ประกาศสำนักงานสถิติแห่งชาติ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงานสถิติแห่งชาติ พ.ศ. ๒๕๖๗

ด้วย สำนักงานสถิติแห่งชาติ มีบทบาทและอำนาจหน้าที่ตามพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ ในฐานะเป็นหน่วยงานกลางของรัฐ เกี่ยวกับการดำเนินการด้านสถิติของประเทศ บริหารจัดการสถิติและสารสนเทศของชาติอย่างเป็นระบบเพื่อการพัฒนา และเสริมสร้างศักยภาพการแข่งขัน โดยการจัดทำสำมะโนหรือสำรวจด้วยตัวอย่าง การอำนวยการเพื่อให้ได้ฐานข้อมูลทางด้านเศรษฐกิจสังคม เทคโนโลยีสารสนเทศ และอื่น ๆ ของประเทศ รวมทั้งการให้ความร่วมมือและประสานงานกับองค์กรระหว่างประเทศในงานเกี่ยวกับสถิติ ปัจจุบันสำนักงานสถิติแห่งชาตินำระบบคอมพิวเตอร์เครือข่าย และวิธีการทางอิเล็กทรอนิกส์มาใช้ในกระบวนการบริหารจัดการระบบสถิติ กระบวนการผลิตข้อมูลสถิติ กระบวนการให้บริการข้อมูลสถิติและสารสนเทศ เพื่อให้เกิดประสิทธิภาพสูงสุดในการปฏิบัติงาน

อาศัยอำนาจตามความใน มาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกอบประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม พ.ศ. ๒๕๕๖ จึงให้ยกเลิกประกาศสำนักงานสถิติแห่งชาติ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติ พ.ศ. ๒๕๖๖ และให้ใช้ประกาศฉบับนี้แทน เพื่อเป็นแนวทางให้ทุกภาคส่วนขององค์กรนำไปปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความเชื่อถือต่อผู้ใช้ข้อมูลและสารสนเทศ โดยมีเนื้อหาสาระดังต่อไปนี้

ข้อ ๑ สำนักงานสถิติแห่งชาติได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติ ดังนี้

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

รายละเอียดตามเอกสารแนบท้ายประกาศ โดยประกอบด้วย ๑๔ หมวด ดังนี้

หมวด ๑ นโยบายความมั่นคงปลอดภัย (Security Policy)

หมวด ๒ โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)

หมวด ๓ การสร้างความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)

หมวด ๔ การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

หมวด ๕ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ (Access Control)

หมวด ๖...

หมวด ๖ การเข้ารหัสข้อมูล (Cryptography)
หมวด ๗ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
หมวด ๘ ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operations Security)
หมวด ๙ ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)
หมวด ๑๐ การจัดหา การพัฒนา และการบำรุงรักษา (Information System Acquisition Development and Maintenance)
หมวด ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)
หมวด ๑๒ การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident Management)
หมวด ๑๓ การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง (Government Continuity Management)
หมวด ๑๔ การปฏิบัติตามข้อกำหนด (Compliance)

ข้อ ๒ ให้ข้าราชการ พนักงานราชการ ลูกจ้าง ผู้ปฏิบัติงานภายในสำนักงานสถิติแห่งชาติและผู้ที่มาติดต่อราชการ ณ สำนักงานสถิติแห่งชาติ ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติโดยเคร่งครัด

ข้อ ๓ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติ ให้มีความทันสมัยเป็นปัจจุบัน และเป็นมาตรฐานที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๖ กันยายน พ.ศ. ๒๕๖๗

(นางปิยนุช วุฒิสอน)
ผู้อำนวยการสำนักงานสถิติแห่งชาติ

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานสถิติแห่งชาติ พ.ศ. ๒๕๖๗

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงานสถิติแห่งชาติ พ.ศ. ๒๕๖๗

คณะทำงานทบทวนนโยบายแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
และความมั่นคงปลอดภัยสารสนเทศ

สารบัญ

องค์ประกอบของนโยบาย

นโยบายความมั่นคงปลอดภัยสารสนเทศได้กำหนดองค์ประกอบที่สำคัญของการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย โดยครอบคลุมทั้งด้านการควบคุมการเข้าถึง การกำหนดขั้นตอนและกระบวนการที่เหมาะสม ตามหลักมาตรฐานสากล ซึ่งมีองค์ประกอบ ๑๔ หมวด ดังนี้

หมวด ๑ นโยบายความมั่นคงปลอดภัย (Security Policy) นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับการใช้งานระบบสารสนเทศของ สสช. เพื่อให้สอดคล้องกับข้อกำหนดทางราชการ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งจัดทำเป็นลายลักษณ์อักษร โดยที่ฝ่ายบริหารเห็นชอบและอนุมัติ และเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับรู้ มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สสช. ตามระยะเวลาที่กำหนดพร้อมทั้งปรับเปลี่ยนนโยบายตามความเหมาะสม

หมวด ๒ โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security) นโยบายนี้มีวัตถุประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์สารสนเทศของ สสช. ที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับบุคคลหรือหน่วยงานภายนอก โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย มีการประสานงานความรับผิดชอบ ประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับหน่วยงานภายนอกและผู้ใช้งานสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สสช.

