ประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช.

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ บัญญัติให้หน่วยงานของรัฐมีหน้าที่ดำเนินมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๒ ให้ยกเลิกประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๔

ข้อ ๓ บรรดาประกาศ หลักเกณฑ์ คำสั่ง หรือแนวปฏิบัติอื่นใดในส่วนที่ได้กำหนดไว้แล้วในประกาศนี้ หรือซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๔ ในประกาศนี้

“นโยบาย” หมายความว่า หลักการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สำนักงาน กสทช. กำหนดขึ้นและประกาศใช้งาน

“แนวปฏิบัติ” หมายความว่า ข้อปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สำนักงาน กสทช. กำหนดขึ้นและประกาศใช้งาน เพื่อให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. มีดังนี้

(๑) ให้มีการเข้าถึงหรือควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช. ได้แก่ ระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายให้บริการระบบงานอุปกรณ์เครือข่าย และอุปกรณ์คอมพิวเตอร์อื่น ๆ ให้เป็นไปอย่างมั่นคงปลอดภัย

(๒) ให้มีการเตรียมความพร้อมของการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช. อย่างต่อเนื่อง โดยการจัดทำแผนและขั้นตอนการปฏิบัติงานกรณีเกิดเหตุฉุกเฉิน และการจัดให้มีระบบสำรอง ให้สามารถรับมือกับกรณีเกิดเหตุฉุกเฉินและเพื่อให้สามารถกู้คืนระบบกลับมาได้ภายในระยะเวลาที่เหมาะสม

(๓) ให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช. อย่างสม่ำเสมอ

(๔) ให้มีการรักษาไว้ซึ่งความลับ ความถูกต้อง ความสมบูรณ์ และความพร้อมใช้ของสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช.

ข้อ ๖ เพื่อให้การดำเนินงานของสำนักงาน กสทช. สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. และสามารถปฏิบัติตามได้อย่างเป็นรูปธรรม สำนักงาน กสทช. จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. ตามแนวปฏิบัติท้ายประกาศนี้

ข้อ ๗ ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรือเกิดอันตรายใด ๆ แก่สำนักงาน กสทช. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. ให้เลขาธิการ กสทช. ในฐานะผู้บริหารระดับสูงสุด (Chief Executive Office : CEO) ของสำนักงาน กสทช. เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๘ ให้สำนักงาน กสทช. ดำเนินการให้ผู้ที่เกี่ยวข้องและผู้ใช้งานทั้งหมดได้รับทราบประกาศนี้โดยทั่วกันผ่านทางเว็บไซต์ https://intranet.nbtc.go.th ของสำนักงาน กสทช. พร้อมทั้งสร้างความรู้ ความเข้าใจ และจัดฝึกอบรมแก่ผู้ใช้งานเพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยคุกคามต่าง ๆ และผลกระทบที่เกิดจากการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

ข้อ ๙ ให้สำนักเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัตินี้ให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๒๕ กุมภาพันธ์ พ.ศ. ๒๕๖๖

(นายไตรรัตน์ วิริยะศิริกุล)
รองเลขาธิการคณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ รักษาการแทน
เลขาธิการคณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช.
พ.ศ. ๒๕๖๖

บทนำ

เพื่อให้การใช้งานระบบสารสนเทศของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเชื่อถือได้ ตลอดจนดำเนินการให้เป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอกนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงกฎหมายอื่นที่กำหนดให้สำนักงาน กสทช. ต้องปฏิบัติ จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช.

วัตถุประสงค์

เพื่อกำหนดทิศทางและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ ประสิทธิผล สอดคล้องกับมาตรฐานสากล และกฎหมาย ระเบียบ และข้อบังคับที่สำนักงาน กสทช. ต้องปฏิบัติตาม

คำนิยาม

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)” หมายความว่า ผู้บริหารระดับสูงที่เลขาธิการ กสทช. แต่งตั้งให้มีหน้าที่รับผิดชอบการบริหารงานด้านสารสนเทศและระบบสารสนเทศของสำนักงาน กสทช.

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน กสทช.

“ผู้ใช้งาน” หมายความว่า บุคคลที่เข้าใช้งานระบบสารสนเทศของสำนักงาน กสทช. แต่ไม่รวมถึงผู้ให้บริการภายนอกที่เข้าใช้งานข้อมูลสาธารณะที่เผยแพร่ในเว็บไซต์ของสำนักงาน กสทช.

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน กสทช.

“หน่วยงานภายใน” หมายความว่า สำนักหรือหน่วยงานภายในที่เรียกชื่ออย่างอื่นตามโครงสร้างของสำนักงาน กสทช.

“ผู้ดูแลระบบ” หมายความว่า พนักงานที่มีหน้าที่ดูแลระบบสารสนเทศของสำนักงาน กสทช. ซึ่งหมายรวมถึงระบบสารสนเทศที่หน่วยงานภายในได้มีการจัดทำขึ้น หรือบุคคลที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่เป็นผู้ดูแลระบบสารสนเทศ (System Administrator) ของสำนักงาน กสทช.

“เจ้าของระบบ (System Owner)” หมายความว่า พนักงานและลูกจ้างของสำนักงาน กสทช. ที่ได้รับมอบหมายให้จัดทำโครงการ/งานด้านเทคโนโลยีสารสนเทศที่มีระบบสารสนเทศ หรือแอปพลิเคชันตามภารกิจของสำนักงาน กสทช. ซึ่งต้องปฏิบัติตามแนวปฏิบัตินี้

“ผู้ให้บริการภายนอก” หมายความว่า บุคคลหรือนิติบุคคลอื่นซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศหรือเป็นผู้อื่นที่มีการเชื่อมต่อกับระบบสารสนเทศของสำนักงาน กสทช. หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสำนักงาน กสทช. หรือข้อมูลของผู้ใช้บริการที่อยู่ภายใต้การควบคุมของสำนักงาน กสทช. โดยผู้ให้บริการภายนอกมีหน้าที่ต้องปฏิบัติตามสัญญาการให้บริการที่มีการจัดทำข้อตกลงร่วมกันกับสำนักงาน กสทช. รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้อง

“ระบบสารสนเทศ” หมายความว่า เครื่องคอมพิวเตอร์แม่ข่าย เครือข่าย เครื่องคอมพิวเตอร์ อุปกรณ์ และระบบหรืออุปกรณ์สนับสนุนการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย รวมถึงโปรแกรมบริหารจัดการฐานข้อมูล โปรแกรมประยุกต์ ระบบปฏิบัติการ แอปพลิเคชัน และระบบงานต่าง ๆ ที่ใช้เทคโนโลยีสารสนเทศของสำนักงาน กสทช.

“ข้อมูลสารสนเทศ” หมายความว่า ข้อมูลที่ผ่านการประมวลผลด้วยวิธีการที่เหมาะสมและถูกต้อง เพื่อให้ได้ผลลัพธ์ตรงตามความต้องการของผู้ใช้งานอย่างทันเวลาทั้งที่เก็บไว้ในรูปแบบของกระดาษ (Hardcopy) ระบบฐานข้อมูล (Database) และไฟล์ข้อมูลอิเล็กทรอนิกส์ (Electronic file)

“บริการที่สำคัญ” หมายความว่า บริการด้านเทคโนโลยีสารสนเทศที่มีความสำคัญของสำนักงาน กสทช. ซึ่งได้ประเมินและวิเคราะห์ผลกระทบทางธุรกิจแล้ว และสอดคล้องตามเกณฑ์ที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศที่เกี่ยวข้องกำหนด

“เจ้าของข้อมูล” หมายความว่า พนักงานซึ่งได้รับมอบหมายจากหน่วยงานภายในที่ซึ่งเป็นผู้สร้าง เปลี่ยนแปลงหรือแก้ไขข้อมูลที่เกี่ยวกับภารกิจของหน่วยงานภายในนั้น รวมทั้งให้สิทธิในการเข้าถึงข้อมูลนั้นแก่ผู้อื่น

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“เจ้าของข้อมูลส่วนบุคคล” หมายความว่า บุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลนั้น และให้หมายความรวมถึงผู้แทนโดยชอบธรรม ผู้อนุบาล หรือผู้พิทักษ์ ของผู้เยาว์ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลนั้น แล้วแต่กรณี

“สินทรัพย์” หมายความว่า เครื่องคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ อุปกรณ์ประกอบ ข้อมูลสารสนเทศ และอุปกรณ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศทั้งหมดที่สำนักงาน กสทช. จัดหาไว้ใช้งาน

“โปรแกรมมาตรฐาน” หมายความว่า โปรแกรมที่สำนักงาน กสทช. กำหนดให้เป็นโปรแกรมมาตรฐานสำหรับใช้งานได้ตามปกติ

“ศูนย์คอมพิวเตอร์” หมายความว่า พื้นที่ที่ใช้จัดวางเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูลภายนอก ระบบเครือข่ายคอมพิวเตอร์ และอุปกรณ์สื่อสารต่าง ๆ ของสำนักงาน กสทช. ไว้เป็นศูนย์กลางในการประมวลผลข้อมูลสารสนเทศสำหรับใช้ปฏิบัติงานของสำนักงาน กสทช.

“เครื่องคอมพิวเตอร์ส่วนตัว” หมายความว่า เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา สมาร์ทโฟน หรืออุปกรณ์คอมพิวเตอร์ที่สามารถจัดเก็บหรือประมวลผลข้อมูลได้ ซึ่งสำนักงาน กสทช. ไม่ได้เป็นผู้จัดหาอุปกรณ์นั้นไว้ใช้งาน

“อุปกรณ์คอมพิวเตอร์” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบสารสนเทศ

“สื่อบันทึกข้อมูล” หมายความว่า สิ่งที่ใช้จัดเก็บข้อมูล ชุดคำสั่ง และสารสนเทศอื่น ๆ เช่น USB drive, SD Card, Memory stick, เทป, CD/DVD, Removable drive, External Hard disk, Flash memory และหน่วยความจำของอุปกรณ์ Router หรือ Switch เป็นต้น

“การเข้ารหัสลับ (Encryption)” หมายความว่า การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปแบบหนึ่งที่อ่านได้ (plain text) ให้อยู่ในอีกรูปแบบหนึ่งที่เปลี่ยนแปลงไปจากเดิมจนไม่สามารถอ่านได้ (cipher text) เพื่อปกปิดข้อมูลให้เป็นความลับ

“พอร์ต (Ports)” หมายความว่า ช่องสัญญาณบนอุปกรณ์เครือข่าย เช่น บน Switch หรือ Router โดยทั่วไปซึ่งช่องสัญญาณนี้สามารถใช้ในการติดต่อสื่อสารข้อมูลกับเครือข่าย คอมพิวเตอร์ และอุปกรณ์เครือข่ายต่าง ๆ และโดยทั่วไปอุปกรณ์เครือข่ายจะมีช่องสัญญาณดังกล่าวจำนวนหนึ่ง และให้หมายความรวมถึงบริการต่าง ๆ บนเครื่อง Server ให้บริการ ซึ่งโดยทั่วไปบริการเหล่านี้จะได้รับการกำหนดหมายเลขเป็นหมายเลขมาตรฐาน เช่น พอร์ต ๘๐ หมายถึง บริการเว็บไซต์ซึ่งบริการข้อมูลต่าง ๆ บนเว็บไซต์หนึ่ง พอร์ต ๒๕ หมายถึง บริการรับส่ง E-Mail บนอินเทอร์เน็ต พอร์ต ๕๓ หมายถึง บริการค้นหา IP Address ของเครื่องหรืออุปกรณ์คอมพิวเตอร์ต่าง ๆ

“อุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile computing devices)” หมายความว่า อุปกรณ์คอมพิวเตอร์ขนาดเล็กที่สามารถพกพาหรือเคลื่อนย้ายไปกับตัวบุคคลไปยังสถานที่ต่าง ๆ ได้โดยง่ายและมีน้ำหนักเบา เช่น เครื่องคอมพิวเตอร์โน้ตบุ๊ค โทรศัพท์มือถือ สมาร์ทโฟน หรือ แท็บเล็ต เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบสารสนเทศของสำนักงาน กสทช. โดยมุ่งเน้นที่การรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ

“บัญชีผู้ใช้งาน (Username)” หมายความว่า บัญชีรายชื่อของผู้ที่ได้รับสิทธิในการใช้งานระบบสารสนเทศของสำนักงาน กสทช.

“รหัสผ่าน (Password)” หมายความว่า กลุ่มชุดตัวอักษร ตัวเลข หรืออักขระพิเศษโดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตนสำหรับเข้าถึงระบบสารสนเทศ

“เครือข่าย” หมายความว่า โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอกองค์กรสามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสารภายในองค์กร และโครงข่ายบนอินเทอร์เน็ตซึ่งทำให้คอมพิวเตอร์ภายในองค์กรหนึ่งสามารถติดต่อสื่อสารกับคอมพิวเตอร์ของอีกองค์กรหนึ่งได้

“เทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network: VPN)” หมายความว่า การใช้การเข้ารหัสลับข้อมูล เช่น โดยผ่านทางซอฟต์แวร์หรือฮาร์ดแวร์อย่างใดอย่างหนึ่ง เพื่อให้การเชื่อมต่อโดยผ่านทางเครือข่ายที่ไม่ปลอดภัย เช่น อินเทอร์เน็ต เครือข่ายไร้สาย มีความมั่นคงปลอดภัย ทั้งนี้เนื่องจากข้อมูลจะได้รับการเข้า

รหัสลับก่อนที่จะมีการส่งผ่านไปบนอินเทอร์เน็ตหรือเครือข่ายไร้สายนั้น และเมื่อกล่าวถึง VPN จะหมายรวมถึงระบบ อุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ หรือฮาร์ดแวร์ ที่ใช้การเข้ารหัสลับข้อมูลก่อนส่งข้อมูลออกไป

“ข้อมูลการจราจรทางคอมพิวเตอร์ (Log)” หมายความว่า ข้อมูลเหตุการณ์ต่าง ๆ ที่เกิดขึ้นบนระบบ ๆ หนึ่ง และได้ถูกบันทึกไว้ในระบบนั้น เช่น ความผิดพลาดในการทำงานของระบบ ทรัพยากรระบบไม่พอ ความพยายามในการบุกรุกระบบ ข้อมูลเหตุการณ์ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดให้มีการบันทึกและจัดเก็บไว้ เป็นต้น ซึ่งใช้เพื่อตรวจและติดตามการทำงานของระบบ เตือนว่ามีเหตุการณ์หนึ่งเกิดขึ้นแล้วในระบบ หรือดำเนินการเชิงป้องกันหรือแก้ไขตามความจำเป็น ซึ่งรวมถึงการใช้เป็นหลักฐานในการดำเนินการทางกฎหมาย เช่น กรณีการบุกรุกระบบ หรือกรณีการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมลซึ่งพาดพิงถึงผู้อื่นและทำให้ผู้นั้นเกิดความเสียหาย เป็นต้น

“ทรัพย์สินทางปัญญา” หมายความว่า ผลงานใด ๆ อันเกิดจากความคิดสร้างสรรค์ของมนุษย์ เป็นทรัพย์สินอีกชนิดหนึ่งที่นอกเหนือจากสังหาริมทรัพย์ และอสังหาริมทรัพย์ ทั้งนี้ ประเภทของทรัพย์สินทางปัญญาประกอบด้วยซึ่งได้รับความคุ้มครองตามกฎหมายว่าด้วยลิขสิทธิ์ (Copyright) กฎหมายว่าด้วยสิทธิบัตร (Patent) กฎหมายว่าด้วยเครื่องหมายการค้า (Trademark) กฎหมายว่าด้วยการคุ้มครองแบบผังภูมิของวงจรรวม (Layout – Designs of Integrated Circuit) กฎหมายว่าด้วยความลับทางการค้า (Trade Secrets) และกฎหมายว่าด้วยการคุ้มครองสิ่งบ่งชี้ทางภูมิศาสตร์และกฎหมายทรัพย์สินทางปัญญาอื่น

“มัลแวร์ (Malware)” หมายความว่า โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบคอมพิวเตอร์ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องได้ ประเภทของมัลแวร์ เช่น

Virus (ไวรัส) เป็นมัลแวร์ที่สามารถแพร่กระจายตัวเองไปยังเครื่องอื่น ๆ ผ่านไฟล์ที่ส่งต่อกันระหว่างเครื่อง เมื่อไวรัสแอบเข้ามายังคอมพิวเตอร์ได้แล้ว ไวรัสจะเข้าไปก่อกวนการทำงานจนทำให้เกิดผลเสียต่อเครื่องคอมพิวเตอร์

Worm (เวิร์ม) เป็นมัลแวร์ที่สามารถแพร่กระจายตัวเองไปยังเครื่องอื่น ๆ ผ่านเครือข่ายคอมพิวเตอร์ได้เองโดยอัตโนมัติ คล้ายกับตัวหนอนที่ชอนไชไปยังเส้นทางต่าง ๆ จนทำให้เครือข่ายล่มหรือใช้งานไม่ได้

