(นบ.)
บันทึกเลขที่
สทช2010/215/2563

บันทึกข้อความ

หน่วยงาน สำนักเทคโนโลยีสารสนเทศ (นบ.) โทร. ๒๙๒๘, ๒๙๘๘

ที่ สทช ๒๐๑๐/ ๒๑๕ **วันที่** ๔ กุมภาพันธ์ ๒๕๖๓

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงาน กสทช. (ฉบับปรับปรุงใหม่)

เรียน ผู้อำนวยการสำนัก ผู้อำนวยการสถาบัน ผู้อำนวยการสำนักงาน กสทช. ภาค ส่วนงานเลขานุการ กสทช.

ตามอนุมัติ เลขาธิการ กสทช. ลงวันที่ ๓๑ มกราคม ๒๕๖๓ ต่อท้ายบันทึก นบ. ที่ สทช ๒๐๑๐/๑๔๗ ลงวันที่ ๒๒ มกราคม ๒๕๖๓ เรื่อง ขออนุมัติแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงาน กสทช. (ฉบับปรับปรุงใหม่) นั้น

เพื่อให้สอดคล้องและครบถ้วนตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานของรัฐ ขอให้สำนัก/ส่วนงาน ถือปฏิบัติตามประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงาน กสทช. (รายละเอียดปรากฏอยู่ในเอกสารแนบ)

จึงเรียนมาเพื่อทราบและถือปฏิบัติต่อไป จักขอบคุณยิ่ง

(นายเนติพงษ์ ตลับนาค)
อนบ.

เรียน พนักงาน ปท.๒
เพื่อทราบและถือปฏิบัติ

ปท.๒
5 ก.พ. 63.

ที่ สทช2010/215/2563
จาก (นบ.) 04 ก.พ. 2563 11:03
รับโดย (ปท.2) เลขรับ 198
04 ก.พ. 2563 14:49

(๓) ให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช. อย่างสม่ำเสมอ

(๔) ให้มีการรักษาไว้ซึ่งความลับ ความถูกต้อง ความสมบูรณ์ และความพร้อมใช้ของสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช.

ข้อ ๖ เพื่อให้การดำเนินการสอดคล้องกับแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. และสามารถปฏิบัติตามได้อย่างเป็นรูปธรรม สำนักงาน กสทช. จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. ตามแนวปฏิบัติท้ายประกาศนี้

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

ข้อ ๘ ประกาศนี้ให้สำนักงาน กสทช. ดำเนินการให้ผู้ที่เกี่ยวข้องและผู้ใช้งานทั้งหมดได้รับทราบโดยทั่วกัน พร้อมทั้งสร้างความรู้ ความเข้าใจ และจัดฝึกอบรมแก่ผู้ใช้งานเพื่อให้เกิดความตระหนักความเข้าใจถึงภัยคุกคามต่าง ๆ และผลกระทบที่เกิดจากการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

ข้อ ๙ ให้สำนักเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนแนวนโยบายและแนวปฏิบัตินี้ให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๓๑ มกราคม พ.ศ. ๒๕๖๓

(นายฐากร ตัณฑสิทธิ์)
เลขาธิการคณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

ประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช.

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ บัญญัติให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐมีหน้าที่ดำเนินมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้

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

ข้อ ๑ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๒ ให้ยกเลิกประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. ลงวันที่ ๑๒ มีนาคม ๒๕๕๘

ข้อ ๓ บรรดาหลักเกณฑ์ คำสั่ง หรือแนวปฏิบัติอื่นใดในส่วนที่ได้กำหนดไว้แล้วในประกาศนี้ หรือซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๔ ในประกาศนี้

"แนวนโยบาย" หมายความว่า หลักการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สำนักงาน กสทช. กำหนดขึ้นและประกาศใช้งาน

"แนวปฏิบัติ" หมายความว่า ข้อปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สำนักงาน กสทช. กำหนดขึ้นและประกาศใช้งาน เพื่อให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

ข้อ ๕ แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช. มีดังนี้

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

(๒) ให้มีการเตรียมความพร้อมของการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช. อย่างต่อเนื่อง โดยการจัดทำแผนและขั้นตอนการปฏิบัติงานกรณีเกิดเหตุฉุกเฉิน และการจัดให้มีระบบสำรอง ให้สามารถรับมือกับกรณีเกิดเหตุฉุกเฉินและเพื่อให้สามารถกู้คืนระบบกลับมาได้ภายในระยะเวลาที่เหมาะสม

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสทช.
พ.ศ. ๒๕๖๓

เพื่อให้การใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช. มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเชื่อถือได้ ตลอดจนดำเนินการให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ สำนักงาน กสทช. จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้ ดังต่อไปนี้

ข้อ ๑ ในแนวปฏิบัตินี้

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)" หมายความว่า ผู้บริหารระดับสูงที่เลขาธิการ กสทช. แต่งตั้งให้มีหน้าที่รับผิดชอบการบริหารงานด้านสารสนเทศและระบบเทคโนโลยีสารสนเทศ ของสำนักงาน กสทช.

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน กสทช.

"ผู้ใช้งาน" หมายความว่า บุคคลที่เข้าใช้งานระบบสารสนเทศของสำนักงาน กสทช. แต่ไม่รวมถึงบุคคลภายนอกที่เข้าใช้งานข้อมูลสาธารณะที่เผยแพร่ในเว็บไซต์ของสำนักงาน กสทช.

"ผู้ดูแลระบบ" หมายความว่า พนักงานที่มีหน้าที่ดูแลระบบสารสนเทศของสำนักงาน กสทช. หรือบุคคลที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลระบบสารสนเทศของสำนักงาน กสทช.

"ระบบสารสนเทศ" หมายความว่า เครื่องคอมพิวเตอร์แม่ข่าย เครือข่าย เครื่องคอมพิวเตอร์อุปกรณ์ และระบบหรืออุปกรณ์สนับสนุนการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย รวมถึงโปรแกรมบริหารจัดการฐานข้อมูล โปรแกรมประยุกต์ ระบบปฏิบัติการ และระบบงานต่าง ๆ ที่ใช้เทคโนโลยีสารสนเทศของสำนักงาน กสทช.

"สินทรัพย์" หมายความว่า เครื่องคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ อุปกรณ์ประกอบ ข้อมูลสารสนเทศ และอุปกรณ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศทั้งหมดที่สำนักงาน กสทช. จัดหาไว้ใช้งาน

"โปรแกรมมาตรฐาน" หมายความว่า โปรแกรมที่สำนักงาน กสทช. กำหนดให้เป็นโปรแกรมมาตรฐานสำหรับใช้งานได้ตามปกติ

"หน่วยงาน" หมายความว่า สำนัก หรือหน่วยงานภายในที่เรียกชื่ออย่างอื่นตามโครงสร้างของสำนักงาน กสทช.

"ศูนย์คอมพิวเตอร์" หมายความว่า พื้นที่ที่ใช้จัดวางเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูลภายนอก ระบบเครือข่ายคอมพิวเตอร์ และอุปกรณ์สื่อสารต่าง ๆ ของสำนักงาน กสทช. ไว้เป็นศูนย์กลางในการประมวลผลข้อมูลสารสนเทศสำหรับใช้ปฏิบัติงานของสำนักงาน กสทช.

"เครื่องคอมพิวเตอร์ส่วนตัว" หมายความว่า เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา สมาร์ทโฟน หรืออุปกรณ์คอมพิวเตอร์ที่สามารถจัดเก็บหรือประมวลผลข้อมูลได้ที่สำนักงาน กสทช. ไม่ได้เป็นผู้จัดหาไว้ใช้งาน

"อุปกรณ์คอมพิวเตอร์" หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบสารสนเทศ

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช. โดยรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ

"การรักษาความลับ (Confidentiality)" หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

"ข้อมูลสารสนเทศ" หมายความว่า ข้อมูลที่ผ่านการเลือกสรรให้เหมาะสมกับการใช้งานให้ทันเวลา ทั้งที่เก็บไว้ในรูปแบบของกระดาษ (Hardcopy) และ ไฟล์ข้อมูลอิเล็กทรอนิกส์ (Electronic file)

"เจ้าของข้อมูล" หมายความว่า พนักงานซึ่งได้รับมอบหมายจากสำนักหรือหน่วยงานภายในที่เรียกชื่ออย่างอื่น ซึ่งเป็นผู้สร้าง เปลี่ยนแปลง หรือแก้ไขข้อมูลที่เกี่ยวกับภารกิจของสำนักหรือหน่วยงานนั้น รวมทั้งให้สิทธิในการเข้าถึงข้อมูลนั้นแก่ผู้อื่น

"สื่อบันทึกข้อมูล" หมายความว่า สิ่งที่ใช้จัดเก็บข้อมูล ชุดคำสั่ง และสารสนเทศอื่น ๆ เช่น USB drive/recorder SD Memory stick เทป CD/DVD กล้อง Removable/External HD Diskette Flash memory หน่วยความจำของอุปกรณ์ Router หรือ Switch เป็นต้น

"การเข้ารหัส (Encryption)" หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

"พอร์ต (Ports)" หมายความว่า ช่องสัญญาณบนอุปกรณ์เครือข่าย เช่น บน Switch หรือ Router โดยทั่วไปช่องสัญญาณนี้สามารถใช้ในการติดต่อสื่อสารข้อมูลกับเครือข่าย คอมพิวเตอร์ และอุปกรณ์เครือข่ายต่าง ๆ โดยทั่วไปอุปกรณ์เครือข่ายจะมีช่องสัญญาณดังกล่าวจำนวนหนึ่ง นอกจากนั้นพอร์ตให้หมายถึง บริการต่าง ๆ บนเครื่อง Server ให้บริการ โดยทั่วไปบริการเหล่านี้จะได้รับการกำหนดหมายเลขเป็นหมายเลขมาตรฐาน เช่น พอร์ต ๘๐ หมายถึง บริการเว็บไวต์ซึ่งบริการข้อมูลต่างๆ บนเว็บไวต์หนึ่ง 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 หรือแทปเลต เป็นต้น

"ผู้ให้บริการภายนอก" หมายความว่า หน่วยงานภายนอกที่รับจ้างปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามความต้องการของสำนักงาน กสทช. เช่น ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการด้านฮาร์ดแวร์ ผู้ให้บริการด้านซอฟต์แวร์ ผู้ให้บริการด้านระบบงาน โดยรวมผู้ให้บริการเหล่านี้มีหน้าที่ที่จะต้องปฏิบัติตามสัญญาการให้บริการที่มีการจัดทำร่วมกันกับสำนักงาน กสทช. รวมทั้งปฏิบัติตามแนวนโยบายและแนวปฏิบัติต่างๆ ที่เกี่ยวข้องกับตนเอง

"บัญชีผู้ใช้งาน (Username)" หมายความว่า บัญชีรายชื่อของผู้ที่ได้รับสิทธิและรหัสผ่านในการใช้งานระบบสารสนเทศของสำนักงาน กสทช.

