ประกาศสำนักงานปลัดกระทรวงคมนาคม
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงคมนาคม

.....

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ตามมาตรา ๕ และมาตรา ๗ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ โดยให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

สำนักงานปลัดกระทรวงคมนาคม จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงคมนาคม ที่เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖ เพื่อเป็นแนวทางในการบริหารจัดการ และรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของสำนักงานปลัดกระทรวงคมนาคม และสำนักงานรัฐมนตรี ได้อย่างมีประสิทธิภาพ และเพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ของสำนักงานปลัดกระทรวงคมนาคม มีความมั่นคงปลอดภัยและเชื่อถือได้ จึงออกประกาศ ดังนี้

ข้อ ๑ ประกาศนี้ เป็นนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงคมนาคม มีสาระสำคัญในเชิงนโยบาย เพื่อเป็นแนวทางในการกำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยที่สำนักงานปลัดกระทรวงคมนาคมได้จัดทำแนวปฏิบัติที่สอดคล้องกับนโยบาย มีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๒ ประกาศนี้มีผลบังคับใช้ ตั้งแต่วันที่ปลัดกระทรวงคมนาคมได้ลงนามในประกาศ

ข้อ ๓ ให้ยกเลิกประกาศสำนักงานปลัดกระทรวงคมนาคม เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงคมนาคม ประกาศ ณ วันที่ ๑๐ พฤษภาคม ๒๕๖๒

ข้อ ๔ คำนิยาม

ความหมายของคำนิยามที่ใช้ในประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงคมนาคม ประกอบด้วย ดังนี้

(๑) เจ้าหน้าที่ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม ซึ่งมีหน้าที่บริหารจัดการระบบคอมพิวเตอร์และเครือข่ายของสำนักงานปลัดกระทรวงคมนาคม และสำนักงานรัฐมนตรี

(๒) เจ้าหน้าที่ผู้พัฒนาระบบ หมายความว่า เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม ซึ่งมีหน้าที่ในการพัฒนาระบบบริหารและระบบบริการอิเล็กทรอนิกส์ ของสำนักงานปลัดกระทรวงคมนาคม

(๓) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หมายความว่า ผู้อยู่ในตำแหน่ง หรือรักษาการในตำแหน่งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

(๔) หัวหน้ากลุ่มนโยบายและบริหารสารสนเทศ หมายความว่า ผู้อยู่ในตำแหน่ง หรือรักษาการในตำแหน่งหัวหน้ากลุ่มนโยบายและบริหารสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

(๕) หัวหน้ากลุ่มพัฒนาระบบภูมิสารสนเทศ หมายความว่า ผู้อยู่ในตำแหน่ง หรือรักษาการในตำแหน่งหัวหน้ากลุ่มพัฒนาระบบภูมิสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

(๖) หัวหน้ากลุ่มพัฒนาระบบบริหารและระบบบริการอิเล็กทรอนิกส์ หมายความว่า ผู้อยู่ในตำแหน่ง หรือรักษาการในตำแหน่งหัวหน้ากลุ่มพัฒนาระบบบริหารและระบบบริการอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

(๗) หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย หมายความว่า ผู้อยู่ในตำแหน่ง หรือรักษาการในตำแหน่งหัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

(๘) ผู้ใช้งาน หมายความว่า ผู้บริหาร ข้าราชการ พนักงานราชการ เจ้าหน้าที่ ลูกจ้าง ของสำนักงานปลัดกระทรวงคมนาคมและสำนักงานรัฐมนตรี

(๙) บุคคลภายนอก หมายความว่า บุคคลผู้มาติดต่อราชการของสำนักงานปลัดกระทรวงคมนาคมและสำนักงานรัฐมนตรี รวมทั้งประชาชนทั่วไป

(๑๐) ผู้รับจ้างภายนอก (Outsource) หมายความว่า ผู้ให้บริการ พัฒนาระบบหรือการบำรุงรักษาและซ่อมแซมแก้ไข ระบบสารสนเทศ ระบบคอมพิวเตอร์และเครือข่าย ของสำนักงานปลัดกระทรวงคมนาคม

(๑๑) ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายความว่า เทคโนโลยีที่เกี่ยวข้องกับระบบคอมพิวเตอร์ (Hardware และ Software) ระบบเครือข่าย ระบบฐานข้อมูล และระบบการสื่อสารต่าง ๆ ซึ่งอยู่ในความรับผิดชอบ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