Trojan (โทรจัน) เป็นมัลแวร์ที่ถูกสร้างขึ้นมาเพื่อหลอกว่าเป็นโปรแกรมทั่วไปที่ดูเหมือนไม่มีพิษภัย แล้วให้ผู้ใช้หลงเชื่อและนำไปติดตั้ง หลังจากนั้นโทรจันก็จะสามารถเข้าไปเล่นงานระบบคอมพิวเตอร์ได้โดยง่าย

Backdoor (แบ็กดอร์) เป็นมัลแวร์ที่มีความสามารถในการเปิดช่องทางให้ผู้ไม่หวังดีสามารถเข้ามาควบคุมเครื่องคอมพิวเตอร์ของเราได้และสามารถทำอะไรก็ได้กับเครื่อง เช่น สั่งลบหรือโอนย้ายข้อมูลได้

“โปรแกรมอรรถประโยชน์” หมายความว่า โปรแกรมประเภทหนึ่งที่ทำงานบนระบบปฏิบัติการ มีคุณสมบัติการใช้งานที่หลากหลาย ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์หรือช่วยสนับสนุนเพิ่มหรือขยายขีดความสามารถของโปรแกรมที่ใช้งานให้มีประสิทธิภาพมากขึ้น

“จดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail)” หมายความว่า ข้อความอิเล็กทรอนิกส์ที่มีการส่งผ่านระบบสารสนเทศและอินเทอร์เน็ตจากผู้ส่งไปยังผู้รับ ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก

ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP POP๓ หรือ IMAP เป็นต้น

“สแปมเมล (Spam Mail)” หมายความว่า จดหมายอิเล็กทรอนิกส์ที่ไม่เป็นประโยชน์หรือไม่เป็นที่ต้องการของผู้รับ

“อีเมลหลอกลวง (Phishing Mail)” หมายความว่า การหลอกลวงโดยใช้อีเมล์หรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น เมื่อผู้เสียหายกดลิงก์ตามเข้ามาที่หน้าเว็บไซต์ปลอมก็จะติดโทรจันโดยอัตโนมัติและหากผู้เสียหายล็อกอินเข้าใช้งานระบบใด ๆ ข้อมูลชื่อผู้ใช้และรหัสผ่าน ของระบบนั้นก็จะถูกส่งไปยังผู้ไม่ประสงค์ดี

“อีเมลลูกโซ่ (Chain E-mail/Letter)” หมายความว่า จดหมายอิเล็กทรอนิกส์ที่มีข้อความในลักษณะที่ต้องการให้ผู้รับส่งต่อข้อความนั้นไปเรื่อย ๆ แบบไม่รู้จบเพื่อให้ข้อความดังกล่าวแพร่กระจายออกไปในวงกว้างโดยที่ข้อความอาจจะเป็นจริงหรือไม่ก็ตาม

“ชุดคำสั่ง (Source Code)” หมายความว่า ไฟล์ซึ่งประกอบด้วยชุดคำสั่งที่สามารถสั่งการให้เครื่องคอมพิวเตอร์ทำงานตามที่ต้องการได้ โดยทั่วไปชุดคำสั่งเหล่านี้จะอยู่ในรูปแบบหรือภาษาที่สามารถอ่านและทำความเข้าใจได้โดยมนุษย์ ไฟล์ชุดคำสั่งนี้จะถูกแปลงโดยโปรแกรมแปลภาษา เช่น Compiler Interpreter หรือ Assembler ไปเป็นโค้ดที่เครื่องคอมพิวเตอร์สามารถตีความและสั่งการให้เครื่องทำงานตามที่ตีความนั้น โดยปกติมนุษย์จะไม่สามารถอ่านและทำความเข้าใจโค้ดประเภทนี้ได้

“ความเสี่ยง” หมายความว่า เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของสำนักงาน กสทช. เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้สำนักงาน กสทช. เสียชื่อเสียง

“ระดับความเสี่ยงที่ยอมรับได้” หมายความว่า ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่งมีค่าน้อยกว่าค่าที่ยอมรับได้จะถือว่าสินทรัพย์สารสนเทศที่เกี่ยวข้องกับเหตุการณ์นั้น มีความมั่นคงปลอดภัยด้านสารสนเทศเพียงพอ

“แผนการลดความเสี่ยง” หมายความว่า แผนการจัดการกับเหตุการณ์ความเสี่ยงซึ่งผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ โดยผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาอนุมัติการดำเนินการ

“Recovery Time Objective (RTO)” หมายความว่า ระยะเวลาในการกู้คืนระบบ

“Recovery Point Objective (RPO)” หมายความว่า ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

“Maximum Tolerance Period of Disruption (MTPD)” หมายความว่า ระยะเวลาสูงสุดที่ยอมให้การดำเนินงานของสำนักงาน กสทช. หยุดชะงัก เพื่อรองรับการดำเนินงานอย่างต่อเนื่องของสำนักงาน กสทช. และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามทางไซเบอร์ เพื่อให้ระบบกลับมาทำงานได้ตามปกติให้เร็วที่สุด

“ไซเบอร์” หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมประสงค์ร้ายโดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่มีความเกี่ยวข้องกับข้อมูลสารสนเทศของสำนักงาน กสทช.

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยอันนำไปสู่การทำลาย การสูญหาย การแก้ไข การเปิดเผย และการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตในขณะที่ข้อมูลส่วนบุคคลนั้นกำลังถูกส่งต่อ ถูกจัดเก็บ หรือถูกประมวลผล

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อรักษาไว้ซึ่งความลับ ความถูกต้อง ความพร้อมใช้ และเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อองค์กร

“คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๒

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของสำนักงาน กสทช. ถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

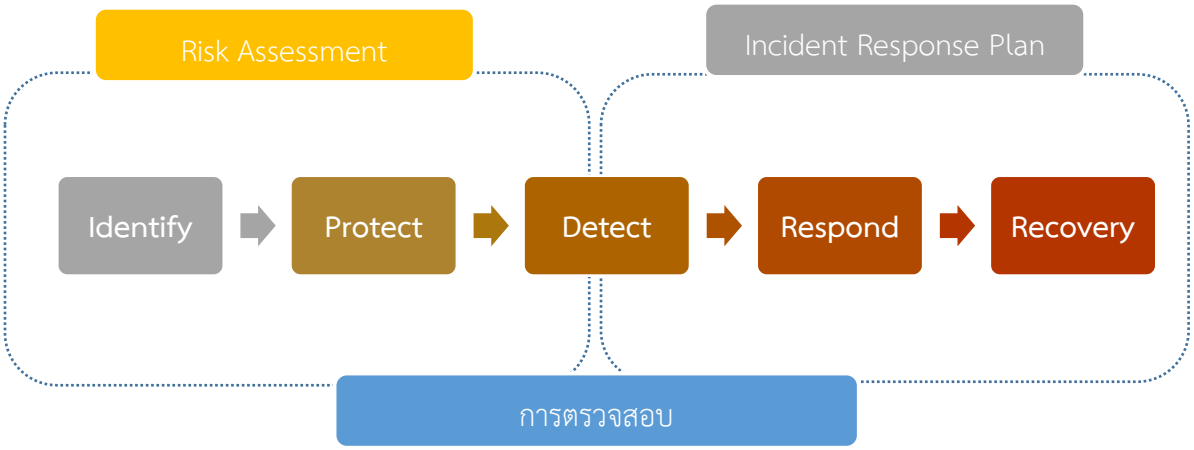
หมวด ๑
แนวปฏิบัติตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑ การปฏิบัติเพื่อให้สอดคล้องตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee: SSMC) ต้องกำหนด จัดทำ และมอบหมายผู้รับผิดชอบในการนำกรอบมาตรฐานตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปประยุกต์ใช้งาน ดังนี้

- การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)
- มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

- มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
- มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
- มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)



ภาพที่ ๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management) ดำเนินการดังนี้

๑.๑.๑ จัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

๑.๑.๒ ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๓ มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy) ดำเนินการดังนี้

๑.๒.๑ ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) และจัดทำทะเบียนประเมินความเสี่ยง

๑.๒.๒ กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยง ที่เกิดขึ้นจากปัจจัยภายนอก อาทิ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๑.๒.๓ ปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๒.๔ กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ การระบุโอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง การระบุผลกระทบของเหตุการณ์ความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้

๑.๒.๕ วิเคราะห์และประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงทรัพย์สินของระบบสารสนเทศที่สำคัญโดยมีการบริหารจัดการความเสี่ยง ดังนี้

(๑) จัดทำแผนการลดความเสี่ยงโดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่า หรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

(๒) นำเสนอแผนการลดความเสี่ยงต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(๓) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนและรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะ ๆ จนกระทั่งเสร็จสิ้น

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ดำเนินการดังนี้

๑.๓.๑ ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ThaiCERT) หรือจากแหล่งอื่นที่น่าเชื่อถือ เป็นต้น

๑.๓.๒ ประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของสำนักงาน กสทช. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญ

๑.๓.๓ การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

(ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

(ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๔ การประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๕ การทดสอบเจาะระบบ (Penetration Testing) สำหรับบริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง (Internet Facing) เพื่อให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๑.๓.๖ ตรวจสอบขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๑.๓.๗ ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง หรือตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๑.๓.๘ การทดสอบเจาะระบบและผู้ให้บริการทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ ต้องมีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ หรือเป็นไปตามที่กฎหมายกำหนด

๑.๓.๙ การทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้การควบคุมดูแลของสำนักงาน กสทช.

๑.๓.๑๐ ติดตาม ปรับปรุง และแก้ไข ตามข้อเสนอแนะจากผลการทดสอบเจาะระบบ และจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤติ และระดับสูง

ทั้งนี้ สำนักงาน กสทช. กำหนดให้สำนักเทคโนโลยีสารสนเทศจัดให้มีการตรวจประเมินช่องโหว่และทดสอบเจาะระบบตามแนวทางที่ได้กำหนดไว้เบื้องต้น และกรณีที่มีการตรวจพบช่องโหว่บนระบบสารสนเทศต้องแจ้งให้ผู้รับผิดชอบระบบสารสนเทศปรับปรุงและแก้ไขช่องโหว่โดยเร่งด่วน โดยเฉพาะอย่างยิ่งช่องโหว่ที่มีความรุนแรงระดับวิกฤตและระดับสูง โดยผู้รับผิดชอบต้องดำเนินการแก้ไขให้แล้วเสร็จโดยไม่ชักช้าหรือไม่เกินกว่า ๗ วัน นับจากวันที่ได้รับแจ้งจากสำนักเทคโนโลยีสารสนเทศ พร้อมทั้งรายงานผลการแก้ไขกลับมายังสำนักเทคโนโลยีสารสนเทศเพื่อทราบและดำเนินการตรวจสอบผลการแก้ไขปรับปรุง หากไม่สามารถดำเนินการแก้ไขช่องโหว่ได้ ผู้รับผิดชอบระบบสารสนเทศต้องชี้แจงความจำเป็นและเหตุผลประกอบที่ไม่อาจปิดช่องโหว่ได้ พร้อมกำหนดมาตรการชดเชยหรือการดำเนินการเพื่อลดความเสี่ยงของช่องโหว่ทางเทคนิคนั้น หรือในกรณีที่มีความจำเป็นอาจต้องปิดการให้บริการระบบสารสนเทศนั้นเป็นการชั่วคราวในระหว่างที่ยังไม่ได้ดำเนินการแก้ไขช่องโหว่ โดยเสนอผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายพิจารณาและให้ความเห็นชอบ

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management) ดำเนินการดังนี้

๑.๔.๑ แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญของสำนักงาน กสทช.

๑.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการทางธุรกิจของสำนักงาน กสทช. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

(ง) สิทธิของสำนักงาน กสทช. ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก (Right to Audit)

๑.๔.๓ สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ตามเงื่อนไขที่ระบุในสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

ข้อ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control) ดำเนินการดังนี้

๒.๑.๑ การเข้าถึงบริการที่สำคัญของสำนักงาน กสทช. ถูกจำกัดไว้ที่

(ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต

(ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๒.๑.๒ ให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของสำนักงาน กสทช. ต้องจัดให้มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

๒.๑.๓ เก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒.๑.๔ ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางสารสนเทศเท่านั้น และทำภายใต้การดูแลของสำนักงาน กสทช.

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ดำเนินการดังนี้

๒.๒.๑ สร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญ

๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

(ข) การแบ่งแยกหน้าที่ (Separation of Duties)

(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(ง) การลบบัญชีที่ไม่ได้ใช้

(จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ (Malware)

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันต่อเหตุการณ์และเหมาะสม

๒.๒.๓ มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ

๒.๒.๔ ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อการรับมือกับภัยคุกคามทางไซเบอร์

๒.๒.๕ จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection) ดำเนินการดังนี้

๒.๓.๑ ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็น

(ข) ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

(ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

(ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

(จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media) ดำเนินการดังนี้

๒.๔.๑ กำหนดมาตรการควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญ โดยปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น กรณีที่ต้องการใช้งานให้แจ้งขึ้นทะเบียนสื่อบันทึกข้อมูล และขออนุมัติการเชื่อมต่อเป็นรายกรณี พร้อมทั้งมีการตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ

๒.๔.๒ เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) บทบาทหน้าที่ความรับผิดชอบ กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การประชาสัมพันธ์และสื่อสารผ่านช่องทางต่าง ๆ ที่สำนักงาน กสทช. กำหนด ให้กับพนักงาน ลูกจ้าง ผู้ให้บริการภายนอก ผู้ใช้งานที่เป็นหน่วยงานภายนอก ที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ และมีการทบทวนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

มีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และวิเคราะห์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของสำนักงาน กสทช. โดยต้องมีการทบทวนกลไกและกระบวนการ อย่างน้อย ปีละ ๑ ครั้ง

ข้อ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ดำเนินการดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การสื่อสาร การฝึกซ้อม การทบทวนและปรับปรุง ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้การรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง

๔.๓ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

มีการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

ข้อ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) ดำเนินการดังนี้

๕.๑.๑ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของสำนักงาน กสทช. สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของสำนักงาน กสทช. เช่น ความสอดคล้องกันของขอบเขต คำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๕.๑.๒ การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และกำหนดบริการสำคัญที่ส่งผลกระทบต่อความต่อเนื่องทางธุรกิจ (Business Impact Analysis: BIA)

๕.๑.๓ บริหารแผนความต่อเนื่องทางธุรกิจ (BIA)

๕.๑.๔ ฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee: SSMC) ดำเนินการ ดังต่อไปนี้

๑) จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง ซึ่งมีขอบเขตของการตรวจสอบ อย่างน้อยดังนี้

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และหลักเกณฑ์อื่นที่คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ประกาศกำหนด

๒) ปฏิบัติหน้าที่อื่นใดตามหลักเกณฑ์ที่ กมช. ประกาศกำหนด

ส่วนที่ ๓ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee: SSMC) ดำเนินการ ดังต่อไปนี้

๑) กำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และจัดทำขั้นตอนปฏิบัติการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง ตามหลักเกณฑ์ที่ กมช. ประกาศกำหนด และเป็นไปตามมาตรฐานสากล

๒.๑) การจัดการความเสี่ยง (Risk Treatment) มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินภารกิจของสำนักงาน กสทช. ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๒.๒) การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๓) การวิเคราะห์และรายงานความเสี่ยง (Risk Analysis and Reporting) มีการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee: SSMC) และต้องทบทวนขั้นตอนปฏิบัติการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงข้อกฎหมายหรือข้อกำหนดที่เกี่ยวข้องอย่างมีนัยสำคัญ

ส่วนที่ ๔ แผนการรับมือภัยคุกคามทางไซเบอร์

คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee: SSMC) ดำเนินการ ดังต่อไปนี้

๑) จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดแนวทางในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒) ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๓) ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของสำนักงาน กสทช. หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่ เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

หมวด ๒
แนวปฏิบัติสำหรับผู้ใช้งาน

ข้อ ๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environment security) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑.๑ ปฏิบัติตามมาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์อย่างเคร่งครัด

๑.๒ ติดบัตรแสดงตัวตนให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ศูนย์คอมพิวเตอร์

๑.๓ ทำการยืนยันตัวตนก่อนเข้าศูนย์คอมพิวเตอร์ทุกครั้ง

๑.๔ ลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ศูนย์คอมพิวเตอร์ในสมุดลงชื่อให้ชัดเจนทุกครั้ง

๑.๕ ไม่นำอาหารและเครื่องดื่มเข้าไปภายในศูนย์คอมพิวเตอร์

๑.๖ ไม่สูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงในบริเวณภายในศูนย์คอมพิวเตอร์

ข้อ ๒ การบริหารจัดการสินทรัพย์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒.๑ ดูแลรักษาสินทรัพย์ที่สำนักงาน กสทช. มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของตนเอง

๒.๒ ห้ามทิ้งสินทรัพย์ของสำนักงาน กสทช. ไว้โดยไม่มีผู้ดูแล ซึ่งรวมถึงการทิ้งไว้ในรถยนต์ที่สามารถมองเห็นได้จากภายนอก

๒.๓ ห้ามนำสินทรัพย์ของสำนักงาน กสทช. ให้ผู้อื่นยืมไปใช้งาน เช่น เพื่อน พี่น้อง หรือญาติ

๒.๔ ใช้งานสินทรัพย์และระบบสารสนเทศต่าง ๆ ในการปฏิบัติงานของสำนักงาน กสทช. เท่านั้น

๒.๕ แจ้งสำนักเทคโนโลยีสารสนเทศก่อนดำเนินการเปลี่ยนจุดติดตั้งหรือส่งซ่อมสินทรัพย์

๒.๖ ส่งคืนสินทรัพย์ให้เจ้าหน้าที่ผู้รับผิดชอบของสำนักเทคโนโลยีสารสนเทศเมื่อผู้ใช้งานต้องการยกเลิกสิทธิการครอบครองสินทรัพย์นั้น ๆ หรือพ้นสภาพการเป็นผู้ปฏิบัติงานของสำนักงาน กสทช.