"เครือข่าย" หมายความว่า โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอกองค์กรสามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสารภายในองค์กร และโครงข่ายบนอินเทอร์เน็ตซึ่งทำให้คอมพิวเตอร์ภายในองค์กรหนึ่งสามารถติดต่อสื่อสารกับคอมพิวเตอร์ขององค์กรหนึ่งได้

"เทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network : VPN)" หมายความว่า การใช้การเข้ารหัสข้อมูล เช่น โดยผ่านทางซอฟต์แวร์หรือฮาร์ดแวร์หนึ่ง เพื่อให้การเชื่อมต่อโดยผ่านทางเครือข่ายที่ไม่ปลอดภัย เช่น อินเทอร์เน็ต เครือข่ายไร้สาย มีความมั่นคงปลอดภัย ทั้งนี้เนื่องมาจากข้อมูลจะได้รับการเข้ารหัสก่อนที่จะมีการส่งผ่านไปบนอินเทอร์เน็ตหรือเครือข่ายไร้สายนั้น เมื่อกล่าวถึง VPN จะหมายรวมถึงระบบ อุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ หรือฮาร์ดแวร์ ที่ใช้การเข้ารหัสข้อมูลก่อนส่งข้อมูลออกไป

"ข้อมูลจราจรทางคอมพิวเตอร์ (Log)" หมายความว่า ข้อมูลเหตุการณ์ต่าง ๆ ที่เกิดขึ้นบนระบบ ๆ หนึ่งและได้ถูกบันทึกไว้ในระบบนั้น เช่น ความผิดพลาดในการทำงานของระบบ ทรัพยากรระบบไม่พอ ความพยายามในการบุกรุกระบบ ข้อมูลเหตุการณ์ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดให้มีการบันทึกและจัดเก็บไว้ เป็นต้น ข้อมูลเหล่านี้สามารถใช้เพื่อตรวจ ติดตามการทำงานของระบบ เตือนว่ามีเหตุการณ์หนึ่งเกิดขึ้นแล้วในระบบ ดำเนินการเชิงป้องกันหรือแก้ไขตามความจำเป็น ซึ่งรวมถึงการใช้เป็นหลักฐานในการดำเนินการทางกฎหมาย เช่น กรณีการบุกรุกระบบ หรือกรณีการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมลซึ่งพาดพิงถึงผู้อื่นและทำให้ผู้นั้นเกิดความเสียหาย เป็นต้น

"ความเสี่ยง" หมายความว่า เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของสำนักงาน กสทช. เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้สำนักงาน กสทช. เสียชื่อเสียง

"ระบบสำรอง" หมายความว่า ระบบสำคัญที่อาจมีการติดตั้งไว้แล้วหรือจะดำเนินการติดตั้งขึ้นมาอย่างรวดเร็ว ณ ศูนย์คอมพิวเตอร์สำรอง โดยปกติจะมีการใช้ระบบสำรองก็ต่อเมื่อระบบเดียวกันที่ศูนย์คอมพิวเตอร์หลักไม่สามารถให้บริการได้ จึงเปลี่ยนมาใช้ระบบสำรองแทน

"ทรัพย์สินทางปัญญา" หมายความว่า ผลงานใด ๆ อันเกิดจากความคิดสร้างสรรค์ของมนุษย์ ทรัพย์สินทางปัญญาเป็นทรัพย์สินอีกชนิดหนึ่งที่นอกเหนือจากสังหาริมทรัพย์ และอสังหาริมทรัพย์ ทั้งนี้ประเภทของทรัพย์สินทางปัญญาประกอบด้วยลิขสิทธิ์ (Copyright) สิทธิบัตร (Patent) เครื่องหมายการค้า (Trademark) แบบผังภูมิของวงจรรวม (Layout - Designs of Integrated Circuit) ความลับทางการค้า (Trade Secrets) และสิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

"รหัสผ่าน (Password)" หมายความว่า กลุ่มชุดตัวอักษร ตัวเลข หรืออักขระพิเศษ โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตนสำหรับเข้าถึงระบบสารสนเทศ

"โปรแกรมไม่พึงประสงค์" หมายความว่า โปรแกรมที่ได้รับการติดตั้งในเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือโดยไม่รู้ตัว อาจก่อให้เกิดความเสียหายต่อข้อมูลในเครื่องคอมพิวเตอร์ อาจสร้างความรำคาญ ทำงานช้า ทำงานผิดปกติ หรือทำงานในลักษณะที่ไม่เป็นประโยชน์ ไม่สร้างสรรค์ หรือไม่เป็นผลดีต่อเครื่องคอมพิวเตอร์นั้น โปรแกรมที่ทำงานในลักษณะดังกล่าวอย่างน้อยให้หมายความรวมถึง

(๑) โปรแกรมที่สามารถสำเนาตัวเองและแพร่กระจายผ่านทางสื่อบันทึกข้อมูลเพื่อข้ามไปยังเครื่องคอมพิวเตอร์อื่น กล่าวคือ เมื่อมีการใช้สื่อบันทึกข้อมูลดังกล่าวกับเครื่องคอมพิวเตอร์หนึ่ง โปรแกรมดังกล่าวก็จะแพร่กระจายหรือติดไปยังเครื่องคอมพิวเตอร์นั้น

(๒) โปรแกรมที่สามารถสำเนาตัวเองข้ามหรือแพร่กระจายไปยังเครื่องคอมพิวเตอร์ปลายทางหนึ่งเครื่องหรือมากกว่าหนึ่งเครื่องก็ได้ เครื่องคอมพิวเตอร์ปลายทางที่ได้รับการแพร่ระบาดนั้นก็สามารถสำเนาและแพร่กระจายตัวเองได้ต่อไป โปรแกรมที่แพร่กระจายในลักษณะดังกล่าวมีชื่อเรียกกันว่า หนอนเครือข่าย (Worm)

(๓) โปรแกรมที่เคลื่อนที่จากเครื่องคอมพิวเตอร์อื่นมายังเครื่องคอมพิวเตอร์ของผู้ใช้งาน หรือที่เรียกกันว่า Mobile Code เช่น โปรแกรมที่เขียนด้วย Java Script หรือ Active X เป็นต้น และถูกสั่งให้ทำงานในเครื่องของผู้ใช้งานนั้น โปรแกรมประเภทนี้อาจฝังตัวอยู่กับโปรแกรมอื่นแต่ถูกเรียกทำงานร่วมกัน เช่น กรณีของการเข้าถึงโปรแกรมบนเว็บไซต์หนึ่งซึ่งมีการเรียกใช้ Java Script ด้วย ก็จะทำให้ Java Script นั้นถูกโอนย้ายเข้ามาและสั่งทำงานบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน เป็นต้น

"จดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail)" หมายความว่า ข้อความอิเล็กทรอนิกส์ที่มีการส่งผ่านระบบเทคโนโลยีสารสนเทศและอินเทอร์เน็ตจากผู้ส่งไปยังผู้รับ ซึ่งมีความหมายตรงกับคำในภาษาอังกฤษว่า Electronic Mail หรือ E-mail ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP POP๓ หรือ IMAP เป็นต้น

"สแปมเมล (Spam Mail)" หมายความว่า จดหมายอิเล็กทรอนิกส์ที่ไม่เป็นประโยชน์หรือไม่เป็นที่ต้องการของผู้รับ

"อีเมลลูกโซ่ (Chain Letter)" หมายความว่า จดหมายอิเล็กทรอนิกส์ที่มีข้อความในลักษณะที่ต้องการให้ผู้รับส่งต่อข้อความนั้นไปเรื่อย ๆ แบบไม่รู้จบเพื่อให้ข้อความดังกล่าวแพร่กระจายออกไปในวงกว้าง โดยที่ข้อความอาจจะเป็นจริงหรือไม่ก็ตาม

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

"ระดับความเสี่ยงที่ยอมรับได้" หมายความว่า ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่งมีค่าน้อยกว่าค่าที่ยอมรับได้นี้จะถือว่าสินทรัพย์สารสนเทศที่เกี่ยวข้องกับเหตุการณ์ มีความความมั่นคงปลอดภัยด้านสารสนเทศเพียงพอ

"แผนการลดความเสี่ยง" หมายความว่า แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาอนุมัติการดำเนินการ

"บุคคล" หมายความว่า บุคคลธรรมดา

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"เจ้าของข้อมูลส่วนบุคคล" หมายความว่า บุคคลผู้เป็นเจ้าของข้อมูลนั้น ผู้แทนโดยชอบธรรม ผู้อนุบาล หรือผู้พิทักษ์ ของเจ้าของข้อมูลส่วนบุคคลที่มีอายุไม่ถึงแปดปีบริบูรณ์

"ไซเบอร์" หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

"ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง

ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่มีความเกี่ยวข้องกับข้อมูลสารสนเทศขององค์กร

"การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อรักษาไว้ซึ่งความลับ ความถูกต้อง ความพร้อมใช้ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อองค์กร

"โปรแกรมอรรถประโยชน์" หมายความว่า โปรแกรมประเภทหนึ่งที่ทำงานบนระบบปฏิบัติการคุณสมบัติการใช้งานนั้นค่อนข้างหลากหลาย ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์ ช่วยสนับสนุน เพิ่ม หรือขยายขีดความสามารถของโปรแกรมที่ใช้งานให้มีประสิทธิภาพมากขึ้น

หมวด ๑
แนวปฏิบัติของผู้ดูแลระบบ

ข้อ ๒ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

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

๒.๒ พิจารณาอนุมัติและกำหนดสิทธิการเข้า-ออก ศูนย์คอมพิวเตอร์ให้เป็นไปตามภารกิจของแต่ละหน่วยงานที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเท่านั้น

๒.๓ ต้องทำการยืนยันตัวตนก่อนเข้าศูนย์คอมพิวเตอร์ทุกครั้งเพื่อป้องกันการเข้า-ออกโดยไม่ได้รับอนุญาต

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

๒.๕ ควบคุมให้ผู้เข้า-ออกติดบัตรแสดงตัวตนให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ศูนย์คอมพิวเตอร์

๒.๖ ดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอก (Visitors) ในขณะที่ปฏิบัติงานในศูนย์คอมพิวเตอร์จนกระทั่งเสร็จสิ้นภารกิจและออกจากศูนย์คอมพิวเตอร์ เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๒.๗ แยกพื้นที่ในการส่งมอบสินทรัพย์ เพื่อตรวจสอบให้เสร็จเรียบร้อยก่อนนำเข้าไปติดตั้งหรือใช้งานภายในศูนย์คอมพิวเตอร์

๒.๘ ประชาสัมพันธ์มาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์ แก่ผู้ใช้งานและบุคคลภายนอก (Visitors)

๒.๙ ห้ามนำอาหารและเครื่องดื่มเข้าไปภายในศูนย์คอมพิวเตอร์

๒.๑๐ ห้ามสูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงในบริเวณภายในศูนย์คอมพิวเตอร์

๒.๑๑ ต้องทำการยกเลิก เพิกถอน หรือเปลี่ยนแปลงการอนุญาตการเข้า-ออกศูนย์คอมพิวเตอร์ของผู้ใช้งานเมื่อมีการออกจากงาน สิ้นสุดการจ้าง เปลี่ยนตำแหน่ง โอน หรือย้ายหน่วยงานสังกัด

๒.๑๒ ทบทวนสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญภายในศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ หรืออย่างน้อยปีละหนึ่งครั้ง

ข้อ ๓ การกำหนดการจัดวางและป้องกันระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๓.๑ จัดวางระบบสารสนเทศที่มีความสำคัญในพื้นที่ที่มีความมั่นคงและปลอดภัย เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงพอร์ตของระบบที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๓.๒ แยกจัดเก็บระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ที่สำคัญไว้ในพื้นที่ความปลอดภัยสูงแยกต่างหาก

ข้อ ๔ การกำหนดและควบคุมการเดินสายสัญญาณสื่อสาร และสายไฟฟ้า ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๔.๑ ควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้าให้เป็นไปด้วยความเรียบร้อยและปลอดภัย

๔.๒ ควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการรบกวนของสัญญาณ

๔.๓ ทำแผนผังการเดินสายสัญญาณสื่อสารและสายไฟฟ้าให้ครบถ้วนและถูกต้อง

๔.๔ ปิดประตูตู้ Rack สำหรับติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณสื่อสาร ให้สนิทรวมถึงการล็อคประตูเพื่อป้องกันการเข้าถึงของบุคคลที่ไม่เกี่ยวข้อง

๔.๕ จัดทำป้ายชื่อสำหรับสายสัญญาณสื่อสารและบนอุปกรณ์เพื่อป้องกันการปฏิบัติงานผิดพลาด

๔.๖ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อความถูกต้องและตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๕ การกำหนดการบำรุงรักษาระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๕.๑ จัดทำสัญญาการบำรุงรักษาสำหรับระบบและอุปกรณ์คอมพิวเตอร์ที่มีความสำคัญ

๕.๒ กำหนดเงื่อนไขของการให้บริการในสัญญาการบำรุงรักษาให้ชัดเจนเพื่อให้ผู้รับจ้างต้องติดต่อกลับและเข้ามาดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในระยะเวลาที่เหมาะสม

๕.๓ ตรวจสอบและกำหนดให้มีการรับประกันความเสียหายของระบบสารสนเทศ

๕.๔ บำรุงรักษาระบบสารสนเทศตามรอบระยะเวลาที่กำหนดไว้ในสัญญาการบำรุงรักษา

๕.๕ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๕.๖ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๕.๗ บันทึกปัญหาและข้อบกพร่องที่พบ และรายงานผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทราบ

๕.๘ ควบคุม และดูแลการปฏิบัติงานของผู้ให้บริการภายนอกให้ปฏิบัติตามสัญญาการจ้างเหมาบำรุงรักษา

๕.๙ กำหนดสิทธิของผู้ให้บริการภายนอกในการเข้าถึงพื้นที่ อุปกรณ์ และข้อมูลที่สำคัญ

ข้อ ๖ การบริหารจัดการสินทรัพย์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๖.๑ บันทึกและตรวจสอบสินทรัพย์ เพื่อเก็บเป็นหลักฐานในการตรวจสอบความถูกต้องและป้องกันการสูญหาย

๖.๒ กำหนดมาตรการหรือเทคนิคในการทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะจำหน่ายหรือนำกลับมาใช้งานใหม่ทุกครั้ง เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

๖.๓ กรณีที่สินทรัพย์เกิดความเสียหายและต้องส่งซ่อม ให้ควบคุมการส่งออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กรณีสินทรัพย์เป็นข้อมูลสำคัญต้องทำการทำลายข้อมูลทิ้งเพื่อไม่ให้ผู้อื่นสามารถเข้าถึงได้

ข้อ ๗ การควบคุมการใช้งานสารสนเทศและบริหารจัดการอุปกรณ์คอมพิวเตอร์แบบพกพา ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๗.๑ ต้องนำอุปกรณ์คอมพิวเตอร์แบบพกพาส่วนตัว หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของสำนักงาน กสทช. ที่ได้รับอนุมัติจากผู้บังคับบัญชาให้เชื่อมต่อระบบเครือข่ายภายในและเข้าถึงระบบสารสนเทศของสำนักงาน กสทช. แจ้งขึ้นทะเบียนอุปกรณ์คอมพิวเตอร์แบบพกพาที่สำนักเทคโนโลยีสารสนเทศ และปฏิบัติตามขั้นตอนปฏิบัติที่สำนักเทคโนโลยีสารสนเทศกำหนด เพื่อป้องกันการเข้าถึงระบบสารสนเทศด้วยอุปกรณ์คอมพิวเตอร์แบบพกพาโดยไม่ได้รับอนุญาต

๗.๒ ต้องกำหนดมาตรการระบุและพิสูจน์ตัวตนก่อนเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาด้วย บัญชีผู้ใช้งานและรหัสผ่าน หรือเทคโนโลยีไบโอเมตริก (biometric) หรือ PIN CODE เพื่อป้องกันการเข้าถึงจากผู้อื่นและระมัดระวังมิให้ผู้อื่นเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาของตน

๗.๓ ต้องดูแลรักษาข้อมูลองค์กรในอุปกรณ์คอมพิวเตอร์แบบพกพาให้สอดคล้องตามข้อกำหนดการบริหารจัดการข้อมูลองค์กร

๗.๔ ต้องแจ้งผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทันทีที่พบว่าอุปกรณ์คอมพิวเตอร์เสียหาย สูญหาย หรือเปลี่ยนเครื่องใหม่ เพื่อจัดการเหตุการณ์ได้อย่างมีประสิทธิภาพ

ข้อ ๘ การควบคุมการใช้งานสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๘.๑ การอนุมัติและกำหนดสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานให้เป็นไปตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาแล้วเท่านั้น

๘.๒ กำหนดการเข้าถึงด้วยบัญชีผู้ใช้งานแยกเป็นรายบุคคลตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานที่ผู้ใช้งานปฏิบัติงาน

๘.๓ จัดเก็บข้อมูลการลงทะเบียนสำหรับสร้างบัญชีผู้ใช้งานไว้เพื่อการตรวจสอบในภายหลัง

๘.๔ กำหนดให้ทำการยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าถึงระบบสารสนเทศ

๘.๕ กำหนดระยะเวลาการออกจากระบบสารสนเทศโดยอัตโนมัติเมื่อไม่มีการใช้งานเกินสามสิบนาที หรือตามความสำคัญของข้อมูลสารสนเทศ

๘.๖ กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศที่สำคัญของสำนักงาน กสทช. ตามภารกิจและความจำเป็นของผู้ใช้งาน

๘.๗ กำหนดให้เครื่องคอมพิวเตอร์ที่จัดหาโดยสำนักงาน กสทช. พักหน้าจอ (Screen saver) โดยอัตโนมัติ หากไม่มีการใช้งานเครื่องคอมพิวเตอร์ติดต่อกันสิบห้านาที

๘.๘ จำกัดระยะเวลาในการเชื่อมต่อ (Limitation of Connection Time) ระบบสารสนเทศ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๘.๙ จำกัดและควบคุมการเข้าถึงฟังก์ชั่น (Functions) ต่าง ๆ ในการใช้งานระบบสารสนเทศของผู้ใช้งานและผู้ดูแลระบบ

๘.๑๐ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสำนักงาน กสทช. ต้องแยกเครือข่ายออกจากระบบอื่น ๆ ต้องมีการควบคุมสภาพแวดล้อมแยกเป็นสัดส่วน และต้องกำหนดสิทธิการใช้งานเฉพาะผู้ที่มีสิทธิเท่านั้น

๘.๑๑ จัดทำระบบบริหารจัดการรหัสผ่านเชิงโต้ตอบสำหรับการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย โดยผู้ใช้งานกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยตามการบริหารจัดการบัญชีผู้ใช้งาน (User Account) ด้วยตนเอง

๘.๑๒ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งานต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อมีการออกจากงาน หรือสิ้นสุดการจ้าง หลังจากได้รับแจ้งจากสำนักทรัพยากรบุคคล

๘.๑๓ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งาน กรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งาน

๘.๑๔ ดำเนินการทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ หรืออย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงเพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๙ การบริหารจัดการความปลอดภัยเครือข่าย ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๙.๑ กำหนดวิธีปฏิบัติเกี่ยวกับการใช้งานเครือข่ายทั้งภายในและภายนอกสำนักงาน กสทช.

