ประกาศสำนักเลขาธิการนายกรัฐมนตรี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561

ตามที่ สำนักเลขาธิการนายกรัฐมนตรีได้ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2554 เมื่อวันที่ 30 กันยายน พ.ศ. 2554 เป็นต้นมานั้น ด้วยความเจริญก้าวหน้าและนวัตกรรมทางเทคโนโลยีดิจิทัลที่มีการนำมาใช้งานในปัจจุบัน ได้ทำให้การดำเนินธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐ มีการเปลี่ยนแปลงไปเป็นอย่างมาก ส่งผลให้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี พ.ศ. 2554 ที่ประกาศใช้ ไม่สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

เพื่อให้การใช้งานด้านสารสนเทศทางอิเล็กทรอนิกส์ของสำนักเลขาธิการนายกรัฐมนตรี มีความมั่นคงปลอดภัยอย่างเหมาะสมและมีประสิทธิภาพเชื่อถือได้ รวมทั้งเพื่อเป็นการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เทคโนโลยีดิจิทัลในลักษณะที่ไม่ถูกต้อง ซึ่งเป็นเหตุให้เกิดภัยคุกคามต่างๆ ที่จะสร้างความเสียหายหรือความเสื่อมเสียแก่สำนักเลขาธิการนายกรัฐมนตรี และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และ/หรือกฎหมายอื่นที่เกี่ยวข้อง สำนักเลขาธิการนายกรัฐมนตรี จึงเห็นสมควรยกเลิกนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2554 และให้ใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561 แทน โดยมีวัตถุประสงค์ นโยบาย และองค์ประกอบ ดังต่อไปนี้

1. <u>วัตถุประสงค์</u>

1.1 กำหนดเป็นนโยบายและแนวปฏิบัติให้ผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลระบบ และบุคคลภายนอกที่มาปฏิบัติงานให้กับสำนักเลขาธิการนายกรัฐมนตรี ใช้ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัดและมีประสิทธิภาพ

1.2 กำหนดขอบเขตการบริหารจัดการ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี ให้มีความเหมาะสม ชัดเจนและสอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสากล (ISO/IEC 27001) โดยทบทวนและปรับปรุงให้ทันสมัยอย่างต่อเนื่อง

1.3 ส่งเสริมให้มีการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี แก่ผู้ใช้ทุกระดับได้รับทราบอย่างทั่วถึง และยอมรับที่จะปฏิบัติตามอย่างเคร่งครัด

2. <u>นโยบาย</u>

2.1 กำกับดูแลผู้ใช้งานให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด หากมีการละเมิดหรือฝ่าฝืนจะต้องมีบทลงโทษตามความเหมาะสม รวมทั้งต้องหามาตรการหรือแนวทางการแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นจากเหตุฉุกเฉิน และต้องติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามระเบียบปฏิบัติ ข้อบังคับ และกฎหมายที่เกี่ยวข้อง

/2.2 กำกับ...

2.2 กำกับดูแลการบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

2.3 เผยแพร่ความรู้ ความเข้าใจ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเสริมสร้างความตระหนักให้กับผู้ใช้งานของสำนักเลขาธิการนายกรัฐมนตรี และหน่วยงานภายนอกที่เกี่ยวข้อง

2.4 ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี ให้สอดคล้องความเจริญก้าวหน้าทางเทคโนโลยีดิจิทัลที่เปลี่ยนแปลงไป

3. <u>องค์ประกอบ</u>

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561 มีรายละเอียดปรากฏตามแนบท้ายประกาศนี้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561 นี้ ผู้ใช้ที่ได้รับสิทธิ์เข้าใช้งานสารสนเทศทางอิเล็กทรอนิกส์และเทคโนโลยีดิจิทัลใดๆ ของสำนักเลขาธิการนายกรัฐมนตรี ทุกระดับและทุกกรณี จะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑ มิถุนายน พ.ศ. 2561

(นางวิสุนี บุนนาค)
รองเลขาธิการนายกรัฐมนตรีฝ่ายบริหาร
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ประจำสำนักเลขาธิการนายกรัฐมนตรี

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักเลขาธิการนายกรัฐมนตรี
พ.ศ. 2561

จัดทำโดย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักเลขาธิการนายกรัฐมนตรี

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการนายกรัฐมนตรี พ.ศ. 2561

1. หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ได้กำหนดให้หน่วยงานภาครัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ มีความมั่นคงปลอดภัยและเชื่อถือได้ สอดคล้องกับมาตรฐานด้านความมั่นคงปลอดภัยสากล อาทิ มาตรฐาน ISO/IEC 27001 และต้องลดผลกระทบจากภัยคุกคามต่างๆ รวมถึงการฟื้นฟูระบบสารสนเทศอย่างรวดเร็วภายหลังสถานการณ์สิ้นสุดลง ตลอดจนต้องจัดหาเครื่องมือที่จำเป็นอย่างเพียงพอที่จะสนับสนุนการปฏิบัติงานด้านสารสนเทศอย่างมีประสิทธิภาพ

ที่ผ่านมา สำนักเลขาธิการนายกรัฐมนตรีได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2554 และประกาศใช้เมื่อวันที่ 30 กันยายน พ.ศ. 2554 เป็นต้นมา ปัจจุบันความเจริญก้าวหน้าและนวัตกรรมทางเทคโนโลยีดิจิทัลที่มีการนำมาใช้งาน ได้ทำให้การดำเนินธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐมีการเปลี่ยนแปลงไปเป็นอย่างมาก ส่งผลกระทบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรีที่กำหนดไว้ จึงเป็นที่มาให้สำนักเลขาธิการนายกรัฐมนตรีต้องดำเนินการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรีขึ้นใหม่ ให้มีความเป็นปัจจุบันสอดคล้องกับความเจริญก้าวหน้าทางเทคโนโลยีดิจิทัลที่เปลี่ยนแปลงไป

2. วัตถุประสงค์

2.1 เพื่อทบทวนและปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี ให้มีความเป็นปัจจุบัน สอดคล้องกับความเจริญก้าวหน้าทางเทคโนโลยีดิจิทัลที่เปลี่ยนแปลงไป

2.2 เพื่อกำหนดทิศทางการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี ให้สอดคล้องกับระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้อง ซึ่งได้รับการปรับปรุงใหม่

3. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี

3.1 กำกับดูแลผู้ใช้งานให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด หากมีการละเมิดหรือฝ่าฝืนจะต้องมีบทลงโทษตามความเหมาะสม รวมทั้งต้องหามาตรการหรือแนวทางการแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นจากเหตุฉุกเฉิน และต้องติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามระเบียบปฏิบัติ ข้อบังคับ และกฎหมายที่เกี่ยวข้อง