๒.๗ ต้องดำเนินการป้องกันการเข้าถึงเครื่องคอมพิวเตอร์ส่วนตัวเมื่อนำมาใช้งานภายในเครือข่ายสำนักงาน กสทช. และเชื่อมต่อกับเครือข่ายของสำนักงาน กสทช. ตามนโยบายที่กำหนดเท่านั้น

๒.๘ จัดวางสินทรัพย์ต่าง ๆ ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๙ ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้บริการตลอด ๒๔ ชั่วโมง

๒.๑๐ ให้ผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศอนุมัติ ก่อนทุกครั้งในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกสำนักงาน กสทช.

๒.๑๑ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่สำนักงาน กสทช. ได้ติดตั้งไว้ให้ใช้งาน

๒.๑๒ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้งานการตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง

๒.๑๓ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของสำนักงาน กสทช. เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้นหรือเครือข่ายของสำนักงาน กสทช.ได้

๒.๑๔ ต้องแจ้งผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทันทีที่พบว่าสินทรัพย์เสียหาย สูญหาย หรือปรากฏว่ามีผู้อื่นเข้าถึงสินทรัพย์ดังกล่าว โดยที่ผู้ใช้งานมิได้อนุญาตเพื่อจัดการเหตุการณ์ได้อย่างมีประสิทธิภาพ

ข้อ ๓ การบริหารจัดการบัญชีผู้ใช้งาน (User account) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๓.๑ เปลี่ยนรหัสผ่านทันทีหลังจากได้รับแจ้งจากผู้ดูแลระบบ

๓.๒ กำหนดรหัสผ่าน (Password) ตามหลักเกณฑ์ดังนี้

(ก) รหัสผ่านต้องประกอบด้วยตัวอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และตัวอักขระพิเศษผสมกันไม่น้อยกว่า ๑๐ ตัว อาทิ Yr!StZ๒๐๒๓

(ข) ไม่ตั้งรหัสผ่านด้วยข้อมูลที่เกี่ยวข้องกับตนเอง เช่น ชื่อตนเองหรือครอบครัว ชื่อเล่น วันเดือนปีเกิด หรือทะเบียนรถยนต์

(ค) ไม่ตั้งรหัสผ่านด้วยคำศัพท์ที่มีอยู่ในพจนานุกรม

(ง) เปลี่ยนรหัสผ่านทุก ๙๐ วัน และห้ามใช้รหัสผ่านที่เคยใช้งานซ้ำ ๓ ครั้งล่าสุด

๓.๓ เก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน ของตนเองเป็นความลับ ไม่เผยแพร่ ไม่แจกจ่าย ไม่ใช้ร่วมกับผู้อื่น หรือทำให้ผู้อื่นล่วงรู้

๓.๔ รับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีผู้ใช้งานไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๓.๕ ไม่จดหรือบันทึกบัญชีผู้ใช้งานไว้ในสถานที่ที่ง่ายต่อการคาดเดาหรือสังเกตเห็นของบุคคลอื่น

๓.๖ ควรปิดการใช้งาน (Lock) เครื่องคอมพิวเตอร์ทุกครั้งเมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์

๓.๗ เปลี่ยนรหัสผ่านทันทีเมื่อคาดว่ามีการล่วงรู้รหัสผ่านจากบุคคลอื่น

๓.๘ ไม่ใช้รหัสผ่านซึ่งเคยใช้มาแล้ว (Password history) อย่างน้อยสามรหัสผ่านที่เคยใช้งานล่าสุด

๓.๙ ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยจำรหัสผ่านโดยอัตโนมัติ

๓.๑๐ หากคีย์รหัสผ่านผิดจำนวน ๓ ครั้งขึ้นไป ระบบจะปิดกั้นการเข้าถึงเป็นเวลา ๑๕ นาที ให้แจ้งผู้ดูแลระบบทันทีหากไม่สามารถใช้งานบัญชีผู้ใช้งานได้

๓.๑๑ กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจออัตโนมัติหากไม่มีการใช้งานเครื่องคอมพิวเตอร์ติดต่อกัน ๑๕ นาที โดยให้ป้อนชื่อผู้ใช้งาน และรหัสผ่านอีกครั้งก่อนใช้งาน

๓.๑๒ หากพบเหตุที่สงสัยว่าถูกผู้อื่นนำรหัสผ่านไปใช้ ให้ผู้ใช้งานระบบสารสนเทศดำเนินการเปลี่ยนรหัสผ่าน และแจ้งหน่วยงาน Helpdesk ของผู้รับผิดชอบระบบสารสนเทศในทันที

ข้อ ๔ การบริหารจัดการความปลอดภัยเครือข่ายของสำนักงาน กสทช. ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๔.๑ ต้องใช้บริการสารสนเทศผ่านระบบเครือข่ายตามที่สำนักงาน กสทช. กำหนดไว้เท่านั้น

๔.๒ ลงทะเบียนคำขอใช้งานและต้องได้รับอนุญาตจากผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศก่อนการเข้าถึงเครือข่ายภายในสำนักงาน กสทช. ด้วยเครื่องคอมพิวเตอร์ส่วนตัว

๔.๓ การใช้งานเครือข่ายอินทราเน็ตผ่านเครือข่ายอินเทอร์เน็ตจากภายนอกสำนักงาน กสทช. ผู้ใช้งานต้องเชื่อมต่อด้วยเทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network : VPN) ตามที่สำนักงาน กสทช. กำหนด

๔.๔ ห้ามกระทำการใด ๆ ที่ส่งผลกระทบ ชะลอ ขัดขวาง หรือรบกวน การส่งผ่านข้อมูลในการดำเนินงานของสำนักงาน กสทช. ในระบบเครือข่ายของสำนักงาน กสทช. จนไม่สามารถทำงานตามปกติได้

ข้อ ๕ การใช้งานอุปกรณ์คอมพิวเตอร์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๕.๑ อุปกรณ์คอมพิวเตอร์ที่สำนักงาน กสทช. จัดไว้ให้ใช้งานถือเป็นสินทรัพย์ของสำนักงาน กสทช. และมีวัตถุประสงค์เพื่อใช้ในการดำเนินงานของสำนักงาน กสทช. เท่านั้น

๕.๒ ดูแลรักษาอุปกรณ์คอมพิวเตอร์โดยจัดเก็บไว้ในที่ปลอดภัย ไม่วางทิ้งไว้ในสถานที่เสี่ยงต่อการสูญหาย และหลีกเลี่ยงการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาในสภาพแวดล้อมที่อาจมีผลกระทบต่อความเสียหายของอุปกรณ์

๕.๓ รับผิดชอบในการป้องกันการสูญหายของข้อมูล ในกรณีที่อุปกรณ์คอมพิวเตอร์สูญหายหรือเสียหาย ผู้ใช้งานต้องแจ้งต่อผู้บังคับบัญชาโดยเร็ว

๕.๔ ดูแลรักษาข้อมูลของสำนักงาน กสทช. ที่จัดเก็บในอุปกรณ์คอมพิวเตอร์ให้สอดคล้องตามการบริหารจัดการข้อมูลองค์กร

๕.๕ เมื่อผู้ใช้งานพ้นสภาพการเป็นพนักงานหรือลูกจ้างของสำนักงาน กสทช. ต้องส่งอุปกรณ์คอมพิวเตอร์และอุปกรณ์เสริมทั้งหมดที่สำนักงาน กสทช. จัดไว้ให้ใช้งาน คืนต่อสำนักงาน กสทช.

๕.๖ การยืม การคืน หรือส่งซ่อมอุปกรณ์คอมพิวเตอร์แบบพกพาที่สำนักงาน กสทช. จัดไว้ให้ใช้งานให้เป็นไปตามขั้นตอนปฏิบัติที่สำนักเทคโนโลยีสารสนเทศกำหนด

๕.๗ ห้ามผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบของอุปกรณ์คอมพิวเตอร์ของสำนักงาน กสทช. โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๕.๘ การใช้อุปกรณ์คอมพิวเตอร์ที่สำนักงาน กสทช. จัดไว้ให้ใช้งานในการเข้าถึงระบบสารสนเทศของสำนักงาน กสทช. ผู้ใช้งานต้องทำการเชื่อมต่อ VPN และยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าถึงระบบสารสนเทศของสำนักงาน กสทช.

๕.๙ เพื่อป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต ผู้ใช้งานจะต้องกำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์ ได้แก่ การใช้บัญชีผู้ใช้งานและรหัสผ่าน หรือเทคโนโลยีไบโอเมตริก (Biometric) หรือพินโค้ด (PIN code)

๕.๑๐ ก่อนการใช้งานกับสื่อบันทึกข้อมูลต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์โดยโปรแกรมป้องกันไวรัสคอมพิวเตอร์

๕.๑๑ ไม่นำอาหาร เครื่องดื่ม หรือสิ่งที่เป็นของเหลว มาวางใกล้บริเวณเครื่องคอมพิวเตอร์

๕.๑๒ ไม่วางของทับบนเครื่องคอมพิวเตอร์ หรือแป้นพิมพ์

๕.๑๓ กรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากที่สูง เป็นต้น

ข้อ ๖ การบริหารจัดการซอฟต์แวร์และทรัพย์สินทางปัญญา ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๖.๑ ไม่คัดลอก แก้ไข ถอดถอนโปรแกรมมาตรฐานต่าง ๆ ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของสำนักงาน กสทช. หรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือนำไปให้ผู้อื่นใช้งาน

๖.๒ ไม่ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดทรัพย์สินทางปัญญา หากมีการตรวจสอบพบความผิดฐานละเมิดทรัพย์สินทางปัญญา สำนักงาน กสทช. ถือว่าเป็นความผิดส่วนบุคคล

๖.๓ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของสำนักงาน กสทช. เพิ่มเติมก่อนได้รับอนุญาตจากผู้ดูแลระบบ

๖.๔ ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของทรัพย์สินทางปัญญาต่าง ๆ ที่สำนักงาน กสทช. หรือผู้ใช้งานมีใช้งานหรือครอบครอง

๖.๕ ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟต์แวร์สำเร็จรูปที่สำนักงาน กสทช. จัดหามาใช้งาน เว้นแต่สำนักงาน กสทช. ได้รับอนุญาตให้เปลี่ยนแปลงแก้ไขได้จากเจ้าของลิขสิทธิ์

๖.๖ ไม่นำผลงานของผู้อื่นหรือผลงานใด ๆ ที่มีลิขสิทธิ์มาทำการ “คัดลอก” หรือ “ดัดแปลง” ก่อนได้รับอนุญาตจากเจ้าของลิขสิทธิ์ หากเกิดกรณีการละเมิดทรัพย์สินทางปัญญาสำนักงาน กสทช. ถือว่าเป็นความผิดส่วนบุคคล

ข้อ ๗ การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๗.๑ ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มา หรือมาจากแหล่งที่มาที่ไม่น่าเชื่อถือ

๗.๒ การนำอุปกรณ์จัดเก็บข้อมูลต่าง ๆ เช่น Thumb drive และ Data storage มาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของสำนักงาน กสทช. ให้นำอุปกรณ์มาลงทะเบียนที่สำนักเทคโนโลยีสารสนเทศและขออนุญาตการใช้งานเป็นรายกรณี โดยก่อนการใช้งานขอให้ตรวจสอบหาโปรแกรมประสงค์ร้ายหรือมัลแวร์ก่อนทุกครั้ง

๗.๓ ตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail) หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนเปิดใช้งาน

๗.๔ ตรวจสอบฐานข้อมูลไวรัสของโปรแกรมป้องกันไวรัส กรณีไม่ปรับปรุงให้เป็นปัจจุบัน ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบโดยทันที

๗.๕ ห้ามถอดถอนโปรแกรมป้องกันไวรัสที่สำนักงาน กสทช. ได้ติดตั้งไว้ให้

๗.๖ ระมัดระวังการเข้าเว็บไซต์ที่มีความเสี่ยงเนื่องจากการเปิดไฟล์หรือเข้าเว็บไซต์อาจได้รับไวรัสจากไฟล์หรือเข้าเว็บไซต์เหล่านั้น

ข้อ ๘ การใช้งานอินเทอร์เน็ต ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๘.๑ ปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๘.๒ ไม่ใช้งานอินเทอร์เน็ตของสำนักงาน กสทช. เพื่อหาประโยชน์ในเชิงธุรกิจ ส่วนตัวและการเข้าสู่เว็บไซต์ที่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาที่เป็นการละเมิดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่กระทบต่อความมั่นคง หรือเว็บไซต์ที่เป็นภัยต่อสังคม

๘.๓ ไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับของสำนักงาน กสทช. โดยไม่ได้รับอนุญาต

๘.๔ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงาน กสทช. ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๘.๕ ไม่เสนอความคิดเห็นหรือใช้ข้อความยั่วยุ ให้ร้ายบุคคลอื่น หรือข้อมูลที่ผิดกฎหมายในการใช้งานกระดานสนทนา (Webboard) สาธารณะ

๘.๖ ไม่ใช้งานโปรแกรมแบบเพียร์ทูเพียร์ (Peer to Peer) ผ่านเครือข่ายสำนักงาน กสทช.

๘.๗ ไม่ใช้โปรแกรมประเภทบริการส่งข้อความทันที (Instant Messaging : IM) เช่น Line Skype หรือ Messenger (Facebook) เป็นต้น นอกเหนือจากการปฏิบัติงานผ่านเครือข่ายสำนักงาน กสทช.

๘.๘ ไม่เข้าเว็บไซต์เครือข่ายสังคม (Social network) เช่น Facebook Twitter หรือ Game online เป็นต้น นอกเหนือจากการปฏิบัติงานผ่านเครือข่ายสำนักงาน กสทช.

๘.๙ ไม่ใช้งานสตรีมมิ่งมีเดีย (Streaming media) นอกเหนือจากการปฏิบัติงานผ่านเครือข่ายสำนักงาน กสทช.

๘.๑๐ ไม่ใช้โปรแกรมควบคุมระยะไกล (Remote administrator) ผ่านเครือข่ายสำนักงาน กสทช.