๙.๒ กำหนดขั้นตอนการขออนุญาตเพื่อเข้าถึงระบบสารสนเทศที่อยู่ภายในเครือข่ายของสำนักงาน กสทช.

๙.๓ กำหนดขั้นตอนการเชื่อมต่อระบบเครือข่ายจากผู้ใช้งานภายนอกสำนักงาน กสทช. อย่างมั่นคงปลอดภัย เช่น การเชื่อมต่อระบบเครือข่ายด้วยเทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network : VPN)

๙.๔ ระบุบริการที่สำนักงาน กสทช. อนุญาตให้ใช้งานหรือบริการผ่านระบบเครือข่ายของสำนักงาน กสทช.

๙.๕ กำหนดให้มีการระบุและพิสูจน์ตัวตนในการเข้าถึงระบบสารสนเทศของสำนักงาน กสทช.

๙.๖ จัดทำทะเบียนอุปกรณ์ที่ใช้งานในระบบเครือข่ายโดยอย่างน้อยประกอบด้วยข้อมูล หมายเลขประจำเครื่อง ตราอักษร แบบรุ่น หมายเลข Mac Address หมายเลข IP Address ที่มา ผู้รับผิดชอบ วันที่เริ่มติดตั้ง วันที่เลิกใช้งาน และเหตุผลที่เลิกใช้งาน

๙.๗ ใช้ข้อมูล MAC Address หรือ IP Address เป็นข้อมูลในการระบุอุปกรณ์บนเครือข่ายเพื่อบ่งชี้อุปกรณ์ที่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่ายของสำนักงาน กสทช. และใช้วิธีการทางเทคนิคที่เหมาะสมเพื่อควบคุมการเข้าถึงอุปกรณ์เครือข่ายเหล่านั้น

๙.๘ กำหนดให้เฉพาะเครื่องคอมพิวเตอร์ของผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถเชื่อมต่อเครือข่ายเพื่อบริหารจัดการระบบและอุปกรณ์เครือข่ายของสำนักงาน กสทช.

๙.๙ ตรวจสอบและปิดพอร์ตบนระบบและอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๙.๑๐ ป้องกันและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการบริหารจัดการอุปกรณ์ในระบบเครือข่ายทั้งจากภายในและภายนอกสำนักงาน กสทช.

๙.๑๑ จัดแบ่งเครือข่ายตามวัตถุประสงค์การใช้งาน บริการ หรือกลุ่มผู้ใช้งาน เช่น เครือข่ายสำหรับผู้ใช้งาน เครือข่ายสำหรับเครื่องแม่ข่าย หรือเครือข่ายสำหรับทดสอบทดลองระบบ เป็นต้น

๙.๑๒ ใช้วิธีการทางเทคนิคบนไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่น ๆ จำกัดเส้นทางบนเครือข่ายที่สำนักงาน กสทช. ไม่อนุญาตให้ใช้งาน เพื่อกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะเส้นทางบนเครือข่ายที่อนุญาตเท่านั้น

๙.๑๓ กำหนดมาตรการป้องกันระบบสารสนเทศที่ต้องเชื่อมโยงกับระบบเครือข่ายสาธารณะอย่างมีประสิทธิภาพ

๙.๑๔ กำหนดมาตรการป้องกันข้อมูลที่ส่งผ่านทางเครือข่ายสาธารณะเพื่อรักษาความลับและความถูกต้องของข้อมูลที่สำคัญ

๙.๑๕ กำหนดเส้นทางบนเครือข่ายที่เหมาะสมเพื่อควบคุมการเชื่อมต่อและการไหลเวียนของสารสนเทศบนเครือข่ายให้มีประสิทธิภาพ

๙.๑๖ ตรวจสอบการใช้งานระบบเครือข่ายด้วยระบบตรวจจับและป้องกันการบุกรุกของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติอย่างสม่ำเสมอ หรืออย่างน้อยเดือนละหนึ่งครั้ง

๙.๑๗ ทดสอบความมั่นคงปลอดภัยของระบบเครือข่ายอย่างน้อยปีละหนึ่งครั้ง หรือตามสถานการณ์ของภัยคุกคามทางไซเบอร์ในระบบเครือข่าย และนำผลที่ได้ไปปรับปรุงความมั่นคงปลอดภัยระบบเครือข่ายของสำนักงาน กสทช. ให้มีความมั่นคงปลอดภัยมากขึ้นและทันต่อภัยคุกคามทางไซเบอร์ในปัจจุบัน

๙.๑๘ ติดตาม ตรวจสอบ ดูแล และปรับปรุงเครือข่ายของสำนักงาน กสทช. ให้มีความมั่นคงปลอดภัยและทันสมัยอยู่เสมอ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานระบบเครือข่ายให้รีบดำเนินการแก้ไขและแจ้งผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทันทีเพื่อป้องกันหรือบรรเทาความเสียหายที่อาจจะเกิดขึ้น

๙.๑๙ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งาน ต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อมีการออกจากงาน หรือสิ้นสุดการจ้าง หลังจากได้รับแจ้งจากสำนักทรัพยากรบุคคล

๙.๒๐ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งาน กรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งาน

๙.๒๑ ดำเนินการทบทวนสิทธิการเข้าถึงเครือข่ายของผู้ใช้งานอย่างสม่ำเสมอ หรืออย่างน้อยปีละหนึ่งครั้งเพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต

ข้อ ๑๐ การบริหารจัดการในการปฏิบัติงาน ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๐.๑ ไม่นำข้อมูลสารสนเทศของสำนักงาน กสทช. ไปเปิดเผยกับบุคคลซึ่งไม่ได้มีความเกี่ยวข้องกับการปฏิบัติหน้าที่เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๑๐.๒ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งาน

๑๐.๓ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) เท่าที่จำเป็นตามที่กำหนดไว้ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑๐.๔ ตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดในสำนักงาน กสทช. ให้ตรงกับเวลาอ้างอิงสากล (Stratum ๐)

๑๐.๕ บันทึกข้อมูลกิจกรรมการใช้งานระบบสารสนเทศและระบบเครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๑๐.๖ ตรวจสอบและดูแลสภาพแวดล้อมของศูนย์คอมพิวเตอร์ รวมทั้งระบบสนับสนุนการทำงานต่าง ๆ เพื่อป้องกันความเสียหายต่อระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ

๑๐.๗ จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับเครื่องคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยด้านสารสนเทศของระบบได้ ดังนั้น เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยด้านสารสนเทศที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดการอนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้ง

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากเครื่องคอมพิวเตอร์

ข้อ ๑๑ การสำรองและกู้คืนข้อมูลสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๑.๑ กำหนดขั้นตอนการสำรองและกู้คืนข้อมูลรวมถึงซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดระบบสารสนเทศสำคัญที่จำเป็นต้องสำรองข้อมูลไว้

(๒) ชื่อระบบสารสนเทศ

(๓) ผู้รับผิดชอบในการสำรองข้อมูล

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

(๕) ความถี่ในการสำรองข้อมูล

(๖) วิธีการสำรองข้อมูล

(๗) สื่อที่ใช้บันทึก

๑๑.๒ สำรองข้อมูลตามขั้นตอนและความถี่ที่กำหนดไว้ในแต่ละระบบ

๑๑.๓ ตรวจสอบผลสำเร็จของการสำรองข้อมูลทุกครั้ง

๑๑.๔ เลือกใช้สื่อที่เหมาะสม โดยมีอายุจัดเก็บตามระยะเวลาที่กำหนด

๑๑.๕ นำข้อมูลสำรองไปเก็บไว้นอกสถานที่อย่างน้อยหนึ่งชุด

๑๑.๖ สุ่มข้อมูลสำรองมาทดสอบกู้คืนเพื่อตรวจสอบความถูกต้องและความพร้อมใช้งานของข้อมูลในกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละหนึ่งครั้ง

๑๑.๗ ทบทวนขั้นตอนการสำรองและกู้คืนข้อมูลและประเมินประสิทธิผลการดำเนินการอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๑๒ การบริหารความต่อเนื่องทางธุรกิจ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๒.๑ กำหนดระบบสารสนเทศสำคัญที่จำเป็นต้องเตรียมการกู้คืนระบบ

๑๒.๒ ประเมินผลกระทบกรณีระบบสารสนเทศสำคัญเกิดการหยุดชะงักหรือไม่สามารถให้บริการได้