(๑๒) ระบบคอมพิวเตอร์และเครือข่าย หมายความว่า ระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งอยู่ในความรับผิดชอบ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

(๑๓) ระบบจดหมายอิเล็กทรอนิกส์ หมายความว่า ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานปลัดกระทรวงคมนาคม

(๑๔) ระบบเครือข่ายภายใน หมายความว่า ระบบเครือข่ายภายในสำนักงานปลัดกระทรวงคมนาคมและสำนักงานรัฐมนตรี

(๑๕) ระบบอินเทอร์เน็ต หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ที่สำนักงานปลัดกระทรวงคมนาคม จัดบริการสำหรับผู้ใช้งาน ในการเข้าใช้ผ่านระบบเครือข่ายในช่องทางใด ๆ เพื่อใช้งานระบบเครือข่ายคอมพิวเตอร์ภายนอกองค์กร

(๑๖) ระบบเครือข่ายสารสนเทศคมนาคม (MOTNET) หมายความว่า ระบบเครือข่ายเชื่อมโยงสำนักงานปลัดกระทรวงคมนาคม กับหน่วยงานในสังกัดทั้งส่วนกลาง และส่วนภูมิภาค เพื่อให้บริการรับส่งข้อมูลสารสนเทศของหน่วยงาน และเชื่อมต่อระบบอินเทอร์เน็ตผ่านสำนักงานปลัดกระทรวงคมนาคม

(๑๗) ระบบเครือข่ายไร้สาย หมายความว่า ระบบเครือข่ายไร้สาย ของสำนักงานปลัดกระทรวงคมนาคมและสำนักงานรัฐมนตรี

(๑๘) อุปกรณ์ระบบเครือข่าย หมายความว่า อุปกรณ์จัดเส้นทางเครือข่าย (Router) อุปกรณ์กระจายสัญญาณเครือข่าย (Switch) และอุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access Point)

(๑๙) อุปกรณ์เชื่อมโยงระบบเครือข่ายไร้สาย หมายความว่า อุปกรณ์เชื่อมต่อระบบอินเทอร์เน็ตผ่านระบบเครือข่ายไร้สาย ได้แก่ เครื่องคอมพิวเตอร์ชนิดพกพา Smart Phone และ Tablets

(๒๐) ข้อมูล หมายความว่า ข้อความ ข่าวสาร คำสั่ง ชุดคำสั่ง ภาพ เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ โดยสภาพของสิ่งนั้นเองหรือโดยผ่านกระบวนการใด ๆ ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์หรือที่อยู่ในรูปสื่อสิ่งพิมพ์

(๒๑) สินทรัพย์ หมายความว่า สิ่งที่มีคุณค่าสำหรับองค์กร ได้แก่ ข้อมูล ระบบข้อมูลและสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงคมนาคม และสำนักงานรัฐมนตรี ได้แก่ ข้อมูลสารสนเทศ เครื่องคอมพิวเตอร์ เครื่องพิมพ์ ระบบคอมพิวเตอร์แม่ข่าย อุปกรณ์ระบบเครือข่ายและซอฟต์แวร์ลิขสิทธิ์

(๒๒) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นใดของผู้ใช้งาน ที่เกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงคมนาคม

(๒๓) การเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน หรือเจ้าหน้าที่ผู้ดูแลระบบเข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

(๒๔) ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Security) หมายความว่า การธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๒๕) เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๒๖) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

หมวด ๑
การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control)

.....

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม ต้องคำนึงถึงการกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ผู้ดูแลระบบ การบริหารจัดการทรัพย์สิน การสร้างความมั่นคง

ปลอดภัยทางกายภาพและสิ่งแวดล้อม ตลอดจนกำหนดคุณสมบัติ สิทธิในการเข้าถึง และการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับเจ้าหน้าที่ผู้ดูแลระบบ และผู้ใช้งาน ดังนี้

ข้อ ๕ การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

เพื่อกำหนดหน้าที่ และความรับผิดชอบของเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม ในด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยสร้างความตระหนัก ให้ความรู้ และฝึกอบรม ตลอดจนจัดให้มีกระบวนการทางวินัยเพื่อลงโทษในกรณีฝ่าฝืนหรือละเมิดระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัย ซึ่งมีรายละเอียด ดังนี้

