรมการ
(๕)	ผู้อำนวยการกองการศึกษา วิจัย และพัฒนา ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	กรรมการ
(๖)	ผู้อำนวยการกองบริการปฏิบัติการสารสนเทศ ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	กรรมการ
(๗)	ผู้อำนวยการสำนักงานเลขาธิการองคมนตรี	กรรมการ
(๘)	รองผู้อำนวยการกองกลาง (๓) กรมบังคับการสำนักพระราชวัง	กรรมการ
(๙)	รองผู้อำนวยการกองการสื่อสารและอิเล็กทรอนิกส์ในพระองค์ (๑)	กรรมการ
(๑๐)	ผู้ช่วยผู้บัญชาการสำนักงานราชองครักษ์ประจำพระองค์ (๑)	กรรมการ
(๑๑)	ผู้อำนวยการกองเทคโนโลยีสารสนเทศ กรมฝ่ายยุทธการ กองบัญชาการทหารมหาดเล็กราชวัลลภรักษาพระองค์	กรรมการ
(๑๒)	เสนาธิการ สำนักงานฝ่ายอำนวยการกองบัญชาการนายตำรวจราชองครักษ์ประจำพระองค์	กรรมการ
(๑๓)	ผู้อำนวยการกองระบบเครือข่ายสารสนเทศและความปลอดภัยศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	กรรมการและเลขานุการ
(๑๔)	รองผู้อำนวยการกองบังคับการศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์	ผู้ช่วยเลขานุการ

(๑๕) รองผู้อำนวยการกองระบบเครือข่ายสารสนเทศและความปลอดภัย ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ — ผู้ช่วยเลขานุการ

(๑๖) หัวหน้าแผนกปฏิบัติการและสนับสนุนความปลอดภัย กองระบบเครือข่ายสารสนเทศ และความปลอดภัย ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ — ผู้ช่วยเลขานุการ

ข้อ ๙ ให้คณะกรรมการดำเนินการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล มีอำนาจ และหน้าที่ ดังต่อไปนี้

(๑) กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ตามข้อกำหนดการบังคับใช้ของกฎหมาย และสอดคล้องกับนโยบายด้านเทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ตลอดจนพิจารณาเสนอ ทบทวน แก้ไข นโยบายด้านเทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ และระเบียบหน่วยราชการในพระองค์ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ตามความเหมาะสม

(๒) กำหนดแนวทางส่งเสริม และสนับสนุน การพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ตลอดจนพิจารณาเสนอทบทวนมาตรการการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีดิจิทัล ตามความเหมาะสม

(๓) จัดทำแผนปฏิบัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยราชการในพระองค์ สำหรับเป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และในสถานการณ์ที่อาจจะเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบายด้านเทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ และแผนแม่บทเทคโนโลยีดิจิทัลหน่วยราชการในพระองค์

(๔) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใด ๆ เพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ให้กับหน่วยงานของหน่วยราชการในพระองค์ และหน่วยงานอื่นที่เกี่ยวข้อง

(๕) ส่งเสริมความรู้ และความเข้าใจให้กับข้าราชบริพารในพระองค์เกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล

(๖) กำกับดูแล ประสานงาน ติดตาม ตรวจสอบ สอบสวน และเร่งรัดการดำเนินการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ในทุกหน่วยงานของหน่วยราชการในพระองค์ รวมถึงหน่วยงานภายนอกที่เข้ามาปฏิบัติหน้าที่ในหน่วยราชการในพระองค์

(๗) รายงานผลการดำเนินการและปัญหาอุปสรรคในการดำเนินการ ในเรื่องของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ต่อคณะกรรมการอำนวยการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล อย่างน้อยปีละ ๑ ครั้ง

(๘) แต่งตั้งคณะทำงาน เพื่อดำเนินงานต่าง ๆ ให้บรรลุวัตถุประสงค์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล

หมวด ๓
บททั่วไป

ข้อ ๑๐ ให้ ทุกหน่วยงานของหน่วยราชการในพระองค์ รวมถึงหน่วยงานภายนอก และบุคคลภายนอก ที่เข้ามาปฏิบัติงานภายในหน่วยราชการในพระองค์ ยึดถือและปฏิบัติตามระเบียบฉบับนี้