๑๒.๓ ประเมินความเสี่ยงระบบสารสนเทศสำคัญ โดยพิจารณาจากกระบวนการดำเนินงาน การวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุเหตุการณ์ที่สามารถทำให้บริการระบบสารสนเทศสำคัญหยุดชะงักหรือไม่สามารถให้บริการได้ กำหนดแผนการลดความเสี่ยง และจัดการกับความเสี่ยงเหล่านั้น ทั้งนี้กำหนดให้มีการทบทวนความเสี่ยงและผลกระทบทางธุรกิจอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงสำคัญ หรืออย่างน้อยปีละหนึ่งครั้ง

๑๒.๔ กำหนดกรอบการดำเนินการในการวางแผนการบริหารความต่อเนื่องทางธุรกิจ ให้มีองค์ประกอบดังนี้

(๑) ขั้นตอนการเตรียมการ คือ รายละเอียดของขั้นตอนต่าง ๆ ที่ต้องทำก่อนเริ่มดำเนินการตามแผน

(๒) ขั้นตอนกรณีฉุกเฉิน คือ การปฏิบัติในกรณีฉุกเฉินเมื่อเกิดเหตุการณ์คุกคามการให้บริการความมั่นคงปลอดภัย หรือชีวิต

(๓) ขั้นตอนการฟื้นฟู คือ สิ่งที่ต้องดำเนินการเพื่อฟื้นฟูกระบวนการและบริการที่มีความสำคัญ

(๔) ขั้นตอนการดำเนินงานต่อไป คือ รายละเอียดเกี่ยวกับขั้นตอนที่ต้องดำเนินการเพื่อกลับคืนสู่การดำเนินงานตามปกติ

๑๒.๕ จัดทำแผนการบริหารความต่อเนื่องทางธุรกิจ โดยอ้างอิงจากมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ซึ่งมีรายละเอียดอย่างน้อยดังนี้

(๑) ลำดับของผู้มีอำนาจในการสั่งการใช้แผนกู้คืนระบบ

(๒) โครงสร้างของทีมกู้คืนระบบ

(๓) รายชื่อและข้อมูลติดต่อของทีมกู้คืนระบบ

(๔) การสั่งการใช้แผนกู้คืนระบบ

(๕) การสั่งย้ายสถานที่ปฏิบัติงานไปยังศูนย์คอมพิวเตอร์สำรอง

(๖) การเก็บรวบรวมเอกสารและอุปกรณ์ที่จำเป็นเพื่อนำไปใช้งานยังศูนย์คอมพิวเตอร์สำรอง

(๗) การเตรียมความพร้อมของศูนย์คอมพิวเตอร์สำรอง (ก่อนเปิดใช้งานกรณีที่ศูนย์คอมพิวเตอร์หลักไม่สามารถใช้งานได้)

(๘) การแจ้งข้อมูลเกี่ยวกับเหตุการณ์ฉุกเฉินให้ผู้ให้บริการภายนอกได้รับทราบ

(๙) การเริ่มต้นปฏิบัติงาน ณ ศูนย์คอมพิวเตอร์สำรอง

(๑๐) การกลับคืนสู่สภาวะการทำงานตามปกติ (ภายหลังจากที่ได้แก้ไขสถานการณ์ของศูนย์คอมพิวเตอร์หลักแล้ว)

(๑๑) ให้ความรู้แก่ผู้ที่เกี่ยวข้องทั้งหมดทั้งทีมกู้คืนระบบและผู้ให้บริการภายนอกเพื่อให้สามารถปฏิบัติได้อย่างถูกต้องเมื่อมีเหตุฉุกเฉินเกิดขึ้น

๑๒.๖ จัดทำแผนการทดสอบการกู้คืนระบบ และดำเนินการทดสอบตามแผนการทดสอบ บันทึกผล สรุปผลและข้อเสนอแนะ พร้อมทั้งติดตามข้อบกพร่องที่พบในระหว่างการทดสอบเพื่อให้มีการปรับปรุงประสิทธิภาพต่อไปอย่างน้อยปีละหนึ่งครั้ง

๑๒.๗ ทบทวนแผนการบริหารความต่อเนื่องทางธุรกิจ โดยคำนึงถึงเหตุการณ์ในปัจจุบันและประสิทธิภาพของการปฏิบัติงานเป็นสำคัญอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๑๓ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๓.๑ เสนอให้สำนักงาน กสทช. แต่งตั้งและแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๑๓.๒ ต้องปฏิบัติตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด

๑๓.๓ จัดให้มีกระบวนการในการบ่งชี้ ป้องกัน ตรวจสอบ รับมือ และกู้คืนต่อภัยคุกคามทางไซเบอร์ของสำนักงาน กสทช. อย่างเป็นระบบ รวมทั้งกระบวนการในการแจ้งเหตุและประสานงานกับหน่วยงานต่าง ๆ ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒ กำหนด

๑๓.๔ จัดให้มีการประเมินความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ และจัดทำแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์ พร้อมพิจารณาทบทวนอย่างน้อยปีละหนึ่งครั้ง

๑๓.๕ จัดให้มีการซักซ้อมแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่สอดคล้องกับบริบทในปัจจุบันหรือตามสถานการณ์ที่ได้ประเมินความเสี่ยงไว้ และนำผลที่ได้จากการซักซ้อมมาแก้ไขปรับปรุงแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างน้อยปีละหนึ่งครั้ง

๑๓.๖ จัดให้มีการอบรม ประชาสัมพันธ์ หรือสื่อสารเพื่อสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์กับผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ

๑๓.๗ ส่งเสริมและสนับสนุนให้ผู้ดูแลระบบได้รับการอบรมเพิ่มพูนความรู้ความเข้าใจและทักษะในการจัดการและรักษาความมั่นคงปลอดภัยทางไซเบอร์

ข้อ ๑๔ การคุ้มครองข้อมูลส่วนบุคคล ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๔.๑ ในกรณีที่หน่วยงานจะต้องมีการร้องขอข้อมูลส่วนบุคคลเพื่อประกอบการดำเนินงาน หน่วยงานนั้นต้องทำการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการจัดเก็บและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลนั้น รวมทั้งจัดเก็บข้อมูลการให้ความยินยอมนั้นไว้เป็นหลักฐาน

๑๔.๒ ข้อมูลส่วนบุคคลที่สำนักงาน กสทช. มีการจัดเก็บต้องจัดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตามมาตรการหรือประกาศที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กำหนด

๑๔.๓ จัดทำและประกาศใช้นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและดำเนินการตามนโยบายและแนวปฏิบัติดังกล่าวอย่างเคร่งครัด รวมทั้งจัดให้มีกระบวนการบริหารจัดการเพื่อรองรับสิทธิของผู้เป็นเจ้าของข้อมูลส่วนบุคคลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนด

๑๔.๔ จัดให้มีกระบวนการในการจัดการและแจ้งเหตุในกรณีที่ข้อมูลส่วนบุคคลถูกละเมิดความมั่นคงปลอดภัย ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลรับทราบภายในระยะเวลาเจ็ดสิบสองชั่วโมงนับแต่เกิดเหตุ

ข้อ ๑๕ การปฏิบัติตามกฎหมาย และมาตรฐานสากล ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๕.๑ ปฏิบัติตามกฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๕.๒ ตรวจสอบและควบคุมมิให้มีการละเมิดทรัพย์สินทางปัญญาด้านเทคโนโลยีสารสนเทศ

๑๕.๓ ตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงาน กสทช. ตามระยะเวลาที่เหมาะสม

๑๕.๔ จัดให้มีการอบรมสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งานอย่างน้อยปีละหนึ่งครั้ง

๑๕.๕ ประชาสัมพันธ์ หรือสื่อสารเพื่อสร้างความตระหนักรู้กฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายผ่านทางระบบอินทราเน็ตของสำนักงาน กสทช. หรือช่องทางที่เหมาะสม

หมวด ๒
แนวปฏิบัติของผู้ใช้งาน

ข้อ ๑๖ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๖.๑ ปฏิบัติตามมาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์อย่างเคร่งครัด

๑๖.๒ ติดบัตรแสดงตัวตนให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ศูนย์คอมพิวเตอร์

๑๖.๓ ทำการยืนยันตัวตนก่อนเข้าศูนย์คอมพิวเตอร์ทุกครั้ง

๑๖.๔ ลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ศูนย์คอมพิวเตอร์ในสมุดลงชื่อให้ชัดเจนทุกครั้ง

๑๖.๕ ไม่นำอาหารและเครื่องดื่มเข้าไปภายในศูนย์คอมพิวเตอร์

๑๖.๖ ไม่สูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงในบริเวณภายในศูนย์คอมพิวเตอร์

ข้อ ๑๗ การบริหารจัดการสินทรัพย์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๗.๑ ดูแลรักษาสินทรัพย์ที่สำนักงาน กสทช. มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของตนเอง

๑๗.๒ ห้ามทิ้งสินทรัพย์ของสำนักงาน กสทช. ไว้โดยไม่มีผู้ดูแล ซึ่งรวมถึงการทิ้งไว้ในรถยนต์ที่สามารถมองเห็นได้จากภายนอก

๑๗.๓ ห้ามให้ผู้อื่นยืมสินทรัพย์ของสำนักงาน กสทช. ไปใช้งาน เช่น เพื่อน พี่น้อง หรือญาติ

๑๗.๔ ใช้งานสินทรัพย์และระบบสารสนเทศต่าง ๆ ในการปฏิบัติงานของสำนักงาน กสทช. เท่านั้น

๑๗.๕ แจ้งสำนักเทคโนโลยีสารสนเทศก่อนดำเนินการเปลี่ยนจุดติดตั้งหรือส่งซ่อมสินทรัพย์

๑๗.๖ ส่งคืนสินทรัพย์ให้เจ้าหน้าที่ผู้รับผิดชอบของสำนักเทคโนโลยีสารสนเทศเมื่อผู้ใช้งานต้องการยกเลิกสิทธิการครอบครองสินทรัพย์นั้น ๆ หรือพ้นสภาพการเป็นผู้ปฏิบัติงานของสำนักงาน กสทช.