(๑) ต้องแบ่งแยกเจ้าหน้าที่ ซึ่งปฏิบัติหน้าที่ในส่วนการพัฒนาระบบ (Developer) ออกจากเจ้าหน้าที่ซึ่งทำหน้าที่ดูแลระบบ (System Administrator)

(๒) กำหนดหน้าที่ความรับผิดชอบของงานในแต่ละหน้าที่อย่างชัดเจนเป็นลายลักษณ์อักษร

(๓) ควรจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น

ข้อ ๖ การกำหนดคุณสมบัติ สิทธิในการเข้าถึง และการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อจัดให้มีขั้นตอนปฏิบัติเป็นลายลักษณ์อักษรสำหรับการควบคุมและจำกัดสิทธิการใช้ข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร ตามความจำเป็นในการปฏิบัติงาน รวมทั้ง การป้องกันการลักลอบเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ที่ไม่มีสิทธิ ทั้งจากภายในและภายนอก โดยมีรายละเอียด ดังนี้

(๑) กำหนดประเภท ระดับความสำคัญหรือชั้นความลับ ลำดับชั้นการเข้าถึงของข้อมูล ช่องทางและเวลาในการเข้าถึงข้อมูลดังกล่าว รวมทั้ง ควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) เข้ารหัส (Encryption) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีจัดเก็บข้อมูลเดียวกันไว้หลายแห่ง (Distributed Database) ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องตรงกัน

(๒) มีการควบคุมการกำหนดสิทธิของผู้ใช้งาน (User Privilege) ของระบบสารสนเทศ และ Functions ของระบบ ให้สอดคล้องกับอำนาจหน้าที่และความจำเป็นของผู้ใช้งานอย่างเคร่งครัด

(๓) กำหนดข้อปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน (User Registration) เมื่อมีการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องกับการปฏิบัติงาน และตัดออกจากทะเบียนเมื่อผู้ใช้งานถูกเพิกถอนสิทธิดังกล่าว

(๔) มีการตรวจสอบและทบทวนคุณสมบัติ และอำนาจหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิให้สอดคล้องกับระดับชั้นการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารทันที

ข้อ ๗ การบริหารจัดการสินทรัพย์ (Asset Management)

เพื่อบริหารจัดการสินทรัพย์ และกำหนดระดับของการป้องกันระบบเทคโนโลยีสารสนเทศและการสื่อสาร จากความเสียหายที่อาจเกิดขึ้นอย่างเหมาะสม โดยมีรายละเอียด ดังนี้

(๑) การจัดทำบัญชีสินทรัพย์ (Inventory of Assets) โดยจัดทำและปรับปรุงแก้ไขบัญชีสินทรัพย์ ให้ถูกต้องอยู่เสมอ

(๒) การระบุผู้เป็นเจ้าของสินทรัพย์ (Ownership of Assets) โดยระบุผู้เป็นเจ้าของสินทรัพย์แต่ละชนิด ตามที่กำหนดไว้ในบัญชีสินทรัพย์

(๓) การจัดหมวดหมู่สินทรัพย์สารสนเทศ (Classification Guidelines) โดยจัดให้มีกระบวนการในการจัดหมวดหมู่ของสินทรัพย์ตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์กร ทั้งนี้ เพื่อกำหนดมาตรการในการป้องกันได้อย่างเหมาะสม

(๔) การจัดทำป้ายชื่อ และการจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Labeling and Handling) โดยกำหนดขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการสินทรัพย์ตามที่ได้จัดหมวดหมู่ไว้แล้ว

(๕) การใช้งานสินทรัพย์ที่เหมาะสม (Acceptable Use of Assets) โดยจัดทำกฎ ระเบียบหรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งสินทรัพย์ที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อสินทรัพย์เหล่านั้นอันเกิดจากการขาดความระมัดระวังและการดูแลเอาใจใส่

ข้อ ๘ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

เพื่อป้องกันมิให้บุคคล ซึ่งไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (Access Risk) แก้ไข เปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหาย (Availability Risk) ต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้ง ป้องกันความเสียหายจากสภาพแวดล้อมและภัยพิบัติต่าง ๆ ทั้งนี้ เพื่อให้การใช้งานระบบเทคโนโลยีและการสื่อสารเป็นไปอย่างถูกต้องและมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