หมวด ๓ การสร้างความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security) นโยบายนี้มีวัตถุประสงค์เพื่อให้ เจ้าหน้าที่ บุคคลภายนอก และหน่วยงานภายนอกเข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงานซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

หมวด ๔ การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management) นโยบายนี้มีวัตถุประสงค์เพื่อป้องกันทรัพย์สินของ สสช. จากความเสียหายที่อาจเกิดขึ้น และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีทรัพย์สิน ระบุผู้เป็นเจ้าของทรัพย์สิน และกำหนดหลักเกณฑ์การใช้งานทรัพย์สินที่เหมาะสม มีการจัดหมวดหมู่ทรัพย์สินตามระดับชั้นความลับ และจัดทำป้ายชื่อ เพื่อการบริหารจัดการทรัพย์สินตามที่ได้จัดหมวดหมู่ไว้

หมวด ๕ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ (Access Control) นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดและจัดทำแนวปฏิบัติตลอดจนกระบวนการในการควบคุมการเข้าใช้งานระบบเครือข่ายและบริการบนเครือข่ายตามความต้องการในการปฏิบัติราชการ โดยการกำหนดการบริหารจัดการและการใช้งานสารสนเทศของผู้ใช้งานรวมถึงการลงทะเบียนผู้ใช้งาน การบริหารจัดการสิทธิในการใช้ระบบการบริหารจัดการข้อมูลและสารสนเทศที่กำหนดชั้นความลับในการพิสูจน์ตัวตนของผู้ใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน การกำหนดหน้าที่

ความรับผิดชอบของผู้ใช้งานในการปฏิบัติตามวิธีปฏิบัติขององค์กร กำหนดระเบียบปฏิบัติงานเรื่องการเข้าถึงระบบ (Login) อย่างปลอดภัย การกำหนดระบบบริหารจัดการรหัสผ่านการใช้ซอฟต์แวร์อรรถประโยชน์ (Utility Program) และการควบคุมการเข้าถึงซอฟต์แวร์ต้นฉบับ (Source Code)

หมวด ๖ การเข้ารหัสข้อมูล (Cryptography) นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดให้มีการเข้ารหัสอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันการเปิดเผยความลับของข้อมูล การปลอมแปลงข้อมูลและรักษาไว้ซึ่งความสมบูรณ์ถูกต้องของข้อมูล โดยมีการกำหนดแนวปฏิบัติและมาตรการเข้ารหัสข้อมูลรวมถึงการบริหารจัดการกุญแจรหัสข้อมูล (Cryptography key)

หมวด ๗ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) นโยบายนี้มีวัตถุประสงค์เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ป้องกันทรัพย์สินไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซงป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันไม่ให้กิจกรรมการดำเนินงานต่าง ๆ ของ สสช. เกิดการติดขัดหรือหยุดชะงัก เช่น การมีระบบกระแสไฟฟ้าสำรองและการมีระบบสื่อสารสำรอง เป็นต้น

หมวด ๘ ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operations Security) นโยบายนี้มีวัตถุประสงค์เพื่อให้การดำเนินงานของอุปกรณ์ที่เกี่ยวข้องเป็นไปอย่างถูกต้องปลอดภัย จึงจัดทำขั้นตอนการปฏิบัติงาน และกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจนสำหรับการป้องกันโปรแกรมประสงค์ร้าย โปรแกรมที่ไม่อนุญาต การสำรองข้อมูล การเก็บข้อมูลประวัติการเข้าใช้งานระบบ (Log File) การเฝ้าระวังการควบคุมการติดตั้งซอฟต์แวร์ รวมถึงการบริหารจัดการช่องโหว่

หมวด ๙ ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security) นโยบายนี้มีวัตถุประสงค์เพื่อสร้างความมั่นคงปลอดภัยข้อมูลและสารสนเทศ บนระบบเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ โดยมีการกำหนดการบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย และการถ่ายโอนข้อมูลและสารสนเทศ รวมถึงข้อกำหนดในการรักษาความลับ หรือการไม่เปิดเผยความลับ ซึ่งมีผลบังคับใช้กับเจ้าหน้าที่ขององค์กร รวมถึงบุคคลภายนอก

หมวด ๑๐ การจัดหา การพัฒนา และบำรุงรักษาระบบ (Information System Acquisition Development and Maintenance) นโยบายนี้มีวัตถุประสงค์เพื่อให้เจ้าของข้อมูลและสารสนเทศ ที่ดำเนินการจัดหา จัดจ้างพัฒนาและบำรุงรักษา ต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่สำคัญขององค์กร โดยพิจารณาทุกขั้นตอนและครอบคลุมถึงระบบที่ใช้ในการพัฒนา ทดสอบ รวมทั้งข้อมูลที่ใช้ในการทดสอบ

หมวด ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships) นโยบายนี้มีวัตถุประสงค์เพื่อป้องกันการเข้าถึงทรัพย์สินขององค์กรจากผู้ให้บริการภายนอก โดยกำหนดแนวทางปฏิบัติการบริหารจัดการและทำข้อตกลงเป็นลายลักษณ์อักษรกับผู้ให้บริการภายนอกในการเข้าถึงทรัพย์สินขององค์กร

หมวด ๑๒ การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident Management) นโยบายนี้มีวัตถุประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สสช. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศของ สสช.

หมวด ๑๓ การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง (Government Continuity Management) นโยบายนี้มีวัตถุประสงค์เพื่อวางแผน จัดทำคู่มือ สำหรับนำไปปฏิบัติ บำรุงรักษา ตรวจสอบ ควบคุม และประเมินผลความต่อเนื่องด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ให้มั่นใจว่าระดับความมั่นคงปลอดภัยอยู่ในเกณฑ์ที่ยอมรับได้ในกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์ รวมถึงมีการเตรียมระบบที่สามารถสร้างความต่อเนื่องของระบบเทคโนโลยีสารสนเทศให้พร้อมใช้งานอยู่เสมอ

หมวด ๑๔ การปฏิบัติตามข้อกำหนด (Compliance) นโยบายนี้มีวัตถุประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อการปฏิบัติราชการน้อยที่สุด

นโยบายความมั่นคงปลอดภัยสารสนเทศแต่ละหมวดที่กล่าวมาข้างต้นประกอบด้วย วัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องในหมวดนั้น ๆ มีรายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสียหายต่อการปฏิบัติงาน เป็นหน่วยงานที่ได้รับการยอมรับจากองค์กรต่าง ๆ ในการปฏิบัติราชการได้อย่างมั่นคงปลอดภัยตามมาตรฐานสากล ซึ่งนโยบายความมั่นคงปลอดภัยสารสนเทศนี้ถือเป็นมาตรฐานด้านความมั่นคงปลอดภัย ซึ่งเจ้าหน้าที่ทุกระดับ บุคคลภายนอก และหน่วยงานภายนอกที่เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรต้องรับทราบ มีความเข้าใจ และสามารถปฏิบัติตามแนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศของสำนักงานสถิติแห่งชาติได้อย่างเคร่งครัด