3.2 กำกับดูแลการบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

3.3 เผยแพร่ความรู้ ความเข้าใจ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเสริมสร้างความตระหนักให้กับผู้ใช้งานของสำนักเลขาธิการนายกรัฐมนตรี และหน่วยงานภายนอกที่เกี่ยวข้อง

3.4 ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี ให้สอดคล้องความเจริญก้าวหน้าทางเทคโนโลยีดิจิทัลที่เปลี่ยนแปลงไป

4. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

ส่วนที่ 1 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical & Environment)

ส่วนที่ 2 แนวปฏิบัติในการควบคุมการใช้งาน (Usage Control)

ส่วนที่ 3 แนวปฏิบัติในการสำรองข้อมูล (Backup)

ส่วนที่ 4 แนวปฏิบัติในการป้องกันโปรแกรมประสงค์ร้าย (Malware)

ส่วนที่ 5 แนวปฏิบัติในการประเมินความเสี่ยง (Risks)

ส่วนที่ 6 แนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Awareness)

ส่วนที่ 7 แนวปฏิบัติในการใช้ Social Media

คำนิยาม

คำนิยามที่ใช้ในประกาศนี้ ประกอบด้วย

การเข้ารหัส (Encryption) หมายถึง กระบวนการแปลงข้อมูลหรือสารสนเทศให้ไปอยู่ในรูปของรหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

การตั้งค่าระบบ (Configuration) หมายถึง ค่าหรือชุดคำสั่งที่ใช้กำหนดการเริ่มต้นทำงานของระบบคอมพิวเตอร์ อุปกรณ์เครือข่ายทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

การถอดรหัส (Decryption) หมายถึง กระบวนการแปลงรหัสให้กลับไปอยู่ในรูปข้อมูลหรือสารสนเทศเดิมก่อนอยู่ในรูปของรหัส

การพิสูจน์ยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัย ในการเข้าใช้ระบบ โดยทั่วไประบบจะทำการพิสูจน์และยืนยันตัวตนโดยให้ระบุ ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

คอมพิวเตอร์ หมายถึง อุปกรณ์คอมพิวเตอร์แบบต่างๆ เช่น เซิร์ฟเวอร์ เดสก์ทอป โน้ตบุ๊ก แทบเล็ต สมาร์ทโฟน เป็นต้น

ความมั่นคงปลอดภัย หมายถึง ความมั่นคงและความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักเลขาธิการนายกรัฐมนตรี

จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง บริการสื่อสารข้อมูลทางอิเล็กทรอนิกส์ที่สำนักเลขาธิการนายกรัฐมนตรีจัดขึ้น เพื่อสนับสนุนการบริหารและปฏิบัติราชการของสำนักเลขาธิการนายกรัฐมนตรี ผู้ใช้จดหมายอิเล็กทรอนิกส์ภายใต้ชื่อโดเมน @thaigov.go.th พึงใช้งานโดยไม่ขัดกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรีและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

ชื่อเครื่องคอมพิวเตอร์ (Computer Name) หมายถึง ชื่อที่กำหนดเฉพาะให้กับ ***"คอมพิวเตอร์"*** โดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องใดในระบบเครือข่าย

ชื่อผู้ใช้งาน (Username) หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อระบุผู้ใช้งาน ***"คอมพิวเตอร์"*** และระบบเครือข่ายตามที่ได้รับการกำหนดสิทธิ์การใช้งานไว้

ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อน หรือข้อบกพร่องในระบบคอมพิวเตอร์ หรือซอฟต์แวร์ซึ่งทำให้เกิดความเสี่ยงในด้านความมั่นคงปลอดภัย

โดเมน (Domain Name) หมายถึง ชื่อเว็บไซต์ ซึ่งเป็นชื่อที่ตั้งขึ้นเพื่อให้จดจำและนำไปใช้งานได้ง่าย สำนักเลขาธิการนายกรัฐมนตรีได้จดทะเบียนโดเมน เป็น thaigov.go.th

โดเมนย่อย (Sub Domain Name) หมายถึง ชื่อกลุ่มย่อยต่างๆ ภายใต้ ***"โดเมน"*** สำนักเลขาธิการนายกรัฐมนตรี ได้กำหนดโดเมนย่อยภายใต้โดเมน thaigov.go.th โดยมีรูปแบบเป็น *.thaigov.go.th เช่น spm.thaigov.go.th edoc.thaigov.go.th webmail.thaigov.go.th เป็นต้น

ทรัพย์สิน หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักเลขาธิการนายกรัฐมนตรี เช่น ***"คอมพิวเตอร์"*** อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

บัญชีผู้ใช้งาน (Account) หมายถึง บัญชีรายละเอียดของผู้มีสิทธิ์ใช้งาน ***"คอมพิวเตอร์"*** และบริการในระบบเครือข่ายของสำนักเลขาธิการนายกรัฐมนตรี

แบนด์วิดท์ (Bandwidth) หมายถึง ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบต่อหน่วยเวลา เป็นการแสดงให้เห็นถึงปริมาณข้อมูล ที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับ-ส่งข้อมูล

ไบออส (BIOS) หมายถึง ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนเมนบอร์ดของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการเริ่มทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนเมนบอร์ด (Main Board)

โปรแกรมประสงค์ร้าย (Malware) หมายถึง โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นโดยมีวัตถุประสงค์ก่อกวน หรือสร้างความเสียหายทั้งทางตรงและทางอ้อมแก่ระบบคอมพิวเตอร์ หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) สปายแวร์ (Spyware) หนอน (Worm) ม้าโทรจัน (Trojan horse) ฟิชชิง (Phishing) จดหมายลูกโซ่ (Mass Mailing) เป็นต้น

ผู้ใช้บริการ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้าง และบุคลากรในสังกัดสำนักเลขาธิการนายกรัฐมนตรี โดยให้หมายความรวมถึงข้าราชการการเมือง และผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และระบบเครือข่ายของสำนักเลขาธิการนายกรัฐมนตรี

ผู้ดูแลระบบ (System/Network Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่าย

ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรับผิดชอบให้สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log)

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักเลขาธิการนายกรัฐมนตรี

แผนผังระบบเครือข่าย (Network Diagram) หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

1. พื้นที่ทำงาน หมายถึง พื้นที่ติดตั้ง ***"คอมพิวเตอร์"*** เพื่อการปฏิบัติงาน รวมถึง พื้นที่ที่ใช้ในการทำงานของ ***"ผู้ดูแลระบบ"***
2. พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย หมายถึง พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บอุปกรณ์สำรองข้อมูลคอมพิวเตอร์
3. พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายถึง พื้นที่ให้บริการระบบเครือข่ายไร้สายของสำนักเลขาธิการนายกรัฐมนตรี

ไฟล์ที่สามารถประมวลผลได้ (Executable file) หมายถึง ไฟล์โปรแกรมที่สามารถเรียกใช้งานให้ทันที เช่น *.exe *.com *.bat *.vbs *.dll เป็นต้น