๘.๑๑ ต้องปิดเว็บบราวเซอร์เมื่อสิ้นสุดการใช้งานเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ข้อ ๙ การใช้งานจดหมายอิเล็กทรอนิกส์หรืออีเมล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๙.๑ การปฏิบัติงานที่เกี่ยวข้องกับสำนักงาน กสทช. ให้ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail address) ของสำนักงาน กสทช. (ชื่อบัญชีผู้ใช้งาน@nbtc.go.th) ที่ผู้ดูแลระบบกำหนดให้เท่านั้น

หากมีการตรวจสอบพบความผิดอันเกิดจากการใช้บัญชีจดหมายอิเล็กทรอนิกส์ส่วนตัว สำนักงาน กสทช. ถือว่าเป็นความผิดส่วนบุคคล

๙.๒ ระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์หรืออีเมลเพื่อไม่ให้เกิดความเสียหายต่อสำนักงาน กสทช. ละเมิดทรัพย์สินทางปัญญา ละเมิดศีลธรรม สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือกระทบต่อความมั่นคงปลอดภัยไซเบอร์ รวมทั้งไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ

๙.๓ ห้ามเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมลของผู้อื่นโดยไม่ได้รับอนุญาต

๙.๔ ห้ามปลอมแปลงจดหมายอิเล็กทรอนิกส์หรืออีเมล

๙.๕ ใช้คำพูดที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมล

๙.๖ สำรองข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมลอย่างสม่ำเสมอ

๙.๗ ออกจากระบบ (Log out) ทุกครั้งเมื่อไม่ใช้งานระบบจดหมายอิเล็กทรอนิกส์หรืออีเมล เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๙.๘ ตรวจสอบเอกสารที่แนบมาจากจดหมายอิเล็กทรอนิกส์หรืออีเมลก่อนทำการเปิดโดยใช้โปรแกรมป้องกันไวรัส

๙.๙ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรืออีเมลที่ได้รับจากผู้ส่งที่ไม่รู้จักหรือมีลักษณะสแปมเมล (Spam mail) เช่น การหลอกลวง การขายสินค้า หรือการสมัครสมาชิก เป็นต้น

๙.๑๐ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นอีเมลลูกโซ่ (Chain E-mail/Letter)

๙.๑๑ ตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์หรืออีเมล (Inbox) ของตนเองทุกวันและควรลบจดหมายอิเล็กทรอนิกส์หรืออีเมลที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่ระบบจดหมายอิเล็กทรอนิกส์หรืออีเมล

๙.๑๒ ในกรณีตรวจพบอีเมลหลอกลวง (Phishing Mail) ห้ามเปิดอ่าน ห้ามคลิกลิงก์ และห้ามเปิดไฟล์แนบ โดยเด็ดขาด รวมถึงต้องแจ้งกับสำนักเทคโนโลยีสารสนเทศในทันที

ข้อ ๑๐ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๐.๑ กรณีจำเป็นต้องใช้การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social network) ในนามของสำนักงาน กสทช. ผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ และสังกัดให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดงสังกัดได้

๑๐.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social network) ควรนำเสนอเกี่ยวกับภารกิจของสำนักงาน กสทช. ได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสารที่เป็นประโยชน์ มีความถูกต้อง ใช้ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้บังคับบัญชาก่อนทุกครั้ง

๑๐.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของสำนักงาน กสทช. ผ่านเครือข่ายสังคมออนไลน์ (Social network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑๐.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่างต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่องที่เกี่ยวข้องต่อไป

๑๐.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากสำนักงาน กสทช. และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑๐.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้น และแจ้งต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๐.๗ ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับสำนักงาน กสทช. จากการใช้งานเครือข่ายสังคมออนไลน์

๑๐.๘ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่สำนักงาน กสทช. ได้กำหนดไว้เท่านั้น

ข้อ ๑๑ การบริหารจัดการข้อมูลองค์กร ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

การจัดหมวดหมู่และจัดระดับชั้นความลับของข้อมูล สำนักงาน กสทช. อ้างอิงตามประกาศสำนักงานพัฒนารัฐบาลดิจิทัล ที่ ๓/๒๕๖๔ เรื่องมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ โดยหลักเกณฑ์การพิจารณาการเปิดเผยหรือไม่เปิดเผยข้อมูลให้พิจารณาตามกฎหมายหรือระเบียบที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ รวมถึงระเบียบ ประกาศ หรือหลักเกณฑ์ของสำนักงาน กสทช. เกี่ยวกับเอกสารลับ โดยมีการจำแนกหมวดหมู่ ดังนี้

(๑) ข้อมูลส่วนบุคคล (Privacy data)

(๒) ข้อมูลความมั่นคง (National security data)

(๓) ข้อมูลความลับทางราชการ (Confidential government data) และ

(๔) ข้อมูลสาธารณะ (Public data)

สำหรับการแบ่งระดับชั้นความลับ สามารถแบ่งเป็น ๔ ระดับ ดังนี้

ระดับข้อมูลเปิดเผยได้ (Public) หมายถึง สารสนเทศที่เปิดเผยสู่สาธารณะชนโดยบุคคลที่มีหน้าที่หรือได้รับมอบอำนาจให้ดำเนินการเผยแพร่ได้ โดยสารสนเทศที่เปิดเผยดังกล่าวได้ถูกพิจารณาแล้วว่าเมื่อมอบให้บุคคลอื่นแล้วจะไม่ก่อให้เกิดความเสียหายต่อองค์กร

ระดับข้อมูลส่วนบุคคล (Personal data) หมายถึง ข้อมูลหรือสารสนเทศเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ซึ่งการดำเนินการและบริหารจัดการข้อมูลส่วนบุคคลจะต้องสอดคล้องตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน กสทช.

ระดับใช้ภายในเท่านั้น (Internal use only หรือ Internal use) หมายถึง สารสนเทศทั่วไปที่ใช้สื่อสารกันภายในเท่านั้น

ระดับลับ (Confidential) หมายถึง สารสนเทศที่ถูกพิจารณาแล้วว่ามีความสำคัญ และหากรั่วไหลไปถึงบุคคลผู้ไม่มีหน้าที่จะทำให้เกิดความเสียหายต่อความมั่นคงและผลประโยชน์ของรัฐอย่างร้ายแรง ซึ่งสามารถแบ่งระดับชั้นความลับได้เป็น ลับ ลับมาก และลับที่สุด ซึ่งตัวอย่างหมวดหมู่ข้อมูลที่จะจัดอยู่ในระดับลับขึ้นไป เช่น หมวดหมู่ข้อมูลความลับของทางราชการ และหมวดหมู่ข้อมูลความมั่นคง เป็นต้น

๑๑.๑ ระดับการเข้าถึง คือ

(ก) การเข้าถึงเพื่อการอ่าน (Read)

(ข) การเข้าถึงเพื่อการเขียน (Write)

(ค) การเข้าถึงเพื่อการแก้ไข (Edit)

(ง) การเข้าถึงเพื่อการลบ (Delete)

ซึ่งผู้ใช้งานต้องได้รับการจัดสรรระดับการเข้าถึงให้สอดคล้องกับรายการข้อมูลที่เปิดเผยหรือไม่สามารถเปิดเผยได้ รวมถึงระดับชั้นความลับของข้อมูล หน้าที่และความรับผิดชอบของเจ้าหน้าที่ผู้ปฏิบัติงาน และสอดคล้องตามหลักการเท่าที่จำเป็นในการใช้งานเท่านั้น

๑๑.๒ ระมัดระวังในการนำสื่อบันทึกข้อมูลให้ผู้อื่นใช้งาน

๑๑.๓ ดูแลรักษาความลับของข้อมูลลับ โดยหากข้อมูลอยู่ในรูปแบบอิเล็กทรอนิกส์จะต้องมีการป้องกันการเข้าถึงจากผู้ไม่มีสิทธิ หรือพิจารณาใช้มาตรการการเข้ารหัสลับ (Encryption) โดยจะต้องใช้เทคโนโลยีที่ทางสำนักงาน กสทช. กำหนดให้ หรืออย่างน้อยจะต้องเป็นเทคโนโลยีที่ได้รับการยอมรับและเป็นที่รู้จักดี

๑๑.๔ ไม่นำข้อมูลไปเปิดเผยกับบุคคลซึ่งไม่มีความเกี่ยวข้องกับการปฏิบัติหน้าที่เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชา

๑๑.๕ กำหนดประเภท ลำดับชั้นความลับ รวมถึงระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงสำหรับข้อมูลสารสนเทศแต่ละชนิดอย่างเหมาะสม

๑๑.๖ เวลาที่ได้เข้าถึง สามารถเข้าถึงข้อมูลได้ตลอดเวลา (๒๔ ชั่วโมง ๗ วัน) หรือตามภารกิจและความจำเป็นของผู้ใช้งานที่ได้รับมอบหมาย โดยผ่านระบบยืนยันตัวตน และในกรณีผู้ใช้งานไม่ใช้งานระบบสารสนเทศเกินกว่า ๓๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Login เพื่อระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ ก่อนเข้าใช้ระบบสารสนเทศอีกครั้ง

๑๑.๗ ช่องทางการเข้าถึง ต้องจำกัดช่องทางการใช้งานหรือการเข้าถึงข้อมูลเท่าที่มีความจำเป็นต่อการใช้งานเท่านั้น โดยสำนักงาน กสทช. กำหนดจำนวนช่องทางที่สามารถเข้าถึง ดังนี้

(ก) ช่องทางที่สามารถเข้าถึงระบบสารสนเทศได้โดยผ่านเครือข่ายทางไกลจากภายนอก (VPN)

(ข) ช่องทางที่สามารถเข้าถึงระบบสารสนเทศได้จากระบบเครือข่ายภายในสำนักงาน กสทช.

(ค) ช่องทางการรับ - ส่งข้อมูลสำคัญโดยผ่านระบบเครือข่ายสาธารณะโดยช่องทางและข้อมูลสำคัญดังกล่าวต้องได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL/TLS หรือ XML Encryption

ข้อ ๑๒ การบริหารจัดการการเข้ารหัสลับ (Encryption) ข้อมูล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเข้ารหัสลับ (Encryption) ข้อมูลที่ครอบคลุม ขอบเขตหน้าที่ ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง ช่องทางการสื่อสารที่ใช้รับส่งข้อมูลสำคัญกับภายนอก วิธีการเข้ารหัสลับข้อมูล (Cryptographic algorithm) ที่สอดคล้องตามระดับความสำคัญของข้อมูล และการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management) โดยอย่างน้อยต้องมีกระบวนการที่มีความรัดกุมปลอดภัยที่ครอบคลุมตั้งแต่การสร้างและติดตั้ง การจัดเก็บ การยกเลิกและทำลายกุญแจเข้ารหัสข้อมูล

ข้อ ๑๓ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๓.๑ ห้ามติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่สำนักงาน กสทช. ไม่อนุญาตให้ใช้งาน และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบสำนักงาน กสทช. ถือว่าเป็นความผิดส่วนบุคคล

๑๓.๒ หากต้องการใช้งานโปรแกรมอรรถประโยชน์ที่ไม่อนุญาต เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้ไม่ปลอดภัย ต้องได้รับความเห็นชอบที่เป็นลายลักษณ์อักษรจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หรือผู้ที่ได้รับมอบหมายให้เป็นผู้พิจารณาอนุญาต

๑๓.๓ กำหนดให้มีการถอดถอนการติดตั้งโปรแกรมอรรถประโยชน์รวมทั้งซอฟต์แวร์ที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน กสทช. ที่ไม่จำเป็นออกจากระบบเมื่อไม่จำเป็นต้องใช้งาน

ข้อ ๑๔ หน้าที่และความรับผิดชอบของผู้ใช้งาน (User responsibilities)

๑๔.๑ ศึกษานโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายการคุ้มครองข้อมูลส่วนบุคคล แนวปฏิบัติและขั้นตอนปฏิบัติต่าง ๆ ที่สำนักงาน กสทช. ประกาศกำหนดและปฏิบัติตามอย่างเคร่งครัด ในกรณีที่ฝ่าฝืนนโยบายและแนวปฏิบัตินี้ อาจนำมาซึ่งความรับผิดทางวินัย โทษทางปกครอง หรือความรับผิดทางอาญาได้ ทั้งนี้ หากเกิดการกระทำความผิด ให้มีการตรวจสอบเพื่อดำเนินการทางวินัยตามระเบียบคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติว่าด้วยการบริหารงานบุคคล

๑๔.๒ ป้องกันการเข้าถึงอุปกรณ์ประมวลผลสารสนเทศทุกชนิด เช่น เครื่องคอมพิวเตอร์พีซี โน้ตบุ๊ค ที่ตนได้รับอนุญาตให้ใช้งาน โดยการกำหนดบัญชีผู้ใช้งานและรหัสผ่านหรือวิธีการอื่น ตามความสามารถของอุปกรณ์ เช่น การใช้ PIN Code เป็นต้น

๑๔.๓ ไม่อนุญาตให้ใช้ USB port ในการเชื่อมต่อกับเครื่องคอมพิวเตอร์ของสำนักงาน กสทช. และทำการถ่ายโอนข้อมูล การใช้งาน USB port มีความเสี่ยง ซึ่งสำนักงาน กสทช. มีความจำเป็นต้องควบคุมอย่างเคร่งครัด หากมีความจำเป็นจะต้องใช้จะต้องได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศเท่านั้น

๑๔.๔ ไม่อนุญาตให้นำข้อมูลส่วนบุคคลที่สำนักงาน กสทช. ประมวลผล ไปจัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลส่วนบุคคล

๑๔.๕ ดูแลรับผิดชอบบัญชีผู้ใช้งานและรหัสผ่าน ไม่อนุญาตให้ผู้อื่นนำไปใช้งาน และเก็บข้อมูลรหัสผ่านหรือข้อมูลที่ใช้ในการพิสูจน์ตัวตนไว้เป็นความลับ

๑๔.๖ ไม่เข้าถึงข้อมูล สารสนเทศและระบบที่ตนไม่ได้รับอนุญาต

๑๔.๗ ดูแลรักษาข้อมูล สารสนเทศ และข้อมูลส่วนบุคคลให้สอดคล้องตามระดับชั้นความลับ ตลอดทั้งวงจรชีวิตของข้อมูล สารสนเทศ และข้อมูลส่วนบุคคลนั้น ตั้งแต่การสร้าง สำเนา แจกจ่าย ถ่ายโอนไปจนกระทั่งลบทำลาย หรือการเก็บรวบรวม ใช้ เปิดเผย ไปจนกระทั่งลบทำลาย

๑๔.๘ ไม่ส่งข้อมูลลับ สารสนเทศลับ และข้อมูลส่วนบุคคลผ่านอีเมล อินเทอร์เน็ต ช่องทางการสื่อสารอื่น ๆ ด้วยวิธีการที่ไม่ปลอดภัย ในกรณีที่มีความจำเป็นต้องใช้มาตรการในการเข้ารหัสเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

๑๔.๙ ไม่แอบดูข้อมูลลับบนเครื่องคอมพิวเตอร์ของผู้อื่น และระมัดระวังการพิมพ์เอกสารที่มีชั้นความลับ

๑๔.๑๐ ไม่จัดเก็บเอกสารที่มีข้อมูลลับไว้นานเกินความจำเป็น และดำเนินการทำลายด้วยวิธีการที่เหมาะสม เช่น ทำลายด้วยเครื่องทำลายเอกสาร เป็นต้น

๑๔.๑๑ ไม่ปล่อยหน้าจอคอมพิวเตอร์ค้างไว้ เมื่อไม่มีการใช้งาน และล็อคหน้าจอก่อนออกไปจากหน้าจอ หรือตั้งค่า Screen Saver ตามระยะเวลาที่กำหนดหรือตามระดับความสำคัญของข้อมูลที่กำลังใช้งาน

๑๔.๑๒ แจ้งผู้บังคับบัญชา หรือหน่วยงานภายในที่รับแจ้งเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยที่สำนักงาน กสทช. กำหนด (NBTC Service Desk, ๒๙๐๐) ทันที เมื่อพบเหตุต้องสงสัย ว่าอาจจะเป็นการละเมิดความมั่นคงปลอดภัยสารสนเทศ หรือการละเมิดข้อมูลส่วนบุคคล

๑๔.๑๓ มีความตระหนักในการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศต่าง ๆ อาทิ เครือข่าย เครื่องให้บริการ เครื่องคอมพิวเตอร์พีซี โน้ตบุ๊ค โดยทรัพยากรสารสนเทศของสำนักงาน กสทช. มีไว้เพื่อใช้ในการปฏิบัติงานเท่านั้น และสำนักงาน กสทช. สำนักเทคโนโลยีสารสนเทศมีสิทธิในการติดตามตรวจสอบการใช้งานที่ไม่เหมาะสม และระงับหรือปิดกั้นการเข้าใช้งานเครือข่ายสารสนเทศของสำนักงาน กสทช. ได้ตามความเหมาะสม

๑๔.๑๔ กรณีที่สำนักเทคโนโลยีสารสนเทศตรวจสอบพบบัญชีผู้ใช้งานใดที่ถูกครอบครองโดยผู้ไม่ประสงค์ดี (Compromised) บัญชีผู้ใช้งานนั้นจะถูกยกเลิกหรืองดใช้งานชั่วคราวตามแต่กรณี และสำนักเทคโนโลยีสารสนเทศจะแจ้งวิธีปฏิบัติต่าง ๆ และการคืนสิทธิให้เมื่อดำเนินการระงับเหตุเรียบร้อยแล้ว

หมวด ๓
แนวปฏิบัติการบริหารจัดการด้านความมั่นคงปลอดภัย สำหรับผู้ดูแลระบบ

ข้อ ๑ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑.๑ กำหนดมาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์ของสำนักงาน กสทช. เพื่อดูแลรักษาความปลอดภัย โดยบุคคลที่ต้องการสิทธิในการเข้า-ออก ศูนย์คอมพิวเตอร์ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อสำนักเทคโนโลยีสารสนเทศ

๑.๒ พิจารณาอนุมัติและกำหนดสิทธิการเข้า-ออก ศูนย์คอมพิวเตอร์ให้เป็นไปตามภารกิจของแต่ละหน่วยงานภายในที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเท่านั้น

๑.๓ ต้องทำการยืนยันตัวตนก่อนเข้าศูนย์คอมพิวเตอร์ทุกครั้งเพื่อป้องกันการเข้า-ออกโดยไม่ได้รับอนุญาต

๑.๔ ควบคุมการลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ของผู้ใช้งานและบุคคลภายนอก (Visitors) ทุกครั้ง

๑.๕ ควบคุมให้ผู้เข้า-ออกติดบัตรแสดงตัวตนให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ศูนย์คอมพิวเตอร์

๑.๖ ตรวจสอบการเข้าถึงอาคารต่าง ๆ ที่มีระบบสารสนเทศที่สำคัญอย่างต่อเนื่อง รวมถึงการจัดให้มีอุปกรณ์หรือเครื่องมือแจ้งเตือน เพื่อตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาตหรือพฤติกรรมที่น่าสงสัย

๑.๗ ดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอก (Visitors) ในขณะที่ปฏิบัติงาน ในศูนย์คอมพิวเตอร์จนกระทั่งเสร็จสิ้นภารกิจและออกจากศูนย์คอมพิวเตอร์ เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๑.๘ แยกพื้นที่ในการส่งมอบสินทรัพย์ เพื่อตรวจสอบให้เสร็จเรียบร้อยก่อนนำเข้าไปติดตั้งหรือใช้งานภายในศูนย์คอมพิวเตอร์

๑.๙ ประชาสัมพันธ์มาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์ แก่ผู้ใช้งานและบุคคลภายนอก (Visitors)

๑.๑๐ ห้ามนำอาหารและเครื่องดื่มเข้าไปภายในศูนย์คอมพิวเตอร์

๑.๑๑ ห้ามสูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงในบริเวณภายในศูนย์คอมพิวเตอร์

๑.๑๒ ต้องทำการยกเลิก เพิกถอน หรือเปลี่ยนแปลงการอนุญาตการเข้า-ออกศูนย์คอมพิวเตอร์ของผู้ใช้งานเมื่อผู้นั้นพ้นสภาพการเป็นพนักงานหรือลูกจ้างของสำนักงาน กสทช.