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดการเสียหาย หรือได้รับอันตรายใด ๆ อันเป็นการสร้างความเสียหายแก่องค์กรหรือผู้หนึ่งผู้ใด เนื่องมาจากความบกพร่อง การละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงสุดต้องเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น และกำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ รวมถึงกำหนดให้มีการปฏิบัติที่ชัดเจนและมีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

คำนิยาม

๑) “สำนักงานสถิติแห่งชาติ” หมายความว่า หน่วยงานภายในสังกัด สำนักงานสถิติแห่งชาติ รวมถึง สำนักงานสถิติจังหวัด

๒) “กระบวนการสถิติ” หมายความว่า กระบวนการผลิตข้อมูลสถิติ กระบวนการให้บริการข้อมูลสถิติ กระบวนการบริหารจัดการระบบสถิติ

๓) “กระบวนการที่สร้างคุณค่า” หมายความว่า กระบวนการที่สร้างคุณค่า และกระบวนการสนับสนุน

๔) “กระบวนการสนับสนุน” หมายความว่า กระบวนการเทคโนโลยีและสารสนเทศ กระบวนการพัฒนาบุคลากร กระบวนการประชาสัมพันธ์ กระบวนการบริหารจัดการองค์ความรู้ด้านสถิติ กระบวนการบริหารทั่วไป กระบวนการประสานความร่วมมือด้านสถิติกับหน่วยงานภายในและต่างประเทศ

๕) “ผู้ใช้งาน” หมายความว่า เจ้าหน้าที่สำนักงานสถิติแห่งชาติ ผู้ติดต่อราชการ และผู้ใช้ภายนอก

๖) “เจ้าหน้าที่สำนักงานสถิติแห่งชาติ” หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว จ้างเหมารายวัน

๗) “ผู้ติดต่อราชการ” หมายความว่า ผู้รับบริการข้อมูล ผู้รับการฝึกอบรม ผู้เข้าร่วมประชุม และผู้สนับสนุนจากภายนอก

๘) “ผู้ใช้ภายนอก” หมายความว่า ผู้ใช้ทั่วไป และผู้ใช้สมาชิก ที่เข้าถึงผ่านระบบเครือข่ายอินเทอร์เน็ต

๙) “ผู้ใช้ทั่วไป” หมายความว่า บุคคลภายนอกที่ใช้ระบบสารสนเทศโดยไม่จำเป็นต้องลงทะเบียนสมาชิก

๑๐) “ผู้ใช้สมาชิก” หมายความว่า บุคคลภายนอกที่ผ่านการลงทะเบียนเพื่อใช้ระบบสารสนเทศที่เปิดให้บริการ

๑๑) “ผู้สนับสนุนจากภายนอก” หมายความว่า เจ้าหน้าที่จากหน่วยงานภายนอกที่เข้ามาสนับสนุนการดำเนินงานให้กับสำนักงานสถิติแห่งชาติ

๑๒) “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับทรัพย์สินสารสนเทศ

๑๓) “ทรัพย์สิน” หมายความว่า ทรัพย์สินสารสนเทศของสำนักงานสถิติแห่งชาติ ประกอบด้วย

(๑) ระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบความมั่นคงปลอดภัย และระบบงานคอมพิวเตอร์

(๒) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(๓) ซอฟต์แวร์ โปรแกรมประยุกต์ และระบบสารสนเทศ

(๔) ข้อมูลและสารสนเทศสถิติ ในรูปข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๑๔) “ระบบสารสนเทศ” หมายความว่า ระบบงานคอมพิวเตอร์ที่สนับสนุนในกระบวนงานของสำนักงานสถิติแห่งชาติ ประกอบด้วย

(๑) ระบบสารสนเทศเพื่อการบริหารจัดการองค์กร

(๒) ระบบสารสนเทศเพื่อการผลิตข้อมูล

(๓) ระบบสารสนเทศเพื่อการบริการข้อมูลและสารสนเทศสถิติ

(๔) ระบบสารสนเทศเพื่อการจัดการระบบสถิติ

๑๕) “ระบบสารสนเทศเพื่อการบริหารจัดการองค์กร” หมายความว่า โปรแกรมประยุกต์ที่ใช้สนับสนุนการบริหารจัดการองค์กร ผู้มีสิทธิเข้าถึงเฉพาะเจ้าหน้าที่สำนักงานสถิติแห่งชาติเท่านั้น

๑๖) “ระบบสารสนเทศเพื่อการผลิตข้อมูล” หมายความว่า โปรแกรมประยุกต์ที่ใช้สนับสนุนการดำเนินงานในกระบวนการจัดเก็บ ประมวลผล และวิเคราะห์ข้อมูล

๑๗) “ระบบสารสนเทศเพื่อการบริการข้อมูลและสารสนเทศสถิติ” หมายความว่า โปรแกรมประยุกต์ที่ใช้สนับสนุนการดำเนินงานในการให้บริการกับผู้ใช้ข้อมูลทั่วไป และผู้ใช้สมาชิก

๑๘) “ระบบสารสนเทศเพื่อการจัดการระบบสถิติ” หมายความว่า โปรแกรมประยุกต์ที่ใช้สนับสนุนการจัดการระบบสถิติของประเทศ