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการรับ - ส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน ระบบอินทราเน็ต ระบบอินเทอร์เน็ต (Internet) เป็นต้น

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ มาช่วยเพิ่มประสิทธิภาพในการปฏิบัติงานให้เกิดความสะดวกรวดเร็ว ทันเหตุการณ์ ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

ระบบแลน (Local Area Network : LAN) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ***"ระบบคอมพิวเตอร์"*** ภายในของสำนักเลขาธิการนายกรัฐมนตรีเข้าด้วยกัน

ระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในของสำนักเลขาธิการนายกรัฐมนตรี

ระบบอินเทอร์เน็ต (Internet) หมายถึงระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ***"ระบบเครือข่าย"*** ของสำนักเลขาธิการนายกรัฐมนตรีเข้ากับเครือข่ายอินเทอร์เน็ตสากล

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ล็อกอิน (Login) หมายถึง กระบวนการที่ผู้ใช้งานจะต้องลงบันทึกเข้าด้วย ***"ชื่อผู้ใช้งาน"*** และ ***"รหัสผ่าน"*** ที่ถูกต้องเพื่อเป็นการพิสูจน์ยืนยันตัวตนในการเข้าใช้งานระบบ

ล็อกเอ้าท์ (Logout) หมายถึง กระบวนการที่ผู้ใช้งานจะต้องลงบันทึกออกเมื่อเสร็จสิ้นการใช้งานระบบ เพื่อเป็นการป้องกันบุคคลอื่นเข้าใช้งานระบบอย่างไม่ถูกต้อง

เวลาอ้างอิงสากล (Stratum 0) หมายถึง การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่าย ที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

สื่อบันทึกพกพา หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk เป็นต้น

หน่วยงาน หมายถึง "สำนักเลขาธิการนายกรัฐมนตรี (สลน.)"

หน่วยงานภายนอก หมายถึง องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของสำนักเลขาธิการนายกรัฐมนตรี โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

อัพเดท (Update) หมายถึง การปรับปรุง ***"ข้อมูลคอมพิวเตอร์"*** ให้เป็นปัจจุบัน รวมถึงการปรับปรุงข้อมูลของ ***"สารสนเทศ"*** ด้านต่าง ๆ เป็นต้น

อุปกรณ์จัดเส้นทาง (Router) หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หมายถึงอุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

Access Point หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

Command Line หมายถึง บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

Default หมายถึง ค่าเครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้า และนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการเป็นอย่างอื่น

DoD 5220.22-M หมายถึง การลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับและใช้งานกับกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้ การลบข้อมูลด้วยวิธีนี้จะกระทำ 3 รอบ รอบแรกด้วยข้อมูลแบบสุ่ม รอบที่สองด้วยบิตที่ตรงกันข้าม รอบสุดท้ายด้วยข้อมูลไบต์สุ่ม

Firewall หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ตแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

Firewall Log หมายถึง การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่า ***"Firewall"*** จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์เพื่อตรวจสอบประเภทของการสื่อสารปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

IEEE 802.1X หมายถึง มาตรฐานใช้ในการพิสูจน์ทราบตัวตนทั้งในเครือข่าย LAN และ WLAN ให้มีความปลอดภัยสูงขึ้น ในกรณีเมื่อผู้ใช้ต้องการเชื่อมต่อเข้าใช้เครือข่าย WLAN จะต้องมีการแสดงหลักฐานประกอบการตรวจสอบ (Credential) ต่อแอ็กเซสพอยต์

IP Address หมายถึง หมายเลขประจำ ***"คอมพิวเตอร์"*** ที่ต่ออยู่ใน ***"ระบบแลน"*** ซึ่งหมายเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข 4 ส่วน (IP V.4) หรือ 8 ส่วน (IP V.6) ที่คั่นด้วยเครื่องหมายจุด (.) และ / หรือทวิภาค (:)

MAC Address (Media Access Control Address) หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

Public IP Address หมายถึง *"IP Address"* ที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน และ/หรือรับ-ส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

Social Media หมายถึง สื่อสังคมออนไลน์ที่มีการตอบสนองทางสังคมได้หลายทิศทาง โดยผ่านเครือข่ายอินเตอร์เน็ต

SSID (Service Set Identifier) หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกันโดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

VPN (Virtual Private Network) หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

Web Server หมายถึง เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่างๆ

WEP (Wired Equivalent Privacy) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับ-ส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

Wireless LAN Client หมายถึง เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ใน***"ระบบแลน"*** โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE 802.11

WPA (Wi-Fi Protected Access) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย ที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง ***"WEP"***

ส่วนที่ 1
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical & Environment)

ข้อ 1 ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนดพื้นที่การใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งพื้นที่การใช้งาน โดยแบ่งเป็นส่วนๆ ดังนี้ พื้นที่ทำงาน พื้นที่ใช้งานระบบเครือข่ายไร้สาย และพื้นที่หวงห้ามเฉพาะที่ใช้ในการติดตั้ง และจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย ทั้งนี้ จะต้องประกาศให้รับทราบทั่วกัน

ข้อ 2 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดสิทธิ์ในการเข้า-ออกพื้นที่หวงห้ามเฉพาะตามข้อ 1

ข้อ 3 ให้มีการควบคุมการเข้า-ออกในบริเวณพื้นที่หวงห้ามเฉพาะ ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออก ได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

ข้อ 4 บุคคลภายนอกหรือผู้มาติดต่อจะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย ก่อนการเข้า-ออกในบริเวณพื้นที่หวงห้ามเฉพาะ และจะต้องลงชื่อบันทึกการเข้า-ออกในแบบฟอร์มตามที่กำหนด

หากมีการนำ***"คอมพิวเตอร์"*** และ/หรือ อุปกรณ์อื่นใดที่เกี่ยวข้อง เข้า-ออกบริเวณพื้นที่หวงห้ามเฉพาะ จะต้องลงบันทึกรายการสิ่งที่นำเข้า-ออกให้ถูกต้อง

ข้อ 5 มาตรการรักษาความมั่นคงปลอดภัยพื้นที่หวงห้ามเฉพาะ

1) ต้องมีระบบป้องกันอัคคีภัย เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน และระบบดับเพลิงอัตโนมัติ เพื่อป้องกันและระงับเหตุได้ทันท่วงที

2) ต้องมีระบบไฟฟ้าสำรองป้องกันความเสียหายที่อาจเกิดขึ้นกับ ***"ระบบเทคโนโลยีสารสนเทศ"*** จากความไม่คงที่ของกระแสไฟฟ้า

3) ต้องมีระบบควบคุมอุณหภูมิและความชื้น โดยทำงานร่วมกับเครื่องปรับอากาศควบคุมความชื้นอัตโนมัติได้อย่างเหมาะสม