๑.๑๓ ทบทวนสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญภายในศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ การกำหนดการจัดวางและป้องกันระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๒.๑ จัดวางระบบสารสนเทศที่มีความสำคัญในพื้นที่ที่มีความมั่นคงและปลอดภัย เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงพอร์ตของระบบที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๒.๒ แยกจัดเก็บระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ที่สำคัญไว้ในพื้นที่ความปลอดภัยสูงแยกต่างหาก

๒.๓ ต้องควบคุมและป้องกันการใช้งานพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย โดยต้องมีการขออนุญาตเข้าถึงพอร์ตดังกล่าวอย่างเป็นลายลักษณ์อักษร และมีการบันทึกการเข้าใช้งานทุกครั้ง รวมถึงมีการตรวจสอบบันทึกการเข้าใช้งาน อย่างสม่ำเสมอทุก ๓ เดือน

ข้อ ๓ การกำหนดและควบคุมการเดินสายสัญญาณสื่อสาร และสายไฟฟ้า ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๓.๑ ควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้าให้เป็นไปด้วยความเรียบร้อยและปลอดภัย

๓.๒ ควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการรบกวนของสัญญาณ

๓.๓ ทำแผนผังการเดินสายสัญญาณสื่อสารและสายไฟฟ้าให้ครบถ้วนและถูกต้อง

๓.๔ ปิดประตูตู้ Rack สำหรับติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณสื่อสารให้สนิทรวมถึงการล็อคประตูเพื่อป้องกันการเข้าถึงของบุคคลที่ไม่เกี่ยวข้อง

๓.๕ จัดทำป้ายชื่อสำหรับสายสัญญาณสื่อสารและบนอุปกรณ์เพื่อป้องกันการปฏิบัติงานผิดพลาด

๓.๖ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อความถูกต้องและตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๔ การกำหนดการบำรุงรักษาระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๔.๑ จัดทำสัญญาการบำรุงรักษาสำหรับระบบและอุปกรณ์คอมพิวเตอร์ที่มีความสำคัญ

๔.๒ กำหนดเงื่อนไขของการให้บริการในสัญญาการบำรุงรักษาให้ชัดเจนเพื่อให้ผู้รับจ้างต้องติดต่อกลับและเข้ามาดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในระยะเวลาที่เหมาะสม

๔.๓ ตรวจสอบและกำหนดให้มีการรับประกันความเสียหายของระบบสารสนเทศ

๔.๔ บำรุงรักษาระบบสารสนเทศตามรอบระยะเวลาที่กำหนดไว้ในสัญญาการบำรุงรักษา

๔.๕ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๔.๖ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๔.๗ บันทึกปัญหาและข้อบกพร่องที่พบ และรายงานผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทราบ

๔.๘ ควบคุม และดูแลการปฏิบัติงานของผู้ให้บริการภายนอกให้ปฏิบัติตามสัญญาการจ้างเหมาบำรุงรักษา

๔.๙ กำหนดสิทธิของผู้ให้บริการภายนอกในการเข้าถึงพื้นที่ อุปกรณ์ และข้อมูลที่สำคัญ

๔.๑๐ การบริหารจัดการช่องโหว่ทางเทคนิคภายหลังจากการติดตั้งและใช้งานระบบสารสนเทศ

๔.๑๐.๑ จัดให้มีผู้รับผิดชอบในการติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศหรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ThaiCERT) เป็นต้น

๔.๑๐.๒ ดำเนินการประเมินระดับความรุนแรงของช่องโหว่ที่มีการประกาศและวิเคราะห์ประเมินผลกระทบในกรณีที่ช่องโหว่นั้นเกิดกับระบบสารสนเทศในความดูแลและวางแผนในการปรับปรุงแก้ไขช่องโหว่ดังกล่าวโดยเร็วที่สุด โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤต และระดับสูง

๔.๑๐.๓ ดำเนินการปรับปรุงและแก้ไขช่องโหว่ตามขั้นตอนปฏิบัติการบริหารจัดการการเปลี่ยนแปลงที่สำนักงาน กสทช. กำหนด และแจ้งผลการปรับปรุงแก้ไขกลับมายังสำนักเทคโนโลยีสารสนเทศเพื่อทราบและตรวจสอบผลการปรับปรุงแก้ไข

ข้อ ๕ การบริหารจัดการสินทรัพย์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๕.๑ บันทึกและตรวจสอบสินทรัพย์ เพื่อเก็บเป็นหลักฐานในการตรวจสอบความถูกต้องและป้องกันการสูญหาย

๕.๒ กำหนดมาตรการหรือขั้นตอนการทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะจำหน่ายหรือนำกลับมาใช้งานใหม่ทุกครั้ง เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญ ให้ผู้ดูแลระบบดำเนินการตามมาตรการทำลายข้อมูล และสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่เหมาะสมกับระดับชั้นความลับของข้อมูลที่สำนักงาน กสทช. ได้กำหนด หมายความรวมถึงสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่อยู่ในอุปกรณ์ที่สำนักงาน กสทช. เช่าใช้งานด้วย เพื่อลดความเสี่ยงของการรั่วไหลของข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามมาตรการ ดังนี้

๕.๒.๑ ผู้ดูแลระบบต้องตรวจสอบประเภทของข้อมูลบนสื่อบันทึกข้อมูลและคัดแยกสื่อบันทึกข้อมูล ออกตามหมวดหมู่หรือประเภทตามระดับชั้นความลับ

๕.๒.๒ ข้อมูลลับ ข้อมูลลับมาก ข้อมูลลับที่สุด หรือข้อมูลส่วนบุคคล ซึ่งอยู่บนกระดาษหรือวัสดุชั่วคราว ต้องดำเนินการทำลายกระดาษหรือวัสดุชั่วคราวนั้นตามนโยบายการเก็บรักษาและการลบทำลาย

ข้อมูลส่วนบุคคล (Data Retention and Disposal Policy) ที่สำนักงาน กสทช. กำหนด รวมถึงขั้นตอนปฏิบัติที่เกี่ยวข้อง

๕.๒.๓ ข้อมูลสารสนเทศที่อยู่บนเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์จะต้องทำการลบ หรือเขียนทับข้อมูลที่มีความสำคัญในสื่อบันทึกข้อมูลด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก ด้วยวิธีการทำลายแยกตามประเภทของสื่อบันทึกข้อมูล ได้แก่

- Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย
- กระดาษ ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสารหรือทำลายตามขั้นตอนปฏิบัติของสำนักงาน กสทช.
- แผ่น CD/DVD ใช้วิธีการหั่นด้วยเครื่องหั่นทำลายเอกสาร
- เทป ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
- ฮาร์ดดิสก์ ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการเขียนทับให้ไม่สามารถนำข้อมูลกลับมาใช้ได้อีก ตามมาตรฐานการทำลายข้อมูลบนสื่อบันทึกข้อมูลอ้างอิงตามมาตรฐาน NIST ๘๐๐-๘๘ Revision ๑ แนวทางการลบทำลายข้อมูลบนสื่อบันทึกข้อมูล (Guideline for Media Sanitization) และคู่มือปฏิบัติงานของสำนักงาน กสทช. เพิ่มเติม

๕.๒.๔ ในการทำลายสื่อบันทึกข้อมูล ผู้ดูแลระบบพิจารณาทำลายสื่อบันทึกข้อมูลด้วยวิธีการทำลายแยกประเภทตามสื่อบันทึกข้อมูลและใช้วิธีการทำลายตามขั้นตอนปฏิบัติของสำนักงาน กสทช.

๕.๓ กรณีที่สินทรัพย์เกิดความเสียหายและต้องส่งซ่อม ให้ควบคุมการส่งออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กรณีสินทรัพย์เป็นข้อมูลสำคัญต้องทำการทำลายข้อมูลทิ้งเพื่อไม่ให้ผู้อื่นสามารถเข้าถึงได้

ข้อ ๖ การควบคุมการใช้งานระบบสารสนเทศและบริหารจัดการอุปกรณ์คอมพิวเตอร์แบบพกพาให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๖.๑ ต้องนำอุปกรณ์คอมพิวเตอร์แบบพกพาส่วนตัวหรืออุปกรณ์คอมพิวเตอร์แบบพกพาของสำนักงาน กสทช. ที่ได้รับอนุมัติจากผู้บังคับบัญชาให้เชื่อมต่อระบบเครือข่ายภายในและเข้าถึงระบบสารสนเทศของสำนักงาน กสทช. แจ้งขึ้นทะเบียนอุปกรณ์คอมพิวเตอร์แบบพกพาที่สำนักเทคโนโลยีสารสนเทศและปฏิบัติตามขั้นตอนปฏิบัติที่สำนักเทคโนโลยีสารสนเทศกำหนด เพื่อป้องกันการเข้าถึงระบบสารสนเทศด้วยอุปกรณ์คอมพิวเตอร์แบบพกพาโดยไม่ได้รับอนุญาต

๖.๒ ต้องกำหนดมาตรการระบุและพิสูจน์ตัวตนก่อนเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาด้วย บัญชีผู้ใช้งานและรหัสผ่าน หรือเทคโนโลยีไบโอเมตริก (Biometric) หรือพินโค้ด (PIN code) เพื่อป้องกันการเข้าถึงจากผู้อื่นและระมัดระวังมิให้ผู้อื่นเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาของตน

๖.๓ ต้องดูแลรักษาข้อมูลองค์กรในอุปกรณ์คอมพิวเตอร์แบบพกพาให้สอดคล้องตามข้อกำหนดการบริหารจัดการข้อมูล

๖.๔ ต้องแจ้งผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทันทีที่พบว่าอุปกรณ์คอมพิวเตอร์เสียหาย สูญหาย หรือเปลี่ยนเครื่องใหม่ เพื่อจัดการเหตุการณ์ได้อย่างมีประสิทธิภาพ

ข้อ ๗ การควบคุมการใช้งานระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

เป็นการควบคุมบุคคลที่ใช้งานระบบสารสนเทศ รวมถึงการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศที่ได้รับอนุญาตให้เข้าถึงได้เท่านั้น โดยให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๗.๑ กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศตามการแบ่งระดับชั้นและสิทธิการเข้าถึง ดังนี้

- ระดับผู้ดูแลระบบ มีหน้าที่ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและเข้าถึงผ่านระบบงานรวมไปถึงวิธีการทำลายข้อมูล
- ระดับเจ้าของข้อมูล มีหน้าที่ตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง
- ระดับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึกข้อมูล ตรวจสอบข้อมูล ปรับปรุงข้อมูลและรายงานข้อมูลตามความต้องการของสำนักงาน กสทช.
- ระดับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามสิทธิที่สำนักงาน กสทช. มอบให้เท่านั้น

๗.๒ ดำเนินการทบทวนและปรับปรุงการใช้งานระบบสารสนเทศให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย โดยผู้ดูแลระบบต้องจัดให้มีการสำรวจ ตรวจสอบหรือประเมินผลการใช้งานระบบสารสนเทศ รวมทั้งมีการรวบรวมและรายงานปัญหาและข้อเสนอแนะการใช้งานระบบสารสนเทศต่อสำนักงาน กสทช. อย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการทบทวน และปรับปรุงการใช้งานระบบสารสนเทศให้เหมาะสมกับภาระงานในปัจจุบัน

๗.๓ การอนุมัติและกำหนดระดับสิทธิของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของผู้ใช้งานให้เป็นไปตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานภายในที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาแล้วเท่านั้น

๗.๔ กำหนดการเข้าถึงด้วยบัญชีผู้ใช้งานแยกเป็นรายบุคคลตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานภายในที่ผู้ใช้งานปฏิบัติงาน

๗.๕ จัดเก็บข้อมูลการลงทะเบียนสำหรับสร้างบัญชีผู้ใช้งานไว้เพื่อการตรวจสอบในภายหลัง

๗.๖ กำหนดให้ทำการยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าถึงระบบสารสนเทศ

๗.๗ กำหนดระยะเวลาการออกจากระบบสารสนเทศโดยอัตโนมัติเมื่อไม่มีการใช้งานเกิน ๓๐ นาที หรือตามความสำคัญของข้อมูลระบบสารสนเทศ

๗.๘ กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศที่สำคัญของสำนักงาน กสทช. ตามภารกิจและความจำเป็นของผู้ใช้งาน

๗.๙ กำหนดให้เครื่องคอมพิวเตอร์ที่จัดหาโดยสำนักงาน กสทช. พักหน้าจอ (Screen saver) โดยอัตโนมัติ หากไม่มีการใช้งานเครื่องคอมพิวเตอร์ติดต่อกัน ๑๕ นาที

๗.๑๐ จำกัดระยะเวลาในการเชื่อมต่อ (Limitation of connection time) ระบบสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูงดังนี้

๗.๑๐.๑ กำหนดให้ระบบสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานไม่เกิน ๘ ชั่วโมง หรือตั้งแต่เวลา ๘.๓๐ - ๑๖.๓๐ น. สำหรับระบบสารสนเทศของสำนักงาน กสทช.

๗.๑๐.๒ กำหนดให้ระบบสารสนเทศที่มีการใช้งานในสถานที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน กสทช. โดยจำกัดช่วงระยะเวลาการเชื่อมต่ออย่างน้อยไม่เกิน ๘ ชั่วโมงต่อ ๑ ครั้งการเชื่อมต่อ

๗.๑๑ จำกัดและควบคุมการเข้าถึงฟังก์ชั่น (Functions) ต่าง ๆ ในการใช้งานระบบสารสนเทศของผู้ใช้งานและผู้ดูแลระบบ

๗.๑๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสำนักงาน กสทช. ต้องแยกเครือข่ายออกจากระบบอื่น ๆ ต้องมีการควบคุมสภาพแวดล้อมแยกเป็นสัดส่วน และต้องกำหนดสิทธิการใช้งานเฉพาะผู้ที่มีสิทธิเท่านั้น

๗.๑๓ จัดทำระบบบริหารจัดการรหัสผ่านเชิงโต้ตอบสำหรับการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย อย่างน้อยดังนี้

- ผู้ใช้งานต้องสามารถกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยตามการบริหารจัดการบัญชีผู้ใช้งาน (User account) ด้วยตนเอง
- ระบบสารสนเทศที่สำคัญต้องมีการใช้งานปัจจัยหลายอย่างในการระบุและพิสูจน์ตัวตน (Multi-Factor Authentication; MFA)
- ต้องจำกัดจำนวนครั้งในการล็อกอินที่ผิดพลาดได้ เช่น ล็อกอินผิดพลาดได้ไม่เกิน ๓ ครั้ง และมีการหน่วงเวลาในการล็อกอินยาวขึ้นเมื่อมีการล็อกอินผิดพลาดเกินกว่า ๓ ครั้ง
- ต้องไม่มีการแสดงฟังก์ชั่นช่วยเหลือใด ๆ ในระหว่างที่ทำการล็อกอินเข้าสู่ระบบ
- ระบบต้องมีการแสดงประวัติวันเวลาที่ล็อกอินเข้าใช้งานระบบย้อนหลังได้ เช่น ๓ - ๕ ครั้ง เป็นต้น

รวมถึงต้องกำหนดให้มีการบริหารจัดการรหัสผ่านอย่างรัดกุม โดยเริ่มตั้งแต่กระบวนการสร้างรหัสผ่านชั่วคราว (Temporary password) ตามสิทธิที่ผู้ใช้งาน (User) ได้รับการส่งมอบรหัสผ่านชั่วคราว (Temporary password) การเปลี่ยนรหัสผ่าน เงื่อนไขการเปลี่ยนรหัสผ่าน และการกำหนดรหัสผ่านใหม่ในกรณีลืมรหัสผ่าน

๗.๑๔ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งานต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อผู้นั้นพ้นสภาพการเป็นพนักงานหรือลูกจ้างของสำนักงาน กสทช. ภายในระยะเวลา ๑ วันทำการ หลังจากที่สำนักทรัพยากรบุคคลบันทึกข้อมูลในระบบ

๗.๑๕ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งานกรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งาน

๗.๑๖ ดำเนินการทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงเพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๘ การบริหารจัดการความปลอดภัยเครือข่าย ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๘.๑ กำหนดวิธีปฏิบัติเกี่ยวกับการใช้งานเครือข่ายทั้งภายในและภายนอกสำนักงาน กสทช.

๘.๒ กำหนดขั้นตอนการขออนุญาตเพื่อเข้าถึงระบบสารสนเทศที่อยู่ภายในเครือข่ายของสำนักงาน กสทช. โดยจัดให้มีมาตรการควบคุมการเชื่อมต่อระยะไกล (Remote Desktop Protocol; RDP) สำหรับผู้ที่ได้รับอนุญาตแล้วเท่านั้นที่ต้องการเชื่อมต่อเข้ามายังเครื่องปลายทางภายในสำนักงาน กสทช.