ข้อ ๑๑ ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ มีหน้าที่เสนอแนะในการปรับปรุงแก้ไขระเบียบนี้ โดยเสนอต่อคณะกรรมการดำเนินการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล

ทั้งนี้ หน่วยงานของหน่วยราชการในพระองค์สามารถเสนอแนะ การปรับปรุงแก้ไข ระเบียบนี้ผ่านศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ได้

ข้อ ๑๒ หากมีเหตุอันเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้รายงานต่อศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ โดยทันที

ข้อ ๑๓ หากมีการตรวจสอบพบว่าผู้ใดล่วงละเมิด และส่งผลกระทบอันก่อให้เกิดความเสียหาย ให้คณะกรรมการดำเนินการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ทำการสอบสวนเพื่อเสนอโทษทางวินัย และดำเนินกระบวนการทางกฎหมาย

ข้อ ๑๔ ระเบียบฉบับนี้ ประกอบด้วย แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ดังนี้

(๑) การระบุความเสี่ยง (Identify)

(๒) การป้องกัน (Protect)

(๓) การตรวจสอบ (Detect)

(๔) การปฏิบัติเมื่อเผชิญเหตุ (Respond)

(๕) การฟื้นฟู (Recover)

หมวด ๔
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล

ข้อ ๑๕ **การระบุความเสี่ยง (Identify)** การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลอื่นที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ซึ่งรวมถึงข้อมูลทรัพย์สินดิจิทัลและบุคคล

๑๕.๑ การจัดการทรัพย์สินดิจิทัล

๑๕.๑.๑ ให้หน่วยงานแต่งตั้งหรือมอบหมายเจ้าหน้าที่เพื่อดำเนินการเกี่ยวกับการจัดการทรัพย์สินดิจิทัล

๑๕.๑.๒ ให้หน่วยงานจัดทำทะเบียนทรัพย์สินดิจิทัล และดูแลรักษาทะเบียนทรัพย์สินดิจิทัลให้เป็นปัจจุบัน ตามวิธีปฏิบัติในการสำรวจและบันทึกข้อมูลที่กองระบบเครือข่ายสารสนเทศและความปลอดภัย ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนด โดยมีข้อมูลอย่างน้อย ดังนี้

(๑) ข้อมูลทั่วไป

(๒) ข้อมูลเฉพาะ

(๓) ข้อมูลการบำรุงรักษา

(๔) ข้อมูลผู้ใช้

๑๕.๑.๓ ให้หน่วยงานตรวจสอบทะเบียนทรัพย์สินดิจิทัล และรายงานวงรอบประจำปี (มกราคม - ธันวาคม) ไปยังศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ภายในเดือนมกราคมของปีถัดไป โดยมีแบบฟอร์มรายงานการปรับปรุงทะเบียนทรัพย์สินดิจิทัลและวิธีปฏิบัติตามที่กองระบบเครือข่ายสารสนเทศ และความปลอดภัย ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนด

๑๕.๑.๔ ในกรณีที่มีการเปลี่ยนแปลงใด ๆ อันเกี่ยวกับทรัพย์สินดิจิทัล ให้หน่วยงานปรับปรุงทะเบียนทรัพย์สินดังกล่าว และรายงานมายังศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ภายในกำหนด ๓๐ วัน นับแต่วันที่มีการเปลี่ยนแปลง

๑๕.๑.๕ ให้หน่วยงานประเมินความเสี่ยงของทรัพย์สินดิจิทัลในความรับผิดชอบตามแนวทางที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์กำหนด อย่างน้อยปีละ ๑ ครั้ง

๑๕.๑.๖ ในกรณีบุคลากรพ้นจากการปฏิบัติหน้าที่ สิ้นสุดการจ้างงาน หรือสิ้นสุดโครงการ ต้องคืนทรัพย์สินดิจิทัลของหน่วยงานที่รับผิดชอบ ส่งคืนแก่เจ้าหน้าที่ตามข้อ ๑๕.๑.๑

๑๕.๒ การประเมินช่องโหว่และการทดสอบระบบความปลอดภัย

๑๕.๒.๑ กำหนดให้หน่วยงานต้องเข้ารับการประเมินช่องโหว่และทดสอบระบบความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง ตามห้วงเวลาและวิธีการปฏิบัติที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนด

๑๕.๒.๒ ในการประเมินช่องโหว่แต่ละครั้ง ให้หน่วยงานพิจารณาระบุขอบเขตหรือข้อยกเว้น ของการประเมินแต่ละรายการ เช่น ข้อมูลที่มีชั้นความลับ เป็นต้น หากมีรายการใดไม่สามารถนำมาประเมินช่องโหว่ได้ ให้ระบุเป็นหมายเหตุไว้ข้างท้าย

๑๕.๒.๓ ระบบสารสนเทศที่เชื่อมต่อกับระบบอินเทอร์เน็ต หรือระบบที่ต้องใช้การประเมินทางเทคนิค ให้หน่วยงานพิจารณาดำเนินการทดสอบความปลอดภัยของระบบเพิ่มเติมร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์

๑๕.๒.๔ ให้หน่วยงานนำผลการประเมินช่องโหว่ไปประกอบการจัดทำทะเบียนความเสี่ยง ตามแนวทางที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนด

๑๕.๓ การประเมินความเสี่ยงและกลยุทธ์ในการบริหารความเสี่ยง

๑๕.๓.๑ ให้หน่วยงานนำทะเบียนความเสี่ยงที่จัดทำขึ้นจากข้อมูลที่ได้รับตามข้อที่ ๑๕.๒ เพื่อนำมาจัดทำแผนการบริหารจัดการความเสี่ยง และดำเนินการร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์

๑๕.๓.๒ ให้หน่วยงานประเมินช่องโหว่และทดสอบความปลอดภัย รวมถึงทบทวนทะเบียนความเสี่ยงทุกครั้ง เมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานทางสารสนเทศ ของหน่วยงานร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ โดยจัดทำเป็นลายลักษณ์อักษร

๑๕.๔ การระบุผู้ให้บริการภายนอกที่เกี่ยวข้องกับหน่วยงาน

๑๕.๔.๑ ให้หน่วยงานพิจารณา ทบทวน และกำกับดูแล ผู้ให้บริการภายนอกเพื่อดำเนินการใด ๆ ให้สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์

๑๕.๔.๒ ให้หน่วยงานจัดทำบัญชีรายชื่อข้อมูลผู้ติดต่อของผู้ให้บริการภายนอกและแจ้งให้ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ทราบ

๑๕.๔.๓ ในการทำสัญญากับผู้ให้บริการภายนอก หน่วยงานต้องระบุเงื่อนไขและมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ให้รัดกุม เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้น

ข้อ ๑๖ **การป้องกัน (Protect)** มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น ให้หน่วยงานปฏิบัติตามแนวทางที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนด เพื่อทำให้ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ มีความมั่นคงปลอดภัย ดังนี้

๑๖.๑ มาตรการควบคุมการเข้าถึงทางกายภาพ

๑๖.๑.๑ ต้องแบ่งพื้นที่อย่างชัดเจน และกำหนดระดับหรือสิทธิในการเข้าถึงโดยมีการติดป้ายแสดงให้เห็นขอบเขตของพื้นที่ให้ชัดเจน เพื่อป้องกันทรัพย์สินดิจิทัลที่มีความสำคัญซึ่งหากถูกละเมิดจะก่อให้เกิดความเสียหายอย่างร้ายแรงต่อหน่วยงาน

๑๖.๑.๒ ต้องจัดทำแผนผังแสดงตำแหน่งของทรัพย์สินดิจิทัลให้เป็นสัดส่วน และประกาศให้ผู้เกี่ยวข้องทราบ โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็น พื้นที่ทำงาน พื้นที่ติดตั้ง พื้นที่จัดเก็บอุปกรณ์ของระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

๑๖.๑.๓ ต้องบันทึกการผ่านเข้า – ออกในพื้นที่ควบคุมที่สำคัญ ตามข้อ ๑๖.๑.๑

๑๖.๑.๔ ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ภายในหน่วยงาน ห้องทำงาน และเครื่องมือต่าง ๆ ตามที่หน่วยงานพิจารณา

๑๖.๒ มาตรการกำกับดูแลบุคลากร

๑๖.๒.๑ ให้หน่วยงานควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศของหน่วยงานตามสิทธิและหน้าที่ โดยบังคับใช้รหัสผ่านที่มีความปลอดภัย และบุคลากรต้องมีความตระหนักในการเก็บรักษาความลับของรหัสผ่าน