๑๗.๗ ต้องดำเนินการป้องกันการเข้าถึงเครื่องคอมพิวเตอร์ส่วนตัวเมื่อนำมาใช้งานภายในเครือข่ายสำนักงาน กสทช.

๑๗.๘ จัดวางสินทรัพย์ต่าง ๆ ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

๑๗.๙ ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้บริการตลอดยี่สิบสี่ชั่วโมง

๑๗.๑๐ ให้ผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศอนุมัติก่อนทุกครั้งในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกสำนักงาน กสทช.

๑๗.๑๑ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่สำนักงาน กสทช. ได้ติดตั้งไว้ให้ใช้งาน

๑๗.๑๒ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้งานการตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง

๑๗.๑๓ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้นหรือเครือข่ายของหน่วยงานได้

๑๗.๑๔ ต้องแจ้งผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทันทีที่พบว่าสินทรัพย์เสียหาย สูญหาย หรือปรากฏว่ามีผู้อื่นเข้าถึงสินทรัพย์ดังกล่าว โดยที่ผู้ใช้งานมิได้อนุญาต เพื่อจัดการเหตุการณ์ได้อย่างมีประสิทธิภาพ

ข้อ ๑๘ การบริหารจัดการบัญชีผู้ใช้งาน (User Account) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๘.๑ เปลี่ยนรหัสผ่านทันทีหลังจากได้รับแจ้งจากผู้ดูแลระบบ

๑๘.๒ กำหนดรหัสผ่าน (Password) ตามหลักเกณฑ์ดังนี้

(๑) รหัสผ่านต้องประกอบด้วยตัวอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และตัวอักขระพิเศษ ผสมกันไม่น้อยกว่า ๘ ตัว เช่น Yr!S๒๐๑๙

(๒) ไม่ตั้งรหัสผ่านด้วยข้อมูลที่เกี่ยวข้องกับตนเอง เช่น ชื่อตนเองหรือครอบครัว ชื่อเล่น วันเดือนปีเกิด หรือทะเบียนรถยนต์

(๓) ไม่ตั้งรหัสผ่านด้วยคำศัพท์ที่มีอยู่ในพจนานุกรม

๑๘.๓ เก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน ของตนเองเป็นความลับ ไม่เผยแพร่ ไม่แจกจ่าย ไม่ใช้ร่วมกับผู้อื่น หรือทำให้ผู้อื่นล่วงรู้

๑๘.๔ รับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีผู้ใช้งานไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๑๘.๕ ไม่จดหรือบันทึกบัญชีผู้ใช้งานไว้ในสถานที่ที่ง่ายต่อการคาดเดาหรือสังเกตเห็นของบุคคลอื่น

๑๘.๖ ควรปิดการใช้งาน (Lock) เครื่องคอมพิวเตอร์ทุกครั้งเมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์

๑๘.๗ เปลี่ยนรหัสผ่านทันทีเมื่อคาดว่ามีการล่วงรู้รหัสผ่านจากบุคคลอื่น

๑๘.๘ ไม่ใช้รหัสผ่านซึ่งเคยใช้มาแล้ว (Password History) อย่างน้อยสามรหัสผ่านที่เคยใช้งานล่าสุด

๑๘.๙ ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยจำรหัสผ่านโดยอัตโนมัติ

๑๘.๑๐ แจ้งผู้ดูแลระบบทันทีหากไม่สามารถใช้งานบัญชีผู้ใช้งานได้

๑๘.๑๑ กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจออัตโนมัติหากไม่มีการใช้งานเครื่องคอมพิวเตอร์ติดต่อกันสิบห้านาที โดยให้ป้อนชื่อผู้ใช้งาน และรหัสผ่านอีกครั้งก่อนใช้งาน

ข้อ ๑๙ การบริหารจัดการความปลอดภัยเครือข่ายของสำนักงาน กสทช. ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๙.๑ ต้องใช้บริการสารสนเทศผ่านระบบเครือข่ายตามที่สำนักงาน กสทช. กำหนดไว้เท่านั้น

๑๙.๒ ลงทะเบียนคำขอใช้งานและต้องได้รับอนุญาตจากผู้บังคับบัญชาและผู้อำนวยการสำนักเทคโนโลยีสารสนเทศก่อนการเข้าถึงเครือข่ายภายในสำนักงาน กสทช. ด้วยเครื่องคอมพิวเตอร์ส่วนตัว

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

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

ข้อ ๒๐ การใช้งานอุปกรณ์คอมพิวเตอร์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๐.๑ อุปกรณ์คอมพิวเตอร์ที่สำนักงาน กสทช. จัดไว้ให้ใช้งานถือเป็นทรัพย์สินของสำนักงาน กสทช. และมีวัตถุประสงค์เพื่อใช้ในการดำเนินงานของสำนักงาน กสทช. เท่านั้น

๒๐.๒ ดูแลรักษาอุปกรณ์คอมพิวเตอร์โดยจัดเก็บไว้ในที่ปลอดภัย ไม่วางทิ้งไว้ในสถานที่เสี่ยงต่อการสูญหาย และหลีกเลี่ยงการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาในสภาพแวดล้อมที่อาจมีผลกระทบต่อความเสียหายของอุปกรณ์

๒๐.๓ รับผิดชอบในการป้องกันการสูญหายของข้อมูล ในกรณีที่อุปกรณ์คอมพิวเตอร์สูญหายหรือเสียหาย ผู้ใช้งานต้องแจ้งต่อผู้บังคับบัญชาโดยเร็ว

๒๐.๔ ดูแลรักษาข้อมูลของสำนักงาน กสทช. ที่จัดเก็บในอุปกรณ์คอมพิวเตอร์ให้สอดคล้องตามการบริหารจัดการข้อมูลองค์กร

๒๐.๕ เมื่อผู้ใช้งานพ้นสภาพการเป็นพนักงานของสำนักงาน กสทช. ต้องส่งอุปกรณ์คอมพิวเตอร์และอุปกรณ์เสริมทั้งหมดที่สำนักงาน กสทช. จัดไว้ให้ใช้งาน คืนต่อสำนักงาน กสทช.

๒๐.๖ การยืม การคืน หรือส่งซ่อมอุปกรณ์คอมพิวเตอร์แบบพกพาที่สำนักงาน กสทช. จัดไว้ให้ใช้งานให้เป็นไปตามขั้นตอนปฏิบัติที่สำนักเทคโนโลยีสารสนเทศกำหนด

๒๐.๗ ห้ามผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบของอุปกรณ์คอมพิวเตอร์ของสำนักงาน กสทช. โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

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

๒๐.๙ เพื่อป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต ผู้ใช้งานจะต้องกำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์ ได้แก่ การใช้บัญชีผู้ใช้งานและรหัสผ่าน หรือเทคโนโลยีไบโอเมตริก (biometric) หรือ PIN CODE

๒๐.๑๐ ก่อนการใช้งานกับสื่อบันทึกข้อมูลต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์โดยโปรแกรมป้องกันไวรัสคอมพิวเตอร์

๒๐.๑๑ ไม่นำอาหาร เครื่องดื่ม หรือสิ่งที่เป็นของเหลว มาวางใกล้บริเวณเครื่องคอมพิวเตอร์

๒๐.๑๒ ไม่วางของทับบนเครื่องคอมพิวเตอร์ หรือแป้นพิมพ์

๒๐.๑๓ กรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากที่สูง เป็นต้น

ข้อ ๒๑ การบริหารจัดการซอฟต์แวร์และทรัพย์สินทางปัญญา ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๑.๑ ไม่คัดลอก แก้ไข ถอดถอนโปรแกรมมาตรฐานต่าง ๆ ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของสำนักงาน กสทช. ที่กำหนดไว้ท้ายแนวปฏิบัตินี้ หรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือนำไปให้ผู้อื่นใช้งาน

๒๑.๒ ไม่ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดทรัพย์สินทางปัญญา หากมีการตรวจสอบพบความผิดฐานละเมิดทรัพย์สินทางปัญญา สำนักงาน กสทช. ถือว่าเป็นความผิดส่วนบุคคล

๒๑.๓ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของสำนักงาน กสทช. เพิ่มเติมก่อนได้รับอนุญาตจากผู้ดูแลระบบ

๒๑.๔ ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของทรัพย์สินทางปัญญาต่าง ๆ ที่สำนักงาน กสทช. หรือผู้ใช้งานมีใช้งานหรือครอบครอง

๒๑.๕ ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟต์แวร์สำเร็จรูปที่สำนักงาน กสทช. จัดหามาใช้งาน เว้นแต่สำนักงาน กสทช. ได้รับอนุญาตให้เปลี่ยนแปลงแก้ไขได้จากเจ้าของลิขสิทธิ์

๒๑.๖ ไม่นำผลงานของผู้อื่นหรือผลงานใด ๆ ที่มีลิขสิทธิ์มาทำการ "คัดลอก" หรือ "ดัดแปลง" ก่อนได้รับอนุญาตจากเจ้าของลิขสิทธิ์

ข้อ ๒๒ การป้องกันโปรแกรมไม่พึงประสงค์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๒.๑ ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มา หรือมาจากแหล่งที่มาที่ไม่น่าเชื่อถือ