(๑) การรักษาความมั่นคงปลอดภัยพื้นที่ (Secure Areas) เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อสินทรัพย์ กำหนดให้ปฏิบัติ ดังนี้

(๑.๑) การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter) ต้องมีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำทางเข้าออก เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งอุปกรณ์ประมวลผลต่าง ๆ

(๑.๒) การควบคุมการเข้าออก (Physical Entry Controls) กำหนดให้มีการควบคุมการเข้าออก ในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้าออกได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๑.๓) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน ระบบคอมพิวเตอร์ต่าง ๆ อุปกรณ์ระบบเครือข่าย และสินทรัพย์อื่น ๆ (Securing Offices, Rooms, Network Equipments and Facilities) โดยจัดให้มีการดำเนินการรักษาความมั่นคงปลอดภัยทางกายภาพ

(๑.๔) การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting Against External and Environmental Threats) ต้องจัดให้มีระบบเตือนภัย หรือการจัดทำแผนการรองรับสถานการณ์ความไม่แน่นอนต่าง ๆ ได้แก่ ไฟไหม้ ภัยพิบัติทางธรรมชาติ และหายนะอื่น ๆ ที่เกิดจากมนุษย์

(๑.๕) การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in Secure Areas) ต้องจัดให้มีระบบป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

(๑.๖) การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงสินทรัพย์ขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ควรจัดเป็นบริเวณแยกออกมาต่างหาก

(๒) ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security) เพื่อป้องกันความเสียหาย การสูญหาย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของสินทรัพย์ กำหนดให้ปฏิบัติ ดังนี้

(๒.๑) การจัดวางและการป้องกันอุปกรณ์ (Equipment Sitting and Protection) กำหนดการจัดวางและป้องกันอุปกรณ์ เพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อม และอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

(๒.๒) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) กำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่าง ๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง ระบบสายสื่อสารสำรอง เป็นต้น

(๒.๓) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) กำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

(๒.๔) การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment) กำหนดให้มีการตรวจสอบสื่อบันทึกข้อมูล เพื่อตรวจสอบข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับแล้ว ก่อนที่จะทิ้งอุปกรณ์ดังกล่าว ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง

(๒.๕) ไม่กำหนดให้นำสินทรัพย์ออกสู่ภายนอก ยกเว้นเมื่อได้รับอนุญาตแล้วเท่านั้น

ข้อ ๙ การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

เพื่อป้องกันมิให้ผู้ใช้งานที่ไม่ได้รับอนุญาต เข้าใช้บริการระบบเครือข่าย และป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาต รวมทั้ง บริหารจัดการระบบเครือข่ายให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

(๑) ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน ได้แก่ ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก และส่วน Demilitarized Zone (DMZ)

(๒) ต้องมีระบบป้องกันการบุกรุกระหว่างระบบเครือข่ายที่มีการแบ่งแยกสัดส่วน

(๓) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก รวมทั้ง ระบุอุปกรณ์ระบบเครือข่ายต่าง ๆ และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๔) กำหนดให้มีการควบคุมการเข้าถึงระบบเครือข่าย รวมทั้ง ระบบที่ใช้สำหรับตรวจสอบและปรับแต่งช่องทางการเชื่อมต่อ (Port) ทั้งทางกายภาพและเครือข่าย

(๕) ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบอย่างสม่ำเสมอ ดังนี้

(๕.๑) ความพยายามในการบุกรุกผ่านระบบเครือข่าย

(๕.๒) การใช้งานในลักษณะที่ผิดปกติ

(๕.๓) การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยผู้ใช้งานที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๖) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์ระบบเครือข่าย และเครื่องคอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย ทั้งนี้ ต้องตัดการเชื่อมต่ออุปกรณ์ดังกล่าวในกรณีที่ส่งผลคุกคามต่อระบบเครือข่ายและเครื่องคอมพิวเตอร์อื่น ๆ