๑๖.๒.๒ ให้หน่วยงานและบุคลากรปฏิบัติตามแนวทางการใช้งานรหัสผ่าน ดังนี้

(๑) รหัสผ่านต้องคาดเดาได้ยาก โดยมีความยาวไม่น้อยกว่า ๑๒ ตัวอักษร ประกอบด้วยตัวเลข ตัวอักษรพิมพ์เล็กหรือพิมพ์ใหญ่ และสัญลักษณ์พิเศษต่าง ๆ ทั้งนี้ควรจะมีการเปลี่ยนรหัสผ่านทุก ๆ ๙๐ วัน

(๒) ให้หน่วยงานร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ พิจารณาการใช้การยืนยันตัวบุคคล ๒ ขั้นตอน (Two-factor authentication) ในการยืนยันตัวตน

๑๖.๒.๓ ในกรณีบุคลากรพ้นจากการปฏิบัติหน้าที่ ให้หน่วยงานดำเนินการตรวจสอบและพิจารณายกเลิกบัญชีผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศโดยเร็วที่สุด

๑๖.๒.๔ บุคลากรต้องมีความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ศึกษาแนวทางการปฏิบัติที่เกี่ยวข้อง และควรมีการจัดอบรมให้ความรู้กับบุคลากรอย่างสม่ำเสมอ ทั้งนี้ให้ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ พิจารณาการจัดอบรมตามความเหมาะสม

๑๖.๒.๕ ให้หน่วยงานกำหนดให้มีเจ้าหน้าที่ และปฏิบัติตามมาตรการการป้องกันรักษาข้อมูลของบุคลากร การควบคุมการเข้าถึงข้อมูลส่วนบุคคล โดยให้สิทธิการเข้าถึงเฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น

๑๖.๓ มาตรการควบคุมการใช้งานอุปกรณ์ด้านเทคโนโลยีดิจิทัล

๑๖.๓.๑ ให้หน่วยงานมีการควบคุมการเข้าถึงของอุปกรณ์ ให้สอดคล้องกับสิทธิและหน้าที่ของบุคลากร

๑๖.๓.๒ ให้หน่วยงานร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ จัดหาและติดตั้งโปรแกรมรักษาความปลอดภัยของอุปกรณ์ และตรวจสอบประสิทธิภาพให้มีความทันสมัยอยู่เสมอ

๑๖.๓.๓ ให้หน่วยงานจัดทำทะเบียนในกรณีที่บุคลากรนำอุปกรณ์ด้านเทคโนโลยีดิจิทัลส่วนตัวมาใช้ในการปฏิบัติงาน และให้บุคลากรดังกล่าว ปฏิบัติตามแนวทางการรักษาความปลอดภัยที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนดโดยเคร่งครัด

๑๖.๔ มาตรการควบคุมการใช้งาน Software และระบบสารสนเทศ

๑๖.๔.๑ หน่วยงานต้องมีการบริหารจัดการฐานข้อมูล รวมถึงการสำรองข้อมูลเพื่อให้หน่วยงานสามารถดำเนินการตามแผนการกู้คืนข้อมูลและนำมาใช้ในการปฏิบัติงานได้ตามปกติ

๑๖.๔.๒ บุคลากรที่ได้รับสิทธิและหน้าที่เท่านั้น จึงจะสามารถเข้าถึงระบบสารสนเทศได้ โดยจะต้องมีกระบวนการตรวจสอบและยืนยันตัวบุคคล (Authentication) ที่ปลอดภัยน่าเชื่อถือ และเหมาะสมก่อนการเข้าใช้งาน เช่น การใช้ชื่อผู้ใช้ และรหัสผ่าน หรือมาตรการเพิ่มเติมอื่น ๆ ตามความเหมาะสม

๑๖.๔.๓ หน่วยงานจะต้องกำหนดให้มีผู้รับผิดชอบ และผู้ดูแลระบบสารสนเทศเพื่อตรวจสอบการใช้งานให้เป็นไปตามมาตรการการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและควบคุมการเข้าถึงตามสิทธิและหน้าที่ของบุคลากร (Authorization)

๑๖.๔.๔ ในกรณีที่บุคลากรเข้าใช้งานระบบสารสนเทศ จะต้องมีการจำกัดเวลาในการเชื่อมต่อ เมื่อไม่มีการใช้งานระยะเวลาหนึ่ง จะต้องถูกบังคับให้ออกจากระบบ