4) ต้องมีระบบเตือนภัยน้ำรั่วซึมภายในศูนย์คอมพิวเตอร์ที่มีการติดตั้งพื้นยกระดับ เพื่อป้องกันและระงับเหตุที่อาจเกิดจากน้ำรั่วซึมได้ทันท่วงที

5) จะต้องเตรียมความพร้อมและบำรุงรักษาเพื่อให้ ***"ระบบเทคโนโลยีสารสนเทศ"*** สามารถใช้งานได้อย่างต่อเนื่องตลอดเวลา

6) ในกรณีที่จะต้องนำ ***"ทรัพย์สิน"*** ออกไปภายนอกพื้นที่หวงห้ามเฉพาะ จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย

7) ข้อมูลที่เก็บอยู่บนสื่อบันทึกข้อมูล เมื่อไม่ต้องการใช้งานแล้วจะต้องทำลาย โดยให้เป็นไปตามแนวปฏิบัติว่าด้วยการทำลายข้อมูลหรือการกำจัดสื่อบันทึกข้อมูล

8) จะต้องกำหนดพื้นที่สำหรับรับ-ส่งสิ่งของ โดยต้องแกะหีบห่อ และตรวจสอบให้เสร็จสิ้นก่อนนำมาติดตั้งในพื้นที่หวงห้ามเฉพาะ

9) ต้องมีระบบเทคโนโลยีเฝ้าระวังและรักษาความปลอดภัยตลอด 24 ชั่วโมง เช่น กล้องวงจรปิด ระบบตรวจจับการบุกรุก และระบบแจ้งเตือน เป็นต้น

ส่วนที่ 2
แนวปฏิบัติในการควบคุมการใช้งาน (Usage Control)

2.1 การควบคุมการใช้งาน

ข้อ 1 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดสิทธิ์การเข้าใช้งานระบบสารสนเทศของ สลน. ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ตามแบบฟอร์มที่กำหนด

ข้อ 2 ***"ผู้ดูแลระบบ"*** มีหน้าที่ควบคุมการใช้งาน ดังนี้

1) กำหนดสิทธิ์การเข้าถึง ***"ระบบเทคโนโลยีสารสนเทศ"*** ให้เหมาะสมกับ ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** และต้องมีการทบทวนสิทธิ์อย่างสม่ำเสมอ

2) ตรวจสอบบันทึกการใช้งานเข้า-ออก***"ระบบเทคโนโลยีสารสนเทศ"*** ของ สลน.อย่างสม่ำเสมอ

3) บันทึกการกำหนดสิทธิ์ การแก้ไขเปลี่ยนแปลง และการเข้าถึง ***"ระบบเทคโนโลยีสารสนเทศ"*** เพื่อเป็นหลักฐานในการตรวจสอบ

4) บันทึกการกำหนดสิทธิ์ การแก้ไขเปลี่ยนแปลง และการผ่านเข้า-ออกพื้นที่หวงห้ามเฉพาะเพื่อเป็นหลักฐานในการตรวจสอบ

2.2 การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ 1 ***"ผู้ดูแลระบบ"*** มีหน้าที่บริหารจัดการสิทธิ์ของ ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"***ดังต่อไปนี้

1) แจ้ง ***"ชื่อผู้ใช้งาน"*** และ ***"รหัสผ่าน"*** ให้กับ ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** ด้วยวิธีการที่ปลอดภัย

2) เพิกถอนสิทธิ์การเข้าถึง ในกรณีที่ยกเลิกการใช้งาน ลาออก พ้นจากตำแหน่ง หรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำนักเลขาธิการนายกรัฐมนตรี พ.ศ. 2561

ข้อ 2 ***"ผู้ดูแลระบบ"*** ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ดังต่อไปนี้

1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

2) กำหนด ***"ชื่อผู้ใช้งาน"*** และ ***"รหัสผ่าน"*** เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้ข้อมูลตามประเภทชั้นความลับ

3) กำหนดระยะเวลาการเข้าถึงข้อมูลตามประเภทชั้นความลับและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา

4) การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายอินเทอร์เน็ต จะต้องเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

5) กำหนดระยะเวลาการเปลี่ยน ***"รหัสผ่าน"*** ตามระดับความสำคัญของข้อมูล

6) ในกรณีที่ต้องนำ ***"คอมพิวเตอร์"*** ไปตรวจซ่อม ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** จะต้องทำการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

2.3 ความรับผิดชอบต่อบัญชีผู้ใช้งาน

ข้อ 1 ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** ที่ได้รับมอบ ***"บัญชีผู้ใช้งาน"*** ต้องเป็นผู้รับผิดชอบในการกระทำใด ๆ ที่เกิดขึ้นจากการใช้ ***"บัญชีผู้ใช้งาน"***

ข้อ 2 ผู้ใช้งานจะต้องเก็บรักษา ***"บัญชีผู้ใช้งาน"*** ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น

ข้อ 3 ผู้ใช้งานจะต้อง ***"ล็อกอิน"*** โดยใช้ ***"บัญชีผู้ใช้งาน"*** ของตนเอง และทำการ ***"ล็อกเอ้าท์"*** ทุกครั้ง เมื่อสิ้นสุดการใช้งาน

ข้อ 4 ผู้ใช้งานต้องแจ้ง ***"ผู้ดูแลระบบ"*** หากการพิสูจน์ตัวตนมีปัญหา ไม่ว่าจะเกิดจาก ***"รหัสผ่าน"*** การระงับสิทธิ์ หรือเกิดจากความผิดพลาดใดๆ

2.4 การกำหนดใช้รหัสผ่าน

ข้อ 1 ***"รหัสผ่าน"*** ควรมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่าง ๆ

ข้อ 2 ไม่ควรกำหนด ***"รหัสผ่าน"*** จากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์

ข้อ 3 ควรเปลี่ยน ***"รหัสผ่าน"*** เป็นประจำ

ข้อ 4 ควรเก็บรักษา ***"รหัสผ่าน"*** โดยถือว่าเป็นความลับเฉพาะบุคคล

2.5 การเข้าถึงระบบเครือข่าย

ข้อ 1 ห้าม ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** นำ ***"คอมพิวเตอร์"*** มาเชื่อมต่อเข้า ***"ระบบเครือข่าย"*** ของ สลน. ก่อนได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ 2 การขออนุญาตใช้งาน ***"Web Server"*** และ***"ชื่อโดเมนย่อย"*** ของ สลน. ***ผู้ใช้บริการ"*** และ***"หน่วยงานภายนอก"*** จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ 3 ห้ามกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการอื่นใดต่ออุปกรณ์ ***"ระบบเครือข่าย"*** เว้นแต่ได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ 4 ***"ผู้ดูแลระบบ"*** ต้องควบคุมการเข้าถึงระบบเครือข่าย ดังต่อไปนี้