๘.๓ ควบคุมการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน กสทช. ที่มีการเข้าใช้งานโดยผู้ให้บริการภายนอกตามขั้นตอนปฏิบัติที่สำนักงาน กสทช. กำหนด

๘.๔ กำหนดขั้นตอนการเชื่อมต่อระบบเครือข่ายจากผู้ใช้งานภายนอกสำนักงาน กสทช. อย่างมั่นคงปลอดภัย เช่น การเชื่อมต่อระบบเครือข่ายด้วยเทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual private network : VPN)

๘.๕ ต้องควบคุมการจัดเส้นทางบนเครือข่ายทั้งหมดของสำนักงาน กสทช. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกรวมทั้งการเชื่อมต่อระหว่างสำนักงาน กสทช. กับหน่วยงานภายนอก โดยต้องเชื่อมต่อผ่านอุปกรณ์ไฟร์วอลล์ และอุปกรณ์ป้องกันการบุกรุกเท่านั้น

๘.๖ ระบุบริการที่สำนักงาน กสทช. อนุญาตให้ใช้งานหรือบริการผ่านระบบเครือข่ายของสำนักงาน กสทช.

๘.๗ กำหนดให้มีการระบุและพิสูจน์ตัวตนในการเข้าถึงระบบสารสนเทศของสำนักงาน กสทช.

๘.๘ จัดทำทะเบียนอุปกรณ์ที่ใช้งานในระบบเครือข่ายโดยอย่างน้อยประกอบด้วยข้อมูล หมายเลขประจำเครื่อง ตราอักษร แบบรุ่น หมายเลข MAC Address หมายเลข IP Address ที่มา ผู้รับผิดชอบ วันที่เริ่มติดตั้ง วันที่เลิกใช้งาน และเหตุผลที่เลิกใช้งาน

๘.๙ ใช้ข้อมูล MAC Address หรือ IP Address เป็นข้อมูลในการระบุอุปกรณ์บนเครือข่าย เพื่อบ่งชี้อุปกรณ์ที่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่ายของสำนักงาน กสทช. และใช้วิธีการทางเทคนิคที่เหมาะสมเพื่อควบคุมการเข้าถึงอุปกรณ์เครือข่ายเหล่านั้น

๘.๑๐ กำหนดให้เฉพาะเครื่องคอมพิวเตอร์ของผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถบริหารจัดการระบบและอุปกรณ์เครือข่ายของสำนักงาน กสทช.

๘.๑๑ ตรวจสอบและปิดพอร์ตบนระบบและอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๘.๑๒ ป้องกันและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการบริหารจัดการอุปกรณ์ในระบบเครือข่ายทั้งจากภายในและภายนอกสำนักงาน กสทช.

๘.๑๓ จัดแบ่งเครือข่ายตามวัตถุประสงค์การใช้งาน บริการ หรือกลุ่มผู้ใช้งาน เช่น เครือข่ายสำหรับผู้ใช้งาน เครือข่ายสำหรับเครื่องแม่ข่าย หรือเครือข่ายสำหรับทดสอบทดลองระบบ เป็นต้น โดยแบ่งแยกเครือข่ายตามกลุ่มของการให้บริการสารสนเทศ กลุ่มการใช้งาน กลุ่มของอุปกรณ์สารสนเทศ และกลุ่มประเภทของเครือข่าย

๘.๑๔ ใช้วิธีการทางเทคนิคบนไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่น ๆ จำกัดเส้นทางบนเครือข่ายที่สำนักงาน กสทช. ไม่อนุญาตให้ใช้งาน เพื่อกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะเส้นทางบนเครือข่ายที่อนุญาตเท่านั้น

๘.๑๕ กำหนดมาตรการป้องกันระบบสารสนเทศที่ต้องเชื่อมโยงกับระบบเครือข่ายสาธารณะอย่างมีประสิทธิภาพ

๘.๑๖ ต้องตรวจสอบและกำหนดเส้นทางเครือข่าย (Network routing control) ให้เหมาะสม โดยต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย ที่ให้บริการสารสนเทศ ได้แก่ ระบบอินเทอร์เน็ต และระบบอินทราเน็ต เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ เพื่อเข้าถึงระบบที่นอกเหนือจากที่ได้รับอนุญาตได้

๘.๑๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงเกิดขึ้น

๘.๑๘ กำหนดมาตรการป้องกันข้อมูลที่ส่งผ่านทางเครือข่ายสาธารณะเพื่อรักษาความลับและความถูกต้องของข้อมูลที่สำคัญ

๘.๑๙ กำหนดเส้นทางบนเครือข่ายที่เหมาะสมเพื่อควบคุมการเชื่อมต่อ และการไหลเวียนของสารสนเทศบนเครือข่ายให้มีประสิทธิภาพ ต้องกำหนดขั้นตอนการปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายในสำนักงาน กสทช. และระหว่างสำนักงาน กสทช. กับหน่วยงานภายนอก โดยการแลกเปลี่ยนสารสนเทศให้ปฏิบัติ ดังนี้

๘.๑๙.๑ ต้องควบคุมให้มีการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางที่ปลอดภัย ทั้งการแลกเปลี่ยนสื่อบันทึกข้อมูลทางกายภาพ และการแลกเปลี่ยนข้อมูลสารสนเทศผ่านระบบเครือข่าย โดยหากเป็นการแลกเปลี่ยนข้อมูลสารสนเทศผ่านระบบเครือข่ายต้องให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมระหว่างการสื่อสารแลกเปลี่ยน รวมถึงการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) หรือการทำธุรกรรมออนไลน์ (Online transaction) เพื่อไม่ให้มีการรับ - ส่งข้อมูลที่ไม่สมบูรณ์ หรือมีการรั่วไหลของข้อมูล หรือมีการแก้ไขข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๘.๑๙.๒ เจ้าของข้อมูลต้องทำการตรวจสอบประเภทของข้อมูลสารสนเทศและลำดับชั้นความลับของข้อมูลสารสนเทศตามที่กำหนดไว้ในขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูลที่จะดำเนินการแลกเปลี่ยน เพื่อควบคุมการแลกเปลี่ยนให้เหมาะสม และป้องกันข้อมูลสำคัญจากการถูกเข้าถึงการเปลี่ยนแปลงแก้ไข การสำเนา และการทำลายโดยไม่ได้รับอนุญาต รวมทั้งการแจกจ่ายหรือส่งผิดตัวผู้รับ

๘.๒๐ ตรวจสอบการใช้งานระบบเครือข่ายด้วยระบบตรวจจับและป้องกันการบุกรุกของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติอย่างสม่ำเสมอ หรืออย่างน้อยเดือนละ ๑ ครั้ง

๘.๒๑ ทดสอบความมั่นคงปลอดภัยของระบบเครือข่ายอย่างน้อยปีละ ๑ ครั้ง หรือตามสถานการณ์ของภัยคุกคามทางไซเบอร์ในระบบเครือข่าย และนำผลที่ได้ไปปรับปรุงความมั่นคงปลอดภัยระบบเครือข่ายของสำนักงาน กสทช. ให้มีความมั่นคงปลอดภัยมากขึ้นและทันต่อภัยคุกคามทางไซเบอร์ในปัจจุบัน

๘.๒๒ ติดตาม ตรวจสอบ ดูแล และปรับปรุงเครือข่ายของสำนักงาน กสทช. ให้มีความมั่นคงปลอดภัยและทันสมัยอยู่เสมอ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานระบบเครือข่ายให้รีบดำเนินการแก้ไขและแจ้งผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทันทีเพื่อป้องกันหรือบรรเทาความเสียหายที่อาจจะเกิดขึ้น

๘.๒๓ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งาน ต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อผู้นั้นพ้นสภาพการเป็นพนักงานหรือลูกจ้างของสำนักงาน กสทช. โดยกำหนดให้ผู้ดูแลระบบยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานภายในระยะเวลา ๑ วันทำการ หลังจากที่สำนักทรัพยากรบุคคลบันทึกข้อมูลในระบบ

๘.๒๔ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งานกรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งาน

๘.๒๕ ดำเนินการทบทวนสิทธิการเข้าถึงเครือข่ายของผู้ใช้งานอย่างสม่ำเสมอหรืออย่างน้อยปีละ ๑ ครั้งเพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต

๘.๒๖ การติดตั้งและใช้งานเครือข่ายไร้สาย (Wi-Fi) ให้ดำเนินการดังนี้

๘.๒๖.๑ ต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน

๘.๒๖.๒ ต้องกำหนดให้ผู้ใช้งานใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (Wi-Fi) รวมถึงทำประกาศความเป็นส่วนตัวแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

๘.๒๖.๓ ต้องกำหนดให้การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายไร้สาย (Wi-Fi) ผู้ใช้งาน (User) จะสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะที่ได้รับอนุญาตตามสิทธิ์ของเครือข่ายไร้สาย (Wi-Fi) เท่านั้น

ข้อ ๙ การบริหารจัดการในการปฏิบัติงาน ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๙.๑ ไม่นำข้อมูลสารสนเทศของสำนักงาน กสทช. ไปเปิดเผยกับบุคคลซึ่งไม่ได้มีความเกี่ยวข้องกับการปฏิบัติหน้าที่เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๙.๒ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งาน

๙.๓ เก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์ (Log) เท่าที่จำเป็นตามที่กำหนดไว้ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๙.๔ ตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดในสำนักงาน กสทช. ให้ตรงกับเวลาอ้างอิงสากล (Stratum ๐)

๙.๕ บันทึกข้อมูลกิจกรรมการใช้งานระบบสารสนเทศและระบบเครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๙.๖ ตรวจสอบและดูแลสภาพแวดล้อมของศูนย์คอมพิวเตอร์ รวมทั้งระบบสนับสนุนการทำงานต่าง ๆ เพื่อป้องกันความเสียหายต่อระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ

๙.๗ จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับเครื่องคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยด้านสารสนเทศของระบบได้ ดังนั้น เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยด้านสารสนเทศที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดการอนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้ง

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากเครื่องคอมพิวเตอร์

ข้อ ๑๐ การสำรองและกู้คืนข้อมูลสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๐.๑ กำหนดขั้นตอนการสำรองและกู้คืนข้อมูลรวมถึงซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดระบบสารสนเทศสำคัญที่จำเป็นต้องสำรองข้อมูลไว้

(๒) ชื่อระบบสารสนเทศ

(๓) ผู้รับผิดชอบในการสำรองข้อมูล

(๔) ประเภทข้อมูล เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้อง ข้อมูลล็อก ข้อมูลบัญชีผู้ใช้งานในระบบ เป็นต้น

(๕) ความถี่ในการสำรองข้อมูล

(๖) วิธีการสำรองข้อมูล

(๗) สื่อที่ใช้บันทึก

๑๐.๒ สำรองข้อมูลตามขั้นตอนและความถี่ที่กำหนดไว้ในแต่ละระบบ

๑๐.๓ ตรวจสอบผลสำเร็จของการสำรองข้อมูลทุกครั้ง

๑๐.๔ เลือกใช้สื่อที่เหมาะสม โดยมีอายุจัดเก็บตามระยะเวลาที่กำหนด

๑๐.๕ นำข้อมูลสำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๑๐.๖ สุ่มข้อมูลสำรองมาทดสอบกู้คืนเพื่อตรวจสอบความถูกต้องและความพร้อมใช้งานของข้อมูลในกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๑๐.๗ ทบทวนขั้นตอนการสำรองและกู้คืนข้อมูลและประเมินประสิทธิผลการดำเนินการอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๑ การบริหารจัดการการเข้ารหัสลับ (Encryption) ข้อมูล ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๑.๑ ร่วมกับคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee: SSMC (คณะกรรมการ SSMC)) ในการจัดทำและปฏิบัติตามขั้นตอนปฏิบัติการเข้ารหัสข้อมูลตามที่สำนักงาน กสทช. กำหนดอย่างเคร่งครัด ซึ่งขั้นตอนปฏิบัติดังกล่าวต้องสอดคล้องตามระดับความสำคัญของข้อมูล ตามที่สำนักงาน กสทช. กำหนด

๑๑.๒ ร่วมกับคณะกรรมการ SSMC พิจารณาใช้อัลกอริทึมที่ทันสมัย และสอดคล้องตามที่สำนักงาน กสทช. กำหนดหลักเกณฑ์ เพื่อให้การดำเนินการเกี่ยวกับการเข้ารหัสข้อมูลเป็นไปในทิศทางเดียวกันและสอดคล้องตามระดับความสำคัญของข้อมูล

๑๑.๓ จัดให้มีและปฏิบัติตามขั้นตอนปฏิบัติการบริหารจัดการกุญแจเข้ารหัสข้อมูล เพื่อให้มีกระบวนการที่รัดกุมตลอดช่วงเวลาการใช้งาน (Key management whole life cycle) โดยมีการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของกุญแจเพื่อเข้ารหัส การจัดเก็บ การใช้งาน และการยกเลิกการใช้งานกุญแจรหัส

๑๑.๔ มีการอนุญาตการเข้าถึงรหัสลับเฉพาะผู้ที่รับผิดชอบเท่านั้น เพื่อป้องกันการถูกแก้ไขหรือเปิดเผยรวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามขั้นตอนปฏิบัติดังกล่าวอย่างเคร่งครัด

ข้อ ๑๒ การบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสำหรับการใช้บริการคลาวด์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๒.๑ ร่วมกับคณะกรรมการ SSMC ในการจัดทำและปฏิบัติตามขั้นตอนปฏิบัติการใช้บริการคลาวด์ ตั้งแต่กระบวนการ ก่อนเริ่มต้นใช้งาน การใช้งาน การบริหารจัดการ และการยกเลิกใช้บริการคลาวด์อย่างมั่นคงปลอดภัย

๑๒.๒ ร่วมกับคณะกรรมการ SSMC ในการจัดทำและปฏิบัติตาม ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการใช้บริการคลาวด์

๑๒.๓ ก่อนดำเนินการคัดเลือกผู้ให้บริการคลาวด์ต้องประเมินและวิเคราะห์ศักยภาพของผู้ให้บริการคลาวด์ (Due Diligence) การพิจารณาถึงการได้รับการรับรองตามมาตรฐานสากลรายงานผลการตรวจประเมินที่น่าเชื่อถือ (เช่น SOC๒ Report) วิธีการที่จะเปลี่ยนหรือยกเลิกการใช้บริการคลาวด์

แนวทางในการถอดถอนบริการออกจากผู้ให้บริการคลาวด์นั้น ๆ และกำหนดหลักเกณฑ์ในการคัดเลือกบริการคลาวด์ให้เหมาะสมกับขอบเขตการใช้งานของสำนักงาน กสทช.