๑๖.๔.๕ ผู้ใช้งานในระบบสารสนเทศของหน่วยงาน ที่เข้าใช้งานจากเครือข่ายภายนอก จะต้องมีกระบวนการตรวจสอบและยืนยันตัวบุคคล (Authentication) ในกรณีที่ผู้ใช้งานมีความประสงค์จะใช้ VPN หรือวิธีการ Remote Access ให้ปฏิบัติตามแนวทางที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนด

๑๖.๔.๖ ในกรณีบุคลากรพ้นจากการปฏิบัติหน้าที่ ให้ผู้ดูแลระบบดำเนินการถอดถอนสิทธิการเข้าถึงระบบสารสนเทศของบุคลากรนั้น และรายงานให้ผู้รับผิดชอบทราบ

๑๖.๔.๗ ให้หน่วยงานร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ตรวจสอบระบบสารสนเทศ รวมถึงปรับปรุง Software ให้ทันสมัยและเหมาะสมอยู่เสมอ

๑๖.๔.๘ ให้หน่วยงานจัดหมวดหมู่ของข้อมูลสารสนเทศ กำหนดระดับการเข้าถึงในหน่วยงานให้กับบุคลากรทุกระดับ และตรวจสอบการใช้ข้อมูลสารสนเทศให้มีความถูกต้องอยู่เสมอ

๑๖.๔.๙ ในกรณีที่หน่วยงานมีความประสงค์ปรับปรุงระบบสารสนเทศใด ๆ ให้ประสานศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ เพื่อดำเนินการในส่วนที่เกี่ยวข้องต่อไป

๑๖.๔.๑๐ หน่วยงานต้องใช้งาน Software ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและผ่านการพิจารณาความเห็นชอบจากศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์

๑๖.๕ มาตรการควบคุมการใช้งานระบบเครือข่าย

๑๖.๕.๑ ให้หน่วยงานควบคุมการเข้าถึงระบบเครือข่าย โดยกำหนดสิทธิและหน้าที่ของบุคลากร ให้เป็นไปตามภารกิจและมาตรการการรักษาความมั่นคงปลอดภัย

๑๖.๕.๒ ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์จะต้องให้การสนับสนุนหน่วยงาน ในการแบ่งแยกเครือข่ายตามกลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยพิจารณาการแบ่งโซนผู้ใช้งานภายนอก โซนผู้ใช้งานภายใน และโซนเครื่องคอมพิวเตอร์แม่ข่าย

๑๖.๕.๓ หน่วยงานต้องกำหนดให้ IP Address คือข้อมูลที่เป็นชั้นความลับและสร้างความตระหนักรู้ให้กับบุคลากร

๑๖.๕.๔ ให้หน่วยงานร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนดแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับระบบเครือข่ายภายในและเครือข่ายภายนอก รวมถึงอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑๖.๕.๕ ให้หน่วยงานกำกับดูแลการใช้งานของบุคลากร ในการเข้าถึงเว็บไซต์ที่ไม่ควรใช้บริการ เช่น เว็บไซต์ที่เกี่ยวกับการพนัน หรือเว็บไซต์อนาจาร เป็นต้น

๑๖.๕.๖ ให้หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่าย เก็บ Log File ไว้ไม่น้อยกว่า ๙๐ วัน ทั้งนี้จะต้องเก็บ System log/ Application log/ Security log/ Audit log และ Web server log เป็นอย่างน้อย

๑๖.๕.๗ ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ เก็บ Log File ไม่น้อยกว่า ๙๐ วัน ทั้งนี้จะต้องเก็บ System log/ Application log/ Security log/ Audit log/ Web server log และ Network log เป็นอย่างน้อย

ข้อ ๑๗ **การตรวจสอบ (Detect)** มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ให้ปฏิบัติตามแนวทางที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์กำหนด ดังนี้

๑๗.๑ ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ มีหน้าที่เฝ้าตรวจภัยคุกคามทางไซเบอร์ จัดประเภท วิเคราะห์เหตุการณ์ และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับหน่วยงานหรือไม่ ทั้งนี้ หากพบว่ามีภัยคุกคามทางไซเบอร์ ให้ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ แจ้งเตือนและกำหนดการปฏิบัติร่วมกับส่วนที่เกี่ยวข้องต่อไป