1) กำหนดสิทธิ์การใช้งานเพื่อควบคุม ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** ให้สามารถใช้งานเฉพาะ ***"ระบบเครือข่าย"*** ที่ได้รับอนุญาตเท่านั้น

2) กำหนด ***"แบนด์วิดท์"*** ที่เหมาะสมเพื่อการใช้งาน ***"ระบบเครือข่าย"*** ร่วมกัน

3) การเชื่อมต่อ ***"ระบบเครือข่าย"*** ของ สลน. ไปยังเครือข่ายภายนอก ต้องเชื่อมต่อผ่านระบบป้องกัน/ตรวจจับการบุกรุก (Intrusion Prevention/Detection System)

4) การเข้าสู่ ***"ระบบเครือข่าย"*** ของ สลน. โดยผ่านทาง ***"ระบบอินเทอร์เน็ต"*** จะต้องมีการ ***"ล็อกอิน"*** เพื่อ ***"การพิสูจน์ยืนยันตัวตน"*** ของ ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"***

5) จัดทำ ***"แผนผังระบบเครือข่าย"*** เพื่อแสดงรายละเอียดเกี่ยวกับ ***"ระบบเครือข่าย"*** ของ สลน. พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

6) การใช้เครื่องมือเพื่อการตรวจสอบ ***"ระบบเครือข่าย"*** ต้องดำเนินการโดย ***"ผู้ดูแลระบบ"*** และได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

ข้อ 5 กำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (มาตรา 26) เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ให้มีความถูกต้อง และสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

1) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง และระบุตัวบุคคลที่เข้าถึงสื่อและข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล

2) ให้มีระบบบันทึกข้อมูลการใช้งานของ ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** และบันทึกข้อมูลจากระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น

3) ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ ***"ระบบคอมพิวเตอร์"*** หรือตามแต่จะได้รับคำสั่งเป็นอย่างอื่น

4) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้อง และนำมาใช้ประโยชน์ได้ ***"ผู้ดูแลระบบ"*** ต้องตั้งเวลาของ ***"ระบบคอมพิวเตอร์"*** ให้ตรงกับ ***"เวลาอ้างอิงสากล"*** โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

ข้อ 6 ***"ข้อมูลคอมพิวเตอร์"*** ที่เกี่ยวข้องกับการปฏิบัติงานของ สลน. เมื่อหมดความจำเป็นในการใช้งาน ให้ลบหรือทำลายอย่างถาวร ด้วยวิธีการที่ได้มาตรฐาน เช่น *"DoD 5220.22-M"* เป็นต้น

ข้อ 7 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนดมาตรการควบคุมการใช้งาน ***"ระบบเครือข่าย"*** เพื่อดูแลรักษาความมั่นคงปลอดภัยสารสนเทศ ดังต่อไปนี้

1) ***"หน่วยงานภายนอก"*** ที่ต้องการสิทธิ์ในการเข้าใช้งาน ***"ระบบเครือข่าย"*** จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2) การเข้าถึง ***"ระบบเครือข่าย"*** จากระยะไกล จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยแสดงหลักฐาน และระบุเหตุผลความจำเป็นที่เหมาะสม

3) ห้ามกระทำการใดโดยมิชอบ เพื่อให้การทำงานของ ***"ระบบคอมพิวเตอร์"*** ของผู้อื่นถูกระงับชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

4) ห้ามกระทำการใดโดยมิชอบ เพื่อดักรับไว้ซึ่ง ***"ข้อมูลคอมพิวเตอร์"*** ของผู้อื่นที่อยู่ในระหว่างการส่งใน ***"ระบบคอมพิวเตอร์"***

5) การตั้ง ***"ชื่อเครื่องคอมพิวเตอร์"*** ของ สลน. จะต้องกำหนดและดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

6) การระงับการใช้งานของ ***"คอมพิวเตอร์"*** ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

2.6 การควบคุมการใช้งานอินเทอร์เน็ต

ข้อ 1 ห้ามไม่ให้ใช้ ***"ระบบอินเทอร์เน็ต"*** ของ สลน. เพื่อหาประโยชน์ในเชิงพาณิชย์และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายแก่ สลน.

ข้อ 2 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของ สลน. ที่ยังไม่ได้ประกาศเป็นทางการ ผ่าน ***"ระบบอินเทอร์เน็ต"*** เช่น การโพสต์สู่ *"Social Media"*

ข้อ 3 ห้ามเสนอความคิดเห็นที่มีลักษณะใช้ข้อความยั่วยุให้ร้ายซึ่งก่อให้เกิดความเสื่อมเสียต่อชื่อเสียงของบุคคลอื่น ผ่าน ***"ระบบอินเทอร์เน็ต"*** เช่น การโพสต์สู่ *"Social Media"*

ข้อ 4 ห้ามเผยแพร่ภาพที่เกิดจากการสร้างขึ้น การตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ซึ่งจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ผ่าน ***"ระบบอินเทอร์เน็ต"*** เช่น การโพสต์สู่ *"Social Media"*

ข้อ 5 ห้ามดาวน์โหลด/อัพโหลด ***"ข้อมูลคอมพิวเตอร์"*** ผ่าน ***"ระบบอินเทอร์เน็ต"*** ที่เป็นการละเมิดลิขสิทธิ์

ข้อ 6 ห้ามดาวน์โหลด/อัพโหลด หรือใช้งานข้อมูล ที่มีลักษณะยึดครองช่องสัญญาณการสื่อสารข้อมูลตลอดเวลา ผ่าน ***"ระบบอินเทอร์เน็ต"*** เช่น เล่นเกม/ดูหนัง/คลิปวิดีโอ ดาวน์โหลด/อัพโหลดไฟล์ที่มีขนาดใหญ่ เป็นต้น ในกรณีผู้ใช้งานมีความจำเป็นต้องดาวน์โหลด/อัพโหลดไฟล์ขนาดใหญ่ ให้ติดต่อ ***"ผู้ดูแลระบบ"*** เท่านั้น

ข้อ 7 เซิร์ฟเวอร์ที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณี

2.7 การควบคุมการใช้ไฟร์วอลล์

ข้อ 1 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีอำนาจหน้าที่ในการบริหารจัดการการติดตั้งและ กำหนดค่าของ ***"ไฟร์วอลล์"***

ข้อ 2 การกำหนดค่า **"Default"** พื้นฐานของทุกเครือข่ายจะต้องเป็นการกำหนดค่าปฏิเสธทั้งหมด

ข้อ 3 บริการอินเทอร์เน็ต และช่องทางการเชื่อมต่อที่ไม่ได้รับอนุญาต จะต้องถูกบล็อก (Block) โดย ***"ไฟร์วอลล์"***

ข้อ 4 จะต้องมี ***"การตั้งค่าระบบ"*** ของ ***"ไฟร์วอลล์"*** ให้ ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** ทำการ ***"ล็อกอิน"*** ก่อนการใช้งานทุกครั้ง