๑๙) “ข้อมูล” หมายความว่า ข้อความจริงเกี่ยวกับเรื่องใดเรื่องหนึ่ง อาจเป็นไปได้ทั้งข้อความและตัวเลขที่ประมวลผลได้ อาทิ ข้อมูลปฐมภูมิ ข้อมูลทุติยภูมิ ข้อมูลอนุกรมเวลา ข้อมูลมาตรวัด ข้อมูลดิบ ข้อมูลระดับย่อย ข้อมูลเฉพาะบุคคลหรือเฉพาะราย ข้อมูลสถิติ

๒๐) “ข้อมูลดิบ” หมายความว่า ข้อมูลที่ยังไม่ผ่านกระบวนการใด ๆ เพื่อให้เกิดผลลัพธ์ที่มีความหมายซึ่งนำไปใช้ประโยชน์ได้

๒๑) “ข้อมูลระดับย่อย” หมายความว่า ข้อมูลดิบทั้งหมดที่ผ่านการตรวจสอบความถูกต้อง ความครบถ้วน และความแนบนัยของข้อมูลไว้เรียบร้อยแล้ว พร้อมที่จะนำไปใช้ในการประมวลผลเป็นสถิติต่อไป

๒๒) “ข้อมูลเฉพาะบุคคลหรือเฉพาะราย” หมายความว่า บรรดาข้อมูลที่ได้มาตามกฎหมายว่าด้วยสถิติ

๒๓) “ข้อมูลสถิติ” หมายความว่า ข้อมูลที่จัดเก็บรวบรวมและประมวลผลด้วยวิธีการเชิงสถิติ

๒๔) “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๒๕) “ระบบคอมพิวเตอร์” หมายความว่า เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่ต่อพ่วง รวมถึงซอฟต์แวร์ที่ใช้งาน

๒๖) “ระบบเครือข่าย” หมายความว่า ระบบเครือข่ายระยะไกล ระบบเครือข่ายภายในระบบเครือข่ายไร้สาย

๒๗) “อุปกรณ์ด้านความมั่นคง” หมายความว่า อุปกรณ์ Firewall อุปกรณ์ IPS/IDS อุปกรณ์ Proxy อุปกรณ์ Web Gateway อุปกรณ์ E-Mail Gateway หรืออุปกรณ์อื่นที่สนับสนุนงานระบบความมั่นคงปลอดภัย

๒๘) “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๒๙) “การธำรงไว้ซึ่งความลับ (Confidentiality)” หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์ จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

๓๐) “การรักษาความถูกต้องครบถ้วน (Integrity)” หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลง แก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

๓๑) “การรักษาสภาพพร้อมใช้งาน (Availability)” หมายความว่า การจัดให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

๓๒) “ผู้ดูแลระบบ” หมายความว่า ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย ผู้ดูแลระบบความมั่นคงปลอดภัย ผู้ดูแลระบบโปรแกรมประยุกต์ ผู้ดูแลระบบฐานข้อมูล ผู้ดูแลระบบสารสนเทศ ผู้ดูแลระบบสำรองข้อมูล

๓๓) “ผู้ดูแลระบบคอมพิวเตอร์” หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบคอมพิวเตอร์แม่ข่าย

๓๔) “ผู้ดูแลระบบเครือข่าย” หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบคอมพิวเตอร์เครือข่าย

๓๕) “ผู้ดูแลระบบความมั่นคงปลอดภัย” หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ

๓๖) “ผู้ดูแลระบบโปรแกรมประยุกต์” หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการโปรแกรมประยุกต์

๓๗) “ผู้ดูแลระบบฐานข้อมูล” หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบฐานข้อมูล

๓๘) “ผู้ดูแลระบบสารสนเทศ” หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบสารสนเทศ

๓๙) “ผู้ดูแลระบบสำรองข้อมูล” หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบสำรองข้อมูลและกู้คืน

๔๐) “วิธีการแบบปลอดภัย” หมายความว่า วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

๔๑) “ธุรกรรม” หมายความว่า การกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนด

๔๒) “ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

๔๓) “ธุรกรรมทางอิเล็กทรอนิกส์” หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน

๔๔) “การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์” หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

๔๕) “การแปลงข้อมูล” หมายความว่า การแปลงข้อมูลจากเอกสารเข้าระบบอิเล็กทรอนิกส์ด้วยวิธีการบันทึกเข้าระบบหรือ Scan เป็นไฟล์ภาพเข้าระบบ

๔๖) “ผู้บริหารระดับสูงสุด” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานสถิติแห่งชาติ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย ตัดสินใจ และแนะนำแนวทางการดำเนินงานของสำนักงานสถิติแห่งชาติ

๔๗) “หน่วยงานภายนอก” หมายความว่า องค์กรซึ่ง สสช. อนุญาตให้มีสิทธิในการเข้าถึง และใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของ สสช. ภายใต้สัญญา/ข้อตกลง โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๔๘) “เจ้าของข้อมูลและสารสนเทศ” หมายความว่า ผู้ที่เป็นผู้สร้างข้อมูลและสารสนเทศ

๔๙) “ข้อมูลอ่อนไหว” หมายความว่า ข้อมูลอ่อนไหวตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๕๐) “ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller)” หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๕๑) “ผู้ประมวลผลข้อมูลส่วนบุคคล (Data processor)” หมายความว่า ผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๕๒) “เจ้าของโครงการ” หมายความว่า ผู้รับผิดชอบหลักของโครงการ กิจกรรม หรืองาน

๕๓) “ข้อมูลนิรนาม (Anonymization)” หมายความว่า การใช้วิธีการทางเทคนิคที่จะทำให้ข้อมูลนั้นไม่สามารถระบุตัวบุคคลได้อีกต่อไป

๕๔) “การบดบังข้อมูล (Data Masking)” หมายความว่า เป็นเทคนิคหนึ่งในการควบคุมความปลอดภัยข้อมูลที่ใช้ในการปกปิดข้อมูลที่เป็นความลับหรือข้อมูลที่ต้องการความคุ้มครอง การทำ Data Masking อาจมีการเปลี่ยนแปลงข้อมูลหรือทำให้ข้อมูลแสดงผลในรูปแบบที่ไม่สามารถตีความได้จริง เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๕๕) “การทำข้อมูลแฝง (Pseudonymization)” หมายความว่า ข้อมูลที่ผ่านกระบวนการอำพรางข้อมูลที่บ่งชี้ตัวบุคคล เช่น การเข้ารหัส ทำให้ระบุตัวตนได้ยาก