๑๗.๒ ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ทบทวนกระบวนการการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์อยู่เสมอ และพิจารณาปรับปรุงแก้ไขตามความเหมาะสมให้สอดคล้องกับสถานการณ์

๑๗.๓ ให้หน่วยงานแต่งตั้งเจ้าหน้าที่ เพื่อปฏิบัติงานร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ในกรณีที่ตรวจพบภัยคุกคามทางไซเบอร์

ข้อ ๑๘ **การปฏิบัติเมื่อเผชิญเหตุ (Respond)** มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ ให้ปฏิบัติตามแนวทางที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนด ดังนี้

๑๘.๑ การจัดทำแผนเผชิญเหตุเมื่อมีภัยคุกคามทางไซเบอร์

๑๘.๑.๑ ให้หน่วยงานจัดทำแผนเผชิญเหตุภัยคุกคามทางไซเบอร์ร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์

๑๘.๑.๒ ให้กำหนดวงรอบการทบทวนแผนเผชิญเหตุภัยคุกคามทางไซเบอร์โดยพิจารณาจากสถานการณ์ปัจจุบัน

๑๘.๒ การกำหนดหน้าที่และความรับผิดชอบ

๑๘.๒.๑ ให้หน่วยงานแต่งตั้งเจ้าหน้าที่ และแบ่งมอบหน้าที่ให้สอดคล้องกับแผนเผชิญเหตุภัยคุกคามทางไซเบอร์ที่จัดทำขึ้น

๑๘.๒.๒ ให้หน่วยงานจัดให้มีความพร้อมที่จะปฏิบัติตามแผนเผชิญเหตุภัยคุกคามทางไซเบอร์ เพื่อแก้ไขและติดตามสถานการณ์อย่างต่อเนื่อง

๑๘.๓ การกำหนดวิธีการปฏิบัติ (Incident Response Cycle) ดังนี้

๑๘.๓.๑ การเตรียมการ

(๑) ระบุทรัพย์สินดิจิทัลและระบบสารสนเทศที่มีความสำคัญ ซึ่งหากถูกละเมิดจะก่อให้เกิดความเสียหายอย่างร้ายแรงต่อหน่วยงาน

(๒) ดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาจากภัยคุกคามและการประเมินช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศ

(๓) เตรียมเครื่องมือที่จะใช้ในการปฏิบัติ เช่น ระบบสำรองข้อมูล เป็นต้น

๑๘.๓.๒ การตรวจจับและวิเคราะห์

(๑) ระบุจำแนกเหตุการณ์ ประเภทภัยคุกคาม และประเมินความรุนแรงของเหตุการณ์ที่เกิดขึ้น

(๒) ควบคุมภัยคุกคาม และดำเนินการเพื่อป้องกันความเสียหายเพิ่มเติม

๑๘.๓.๓ การจำกัด (Containment) การกำจัด (Quarantine) และการกู้คืน (Recovery)

(๑) กำจัดภัยคุกคามที่เกิดขึ้น ลบมัลแวร์ แก้ไขช่องโหว่ และปิดช่องโหว่เพื่อป้องกันการโจมตีต่อเนื่อง และไม่ให้ภัยคุกคามเกิดขึ้นซ้ำ

(๒) กู้คืนระบบและข้อมูลที่ได้รับผลกระทบ

(๓) บันทึกรายละเอียดของเหตุการณ์ และการปฏิบัติต่าง ๆ ในขณะเผชิญเหตุ

(๔) ให้ดำเนินการบันทึกกิจกรรมต่าง ๆ ในเครื่องคอมพิวเตอร์และระบบเครือข่าย (Log File) ไม่น้อยกว่า ๙๐ วัน

๑๘.๓.๔ การปฏิบัติหลังจากเกิดเหตุการณ์

(๑) ให้มีการทบทวนหลังการปฏิบัติ โดยนำเหตุการณ์ต่าง ๆ มาวิเคราะห์ร่วมกับผลการปฏิบัติ เพื่อนำไปสรุปเป็นบทเรียน และนำไปสู่การปรับปรุงแก้ไขแผนเผชิญเหตุฯ ต่อไป

(๒) รายงานเหตุการณ์และผลการปฏิบัติให้ส่วนที่เกี่ยวข้องทราบโดยเร็ว

๑๘.๔ การซักซ้อมการปฏิบัติ

๑๘.๔.๑ ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ จัดการฝึกอบรมให้บุคลากรมีความรู้ ความเข้าใจ มีทักษะ ความสามารถ และมีความพร้อมในการปฏิบัติ เมื่อเผชิญเหตุจากภัยคุกคามทางไซเบอร์