๒๒.๒ การนำอุปกรณ์จัดเก็บข้อมูลต่าง ๆ เช่น Thumb Drive และ Data Storage มาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของสำนักงาน กสทช. ให้ตรวจสอบหาโปรแกรมไม่พึงประสงค์ก่อนทุกครั้ง

๒๒.๓ ตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail) หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนเปิดใช้งาน

๒๒.๔ ตรวจสอบฐานข้อมูลไวรัสของโปรแกรมป้องกันไวรัส กรณีไม่ปรับปรุงให้เป็นปัจจุบันผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบโดยทันที

๒๒.๕ ห้ามถอดถอนโปรแกรมป้องกันไวรัสที่สำนักงาน กสทช. ได้ติดตั้งไว้ให้

๒๒.๖ ระมัดระวังการเข้าเว็บไซต์ที่มีความเสี่ยงเนื่องจากการเปิดไฟล์หรือเข้าเว็บไซต์อาจได้รับไวรัสจากไฟล์หรือเข้าเว็บไซต์เหล่านั้น

ข้อ ๒๓ การใช้งานอินเทอร์เน็ต ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๓.๑ ปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๒๓.๒ ไม่ใช้งานอินเทอร์เน็ตของสำนักงาน กสทช. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและการเข้าสู่เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

๒๓.๓ ไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับของสำนักงาน กสทช. โดยไม่ได้รับอนุญาต

๒๓.๔ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงาน กสทช. ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒๓.๕ ไม่เสนอความคิดเห็นหรือใช้ข้อความยั่วยุ ให้ร้ายบุคคลอื่น หรือข้อมูลที่ผิดกฎหมายในการใช้งานกระดานสนทนา (Webboard) สาธารณะ

๒๓.๖ ไม่ใช้งานโปรแกรมแบบเพียร์ทูเพียร์ (Peer to Peer : P๒P) ผ่านเครือข่ายสำนักงาน กสทช.

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

๒๓.๘ ไม่เข้าเว็บไซต์เครือข่ายสังคม (Social Network) เช่น Facebook Twitter หรือ Game online เป็นต้น นอกเหนือจากการปฏิบัติงานผ่านเครือข่ายสำนักงาน กสทช.

๒๓.๙ ไม่ใช้งานสตรีมมิ่งมีเดีย (Streaming Media) นอกเหนือจากการปฏิบัติงานผ่านเครือข่ายสำนักงาน กสทช.

๒๓.๑๐ ไม่ใช้โปรแกรมควบคุมระยะไกล (Remote Administrator) ผ่านเครือข่ายสำนักงาน กสทช.

๒๓.๑๑ ต้องปิดเว็บบราวเซอร์เมื่อสิ้นสุดการใช้งานเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ข้อ ๒๔ การใช้งานจดหมายอิเล็กทรอนิกส์หรืออีเมล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

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

๒๔.๒ ระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์หรืออีเมลเพื่อไม่ให้เกิดความเสียหายต่อสำนักงาน กสทช. ละเมิดทรัพย์สินทางปัญญา ละเมิดศีลธรรม สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมาย รวมทั้งไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ

๒๔.๓ ห้ามเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมลของผู้อื่นโดยไม่ได้รับอนุญาต

๒๔.๔ ห้ามปลอมแปลงจดหมายอิเล็กทรอนิกส์หรืออีเมล

๒๔.๕ ใช้คำพูดที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมล

๒๔.๖ สำรองข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมลอย่างสม่ำเสมอ

๒๔.๗ ออกจากระบบ (Log out) ทุกครั้งเมื่อไม่ใช้งานระบบจดหมายอิเล็กทรอนิกส์หรืออีเมลเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๒๔.๘ ตรวจสอบเอกสารที่แนบมาจากจดหมายอิเล็กทรอนิกส์หรืออีเมลก่อนทำการเปิดโดยใช้โปรแกรมป้องกันไวรัส

๒๔.๙ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรืออีเมลที่ได้รับจากผู้ส่งที่ไม่รู้จักหรือมีลักษณะสแปมเมล (Spam Mail) เช่น การหลอกลวง การขายสินค้า หรือการสมัครสมาชิก เป็นต้น

๒๔.๑๐ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นอีเมลลูกโซ่ (Chain E-mail/Letter)

๒๔.๑๑ ตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์หรืออีเมล (Inbox) ของตนเองทุกวันและควรลบจดหมายอิเล็กทรอนิกส์หรืออีเมลที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่ระบบจดหมายอิเล็กทรอนิกส์หรืออีเมล

ข้อ ๒๕ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๕.๑ กรณีจำเป็นต้องใช้การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของสำนักงาน กสทช. ผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ และสังกัดให้ชัดเจนเพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดงสังกัดได้

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

๒๕.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของสำนักงาน กสทช. ผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๕.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่างต้องชี้แจงด้วยเหตุผลงดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่องที่เกี่ยวข้องต่อไป

๒๕.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากสำนักงาน กสทช. และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๒๕.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้น และแจ้งต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศโดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

๒๕.๗ ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใดๆ.ที่มีผลกระทบกับสำนักงาน กสทช. จากการใช้งานเครือข่ายสังคมออนไลน์

๒๕.๘ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่สำนักงาน กสทช. ได้กำหนดไว้เท่านั้น

ข้อ ๒๖ การบริหารจัดการข้อมูลองค์กร ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๖.๑ ระมัดระวังในการนำสื่อบันทึกข้อมูลให้ผู้อื่นใช้งาน

๒๖.๒ ดูแลรักษาความลับของข้อมูลลับ โดยหากข้อมูลอยู่ในรูปแบบอิเล็กทรอนิกส์จะต้องมีการป้องกันการเข้าถึงจากผู้ไม่มีสิทธิ หรือพิจารณาใช้มาตรการการเข้ารหัสโดยจะต้องใช้เทคโนโลยีที่ทางสำนักงาน กสทช. กำหนดให้ หรืออย่างน้อยจะต้องเป็นเทคโนโลยีที่ได้รับการยอมรับและเป็นที่รู้จักดี

๒๖.๓ ไม่นำข้อมูลไปเปิดเผยกับบุคคลซึ่งไม่มีความเกี่ยวข้องกับการปฏิบัติหน้าที่ เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชา

๒๖.๔ กำหนดประเภท ลำดับชั้นความลับ รวมถึงระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงสำหรับข้อมูลสารสนเทศแต่ละชนิดอย่างเหมาะสม

๒๖.๕ การจัดลำดับชั้นความลับของข้อมูล แบ่งออกเป็น ๕ ระดับ ดังนี้

(๑) ระดับเปิดเผยได้ (Public) หมายถึง สารสนเทศที่เปิดเผยสู่สาธารณะชนโดยบุคคลที่มีหน้าที่หรือได้รับมอบอำนาจให้ดำเนินการเผยแพร่ได้ โดยสารสนเทศที่เปิดเผยดังกล่าวได้ถูกพิจารณาแล้วว่าเมื่อมอบให้บุคคลอื่นแล้วจะไม่ก่อให้เกิดความเสียหายต่อองค์กร

(๒) ระดับส่วนบุคคลของผู้ปฏิบัติงาน (Personal) หมายถึง สารสนเทศที่เป็นข้อมูลของแต่ละบุคคลที่ใช้ในการปฏิบัติงาน

(๓) ระดับส่วนบุคคลของผู้ใช้บริการ (Data Privacy) หมายถึง สารสนเทศที่เป็นข้อมูลของผู้ใช้บริการจัดเก็บไว้ในระบบหรือระบบงานเพื่อดำเนินการต่าง ๆ

(๔) ระดับใช้ภายในเท่านั้น (Internal Use Only หรือ Internal Use) หมายถึง สารสนเทศทั่วไปที่ใช้สื่อสารกันภายในเท่านั้น

(๕) ระดับลับ (Confidential) หมายถึง สารสนเทศที่ถูกพิจารณาแล้วว่า มีความสำคัญ

๒๖.๖ ระดับการเข้าถึง คือ

(๑) การเข้าถึงเพื่อการอ่าน (Read)

(๒) การเข้าถึงเพื่อการเขียน (Write)

(๓) การเข้าถึงเพื่อการแก้ไข (Edit)

(๔) การเข้าถึงเพื่อการลบ (Delete)

๒๖.๗ เวลาที่ได้เข้าถึง สามารถเข้าถึงข้อมูลได้ตลอดเวลายี่สิบสี่ชั่วโมง เจ็ดวัน หรือตามภารกิจและความจำเป็นของผู้ใช้งานที่ได้รับมอบหมาย

๒๖.๘ ช่องทางการเข้าถึง ต้องจำกัดช่องทางการใช้งานหรือการเข้าถึงข้อมูลเท่าที่มีความจำเป็นต่อการใช้งานเท่านั้น

ข้อ ๒๗ การบริหารจัดการการเข้ารหัสข้อมูล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๗.๑ กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูล ครอบคลุม ขอบเขตหน้าที่ ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการเข้ารหัสข้อมูล (cryptographic algorithm) ที่สอดคล้องตามระดับความสำคัญของข้อมูล และการบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management)

๒๗.๒ กำหนดให้มีการเข้ารหัสข้อมูลสำคัญและช่องทางการสื่อสารที่ใช้รับส่งข้อมูลสำคัญกับภายนอก

๒๗.๓ วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล เช่น การเข้ารหัสข้อมูลแบบสมมาตร (เช่น AES) หรือการเข้ารหัสข้อมูลแบบอสมมาตร (เช่น public key cryptography) เป็นต้น โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

๒๗.๔ การบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management) ควรกำหนดกระบวนการที่มีความรัดกุม ปลอดภัยครอบคลุมตั้งแต่การสร้างและติดตั้ง การจัดเก็บ และการยกเลิกกุญแจเข้ารหัสข้อมูล ดังนี้