ข้อ 5 จะต้องมี ***"การตั้งค่าระบบ"*** ของ ***"ไฟร์วอลล์"*** ให้ส่งข้อมูลจราจรทางคอมพิวเตอร์ไปยังอุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

ข้อ 6 จะต้องมี ***"การตั้งค่าระบบ"*** ของ ***"ไฟร์วอลล์"*** อนุญาตให้เซิร์ฟเวอร์สามารถใช้พอร์ตการเชื่อมต่อเฉพาะที่จำเป็นเท่านั้น

ข้อ 7 จะต้องมีการจดบันทึกและสำรอง ***"การตั้งค่าระบบ"*** ของ ***"ไฟร์วอลล์"*** เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลง

ข้อ 8 ผู้ละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการนายกรัฐมนตรี จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

2.8 การควบคุมการใช้เครือข่ายไร้สาย

ข้อ 1 ***"ผู้ดูแลระบบ"*** มีหน้าที่ควบคุมการใช้งานเครือข่ายไร้สาย ดังนี้

1) ต้องควบคุมการกระจายสัญญาณของ *"Access Point"* ให้รั่วไหลออกนอก ***"พื้นที่ใช้งานระบบเครือข่ายไร้สาย"*** ให้น้อยที่สุด

2) ต้องทำการเปลี่ยนค่า **"Default"** ของ SSID (Service Set Identifier) เป็นค่าที่เหมาะสมทันที ก่อนนำ *"Access Point"* มาใช้งาน

3) ต้องกำหนดค่าให้มีการเข้ารหัสข้อมูลที่สื่อสารระหว่าง *"Access Point"* และ *"Wireless LAN Client"* ตามมาตรฐาน *"IEEE 802.1X"* หรือ *"WPA"*

4) ควรเลือกใช้วิธีการควบคุม ***"ชื่อผู้ใช้งาน"*** และ ***"รหัสผ่าน"*** ของ ***"ผู้ใช้บริการ"***และ ***"หน่วยงานภายนอก"*** ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี ***"ชื่อผู้ใช้งาน"*** และ ***"รหัสผ่าน"*** ตามที่กำหนดไว้เท่านั้น

5) จะต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุกๆ 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ ***"ผู้ดูแลระบบ"***รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ 2 ***"ผู้ดูแลระบบ"*** มีหน้าที่ควบคุมการใช้งานเครือข่ายไร้สายของ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"*** ดังนี้

1) กำหนดให้ ***"ผู้ใช้บริการ"***และ ***"หน่วยงานภายนอก"*** ในระบบเครือข่ายไร้สาย ผ่านระบบเครือข่ายภายนอก สามารถติดต่อสื่อสารกับเครือข่ายภายในของ สลน. ผ่านระบบ *"VPN"* เท่านั้น

2) ต้องควบคุมดูแลไม่ให้***"ผู้ใช้บริการ"***และ ***"หน่วยงานภายนอก"***ที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สาย ในการเข้าสู่ระบบ ***"ระบบอินทราเน็ต"*** และฐานข้อมูลภายในของหน่วยงาน

2.9 การควบคุมการใช้จดหมายอิเล็กทรอนิกส์

ข้อ 1 ***"ผู้ใช้บริการ"*** ต้องลงทะเบียนบัญชีผู้ใช้ ***"จดหมายอิเล็กทรอนิกส์"*** โดยทำการกรอกข้อมูลขอรับบริการ ***"จดหมายอิเล็กทรอนิกส์"***

ข้อ 2 ***"ผู้ใช้บริการ"*** ที่ได้รับ ***"บัญชีผู้ใช้งาน"*** ***"จดหมายอิเล็กทรอนิกส์"*** จากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องปฏิบัติดังนี้

1) พึงระวังไม่ให้ผู้อื่นเข้าถึง ***"บัญชีผู้ใช้งาน"*** ของตนเอง เพื่อรักษาความลับเฉพาะบุคคล และไม่อนุญาตให้ผู้อื่นเข้าใช้ ***"จดหมายอิเล็กทรอนิกส์"*** ในนามของตนเองในทุกกรณี โดยเป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้ ***"จดหมายอิเล็กทรอนิกส์"***

2) พึงทราบว่า ***"ผู้ดูแลระบบ"*** ไม่มีสิทธิหน้าที่ที่จะถามหรือร้องขอให้ ***"ผู้ใช้บริการ"*** เปิดเผย ***"รหัสผ่าน"*** เพื่อเข้าถึงบัญชี ***"จดหมายอิเล็กทรอนิกส์"***

3) **ห้าม**ไม่ให้ใช้ ***"จดหมายอิเล็กทรอนิกส์"*** ในลักษณะต่อไปนี้

(1) เพื่อการประกอบธุรกิจ

(2) ส่งเป็นจดหมายลูกโซ่

(3) เผยแพร่ข้อมูลที่มีชั้นความลับของทางราชการ

(4) ปลอมแปลงหรือดัดแปลงชื่อผู้ส่งว่าเป็นบุคคลอื่น

(5) ปกปิดหรือดัดแปลงให้ไม่ทราบชื่อผู้ส่ง

(6) ปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันและเวลาการส่ง

(7) เผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่มีลักษณะ ดังนี้

(7.1) กล่าวร้าย ดูหมิ่น เหยียดหยาม หรือแบ่งแยกทาง ศาสนา เชื้อชาติ หรือเพศ ต่อบุคคลหรือกลุ่มบุคคล

(7.2) หยาบคาย หรือลามกอนาจาร

(7.3) โปรแกรมหรืองาน หรือรหัสสำหรับใช้เข้าถึงโปรแกรมหรืองานในลักษณะที่ละเมิดลิขสิทธิ์

(7.4) ความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

(7.5) โฆษณาสินค้า ผลิตภัณฑ์ หรือส่งข้อความลักษณะของ สแปมเมล (Spam)

(8) ส่ง ***"จดหมายอิเล็กทรอนิกส์"*** ซึ่งอาจส่งผลกระทบต่อประสิทธิภาพการทำงานของ ***"จดหมายอิเล็กทรอนิกส์"*** หรือ ***"ระบบเครือข่าย"***

(9) ส่งต่อ ***"จดหมายอิเล็กทรอนิกส์"*** ที่ไม่ทราบแหล่งที่มา หรือมีแหล่งที่มาไม่น่าเชื่อถือ

(10) ส่งต่อ ***"จดหมายอิเล็กทรอนิกส์"*** เพื่อใช้ประโยชน์ในเชิงธุรกิจ หรือการพาณิชย์

ข้อ 3 การใช้บัญชีรายชื่อผู้ใช้จดหมายอิเล็กทรอนิกส์ (Global Address List) มีแนวทางปฏิบัติดังนี้