๕๖) “การเข้ารหัสข้อมูล (Cryptography)” หมายความว่า กระบวนการสำหรับการแปรรูปข้อมูลอิเล็กทรอนิกส์ธรรมดา (Plain text) ไปเป็นข้อมูลที่บุคคลทั่วไปไม่สามารถอ่านเข้าใจได้ (Cipher text) โดยใช้กุญแจร่วมกับแบบแผนของการเข้ารหัส เพื่อปกป้องข้อมูลที่เป็นความลับ

๕๗) “ข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)” หมายความว่า สัญญาจ้างผู้ให้บริการภายนอกและเทคโนโลยีที่ระบุระดับการบริการที่ซัพพลายเออร์สัญญาว่าจะส่งมอบให้กับลูกค้า เช่น เวลาทำงาน เวลาจัดส่ง เวลาตอบสนอง และเวลาแก้ปัญหา SLA ยังให้รายละเอียดการดำเนินการเมื่อไม่เป็นไปตามข้อกำหนด เช่น การสนับสนุนเพิ่มเติมหรือส่วนลดราคา โดยทั่วไป SLA จะตกลงกันระหว่างลูกค้าและผู้ให้บริการ แม้ว่าหน่วยธุรกิจภายในบริษัทเดียวกันจะสามารถสร้าง SLA ร่วมกันได้

๕๘) “การทบทวนสิทธิของผู้ใช้งาน” หมายความว่า การทบทวนสิทธิของผู้ใช้งาน อาทิ สิทธิการใช้งานระบบสารสนเทศ หรือบริการพื้นฐานทั้งหมด การเรียกคืนทรัพย์สินสารสนเทศทั้งหมด สำหรับบุคคลที่ไม่มีสิทธิการใช้งานได้แก่ เครื่องคอมพิวเตอร์ บัตรประจำตัว เป็นต้น

๕๙) “องค์ประกอบความมั่นคงปลอดภัย” หมายความว่า การจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศมีคุณสมบัติการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)

หมวด ๑ นโยบายความมั่นคงปลอดภัย (Security Policy)

วัตถุประสงค์

เพื่อให้การจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศมีคุณสมบัติการรักษาความลับ (Confidentiality) ความครบถ้วน (Integrity) และการรักษาสภาพความพร้อมใช้งาน (Availability) การดำเนินการจึงต้องมีวงจรการบริหารแบบคุณภาพ (PDCA) กำกับการดำเนินงาน ประกอบด้วย การวางแผน (Plan) การปฏิบัติตามแผน (Do) การตรวจสอบ (Check) และ การปรับปรุงแก้ไข (Act) โดย สสช. ได้กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยมีวัตถุประสงค์เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของ สสช. ทำให้การปฏิบัติราชการมีประสิทธิภาพและประสิทธิผล ดังต่อไปนี้

- เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับใน สสช. ได้รับทราบ และทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- เพื่อสร้างความตระหนักให้ เจ้าหน้าที่ และหน่วยงานภายนอกที่ปฏิบัติงานให้กับ สสช. ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศ
- เพื่อดำเนินการหรือประสานงานกับหน่วยงานอื่น ๆ ในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงปลอดภัย ที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

แนวทางปฏิบัติ

๑. ให้มีการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยในกระบวนการสถิติ พร้อมระบุวิธีการแบบปลอดภัยในกระบวนการสถิติ ทั้งกระบวนการสร้างคุณค่า และกระบวนการสนับสนุน เพื่อใช้เป็นกรอบการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ

๒. การจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศต้องไม่ส่งผลกระทบต่อผู้รับบริการ

๓. ให้กำหนดกิจกรรมการบริหารระบบความมั่นคงปลอดภัย (Information Security Management System) เพื่อใช้เป็นกระบวนการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

๑) กิจกรรมในการวางแผนมีข้อกำหนด ดังนี้

(๑) ให้จัดทำ ทบทวน ปรับปรุง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๑๔ หมวด และสถาปัตยกรรมระบบความมั่นคงปลอดภัยอย่างสม่ำเสมอทุก ๑ ปี เพื่อให้สอดคล้องกับความต้องการของกระบวนการสถิติ สภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศที่เปลี่ยนแปลง และข้อบังคับของกฎหมาย

(๒) ให้วางแผนปรับปรุงเทคโนโลยีด้านความมั่นคงปลอดภัยสารสนเทศ

(๓) ให้วางแผนการประเมินผลด้วยตนเองอย่างสม่ำเสมอเพื่อติดตามความครบถ้วนการดำเนินงานในกระบวนการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

๒) กิจกรรมการปฏิบัติตามแผนมีข้อกำหนด ดังนี้

(๑) ให้ประกาศให้ทุกภาคส่วนของสำนักงานสถิติแห่งชาติได้รับทราบถึง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๑๔ หมวด รวมทั้งระเบียบการใช้งานทรัพย์สินสารสนเทศ ให้ทราบทั่วกัน

(๒) ให้นำแนวปฏิบัติด้านความมั่นคงปลอดภัยในการรักษาสารสนเทศทั้ง ๑๔ หมวด มาดำเนินงาน โดยให้มีการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นเป็นประจำวัน และการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(๓) ให้รายงานผู้บริหารให้รับทราบเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศขึ้นในสำนักงานสถิติแห่งชาติ

(๔) ให้เผยแพร่ข้อมูล และให้ความรู้กับบุคลากรให้รู้ทันภัยร้าย และตระหนักในความมั่นคงปลอดภัยด้านสารสนเทศเป็นประจำสม่ำเสมอ