๒๗.๔.๑ การสร้างและติดตั้งกุญแจเข้ารหัสข้อมูล ให้ปฏิบัติดังนี้

(๑) มีการควบคุมสภาพแวดล้อมในการสร้างรหัสที่มีความรัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (Certification Authority) ที่น่าเชื่อถือ มีขั้นตอนการทำลายหลักฐานที่ใช้หลังจากสร้างกุญแจแล้วเสร็จ

(๒) กุญแจเข้ารหัสข้อมูลจะต้องไม่มีพนักงานหรือบุคคลใดบุคคลหนึ่งรู้รหัสทั้งหมด

(๓) กำหนดขนาดของกุญแจเข้ารหัสข้อมูลที่มีความยาวเพียงพอในการป้องกันการถูกถอดรหัส เช่น การถูกโจมตีแบบ brute force เป็นต้น

(๔) การแลกเปลี่ยนกุญแจต้องผ่านกระบวนการและช่องทางที่ปลอดภัย

(๕) กำหนดไม่ให้ใช้กุญแจเข้ารหัสข้อมูลเดียวกันกับหลายระบบสารสนเทศ

๒๗.๔.๒ การจัดเก็บกุญแจเข้ารหัสข้อมูล ให้ปฏิบัติดังนี้

(๑) มีการรักษาความปลอดภัยของกุญแจเข้ารหัสข้อมูลทั้งด้าน physical และ logical โดยใช้อุปกรณ์รักษาความปลอดภัย HSM หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน

(๒) มีการสำรองข้อมูลกุญแจเข้ารหัสข้อมูล โดยวิธีการเก็บรักษากุญแจเข้ารหัสข้อมูลชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสข้อมูลชุดหลัก

๒๗.๔.๓ การเปลี่ยนและเพิกถอนกุญแจเข้ารหัสข้อมูล ให้ปฏิบัติดังนี้

(๑) กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัสข้อมูล เช่น กรณีกุญแจหมดอายุ ล้าสมัย หรือไม่ปลอดภัย เป็นต้น

(๒) กำหนดกระบวนการทำลายกุญแจโดยต้องมั่นใจว่าไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก

ข้อ ๒๘ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๘.๑ ห้ามติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่สำนักงาน กสทช. ไม่อนุญาตให้ใช้งาน

๒๘.๒ ซอฟต์แวร์ที่ใช้ต้องมีลิขสิทธิ์การใช้งานที่ถูกต้อง ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๒๘.๓ หากต้องการใช้งานโปรแกรมอรรถประโยชน์ที่ไม่อนุญาต เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้ไม่ปลอดภัย ต้องได้รับความเห็นชอบที่เป็นลายลักษณ์อักษรจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้ที่ได้รับมอบหมายให้เป็นผู้พิจารณาอนุญาต

๒๘.๔ กำหนดให้มีการถอดถอนการติดตั้งโปรแกรมอรรถประโยชน์รวมทั้งซอฟต์แวร์ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสทช. ที่ไม่จำเป็นออกจากระบบ เมื่อไม่จำเป็นต้องใช้งาน

หมวด ๓
การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ

ข้อ ๒๙ การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศของสำนักงาน กสทช. ให้ปฏิบัติดังต่อไปนี้

๒๙.๑ การจัดหาและพัฒนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ ให้หน่วยงานประสานงานกับสำนักเทคโนโลยีสารสนเทศ เพื่อพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย และความสอดคล้องกับโครงสร้างพื้นฐานและเครือข่ายของสำนักงาน กสทช. ก่อนนำเสนอพิจารณาอนุมัติจัดหาและพัฒนาทุกครั้ง

๒๙.๒ การจัดหาและพัฒนาที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่มีความสำคัญยิ่งยวดและมีลักษณะสุ่มเสี่ยงต่อความล้มเหลวในการให้บริการหากมีเพียงชุดเดียว ให้ผู้รับผิดชอบพิจารณาจัดหาอุปกรณ์สำรองไว้ ทั้งนี้ ต้องได้รับความเห็นชอบจากผู้บริหาร

๒๙.๓ การพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย ให้คำนึงถึงเรื่องดังต่อไปนี้

(๑) สิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนา

(๒) การตรวจสอบด้านคุณภาพและความถูกต้องของระบบสารสนเทศ

(๓) การตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์

(๔) ข้อจำกัดในการเปิดเผยข้อมูลของสำนักงาน กสทช.

(๕) มาตรฐานและคุณภาพการให้บริการด้านความมั่นคง

(๖) การทดสอบระบบสารสนเทศ

๒๙.๔ ไม่อนุญาตให้นำข้อมูลสำคัญของสำนักงาน กสทช. เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลใช้ภายในเท่านั้น ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นแต่ได้รับการอนุมัติจากผู้บังคับบัญชาก่อน

๒๙.๕ ดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบสารสนเทศจากภายนอก (outsourced system development) ให้เป็นไปตามนโยบายการพัฒนาระบบสารสนเทศของสำนักงาน กสทช.

๒๙.๖ ต้องทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งานหรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้ถูกต้องตรงความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ สำนักงาน กสทช. ควรระมัดระวังโดยจัดให้มีแนวทางควบคุมและป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบหากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

๒๙.๗ ต้องทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity plan) ให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

๒๙.๘ ต้องควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ (development environment) ซึ่งได้แก่ บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ และเทคโนโลยีสำหรับการพัฒนาระบบให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบโดยคำนึงถึงเรื่องดังนี้

(๑) การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ ส่งผ่านระบบการควบคุม การนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

(๒) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

(๓) การติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

(๔) มีการจัดเก็บข้อมูลสำรองในพื้นที่นอกสำนักงาน กสทช. ที่มีความมั่นคงปลอดภัย

๒๙.๙ ควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ โดยอย่างน้อยต้องมีในเรื่องดังต่อไปนี้

(๑) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

(๒) กำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจ ต้องควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข มีการตรวจรับจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งมีการจัดเก็บรายละเอียดของคำขอไว้ เป็นต้น

(๓) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง

(๔) ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

(๕) จัดเก็บโปรแกรม version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (fall-back) ของระบบงานในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

(๖) มีการสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

(๗) บันทึกและจัดเก็บหลักฐานทั้งหมด (audit trail) ที่เกี่ยวข้องกับการเปลี่ยนแปลงเพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

หมวด ๔
การบริหารจัดการความเสี่ยงและการตรวจสอบด้านเทคโนโลยีสารสนเทศ

ข้อ ๓๐ การบริหารจัดการความเสี่ยง ให้สำนักเทคโนโลยีสารสนเทศปฏิบัติดังต่อไปนี้

๓๐.๑ กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยง โดยอย่างน้อยต้องกำหนดในเรื่องดังต่อไปนี้

(๑) เป้าหมายการประเมินความเสี่ยง

(๒) กระบวนการ วัตถุประสงค์ และข้อกำหนดทางธุรกิจ

(๓) กฎ ระเบียบ ข้อกำหนดในสัญญา และข้อบังคับที่สำนักงาน กสทช. ต้องปฏิบัติ

(๔) ข้อกำหนดด้านความมั่นคงปลอดภัย

(๕) เทคโนโลยีสารสนเทศที่สำนักงาน กสทช. ใช้งาน

(๖) ผลกระทบที่เกิดขึ้นหากระบบสารสนเทศไม่สามารถใช้งานได้

(๗) โอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง

๓๐.๒ กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ วิธีการคิดโอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง และวิธีการคิดผลกระทบของเหตุการณ์ความเสี่ยง

๓๐.๓ กำหนดระดับความเสี่ยงที่ยอมรับได้

๓๐.๔ วิเคราะห์และประเมินความเสี่ยงต่อสินทรัพย์สารสนเทศอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงสินทรัพย์ของระบบสารสนเทศสำคัญแล้วส่งผลกระทบสูงต่อผลการประเมินความเสี่ยงล่าสุด และบริหารจัดการความเสี่ยงเหล่านั้น ดังนี้

(๑) จัดทำแผนการลดความเสี่ยงโดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่า หรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

(๒) นำเสนอแผนการลดความเสี่ยงต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(๓) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนและรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะ ๆ จนกระทั่งเสร็จสิ้น

ข้อ ๓๑ การตรวจสอบด้านเทคโนโลยีสารสนเทศ ให้สำนักเทคโนโลยีสารสนเทศปฏิบัติดังต่อไปนี้

๓๑.๑ จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศตามมาตรฐานสากลจากผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละหนึ่งครั้ง

๓๑.๒ จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศด้วยวิธีทางเทคนิคอย่างน้อยปีละหนึ่งครั้ง

โปรแกรมคอมพิวเตอร์มาตรฐาน
สำหรับการใช้งานของสำนักงาน กสทช.

๑. Microsoft Windows
๒. Microsoft Office
๓. Microsoft Siverlight
๔. Microsoft .Net Framework
๕. Microsoft Visual C++
๖. Adobe Reader
๗. Adobe Flash Player
๘. Anti-Virus
๙. ๗Zip
๑๐. Mozilla Firefox
๑๑. Mozilla Maintenance Service
๑๒. Chrome
๑๓. CDBurnerXP
๑๔. Citrix Workspace
๑๕. Java
๑๖. PDF Creator
๑๗. VLC media player
๑๘. LEXiTRON Dictionary
๑๙. Line for PC
๒๐. StarCat Agent
๒๑. โปรแกรมสำหรับการใช้งานเครือข่าย VPN ที่สำนักงาน กสทช. จัดหา
๒๒. โปรแกรมมาตรฐานที่มาพร้อมกับเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่สำนักงาน กสทช. จัดหา