1) ***"ผู้ใช้บริการ"*** สามารถใช้บัญชีรายชื่อผู้ใช้จดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลข่าวสารและประชาสัมพันธ์ได้

2) ***"ผู้ใช้บริการ"*** อาจร้องขอให้ ***"ผู้ดูแลระบบ"*** จัดทำบัญชีรายชื่อผู้ใช้จดหมายอิเล็กทรอนิกส์ ในลักษณะกลุ่ม (Group Address List) เพื่อให้ผู้ใช้สมัครเข้าเป็นสมาชิกกลุ่มเพื่อรับข่าวสาร โดยสามารถถอนการเป็นสมาชิกเพื่องดรับข่าวสารนั้นได้ตลอดเวลา

3) ***"ผู้ดูแลระบบ"*** สามารถใช้บัญชีรายชื่อผู้ใช้จดหมายอิเล็กทรอนิกส์ เพื่อแจ้งเตือน หรือแจ้งข่าวที่เกี่ยวข้องกับความมั่นคงปลอดภัยของ ***"คอมพิวเตอร์"***และ ***"ระบบเครือข่าย"***

ข้อ 4 การตรวจสอบและเฝ้าระวังการใช้งาน ***"จดหมายอิเล็กทรอนิกส์"***

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารสงวนสิทธิ์ในการใช้ระบบเฝ้าระวัง เพื่อตรวจเนื้อหา ***"จดหมายอิเล็กทรอนิกส์"*** ที่เป็นภัยต่อ ***"ระบบคอมพิวเตอร์"*** และกลั่นกรองหรือระงับการเผยแพร่นั้นโดยอัตโนมัติ ตลอดจนสงวนสิทธิ์การเข้าถึง ***"จดหมายอิเล็กทรอนิกส์"*** เพื่อสืบสวน สอบสวน เมื่อระบบเฝ้าระวังแจ้งเตือนถึงปัญหาด้านความมั่นคงปลอดภัยจากการใช้ ***"จดหมายอิเล็กทรอนิกส์"*** หรือการร้องขอจากเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

ข้อ 5 การระงับและเพิกถอนสิทธิ์การใช้งาน ***"จดหมายอิเล็กทรอนิกส์"***

1) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่ในการระงับและเพิกถอนสิทธิ์การใช้งานโดยไม่ต้องแจ้งให้ ***"ผู้ใช้บริการ"*** ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหาความมั่นคงปลอดภัยหรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ

2) เมื่อ ***"ผู้ใช้บริการ"*** พ้นสภาพการเป็นบุคลากรในสังกัดของ สลน. ***"ผู้ดูแลระบบ"*** มีหน้าที่ในการระงับและเพิกถอนสิทธิ์การใช้งานของ ***"ผู้ใช้บริการ"***

ส่วนที่ 3
แนวปฏิบัติในการสำรองข้อมูล (Backup)

ข้อ 1 การ Backup ข้อมูลใน ***"คอมพิวเตอร์"***

"ผู้ใช้บริการ" และ ***"หน่วยงานภายนอก"*** มีหน้าที่ Backup และเก็บรักษาข้อมูลของตนเอง

ข้อ 2 การ Backup ข้อมูลของเซิร์ฟเวอร์ และอุปกรณ์เครือข่าย

"ผู้ดูแลระบบ" มีหน้าที่ Backup โปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ ระบบฐานข้อมูล และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ในรูปแบบของ System Images เพื่อง่ายต่อการ Restore หรือ Recovery ระบบให้สามารถกลับคืนมาให้บริการได้ดีดังเดิม

ข้อ 3 การดำเนินงานตามข้อ 2 ***"ผู้ดูแลระบบ"*** มีหน้าที่จัดทำรายละเอียดการดำเนินงานอย่างน้อยดังนี้

1) ข้อมูลที่ต้อง Backup และความถี่ในการ Backup

2) ประเภทสื่อที่ใช้ Backup

3) จำนวนที่ต้อง Backup

4) วิธีการเก็บรักษาสื่อที่ใช้ Backup

5) จัดทำป้ายชื่อระบุประเภทข้อมูลที่ Backup วันที่ เวลา ที่ Backup ข้อมูล และผู้รับผิดชอบในการ Backup ข้อมูลไว้อย่างชัดเจน

ข้อ 4 ควรมีขั้นตอนการปฏิบัติและความถี่ในการทดสอบ Restore จากสื่อที่ใช้ Backup

ข้อ 5 ต้องจัดเก็บสื่อที่ใช้ Backup พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้า-ออก และระบบป้องกันความเสียหายจากสภาพแวดล้อมหรือภัยพิบัติต่างๆ

ข้อ 6 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถ Restore หรือ Recovery กลับคืนมาได้ภายในระยะเวลาที่เหมาะสม โดยแผนฉุกเฉินมีรายละเอียดดังนี้

1) ต้องจัดลำดับความสำคัญของระบบงาน และระยะเวลาในการ Restore หรือ Recovery

2) ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

3) ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

4) ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

5) ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น คุณลักษณะของ ***"คอมพิวเตอร์"*** และอุปกรณ์เครือข่าย เป็นต้น

6) ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น

7) ต้องปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ ควรเก็บแผนฉุกเฉินไว้นอกสถานที่ และต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง เป็นการทดสอบในลักษณะการจำลองสถานการณ์จริงเพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบ

8) แผนฉุกเฉินจะต้องให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

9) ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหาและวิธีการแก้ไขปัญหา

ส่วนที่ 4
แนวปฏิบัติในการป้องกันโปรแกรมประสงค์ร้าย (Malware)

ข้อ 1 ***"คอมพิวเตอร์"*** ของ ***"ผู้ใช้บริการ"*** ต้องติดตั้งโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัด ***"โปรแกรมประสงค์ร้าย"*** และต้องปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ 2 ***"ผู้ใช้บริการ"*** ควรทำการ Update patch หรือ upgrade ซอฟต์แวร์ รวมถึงซอฟต์แวร์ระบบปฏิบัติการอย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เพื่อป้องกันการโจมตีจากภัยคุกคาม

ข้อ 3 ห้ามติดตั้งโปรแกรมหรือซอฟต์แวร์ต่างๆ ที่ได้มาจากแหล่งที่ไม่น่าเชื่อถือ เช่น ได้มาจากเว็บไซต์ที่ให้ดาวน์โหลดซอฟต์แวร์ที่มีการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต หรือติดตั้งโปรแกรมที่เป็นการละเมิดลิขสิทธิ์หรือนโยบายของหน่วยงาน ซึ่งอาจทำให้เครื่องคอมพิวเตอร์มีความเสี่ยงกับ***"โปรแกรมประสงค์ร้าย"***