๑๒.๔ กำหนดบทบาทหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการใช้ การบริหารจัดการบริการคลาวด์ และการรักษาความมั่นคงปลอดภัยไว้อย่างชัดเจน

๑๒.๕ พิจารณาอย่างรอบคอบเกี่ยวกับกระบวนการและวิธีในการบริหารจัดการบริการคลาวด์อย่างมั่นคงปลอดภัย เพื่อให้มั่นใจว่ามีการวางมาตรการรักษาความมั่นคงปลอดภัยระหว่างสำนักงาน กสทช. กับผู้ให้บริการคลาวด์อย่างเหมาะสม

๑๒.๖ กำหนดขั้นตอนปฏิบัติในการบริหารจัดการการเปลี่ยนแปลงระหว่างสำนักงาน กสทช. กับผู้ให้บริการคลาวด์ รวมถึงเงื่อนไขการแจ้งล่วงหน้าสำหรับการดำเนินการเปลี่ยนแปลงเพื่อป้องกันการขาดสภาพความพร้อมใช้งาน

๑๒.๗ กำหนดผู้ประสานงาน และระยะเวลาในการติดต่อประสานงานไว้อย่างชัดเจน รวมถึงขั้นตอนปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้มั่นใจว่าเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้นจะได้รับการแจ้ง และบริหารจัดการภายในระยะเวลาที่กำหนด

๑๒.๘ ประเมินความเสี่ยง พิจารณาถึงกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องกับข้อมูลหรือสารสนเทศที่จะนำไปไว้บนคลาวด์ และวางมาตรการเพื่อบริหารจัดการความเสี่ยงต่อการปฏิบัติตามกฎหมาย การปกป้องข้อมูลและการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมรวมถึงติดตามการดำเนินมาตรการต่าง ๆ และทบทวนอย่างสม่ำเสมอ

ข้อ ๑๓ การบริหารจัดการค่าคอนฟิกกูเรชั่น (Configuration Management) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๓.๑ กำหนดกระบวนการและเครื่องมือในการบังคับใช้ให้ฮาร์ดแวร์ ซอฟต์แวร์ บริการและเครือข่ายของสำนักงาน กสทช. ได้รับการกำหนดและปรับแต่งค่าตามที่สำนักงาน กสทช. กำหนดไว้ให้ใช้งาน

๑๓.๒ ต้องจัดทำเทมเพลตมาตรฐานสำหรับการกำหนดค่าฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายที่มั่นคงปลอดภัย

๑๓.๓ ทบทวนเทมเพลตมาตรฐานเป็นระยะ ๆ และทำการอัปเดตเมื่อจำเป็นต้องแก้ไขหรือมีภัยคุกคาม หรือช่องโหว่ใหม่ หรือเมื่อมีการเริ่มต้นใช้งานซอฟต์แวร์หรือฮาร์ดแวร์เวอร์ชั่นใหม่

๑๓.๔ จัดให้มีการตรวจสอบการปรับแต่งค่าให้มีความสอดคล้องกับค่ามาตรฐานเป็นระยะ ๆ เพื่อลดความเสี่ยงในการเปิดจุดอ่อนหรือช่องโหว่ให้กับผู้ไม่ประสงค์ดี

ข้อ ๑๔ การบริหารจัดการการลบสารสนเทศ (Information Deletion Management) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๔.๑ ต้องไม่จัดเก็บสารสนเทศที่ละเอียดอ่อนไว้นานเกินกว่าที่จำเป็นเพื่อลดความเสี่ยงจากการถูกเปิดเผยที่ไม่พึงประสงค์

๑๔.๒ เมื่อต้องลบสารสนเทศออกจากระบบ แอปพลิเคชัน หรือบริการต่าง ๆ ต้องพิจารณากำหนดวิธีการลบให้สอดคล้องตามข้อกำหนดทางธุรกิจและกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง

๑๔.๓ บันทึกผลการลบสารสนเทศไว้เป็นหลักฐาน รวมถึงในกรณีที่เมื่อมีการใช้ผู้ให้บริการลบสารสนเทศต้องจัดเก็บหลักฐานการลบสารสนเทศจากผู้ให้บริการเหล่านั้น รวมถึงในกรณีที่ใช้บริการคลาวด์และกระบวนการลบสารสนเทศนั้นจะต้องสามารถสอบทวนได้

ข้อ ๑๕ การบริหารจัดการการปิดบัง/ซ่อนข้อมูล (Data Masking Management) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๕.๑ ร่วมกับคณะกรรมการ SSMC จัดทำขั้นตอนปฏิบัติที่เกี่ยวข้องกับการปิดบัง/ซ่อนข้อมูล พิจารณาประกาศใช้งาน คัดเลือกและจัดหาเครื่องมือหรือวิธีการทางเทคนิคที่เหมาะสมในการปิดบัง/ซ่อนข้อมูลสำหรับข้อมูลส่วนบุคคลเพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและเพื่อให้สอดคล้องตามกฎหมาย ระเบียบ ข้อบังคับและสัญญาที่เกี่ยวข้อง

๑๕.๒ ร่วมกับคณะกรรมการ SSMC พิจารณาหลักเกณฑ์ที่เหมาะสมสำหรับการใช้เทคนิคการปกปิด/ซ่อน การใช้นามแฝงหรือการปิดบังชื่อ (Pseudonymization) และการทำให้ไม่สามารถระบุตัวบุคคลได้อีก (Anonymization) ในกรณีที่มีการใช้เทคนิคการทำให้ไม่สามารถระบุตัวบุคคลได้อีก (Anonymization) กับข้อมูลส่วนบุคคล ที่สำนักงาน กสทช. ถือครองอยู่เพื่อประมวลผล จะต้องมั่นใจว่าเทคนิควิธีดังกล่าวจะไม่สามารถระบุตัวบุคคลทั้งทางตรงและทางอ้อมคืนมาได้อีก ทั้งนี้ เทคนิควิธีเหล่านี้ให้สอดคล้องตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะประกาศกำหนด

๑๕.๓ เมื่อมีกิจกรรมที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล ให้ผู้รับผิดชอบกิจกรรมนั้น ๆ ประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และขอคำปรึกษาจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และแจ้งต่อสำนักเทคโนโลยีสารสนเทศในกรณีที่ต้องพิจารณาใช้มาตรการในการปิดบัง/ซ่อนข้อมูลส่วนบุคคล (Data Masking) เพื่อเป็นการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องตามกฎหมาย ระเบียบ ข้อบังคับและสัญญาที่เกี่ยวข้อง

ข้อ ๑๖ การป้องกันข้อมูลส่วนบุคคล/ข้อมูลที่มีความสำคัญรั่วไหล (Data Leakage Prevention) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๖.๑ ร่วมกับคณะกรรมการ SSMC พิจารณาจัดหาเครื่องมือหรือวิธีการทางเทคนิคเพื่อนำมาใช้เป็นมาตรการป้องกันข้อมูลรั่วไหลกับระบบ เครือข่าย และอุปกรณ์ประมวลผลสารสนเทศอื่น ๆ ในการจัดเก็บหรือถ่ายโอนข้อมูลส่วนบุคคล และข้อมูลที่มีความสำคัญ

๑๖.๒ แนวทางปฏิบัติในการป้องกันข้อมูลรั่วไหล ควรประกอบด้วย

(ก) ระบุและจัดหมวดหมู่ข้อมูลสารสนเทศ ตามระดับความสำคัญและความอ่อนไหวของสารสนเทศ

(ข) กำหนดให้มีเทคนิคในการเฝ้าระวังติดตามช่องทางที่ข้อมูลสารสนเทศของสำนักงาน กสทช. อาจรั่วไหล เช่น การส่งผ่านอีเมล การถ่ายโอนไฟล์ การจัดเก็บในสื่อบันทึกข้อมูลแบบเคลื่อนที่ได้ เป็นต้น

(ค) ดำเนินการเพื่อป้องกันสารสนเทศรั่วไหล เช่น การกักอีเมลที่มีข้อมูลที่มีความอ่อนไหว เป็นต้น

๑๖.๓ ในกรณีที่ใช้เครื่องมือป้องกันข้อมูลรั่วไหล เครื่องมือนั้นจะต้องสามารถ

(ก) ระบุและเฝ้าติดตามสารสนเทศที่อ่อนไหวซึ่งเสี่ยงต่อการถูกเปิดเผยโดยไม่ได้รับอนุญาต

(ข) ตรวจจับการเปิดเผยสารสนเทศที่อ่อนไหว

(ค) บล็อกการดำเนินการของผู้ใช้หรือการส่งผ่านเครือข่ายที่แสดงสารสนเทศที่อ่อนไหวได้

๑๖.๔ หากมีความจำเป็นต้องส่งออกสารสนเทศนั้น จะต้องมีการขออนุญาตการส่งออกและผู้อนุญาตต้องรับผิดชอบต่อความเสี่ยงดังกล่าว

๑๖.๕ จัดทำข้อกำหนดให้กับผู้ใช้งานเพิ่มเติมเกี่ยวกับการห้ามใช้โปรแกรมจับภาพหน้าจอหรือการถ่ายภาพหน้าจอสำหรับสารสนเทศที่มีความอ่อนไหว รวมถึงสำนักงาน กสทช. ต้องจัดให้มีการสร้างความตระหนักรู้ต่อการรั่วไหลของสารสนเทศในกรณีดังกล่าว

๑๖.๖ สำหรับข้อมูลที่ได้มีการสำรองไว้ ต้องมีมาตรการควบคุมอื่น ๆ เพิ่มเติม เช่น การเข้ารหัส การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำรองไว้นั้นได้รับการปกป้องอย่างเหมาะสม

ข้อ ๑๗ การบริหารจัดการการติดตามกิจกรรมทางเทคโนโลยีสารสนเทศ (Monitoring activities) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๗.๑ ควรเฝ้าติดตามเครือข่าย ระบบ และแอปพลิเคชัน เพื่อหาพฤติกรรมที่ผิดปกติและการดำเนินการที่เหมาะสมเพื่อประเมินอุบัติการณ์ (event) และเหตุการณ์ด้านการรักษาความปลอดภัยของสารสนเทศ (incident) ที่อาจเกิดขึ้น

๑๗.๒ ควรกำหนดขอบเขตและระดับการเฝ้าติดตามตามที่สอดคล้องตามข้อกำหนดทางธุรกิจและการรักษาความปลอดภัยของสารสนเทศ รวมถึงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

๑๗.๓ จัดเก็บข้อมูลล็อกหรือบันทึกหลักฐานต่าง ๆ ไว้ตามระยะเวลาที่กำหนด

๑๗.๔ จัดทำขั้นตอนปฏิบัติในการจัดเก็บและเฝ้าระวังติดตามกิจกรรมของระบบ แอปพลิเคชัน เครือข่าย และเพื่อกำหนดข้อมูลล็อกที่ต้องจัดเก็บ และรายละเอียดที่เกี่ยวข้อง

๑๗.๕ กำหนดเงื่อนไขในการแจ้งเตือน อาทิ ตำแหน่งการเข้าถึง ความถี่ในการเข้าถึง ช่วงเวลาปกติและช่วงเวลาสูงสุด เป็นต้น และระบุลักษณะพฤติกรรมที่ผิดปกติ อาทิ

(ก) ระบบหรือแอปพลิเคชันหยุดการทำงานโดยไม่ได้วางแผน

(ข) กิจกรรมที่มักเกี่ยวข้องกับมัลแวร์หรือการรับส่งข้อมูลที่มาจากแหล่งไอพี หรือโดเมนเครือข่ายที่เป็นอันตราย เช่น คำสั่งควบคุมและสั่งการเซิร์ฟเวอร์ (Command & Control Server)

(ค) ลักษณะการโจมตีที่ทราบ เช่น การปฏิเสธบริการและหน่วยความจำล้น (Buffer Overflow)

(ง) พฤติกรรมของระบบที่ผิดปกติ เช่น การบันทึกการกดแป้นพิมพ์ การเบี่ยงเบนในการใช้โปรโตคอลมาตรฐาน

(จ) สภาพคอขวดหรือปริมาณทราฟฟิกมากเกินไป ทำให้เกิดความล่าช้าของเครือข่าย

(ฉ) การเข้าถึงโดยไม่ได้รับอนุญาต

(ช) การสแกนแอปพลิเคชัน ระบบ และเครือข่ายโดยไม่ได้รับอนุญาต

(ซ) ความพยายามในการเข้าถึงทรัพยากรที่มีการป้องกัน

(ฌ) ผู้ใช้งานที่ผิดปกติและพฤติกรรมของระบบที่คาดหวังที่อาจเกิดขึ้น

๑๗.๖ ต้องดำเนินการเฝ้าระวังติดตามอย่างต่อเนื่อง และเป็นปัจจุบัน หรือเป็นระยะ ๆ สอดคล้องตามอำนาจ หน้าที่ และการดำเนินงานของสำนักงาน กสทช. และควรปรับปรุงให้สอดคล้องกับบริบทอย่างเหมาะสม

๑๗.๗ จัดให้มีการฝึกอบรมกับเจ้าหน้าที่ที่เกี่ยวข้อง โดยเจ้าหน้าที่ต้องตระหนักรู้ถึงความสำคัญของอุบัติการณ์และเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น และเมื่อมีความสงสัยว่าอาจจะเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย ต้องมีขั้นตอนปฏิบัติในการแจ้งผู้ที่เกี่ยวข้องให้ได้รับทราบและติดตามแก้ไขเหตุที่เกิดขึ้นได้อย่างทันท่วงที

ข้อ ๑๘ การบริหารจัดการการเข้าถึงเว็บไซต์ภายนอก (Web Filtering) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๘.๑ จัดให้มีเครื่องมือทางเทคนิคในการบริหารจัดการการเข้าถึงเว็บไซต์ภายนอก เช่น การดำเนินการบล็อกไอพี หรือโดเมนของเว็บไซต์ เป็นต้น เพื่อลดความเสี่ยงจากข้อมูลที่มุ่งร้ายอันเกิดจากการที่เจ้าหน้าที่ของสำนักงาน กสทช. อาจเข้าถึงเว็บไซต์ที่มีลักษณะผิดกฎหมาย หรือมีมัลแวร์ หรืออาจแฝงด้วยภัยอันตรายประเภทฟิชชิ่ง มีการจำกัดการเข้าถึง เว็บไซต์ และแอปพลิเคชัน ที่ควรเข้าถึง (Whitelist) หรือไม่ควรเข้าถึง (Blacklist) อย่างเหมาะสม และควรอัพเดตรายการอย่างสม่ำเสมอ

๑๘.๒ กำหนดกฎระเบียบให้กับผู้ใช้งานได้ทราบถึงการใช้งานทรัพยากรออนไลน์อย่างปลอดภัยและเหมาะสม ก่อนที่จะดำเนินการควบคุมทางเทคนิค รวมถึงสื่อสารให้ผู้ใช้งานได้รับทราบ

๑๘.๓ จัดอบรมสร้างความตระหนักรู้ให้กับผู้ใช้งานเพื่อเสริมสร้างนิสัยในการใช้งานทรัพยากรออนไลน์อย่างปลอดภัยและเหมาะสม

ข้อ ๑๙ การเขียนโค้ดอย่างมั่นคงปลอดภัย (Secure Coding) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๙.๑ ปฏิบัติตามหลักการเขียนโค้ดอย่างมั่นคงปลอดภัย เพื่อช่วยลดช่องโหว่ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นในซอฟต์แวร์

๑๙.๒ สนับสนุนการนำหลักการเขียนโค้ดอย่างมั่นคงปลอดภัยให้สามารถประยุกต์ใช้งานทั่วทั้งสำนักงาน กสทช. พร้อมทั้งให้คำแนะนำและช่วยกันดูแลให้มีการเขียนโค้ดอย่างมั่นคงปลอดภัยครอบคลุมทั้งซอฟต์แวร์จากบุคคลภายนอกและซอฟต์แวร์แบบโอเพ่นซอร์ส

๑๙.๓ ติดตามข่าวสารและคำแนะนำเกี่ยวกับช่องโหว่ของซอฟต์แวร์และนำมาปรับปรุงแก้ไขหลักการเขียนโค้ดอย่างต่อเนื่อง

ข้อ ๒๐ การปฏิบัติตามกรอบประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๒๐.๑ ปฏิบัติตามคำสั่งคณะกรรมการ SSMC เพื่อปฏิบัติให้สอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หมวดที่ ๑)

๒๐.๒ ให้ความร่วมมือในการสนับสนุนและรับตรวจสำหรับการตรวจสอบตามแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ส่วนที่ ๒)

๒๐.๓ ดำเนินการอย่างเป็นรูปธรรมเพื่อให้สอดคล้องตามขั้นตอนปฏิบัติการประเมินความเสี่ยงที่คณะกรรมการ SSMC ประกาศกำหนดและจัดเก็บหลักฐานผลการประเมินความเสี่ยงเพื่อแสดงถึงการปฏิบัติอย่างสอดคล้องตามกฎหมาย (ส่วนที่ ๓)

๒๐.๔ ให้ความร่วมมือในการซักซ้อม และปฏิบัติตามบทบาทหน้าที่ที่ตนได้รับมอบหมายตามแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อให้เกิดประสิทธิภาพประสิทธิผลในการรับมือกับภัยคุกคามทางไซเบอร์อย่างสูงสุด

หมวด ๔
แนวปฏิบัติสำหรับเจ้าของระบบ (System Owner)

ข้อ ๑ การบริหารจัดการโครงการ/งานด้านเทคโนโลยีสารสนเทศ

เมื่อมี โครงการ/งาน ด้านเทคโนโลยีสารสนเทศ เจ้าของระบบต้องดำเนินการ ดังนี้

๑.๑ ประเมินและบริหารจัดการต่อความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ ข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยไซเบอร์ รวมถึงความเสี่ยงที่เกี่ยวข้องกับการทำโครงการ อาทิ ความเสี่ยงด้านการรักษาความปลอดภัยในด้านการสื่อสารภายในและภายนอก ทั้งนี้ ต้องเริ่มตั้งแต่ระยะแรก และเป็นระยะ ๆ ตลอดวงจรชีวิตโครงการ

๑.๒ ประยุกต์ใช้ข้อกำหนดในการรักษาความมั่นคงปลอดภัย (Security Requirement) หลักการวิศวกรรมด้านความมั่นคงปลอดภัย (System Engineering Principle) ข้อกำหนดด้านการใช้บริการคลาวด์ (Cloud Security Requirement) ข้อกำหนดด้านความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Privacy by Design by Default) ข้อกำหนดในการปฏิบัติตามสิทธิในทรัพย์สินทางปัญญา ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัย และการปฏิบัติให้สอดคล้องตามกฎหมาย ก่อนเริ่มดำเนินการ

๑.๓ จัดทำสถาปัตยกรรมระบบเพื่อแสดงให้เห็นถึงองค์ประกอบของระบบ ส่วนที่เป็นการรักษาความมั่นคงปลอดภัยระบบ และการเชื่อมต่อกับเครือข่ายและระบบภายในของสำนักงาน กสทช. แจ้งต่อสำนักเทคโนโลยีสารสนเทศ

๑.๔ จัดส่งรายงานผลการประเมินและบริหารจัดการต่อความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศมายังส่วนงานความมั่นคงปลอดภัย สำนักเทคโนโลยีสารสนเทศ เพื่อให้คำแนะนำและประเมินความเหมาะสมและเพียงพอของมาตรการด้านความมั่นคงปลอดภัยที่เจ้าของระบบได้วางไว้ เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยของสำนักงาน กสทช. เป็นไปอย่างมีประสิทธิภาพประสิทธิผลสูงสุด และสอดคล้องตามข้อกำหนดของกฎหมาย