(๕) ให้ประสานความร่วมมือกับหน่วยงานภายใน หน่วยงานภาย และต่างประเทศเพื่อรู้เท่าทันภัยคุกคามบนระบบเครือข่ายที่อาจเกิดขึ้น

๓) กิจกรรมการตรวจสอบมีข้อกำหนด ดังนี้

(๑) ให้ประเมินความเสี่ยงและจัดการกับความเสี่ยงที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญเป็นประจำอย่างสม่ำเสมอ โดยมีขั้นตอน การระบุปัจจัยที่มีผลทำให้เกิดความเสี่ยงและการระบุความเสี่ยงที่มีโอกาสเกิดขึ้น (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการบริหารจัดการกับความเสี่ยง (Risk Management) อย่างน้อยปีละ ๑ ครั้ง

(๒) ให้ตรวจสอบช่องโหว่ (Vulnerability Scanning) ของทรัพย์สินสารสนเทศที่สำคัญเป็นประจำอย่างสม่ำเสมอ และให้ปิดช่องโหว่ (Hardening) ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย อุปกรณ์ด้านความมั่นคงปลอดภัย โปรแกรมประยุกต์ที่ได้จากการตรวจพบ และแจ้งให้ผู้มีส่วนร่วมได้รับทราบเพื่อแก้ไขและเฝ้าระวัง

(๓) ให้ทดสอบแผนการจัดการเหตุการณ์ที่ไม่คาดฝันเป็นประจำอย่างสม่ำเสมอ

(๔) ให้ตรวจสอบพฤติกรรมการใช้งานของผู้ใช้เป็นประจำสม่ำเสมอและแจ้งเตือนให้รับทราบ และควบคุมการใช้งานที่สร้างความเสียหายต่อผู้ใช้ในการปฏิบัติราชการและการให้บริการต่อผู้รับบริการ

๔) การปรับปรุงแก้ไขมีข้อกำหนด ดังนี้

(๑) ให้มีการตรวจสอบและประเมินระบบความมั่นคงปลอดภัยด้านสารสนเทศเป็นประจำอย่างสม่ำเสมอและให้นำผลการตรวจสอบและการประเมินมาใช้ในกิจกรรมวางแผนเพื่อปรับปรุงระบบความมั่นคงปลอดภัยด้านสารสนเทศต่อไป

(๒) ให้ทบทวนและวิเคราะห์ช่องว่างการบริหารระบบความมั่นคงปลอดภัย (Gap Analysis)

หมวด ๒ โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร
(Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดผู้รับผิดชอบในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศและการดำเนินงานในกิจกรรมที่เกี่ยวเนื่อง ซึ่งประกอบด้วยผู้รับผิดชอบหลักที่เป็นเจ้าหน้าที่ของสำนักงานสถิติแห่งชาติและผู้สนับสนุนจากภายนอก

แนวทางปฏิบัติ

๑. กำหนดให้ผู้อำนวยการสำนักงานสถิติแห่งชาติ เป็นผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติ

๒. ให้คณะทำงานทบทวนนโยบายแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยสารสนเทศ ปรับปรุง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๓. ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทำหน้าที่ในการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ และกำหนดสถาปัตยกรรมระบบความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับภารกิจของสำนักงานสถิติแห่งชาติ

๔. ให้สำนักงานสถิติจังหวัดทำหน้าที่ในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติจังหวัดให้สอดคล้องกับภารกิจของสำนักงานสถิติจังหวัดใน ๖ หมวด ประกอบด้วย

- หมวด ๓ การสร้างความมั่นคงปลอดภัยด้านทรัพยากรบุคคล
- หมวด ๔ การบริหารจัดการทรัพย์สินสารสนเทศ
- หมวด ๕ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ
- หมวด ๗ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวด ๘ ความมั่นคงปลอดภัยในการปฏิบัติงาน
- หมวด ๑๓ การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง

๕. ให้กลุ่มนิติการทำหน้าที่ประสานงานการดำเนินงานทางคดีหากมีการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือพระราชบัญญัติอื่นที่เกี่ยวข้อง

๖. ให้กลุ่มการเจ้าหน้าที่ทำหน้าที่ในการแจ้งรายชื่อบุคลากรของสำนักงานสถิติแห่งชาติที่ลาออกให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารรับทราบเป็นรายเดือน เพื่อใช้ในการยกเลิกสิทธิผู้ใช้งานออกจากระบบการใช้งาน

๗. ให้กลุ่มตรวจสอบภายในทำหน้าที่ในการบริหารและจัดการระบบการตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติ

๘. ให้มีการจัดทำข้อตกลงการปกปิดข้อมูลและห้ามเปิดเผยข้อมูลที่เป็นความลับสำหรับผู้สนับสนุนจากภายนอกที่เข้ามาดำเนินงานติดตั้ง งานบำรุงรักษา และงานที่มีความเกี่ยวเนื่องกับระบบความมั่นคงปลอดภัยด้านสารสนเทศ

๙. ให้ผู้รับผิดชอบในระบบแลกเปลี่ยนข้อมูลจัดทำข้อตกลงการปกปิดข้อมูล การดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง สำหรับหน่วยงานภายนอกที่สำนักงานสถิติแห่งชาติได้นำไปติดตั้งตามกระทรวงต่าง ๆ

๑๐. ให้ผู้ดูแลระบบซึ่งประกอบด้วย ผู้ดูแลระบบสารสนเทศ ผู้ดูแลโปรแกรมประยุกต์ ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสำรองข้อมูล ทำหน้าที่ในการบริหารจัดการระบบตามหน้าที่ที่ได้รับมอบหมายและปฏิบัติตามข้อกำหนดในแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนงานที่เกี่ยวเนื่อง

๑๑. ให้มีคณะทำงานประสานงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่ออำนวยการและประสานการดำเนินงานเมื่อเกิดภัยพิบัติในภาวะวิกฤต