(๗) การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร จากภายนอกสำนักงานปลัดกระทรวงคมนาคม ในลักษณะ Remote Access เพื่อการปฏิบัติราชการ ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด โดยมีการจำกัดการเข้าถึงเฉพาะระบบเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็น มีการยืนยันตัวตนและสิทธิของผู้ใช้งาน การบันทึกข้อมูลจราจรทางคอมพิวเตอร์ และต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว

(๘) กำหนดบุคคลรับผิดชอบในการกำหนด หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของอุปกรณ์ระบบเครือข่าย และการกำหนดช่องทางการเชื่อมต่อของเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายทุกชนิดในระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้ง บริหารจัดการการเชื่อมต่อและการจัดเส้นทางบนระบบเครือข่ายระหว่างหน่วยงาน ทั้งนี้ ควรมีการทบทวนหลักเกณฑ์การเชื่อมต่อบนระบบไฟร์วอลล์ (Firewall Policy) ของเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายทุกชนิดในระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงการกำหนดช่องทางการเชื่อมต่อของเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายและการจัดเส้นทางบนระบบเครือข่ายระหว่างหน่วยงาน ก็ควรแจ้งเจ้าหน้าที่ที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๙) การใช้งานระบบหรืออุปกรณ์ตรวจสอบระบบเครือข่ายต่าง ๆ (Tools) ต้องได้รับการควบคุม และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑๐) สำหรับอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่จะเชื่อมโยงเข้าถึงระบบเครือข่าย ต้องมีการกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงที่อาจเกิดจากการใช้งานอุปกรณ์ดังกล่าว

(๑๑) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมภายนอก

ข้อ ๑๐ การควบคุมการเข้าถึงโปรแกรมประยุกต์ ระบบปฏิบัติการ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Application, Operating System, and Information and Communication Technology System Access Control)

เพื่อจำกัดการใช้งานโปรแกรมประยุกต์ ระบบปฏิบัติการ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้สอดคล้องกับหน้าที่ของผู้ใช้งาน และป้องกันการลักลอบเข้าถึง โดยไม่ได้รับอนุญาต ซึ่งมีรายละเอียด ดังนี้

(๑) กำหนดขั้นตอนปฏิบัติในการเข้าถึง และใช้งานโปรแกรมประยุกต์ ระบบปฏิบัติการ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับผู้ใช้งานเป็นลายลักษณ์อักษรอย่างชัดเจนรวมทั้งประกาศให้ผู้ใช้งานทราบเพื่อส่งเสริมให้ผู้ใช้งานตระหนักในความสำคัญของความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๒) มีการควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) โดยมีระบบตรวจสอบตัวตนและสิทธิของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบคอมพิวเตอร์ และมีระบบการเข้ารหัส (Encryption) ของระบบฐานข้อมูลรหัสผ่าน เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงรหัสผ่าน

(๓) กำหนดมาตรการหรือข้อปฏิบัติสำหรับบริหารจัดการรหัสผ่าน สำหรับเจ้าหน้าที่ผู้ดูแลระบบและผู้ใช้งาน โดยกำหนดรหัสผ่านให้ยากแก่การคาดเดา การเก็บรักษา และการเปลี่ยนรหัสผ่านอย่างมีคุณภาพ

(๔) จัดทำกระบวนการหรือจัดให้มีระบบบริหารจัดการรหัสผ่าน (Password Management System) ที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือในลักษณะอัตโนมัติ ซึ่งสนับสนุนการกำหนดรหัสผ่านที่มีคุณภาพ

(๕) จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (System Utilities) โปรแกรมประยุกต์ (Application) และระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology System) ให้สอดคล้องกับหน้าที่ของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุนการใช้งาน

(๖) กำหนดมาตรการป้องกันการใช้งานเครื่องคอมพิวเตอร์ ระบบปฏิบัติการ และระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยบุคคลอื่น ในกรณีที่ไม่มีการปฏิบัติงานในระยะเวลาหนึ่ง (Session Time Out)

(๗) จำกัดเวลาในการเชื่อมต่อ (Limitation of Connection Time) สำหรับระบบปฏิบัติการและระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีความสำคัญหรือความเสี่ยงสูง

ข้อ ๑๑ แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ให้ดำเนินการแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร ตามเอกสารแนบท้ายประกาศนี้ ดังนี้

(๑) การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

(๒) การใช้งานระบบคอมพิวเตอร์และเครือข่าย

(๓) ขั้นตอนปฏิบัติของผู้รับจ้างภายนอก (Outsource)