๑๘.๔.๒ ให้หน่วยงานกำหนดวงรอบการซักซ้อมการปฏิบัติร่วมกับ ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ อย่างน้อยปีละ ๑ ครั้ง เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์

ข้อ ๑๙ **การฟื้นฟู (Recover)** มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ให้ปฏิบัติตามแนวทางที่ศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ กำหนด ดังนี้

๑๙.๑ การจัดทำแผน

๑๙.๑.๑ ให้หน่วยงานจัดทำแผนการสำรองข้อมูลและระบบสารสนเทศร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ตามลำดับความสำคัญของระบบสารสนเทศที่มีความจำเป็นต่อภารกิจของหน่วยงาน

๑๙.๑.๒ ให้หน่วยงานจัดทำแผนฟื้นฟูความเสียหาย / แผนการกู้คืนข้อมูลและระบบสารสนเทศ ร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์

๑๙.๒ การกำหนดหน้าที่และความรับผิดชอบ

ให้หน่วยงานแต่งตั้งเจ้าหน้าที่ เพื่อปฏิบัติงานร่วมกับศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ ในการฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ตามข้อ ๑๙.๑

๑๙.๓ การกำหนดวิธีการปฏิบัติ

๑๙.๓.๑ การประเมิน

(๑) ประเมินความเสียหายที่เกิดขึ้นต่อข้อมูลและระบบสารสนเทศ

(๒) ระบุข้อมูลและระบบสารสนเทศที่ต้องกู้คืน เพื่อให้หน่วยงานนำมาใช้ในการปฏิบัติงานได้ตามปกติ

(๓) กำหนดลำดับความสำคัญของการกู้คืนข้อมูลและระบบสารสนเทศ

๑๙.๓.๒ การกู้คืน

(๑) กู้คืนข้อมูลและระบบสารสนเทศจากระบบการสำรองข้อมูล (Backup)

(๒) ตรวจสอบความถูกต้องของข้อมูลที่กู้คืนให้มีความถูกต้องครบถ้วน และสมบูรณ์

(๓) ตรวจสอบระบบสารสนเทศ เพื่อให้มั่นใจว่าระบบกลับมาทำงานได้อย่างถูกต้อง หลังจากการกู้คืน

๑๙.๓.๓ การทบทวนหลังการปฏิบัติ

(๑) สรุปผลการปฏิบัติ พร้อมทั้งระบุบทเรียนจากเหตุการณ์เพื่อนำไปปรับใช้กับแผนการกู้คืนข้อมูลและระบบสารสนเทศในอนาคต

(๒) ประเมินประสิทธิภาพของแผนการกู้คืนข้อมูลและระบบสารสนเทศเพื่อนำไปพิจารณาปรับปรุงแผนการกู้คืนฯ ต่อไป

๑๙.๓.๔ รายงานเหตุการณ์และผลการปฏิบัติให้ส่วนที่เกี่ยวข้องทราบโดยเร็ว

๑๙.๔ การซักซ้อมการปฏิบัติ

ให้หน่วยงานกำหนดวงรอบการซักซ้อมการปฏิบัติตามแผนการกู้คืนข้อมูลและระบบสารสนเทศ เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ และให้หน่วยงานสามารถกลับมาดำเนินงานได้ตามปกติหลังเกิดเหตุการณ์

ข้อ ๒๐ ในกรณีที่หน่วยงานมีข้อสงสัยเกี่ยวกับการปฏิบัติใด ๆ ในข้อ ๑๕ ถึงข้อ ๑๙ ให้ประสานมายังศูนย์เทคโนโลยีดิจิทัล หน่วยราชการในพระองค์ เพื่อดำเนินการต่อไป

ข้อ ๒๑ คำสั่ง หรือระเบียบใดที่ขัดต่อระเบียบนี้ ให้เป็นอำนาจของ ประธานข้าราชบริพารในพระองค์ วินิจฉัยเป็นที่สุด

ประกาศ ณ วันที่ ๒๗ มีนาคม พ.ศ. ๒๕๖๗

พลอากาศเอก

(สถิตย์พงษ์ สุขวิมล)

ประธานข้าราชบริพารในพระองค์