๑๒. ให้มีคณะทำงานตอบสนองต่อภัยพิบัติด้านสารสนเทศ เพื่อจัดทำแผนสร้างความต่อเนื่องและสนับสนุนการกู้คืนระบบสารสนเทศให้กลับสู่ภาวะปกติ

๑๓. สำหรับในภารกิจที่ไม่ปรากฏผู้รับผิดชอบและหน้าที่ไว้เป็นการเฉพาะและมีเหตุต้องจัดการกับภารกิจนั้น ให้แต่งตั้งคณะทำงานเฉพาะขึ้นมาเพื่อดำเนินการแทน

๑๔. ให้ศูนย์ สำนัก/กอง สำนักงานสถิติจังหวัด นำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไปใช้ในการปฏิบัติงานประจำ

หมวด ๓ การสร้างความมั่นคงปลอดภัยด้านทรัพยากรบุคคล
(Human Resource Security)

วัตถุประสงค์

เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดจากบุคลากรเป็นสำคัญ โดยให้มีการแจ้งระเบียบการใช้งานทรัพย์สินสารสนเทศก่อนทำหน้าที่และการให้ความรู้และตระหนักถึงภัยร้ายเพื่อไม่ตกเป็นผู้กระทำความผิดสร้างความเสียหายให้เกิดกับองค์กรและผู้อื่นโดยขาดความระมัดระวัง รวมทั้งการยกเลิกสิทธิและเรียกคืนทรัพย์สินที่ใช้งานในหน้าที่กลับคืนเมื่อพ้นหน้าที่ความรับผิดชอบ

แนวทางปฏิบัติ

๑. ให้มีการชี้แจงความรับผิดชอบ และการอบรมให้กับเจ้าหน้าที่ที่เข้าใหม่ของสำนักงานสถิติแห่งชาติให้สามารถใช้งานทรัพย์สินสารสนเทศได้อย่างปลอดภัย และรับทราบระเบียบการใช้งานทรัพย์สินสารสนเทศและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ให้มีการชี้แจงการรักษาความลับข้อมูลเฉพาะบุคคลหรือเฉพาะราย ในพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ มิให้ถูกเปิดเผยไม่ว่าด้วยวิธีการใดก็ตามให้กับเจ้าหน้าที่ที่เข้าใหม่ได้รับทราบ

๓. ให้เจ้าหน้าที่ที่มีหน้าที่ความรับผิดชอบเกี่ยวกับข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคล หรือเฉพาะรายปฏิบัติหน้าที่ให้เป็นไปตามอำนาจหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา โดยให้สอดคล้องกับอำนาจหน้าที่ของสำนักงานสถิติแห่งชาติที่บัญญัติไว้ในพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ และการปฏิบัติงานภายใต้ภารกิจหรือนโยบายของสำนักงานสถิติแห่งชาติ และจะต้องเป็นผู้ดูแลรับผิดชอบข้อมูลส่วนบุคคลดังกล่าวตามอำนาจหน้าที่ที่ได้รับมอบหมาย ส่วนเจ้าหน้าที่ที่เป็นผู้ดูแลระบบสารสนเทศ ให้มีอำนาจหน้าที่ในการกำหนดสิทธิการใช้งานระบบเท่านั้น และจะต้องไม่เข้าถึงข้อมูลส่วนบุคคลที่จัดเก็บไว้ในระบบ โดยจะต้องปฏิบัติตามกฎหมายหรือระเบียบที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างเคร่งครัด

๔. ให้มีการป้องกันการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายโดยมิชอบ โดยข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายของสำนักงานสถิติแห่งชาติที่ได้มาตามอำนาจหน้าที่ที่บัญญัติไว้ในพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ จะได้รับการคุ้มครองตามบทบัญญัติในมาตรา ๑๔ ถึงมาตรา ๑๖ หากผู้ใดฝ่าฝืนจะต้องได้รับโทษตามบทบัญญัติในมาตรา ๒๐ แห่งพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ และในการปฏิบัติงานจะต้องปฏิบัติตามระเบียบอื่น ๆ ได้แก่ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ระเบียบสำนักงานสถิติแห่งชาติว่าด้วยการดำเนินการต่อเรื่องร้องเรียน พ.ศ. ๒๕๕๕ และระเบียบสำนักงานเศรษฐกิจแห่งชาติว่าด้วยการใช้งานทรัพย์สินสารสนเทศ พ.ศ ๒๕๕๕

๕. ให้มีการอบรมให้กับเจ้าหน้าที่เป็นประจำ เพื่อให้มีองค์ความรู้และความตระหนักในด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่องเป็นประจำอย่างสม่ำเสมอ เพื่อมิให้ตกเป็นผู้กระทำความผิดตามกฎหมายหรือละเมิดระเบียบที่สำนักงานสถิติแห่งชาติประกาศใช้งาน

๖. ให้มีการทบทวนสิทธิของผู้ใช้ระบบสารสนเทศเป็นประจำทุกปี ดังต่อไปนี้

๑) ยกเลิกสิทธิของผู้ใช้งานระบบสารสนเทศ หรือบริการพื้นฐานทั้งหมด ในกรณีพ้นสภาพจากการเป็นเจ้าหน้าที่สำนักงานสถิติแห่งชาติ และมีการทบทวนสิทธิการใช้งานระบบสารสนเทศ ตามรายชื่อที่กลุ่มการเจ้าหน้าที่แจ้ง เมื่อมีการปรับเปลี่ยนหน้าที่หรือพ้นจากหน้าที่ความรับผิดชอบ

๒) เรียกคืนทรัพย์สินสารสนเทศทั้งหมด สำหรับบุคคลที่ไม่มีสิทธิการใช้งานได้แก่ เครื่องคอมพิวเตอร์ บัตรประจำตัว เป็นต้น