(๔) การบริหารจัดการสินทรัพย์ (Asset Management)

(๕) การบริหารจัดการระบบไฟร์วอลล์

(๖) ความปลอดภัยในการให้บริการระบบอินเทอร์เน็ต

(๗) ความปลอดภัยในการให้บริการระบบเครือข่ายสารสนเทศคมนาคม (MOTNET)

(๘) การให้บริการระบบเครือข่ายไร้สาย

(๙) การให้บริการจดหมายอิเล็กทรอนิกส์

หมวด ๒
การสำรอง ฟื้นฟูข้อมูลสารสนเทศ และแผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Backup, Recovery and ICT Contingency Plan)

.....

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม ต้องจัดทำระบบสำรองและทดสอบการฟื้นฟูข้อมูลสารสนเทศ รวมทั้ง จัดทำแผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้ข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศและการสื่อสารสามารถใช้งานได้อย่างต่อเนื่อง และมีประสิทธิภาพ ดังนี้

ข้อ ๑๒ การสำรองข้อมูลสารสนเทศ (Backup)

เพื่อรักษาความถูกต้องสมบูรณ์ และความพร้อมใช้ของข้อมูลสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศที่เกี่ยวข้อง โดยมีรายละเอียด ดังนี้

(๑) พิจารณาคัดเลือก และจัดทำระบบหรือแผนการดำเนินการสำรองข้อมูลสารสนเทศตามความเหมาะสม

(๒) กำหนดขั้นตอนในการสำรองข้อมูลสารสนเทศ โดยมีรายละเอียด ดังนี้

(๒.๑) กำหนดข้อมูลสารสนเทศที่ต้องดำเนินการสำรอง

(๒.๒) ชนิดของสื่อบันทึกข้อมูลสารสนเทศ (Media)

(๒.๓) จำนวนของสื่อบันทึกข้อมูล (Copy)

(๒.๔) วิธีการสำรองข้อมูลสารสนเทศโดยละเอียด

(๒.๕) กำหนดรอบระยะเวลาในการสำรองข้อมูลสารสนเทศให้เพียงพอต่อความเสี่ยงที่ยอมรับได้

(๓) จัดเก็บสื่อบันทึกข้อมูลสารสนเทศสำรอง และสำเนาขั้นตอนในการสำรองข้อมูลสารสนเทศ ในสถานที่ปลอดภัย

(๔) ควรติดป้ายที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสารสนเทศสำรอง เพื่อการค้นหาอย่างรวดเร็ว และเพื่อป้องกันความผิดพลาด

(๕) กำหนดรายชื่อ หน้าที่ และความรับผิดชอบ ของผู้รับผิดชอบในการสำรองข้อมูลสารสนเทศ รวมทั้ง จัดทำบันทึกผลการสำรองข้อมูลสารสนเทศ

ข้อ ๑๓ การฟื้นฟูข้อมูลสารสนเทศ (Recovery)

เพื่อทดสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูลสารสนเทศ และเตรียมความพร้อมสำหรับการฟื้นฟูข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศที่เกี่ยวข้อง โดยมีรายละเอียด ดังนี้

(๑) กำหนดขั้นตอนในการฟื้นฟูข้อมูลสารสนเทศ ประกอบด้วย

(๑.๑) กำหนดข้อมูลสารสนเทศที่ต้องดำเนินการฟื้นฟู

(๑.๒) วิธีการฟื้นฟูข้อมูลสารสนเทศโดยละเอียด

(๑.๓) กำหนดรอบระยะเวลาในการทดสอบการฟื้นฟูข้อมูลสารสนเทศ

(๒) กำหนดรายชื่อ หน้าที่ และความรับผิดชอบ ของผู้รับผิดชอบในการฟื้นฟูข้อมูลสารสนเทศ รวมทั้ง จัดทำบันทึกผลในการทดสอบการฟื้นฟูข้อมูลสารสนเทศ

ข้อ ๑๔ แผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Contingency Plan)

เพื่อเตรียมความพร้อมสำหรับสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยให้ระบบสามารถใช้งานได้ตามปกติอย่างต่อเนื่อง ซึ่งมีรายละเอียด ดังนี้