๑.๕ กำหนดหน้าที่และความรับผิดชอบด้านการรักษาความปลอดภัยระหว่างเจ้าของระบบ ผู้ดูแลระบบ และผู้ให้บริการภายนอก และสำนักเทคโนโลยีสารสนเทศ ให้ชัดเจนเพื่อป้องกันการปฏิเสธความรับผิดชอบในกรณีเกิดอุบัติการณ์หรือเหตุการณ์ด้านความมั่นคงปลอดภัย

๑.๖ กำกับดูแลให้ผู้ปฏิบัติงานในโครงการดำเนินการตามนโยบายและแนวปฏิบัตินี้ และเฝ้าระวังติดตามการดำเนินโครงการอย่างเป็นระยะ ๆ รวมทั้ง ต้องแจ้งปัญหาอุปสรรคที่พบในการปฏิบัติงานหากไม่สามารถดำเนินการตามมาตรการที่จัดวางไว้ได้ จะต้องแจ้งสำนักเทคโนโลยีสารสนเทศ เพื่อหาร่วมแก้ไขปัญหา

๑.๗ ทดสอบประสิทธิภาพของมาตรการต่าง ๆ ที่จัดให้มีในระบบ แอปพลิเคชันนั้น ก่อนส่งมอบงาน

๑.๘ ประสานงานกับสำนักเทคโนโลยีสารสนเทศ เพื่อตรวจประเมินและแก้ไขด้านความมั่นคงปลอดภัยให้กับระบบ แอปพลิเคชัน ก่อนนำออกสู่การให้บริการ ในกรณีที่ต้องการนำระบบ แอปพลิเคชันไว้ที่สำนักเทคโนโลยีสารสนเทศต้องดำเนินการตามขั้นตอนปฏิบัติที่สำนักเทคโนโลยีสารสนเทศกำหนด

๑.๙ ต้องมีการดูแลและปรับปรุงด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๑.๑๐ เมื่อสำนักเทคโนโลยีสารสนเทศดำเนินการตรวจประเมินช่องโหว่ หรือทำการทดสอบเจาะระบบประจำปี และพบว่าระบบ แอปพลิเคชัน ภายใต้การดูแลของเจ้าของระบบมีช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัย เจ้าของระบบจะต้องสั่งการให้มีการดำเนินการแก้ไขระบบ แอปพลิเคชัน โดยไม่ชักช้า

หรือภายใน ๗ วันทำการสำหรับช่องโหว่ระดับวิกฤติ และระดับสูง และต้องดำเนินการตามข้อกำหนดอื่น ๆ ที่เกี่ยวข้องในนโยบายและแนวปฏิบัตินี้

๑.๑๑ เมื่อปิดโครงการ/งาน ควรมีการถอดบทเรียน (Lesson leaned) จากผู้ที่มีส่วนร่วมในโครงการ/งานเพื่อรวบรวมจัดทำรายงานเสนอแนะการปรับปรุงการดำเนินโครงการ/งาน ไว้ใช้ในการปรับปรุงการบริหารโครงการ/งาน อื่นต่อไป

หมวด ๕
แนวปฏิบัติสำหรับการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ และการกำกับผู้ให้บริการภายนอก (System Acquisition, Development, Maintenance and Third Party Management)

เพื่อกำหนดแนวทางในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ และการบริหารจัดการผู้ให้บริการภายนอก การทำสัญญาจ้าง การประเมินความเหมาะสม การติดตามและประเมินผลการปฏิบัติงาน และการสอบทานผลการปฏิบัติงาน เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถปฏิบัติงานให้สำนักงาน กสทช. ได้ตามเป้าหมายและเงื่อนไขที่กำหนด โดยไม่ก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์จนส่งผลกระทบต่อการดำเนินงานและการให้บริการของสำนักงาน กสทช. อย่างมีนัยสำคัญ

ข้อ ๑ การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศของสำนักงาน กสทช. ผู้ที่ได้รับมอบหมายในการจัดหาพัฒนา และดูแลรักษาระบบ ต้องดำเนินการดังนี้

๑.๑ การจัดหาและพัฒนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ ให้ประสานงานกับสำนักเทคโนโลยีสารสนเทศ เพื่อพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย และความสอดคล้องกับโครงสร้างพื้นฐานและเครือข่ายสารสนเทศของสำนักงาน กสทช. ก่อนนำเสนอพิจารณาอนุมัติจัดหาและพัฒนาทุกครั้ง

๑.๒ การจัดหาและพัฒนาที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่มีความสำคัญยิ่งยวดและมีลักษณะสุ่มเสี่ยงต่อความล้มเหลวในการให้บริการหากมีเพียงชุดเดียว ให้ผู้รับผิดชอบพิจารณาจัดหาอุปกรณ์สำรองไว้ โดยขอความเห็นชอบจากผู้บังคับบัญชา

๑.๓ การพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย ให้คำนึงถึงเรื่องดังต่อไปนี้

(ก) สิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนา

(ข) การตรวจสอบด้านคุณภาพและความถูกต้องของระบบสารสนเทศ

(ค) การตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์

(ง) ข้อจำกัดในการเปิดเผยข้อมูลของสำนักงาน กสทช.

(จ) มาตรฐานและคุณภาพการให้บริการด้านความมั่นคง

(ฉ) การทดสอบระบบสารสนเทศ

๑.๔ ไม่อนุญาตให้นำข้อมูลสำคัญของสำนักงาน กสทช. เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลใช้ภายในเท่านั้น ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นแต่ได้รับการอนุมัติจากผู้บังคับบัญชา หรือได้รับความยินยอมโดยชัดแจ้ง หรือมีการแจ้งเจ้าของข้อมูลส่วนบุคคลตามแต่กรณีไว้ก่อนแล้ว

๑.๕ ต้องกำกับดูแลการออกแบบและพัฒนาระบบให้จัดทำและปฏิบัติตามหลักการวิศวกรรมด้านความมั่นคงปลอดภัย และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช.

๑.๖ ต้องกำกับดูแลการออกแบบและพัฒนาระบบ Website และ Web Application ให้สอดคล้องตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Standard: WSS) และมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ (Web Application Security Standard: WAS) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เพื่อให้ระบบมีความมั่นคงปลอดภัย

๑.๗ ดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบสารสนเทศจากภายนอก (Outsourced system development) ให้เป็นไปตามขั้นตอนปฏิบัติการพัฒนาระบบสารสนเทศของสำนักงาน กสทช.

๑.๘ ต้องทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งานหรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้ถูกต้องตรงความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ สำนักงาน กสทช. ควรระมัดระวังโดยจัดให้มีแนวทางควบคุมและป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบหากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

๑.๙ ต้องทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

๑.๑๐ กำหนดผู้รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System software) อย่างชัดเจน รวมถึงเพื่อประสานงานกับสำนักเทคโนโลยีสารสนเทศก่อนที่จะนำระบบสารสนเทศที่พัฒนาติดตั้งขึ้นให้บริการ

๑.๑๑ ในระหว่างการพัฒนาระบบสารสนเทศ ต้องกำกับ หรือจัดให้มีการตรวจสอบซอร์สโค้ด (Source code review) ด้วยวิธีการที่เหมาะสม และดำเนินการแก้ไขในกรณีที่พบว่าซอร์สโค้ดดังกล่าวอาจเป็นความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

๑.๑๒ ก่อนนำระบบสารสนเทศขึ้นให้บริการ ทดสอบด้านความมั่นคงปลอดภัยก่อนนำขึ้นให้บริการ ต้องทำการตรวจสอบช่องโหว่ทางเทคนิค ปิดช่องโหว่ที่ตรวจพบ อัพเดตระบบให้เป็นเวอร์ชั่นล่าสุด ต้องปรับแต่งค่าด้านความมั่นคงปลอดภัยให้เหมาะสม (Hardening) และสอดคล้องกับค่าพื้นฐานที่สำนักงาน กสทช. กำหนด (Configuration baseline) รวมทั้งประสานงานกับสำนักเทคโนโลยีสารสนเทศ ทราบถึงแผนและแนวทางในการติดตั้งและเปิดใช้งานระบบ เพื่อให้ผู้ที่ได้รับมอบหมายดำเนินการตรวจสอบการปรับแต่งค่าต่าง ๆ ของระบบให้มีความมั่นคงปลอดภัยก่อนการเปิดให้บริการ

๑.๑๓ ต้องควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ (Development environment) ซึ่งได้แก่ บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ และเทคโนโลยีสำหรับการพัฒนาระบบให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบโดยคำนึงถึงเรื่องดังนี้

(ก) การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ ส่งผ่านระบบการควบคุมการนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

(ข) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

(ค) การติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

(ง) มีการจัดเก็บข้อมูลสำรองในพื้นที่นอกสำนักงาน กสทช. ที่มีความมั่นคงปลอดภัย

๑.๑๔ ควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ โดยอย่างน้อยต้องมีในเรื่องดังต่อไปนี้

(ก) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

(ข) กำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจ ต้องควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข มีการตรวจรับจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งมีการจัดเก็บรายละเอียดของคำขอไว้ เป็นต้น

(ค) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง

(ง) ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

(จ) จัดเก็บโปรแกรมเวอร์ชั่น (Program version) ก่อนการเปลี่ยนแปลงไว้ใช้งานหรือมีกระบวนการถอยกลับสู่สภาพเดิม (Fall- back) ของระบบงานในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

(ฉ) มีการสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

(ช) บันทึกและจัดเก็บหลักฐานทั้งหมด (Audit trail) ที่เกี่ยวข้องกับการเปลี่ยนแปลงเพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

ข้อ ๒ การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลโดยผู้ให้บริการภายนอก ผู้ที่ได้รับมอบหมายต้องดำเนินการดังนี้

๒.๑ ต้องปฏิบัติตามขั้นตอนปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกิดจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

๒.๒ จัดทำผังแสดงการเชื่อมโยงเครือข่าย ระบบ และการไหลของข้อมูล (Network and System’s Data Flow Diagram) ที่แสดงถึงรายละเอียด Data Flow และการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกอย่างชัดเจน โดยได้รับอนุมัติจากผู้มีอำนาจ จัดเก็บไว้เป็นความลับและควบคุมการเข้าถึงอย่างเข้มงวด

๒.๓ ติดตามและทดสอบสภาพความพร้อมใช้งาน (Availability) ของการเชื่อมต่อหลักและการเชื่อมต่อสำรองกับผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๒.๔ กำหนดมาตรการด้านความมั่นคงปลอดภัย (Security Controls) เพื่อตรวจจับและป้องกันการบุกรุกผ่านการเชื่อมต่อระบบเครือข่ายของผู้ให้บริการภายนอกอย่างรัดกุมเพียงพอและมีการสอบทานมาตรการด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๒.๕ การเปลี่ยนแปลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกต้องผ่านขั้นตอนปฏิบัติการบริหารจัดการการเปลี่ยนแปลงที่สำนักงาน กสทช. กำหนด

๒.๖ กำหนดให้มีหน่วยงานภายในหรือผู้รับผิดชอบในการประสานงานกับผู้ให้บริการภายนอกที่ให้บริการ สถาบันการเงิน เพื่อร่วมกันพัฒนาปรับปรุงการรักษาความมั่นคงปลอดภัยของการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกอย่างต่อเนื่อง

ข้อ ๓ การประเมินและวิเคราะห์ศักยภาพของผู้ให้บริการภายนอกในขั้นตอนของการคัดเลือก (Due Diligence) และการบริหารจัดการสัญญา ผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๓.๑ กำหนดให้มีการประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ก่อนทำสัญญาว่าจ้างผู้ให้บริการภายนอก (Due Diligence) รวมถึงมีการจัดเก็บและปรับปรุงรายชื่อผู้ให้บริการภายนอกให้เป็นปัจจุบันอยู่เสมอ

๓.๒ จัดทำสัญญากับผู้ให้บริการภายนอก โดยมีการระบุข้อกำหนดในการรักษาความมั่นคงปลอดภัย (Security Requirement) หลักการวิศวกรรมด้านความมั่นคงปลอดภัย ข้อกำหนดด้านการใช้บริการคลาวด์ มาตรฐานทางเทคนิคอื่น ๆ ที่สำนักงาน กสทช. กำหนด รวมถึงข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ซึ่งผู้ให้บริการภายนอกต้องปฏิบัติไว้ในสัญญาอย่างชัดเจน ทั้งนี้ข้อกำหนดดังกล่าวต้องสอดคล้องตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยที่สำนักงาน กสทช. กำหนด

๓.๓ สัญญาที่จัดทำกับผู้ให้บริการภายนอกต้องระบุถึงความรับผิดชอบในการรักษาความมั่นคงปลอดภัยข้อมูล/ข้อมูลส่วนบุคคล ของสำนักงาน กสทช. ที่ผู้ให้บริการภายนอกเป็นผู้ดูแล รับส่ง จัดเก็บ และประมวลผล

๓.๔ สัญญาที่จัดทำกับผู้ให้บริการภายนอกต้องระบุถึงความรับผิดชอบในการรับมือต่อเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยไว้อย่างชัดเจน

๓.๕ สัญญาที่จัดทำกับผู้ให้บริการภายนอกต้องระบุถึงแนวทางการรักษาความมั่งคงปลอดภัยสำหรับการส่งคืนข้อมูลสำคัญหรือการทำลายข้อมูลสำคัญในกรณีที่มีการยกเลิกสัญญา

๓.๖ สัญญาที่จัดทำกับผู้ให้บริการภายนอกต้องมีการระบุสิทธิเรียกร้องค่าเสียหายในกรณีที่ผู้ให้บริการภายนอกไม่สามารถปฏิบัติตามที่สำนักงาน กสทช. กำหนดไว้

๓.๗ สัญญาที่จัดทำกับผู้ให้บริการภายนอกมีการระบุบทบาท หน้าที่ และความรับผิดชอบในการรายงานช่องโหว่และเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยแก่สำนักงาน กสทช.

๓.๘ มีแนวทางรองรับกรณียกเลิกหรือยุติการใช้บริการ (Termination/Exit Strategy) จากผู้ให้บริการภายนอกเพื่อลดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของสำนักงาน กสทช.

ข้อ ๔ การติดตามความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก ผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๔.๑ ประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกที่สำคัญอย่างสม่ำเสมอ

๔.๒ มีการสอบทานแผนรับมือจากเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Resilience Plan) ของผู้ให้บริการภายนอกที่สำคัญอย่างสม่ำเสมอ

๔.๓ กำหนดให้มีการติดตามดูแลการเข้าถึงทางกายภาพ (Physical) และทาง Logical จากผู้ให้บริการภายนอก

๔.๔ จัดให้มีการตรวจสอบการบริหารจัดการผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า สำนักงาน กสทช. มีกระบวนการติดตาม รายงาน และแก้ไขปัญหาอย่างมีประสิทธิภาพ

๔.๕ กำหนดขอบเขตและความถี่ในการติดตามการปฏิบัติงานตามระดับความเสี่ยงของผู้ให้บริการภายนอก

๔.๖ ระบุการควบคุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เมื่อมีความจำเป็นต้องรวบรวมและจัดเก็บข้อมูลที่ได้มาจากผู้ให้บริการภายนอก

๔.๗ ตรวจสอบ หรือสอบทานรายงานตรวจสอบจากผู้ตรวจสอบหรือผู้เชี่ยวชาญภายนอกที่มีมาตรฐานเป็นที่ยอมรับ (เช่น SSAE ๑๘ Type II SOC ๒) เพื่อประเมินความเพียงพอของการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกที่สำคัญ เช่น ที่ให้บริการประมวลผล จัดเก็บ รับส่งข้อมูล เป็นต้น

๔.๘ ติดตามการเข้าถึงข้อมูลสำคัญ (Sensitive Data) /ข้อมูลส่วนบุคคล (Data Privacy) จากผู้ให้บริการภายนอก ทั้งข้อมูลที่อยู่ในระบบของสำนักงาน กสทช. และระบบที่ใช้บริการจากผู้ให้บริการภายนอกให้เป็นไปตามหลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege) พร้อมทั้งกำกับดูแลการปฏิบัติตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคลหากผู้ให้บริการภายนอกมีการประมวลผลข้อมูลส่วนบุคคลในระบบสารสนเทศนั้น

ข้อ ๕ โปรแกรมคอมพิวเตอร์มาตรฐานสำหรับการใช้งานของสำนักงาน กสทช.

สำนักงาน กสทช. ได้มีการจัดทำรายการโปรแกรมคอมพิวเตอร์มาตรฐานที่อนุญาตให้ใช้งานและประกาศไว้บนอินทราเน็ต ซึ่งผู้ใช้งาน ผู้ดูแลระบบ และเจ้าของระบบ ต้องตรวจสอบรายการดังกล่าวอย่างสม่ำเสมอ เพื่อป้องกันมิให้มีการติดตั้งโปรแกรมคอมพิวเตอร์ที่นอกเหนือจากที่สำนักงาน กสทช. กำหนด ในกรณีที่พบการติดตั้งโปรแกรมคอมพิวเตอร์ที่ไม่ได้อยู่ในรายการจะถือเป็นความผิดส่วนบุคคล และถือว่าได้ละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช.