ข้อ 4 กรณีที่ต้องแชร์ไฟล์ข้อมูลต่างๆ ให้ทำการแชร์แบบอ่านอย่างเดียว (Read Only) เพื่อป้องกันปัญหาเกี่ยวกับ***"โปรแกรมประสงค์ร้าย"*** ถ้าจำเป็นต้องทำการแชร์แบบ Read-Write ให้กำหนดรหัสผ่านสำหรับการแชร์แบบ Write ทุกครั้ง

ข้อ 5 การใช้ ***"สื่อบันทึกพกพา"*** หรือการรับ-ส่ง ***"ข้อมูลคอมพิวเตอร์"*** หรือ ***"สารสนเทศ"*** ผ่านทาง ***"ระบบเครือข่าย"*** ควรมีการตรวจสอบเพื่อป้องกันและกำจัด ***"โปรแกรมประสงค์ร้าย"***

ข้อ 6 ถ้า ***"ผู้ใช้บริการ"*** หรือ ***"หน่วยงานภายนอก"*** พบหรือสงสัยว่า ***"คอมพิวเตอร์"*** ติด ***"โปรแกรมประสงค์ร้าย"*** ให้แจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทันที

ข้อ 7 ***"ผู้ใช้บริการ"*** หรือ ***"หน่วยงานภายนอก"*** ควรตรวจสอบ ***"ไฟล์ที่สามารถประมวลผลได้"*** ก่อนทำการเปิดใช้งาน

ส่วนที่ 5
แนวปฏิบัติในการประเมินความเสี่ยง (Risks)

ข้อ 1 ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยง ดังต่อไปนี้

1) ความเสี่ยงของ ***"ระบบคอมพิวเตอร์"*** และ ***"ระบบเครือข่าย"***

2) ความเสี่ยงจากสภาพแวดล้อมทางกายภาพ เช่น เหตุการณ์ความไม่สงบของบ้านเมือง ภัยพิบัติทางธรรมชาติต่างๆ ระบบไฟฟ้า เป็นต้น

3) ความเสี่ยงที่เกิดจากการปฏิบัติงานของ ***"ผู้ดูแลระบบ"*** ***"ผู้ใช้บริการ"*** และ ***"หน่วยงานภายนอก"***

4) ความเสี่ยงของการเข้าถึง ***"สารสนเทศ"*** และ **"ระบบเทคโนโลยีสารสนเทศ"**

5) ความเสี่ยงต่อการละเมิดทางกฎหมาย

ข้อ 2 กำหนดวิธีการประเมินความเสี่ยงที่เหมาะสมกับการบริหารจัดการ **"ระบบเทคโนโลยีสารสนเทศ"** ของ สลน.โดยกำหนดเกณฑ์ในการยอมรับความเสี่ยง และระบุความเสี่ยงที่ยอมรับได้

ข้อ 3 วิเคราะห์และประเมินความเสี่ยงโดยคำนึงถึงองค์ประกอบดังต่อไปนี้

1) ความรุนแรงของผลกระทบที่เกิดจากเหตุการณ์ที่ระบุ

2) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ รวมถึงความเป็นไปได้ที่จะเกิดขึ้น

3) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

ข้อ 4 การประเมินผลในภาพรวมของความเสี่ยงที่ระบุต้องจัดทำเป็นคะแนนโดยมีคะแนนเต็ม 100 คะแนน และกำหนดให้มีเกณฑ์ในการพิจารณาว่าความเสี่ยงที่ระบุนั้นต้องมีการบริหารจัดการเพื่อลดความเสี่ยงนั้นหรือไม่ โดยให้เกณฑ์เป็น 80 คะแนนขึ้นไป

ส่วนที่ 6
แนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ (Awareness)

ข้อ 1 จัดให้บุคลากรที่ได้รับมอบหมายดูแลนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ เข้ารับการอบรมอย่างสม่ำเสมอ เพื่อให้มีความตระหนักรู้ ศักยภาพ และขีดความสามารถที่จะปฏิบัติงานตามที่กำหนด

ข้อ 2 จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักให้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสาสนเทศแก่บุคลากรของ สลน. การจัดสัมมนาควรจัดปีละไม่น้อยกว่า 1 ครั้ง และเชิญวิทยากรจากภายนอกที่มีความเชี่ยวชาญ ประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาให้ความรู้แก่บุคลากรของ สลน.

ข้อ 3 เผยแพร่ความรู้เกี่ยวกับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้ หรือข้อควรระวังให้กับบุคลากรของ สลน.ได้รับทราบในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยผ่านทาง ***"ระบบเครือข่าย"*** ภายในหน่วยงาน (Intranet) และติดประกาศโดยมีการปรับปรุงเกร็ดความรู้ให้ทันต่อความเจริญก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไป

ข้อ 4 ต้องมีการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้มีการดำเนินการที่เหมาะสมพอเพียงและสัมฤทธิ์ผล

ส่วนที่ 7
แนวปฏิบัติในการใช้ Social Media

"ผู้ใช้บริการ" และ***"หน่วยงานภายนอก"*** ต้องตระหนักในการใช้ *"Social Media"* ดังนี้

ข้อ 1 ระมัดระวังในการสื่อสารข้อมูลหรือความคิดเห็นที่อาจนำไปสู่การโต้แย้งที่รุนแรง เช่น ประเด็นทางการเมือง เชื้อชาติ ศาสนา รวมทั้งการวิพากษ์วิจารณ์องค์กรและสถาบันต่างๆ เป็นต้น

ข้อ 2 ไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น จะต้องระบุแหล่งที่มาของข้อมูลที่นำใช้กล่าวอ้างอิง

ข้อ 3 ต้องรับผิดชอบต่อสิ่งที่เผยแพร่ผ่านสื่อสังคมออนไลน์ที่สามารถเข้าถึงโดยสาธารณะ หากการกระทำนั้นก่อให้เกิดความเสียหายแก่บุคคลอื่น

ข้อ 4 นำเสนอข้อมูลที่ตรงกับความเป็นจริง รวมถึงการใช้ถ้อยคำและภาษาที่เหมาะสม โดยแยกแยะระหว่างข้อมูล ข้อเท็จจริง และข่าวสาร หลีกเลี่ยงการนำเสนอข้อมูลที่อาจก่อให้เกิดความเข้าใจผิด

เอกสารอ้างอิง

1. พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
2. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.0) ประจำปี 2549 คณะอนุกรรมการด้านความมั่นคง ในคณะกรรมการธุรกรรมอิเล็กทรอนิส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
3. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
4. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551
5. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
6. แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานภาครัฐ สุรางคณา วายุภาพ ผอ. ฝ่ายกฎหมาย สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
7. แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี พ.ศ.2554
8. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
9. การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO 27001 http://www.acinfotec.com ค้นคืนวันที่ 15 พฤษภาคม 2561
10. มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001 และ ISO/IEC 17799 ฉบับประเทศไทย http://www.oknation.net ค้นคืนวันที่ 15 พฤษภาคม 2561