(๑) วิเคราะห์และระบุความเสี่ยง และการดำเนินงานที่สำคัญ

(๒) จัดทำแผนเป็นลายลักษณ์อักษร กำหนดขั้นตอนรายละเอียดการดำเนินการเมื่อมีสถานการณ์ความไม่แน่นอนและภัยพิบัติเกิดขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารสามารถกลับมาดำเนินงานได้ตามระยะเวลาที่กำหนด โดยมีรายละเอียด ดังนี้

(๒.๑) ชื่อแผน

(๒.๒) วัตถุประสงค์ และขอบเขตของแผน

(๒.๓) โครงสร้างผู้รับผิดชอบ ผู้มีอำนาจตัดสินใจ การติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอก

(๒.๔) วิธีการปฏิบัติกรณีเกิดปัญหา

(๓) มีการฝึกซ้อมการปฏิบัติตามแผนอย่างน้อยปีละ ๑ ครั้ง โดยการจำลองสถานการณ์

(๔) ทบทวนแผนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยง

ข้อ ๑๕ การปฏิบัติในการสำรอง การฟื้นฟูข้อมูลสารสนเทศ และการดำเนินการเมื่อเกิดปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ให้ดำเนินการตามกระบวนการและแผนการปฏิบัติ ดังนี้

(๑) กระบวนการในการสำรองและกู้คืนข้อมูลสารสนเทศ

(๒) แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร (กรณีไฟไหม้)

(๓) แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร (กรณีโดนเจาะระบบ)

ข้อ ๑๖ การทดสอบสภาพความพร้อมใช้งานของการฟื้นฟูข้อมูลสารสนเทศ และการปฏิบัติตามแผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

กำหนดให้มีความถี่ในการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของสำนักงานปลัดกระทรวงคมนาคม

หมวด ๓
การตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
(Information and Communication Technology Audit and Assessment)

.....

สำนักงานปลัดกระทรวงคมนาคม ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่านโยบายและระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องกับการให้บริการเป็นไปอย่างมีประสิทธิภาพ สามารถให้บริการได้อย่างต่อเนื่อง และมีความมั่นคงปลอดภัย โดยมีรายละเอียด ดังนี้

ข้อ ๑๗ กลุ่มนโยบายและบริหารสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม เป็นผู้รับผิดชอบการตรวจสอบการดำเนินงาน และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Self Assessment) โดยดำเนินการอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๘ กลุ่มตรวจสอบภายใน สำนักงานปลัดกระทรวงคมนาคม เป็นผู้ตรวจสอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม (Internal Audit) โดยดำเนินการอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๙ ในกรณีที่มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญและมีผลกระทบต่อการดำเนินงานในภาพรวมของสำนักงานปลัดกระทรวงคมนาคมและสำนักงานรัฐมนตรี กำหนดให้มีการตรวจสอบภัยคุกคามที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีที่ปรึกษาหรือหน่วยงานภายนอกที่มีความเชี่ยวชาญร่วมดำเนินการด้วย (External Audit)

หมวด ๔
การสร้างความรู้ความเข้าใจในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับผู้ใช้งาน

.....

ข้อ ๒๐ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม ต้องดำเนินการส่งเสริมความรู้ความเข้าใจของผู้ใช้งานในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยหรือผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ซึ่งมีรายละเอียด ดังนี้

(๑) ประกาศนโยบายและระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้ง มีการทบทวนปรับปรุงให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

(๒) กำหนดมาตรการเพื่อส่งเสริมความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

หมวด ๕
การกำหนดผู้รับผิดชอบให้มีการปฏิบัติตามนโยบายและระเบียบปฏิบัติ

.....

ข้อ ๒๑ ปลัดกระทรวงคมนาคม เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงคมนาคม เกิดความเสียหายหรืออันตรายใด ๆ แก่สำนักงานปลัดกระทรวงคมนาคม หรือผู้หนึ่งผู้ใด อันเนื่องจากความบกพร่อง ละเลย หรือฝ่าฝืน การปฏิบัติตามนโยบายและระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงคมนาคม

ประกาศ ณ วันที่ ๓๐ พฤศจิกายน พ.ศ. ๒๕๖๓

(นายชยธรรม์ พรหมศร)
ปลัดกระทรวงคมนาคม