หมวด ๔ การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

วัตถุประสงค์

เพื่อจัดการทรัพย์สินสารสนเทศของสำนักงานสถิติแห่งชาติ ประกอบด้วย ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบความมั่นคงปลอดภัย ระบบงานคอมพิวเตอร์ เอกสาร ข้อมูลสารสนเทศ และทรัพย์สินอื่น ๆ ให้มีความพร้อมต่อการใช้ในการปฏิบัติงานและการให้บริการ

แนวทางปฏิบัติ

๑. ให้จัดทำระเบียบการใช้งานทรัพย์สินสารสนเทศอย่างเป็นลายลักษณ์อักษรและประกาศให้ผู้ใช้งานได้รับทราบถึงวิธีการใช้งานที่ถูกต้อง ข้อห้าม และบทลงโทษหากมีการฝ่าฝืนหรือละเมิดการใช้งาน

๒. ให้จัดทำทะเบียนทรัพย์สินและปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอทุกปี โดยต้องมีข้อมูลดังนี้

๑) หมายเลขครุภัณฑ์

๒) ประเภทครุภัณฑ์

๓) ผู้ครอบครองหรือผู้ดูแล

๔) สถานที่ใช้งาน

๕) ระดับความสำคัญ

๖) มูลค่าการจัดหา

๗) วิธีการเก็บรักษา

๘) การควบคุมการใช้งาน

๓. ให้จัดการทรัพย์สิน เครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล ระบบความมั่นคงปลอดภัย ระบบงานคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้ทำข้อตกลงการใช้ทรัพย์สินสารสนเทศก่อนการใช้งานให้เป็นไปตามระเบียบการใช้งานทรัพย์สินสารสนเทศ

๒) ให้ทำระบบการยืม/คืน ทรัพย์สินสารสนเทศที่สำคัญในการปฏิบัติงานภายนอกเพื่อตรวจสอบและป้องกันความเสียหาย

๓) ให้มีการควบคุมการเคลื่อนย้ายทรัพย์สินที่ต้องนำออกไปภายนอกและการนำทรัพย์สินจากภายนอกเข้ามาใช้งานภายในองค์กร

๔. ให้จัดการทรัพย์สิน ซอฟต์แวร์ โปรแกรมประยุกต์ ระบบสารสนเทศ ตามข้อกำหนดดังต่อไปนี้

๑) จำแนกหมวดหมู่ของระบบสารสนเทศออกเป็น สารสนเทศเพื่อการบริหารจัดการองค์กร สารสนเทศเพื่อการผลิตข้อมูล สารสนเทศเพื่อการบริการข้อมูลและสารสนเทศสถิติ และสารสนเทศเพื่อการจัดการระบบสถิติ

๒) จำแนกทะเบียนโปรแกรมประยุกต์ตามหมวดหมู่ของระบบสารสนเทศและมีข้อมูลดังต่อไปนี้

(๑) ผู้ใช้งาน

(๒) เจ้าของระบบ

(๓) ผู้ดูแลระบบ

(๔) ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

(๕) ระดับชั้นการเข้าถึง

(๖) เวลาที่ได้เข้าถึง

(๗) ช่องทางการเข้าถึง

๓) จำแนกทะเบียนซอฟต์แวร์และมีข้อมูลดังต่อไปนี้

(๑) ผู้ใช้งาน

(๒) สถานที่เก็บ

(๓) การใช้งาน

(๔) การอ้างอิงลิขสิทธิ์การใช้งาน

๕. ให้จัดการทรัพย์สิน ข้อมูลและสารสนเทศ ในรูปข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดทำทะเบียนข้อมูลและเอกสารที่สำคัญที่ต้องมีชั้นความลับในการควบคุม และกำหนดใช้วิธีการจัดการและควบคุม ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๒) ให้มีการจำแนกทะเบียนเอกสารที่สำคัญดังต่อไปนี้

(๑) เปิดเผยต่อสาธารณะ เฉพาะสมาชิก หรือเฉพาะกลุ่ม

(๒) ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

(๓) ระดับชั้นการเข้าถึง

(๔) เวลาที่ได้เข้าถึง

(๕) ช่องทางการเข้าถึง

๓) ให้มีการจำแนกทะเบียนข้อมูลดังต่อไปนี้

(๑) ประเภทของข้อมูล

(๒) ลำดับความสำคัญ ลำดับชั้นความลับ และชั้นความปลอดภัยของข้อมูล

(๓) ระดับชั้นการเข้าถึง

(๔) เวลาที่ได้เข้าถึง

(๕) ช่องทางการเข้าถึง

๔) กำหนดการจัดแบ่งระดับความสำคัญของข้อมูล แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับที่ ๑ ข้อมูลที่มีระดับความสำคัญมาก

(๒) ระดับที่ ๒ ข้อมูลที่มีระดับความสำคัญปานกลาง

(๓) ระดับที่ ๓ ข้อมูลที่มีระดับความสำคัญน้อย

๕) จัดแบ่งลำดับชั้นความลับของข้อมูลดังนี้

(๑) “ลับที่สุด” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

(๒) “ลับมาก” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง

(๓) “ลับ” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหาย

๖) การจัดแบ่งระดับชั้นการเข้าถึง

(๑) ระดับที่ ๑ ระดับชั้นสำหรับผู้บริหาร

(๒) ระดับที่ ๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(๓) ระดับที่ ๓ ระดับชั้นสำหรับผู้ใช้แบบสมาชิก

(๔) ระดับที่ ๔ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๗) กำหนดช่องทางการเข้าถึงข้อมูลที่มี

(๑) ระดับความสำคัญปานกลางในระบบอินทราเน็ตที่เป็นระบบปิดภายในตลอด ๒๔ ชั่วโมง สำหรับผู้ใช้งานภายใน

(๒) ระดับความสำคัญปานกลางในระบบเชื่อมโยงสื่อสารข้อมูลหน่วยงานภาครัฐตลอด ๒๔ ชั่วโมง สำหรับสำนักงานสถิติจังหวัด

(๓) ระดับความสำคัญน้อยผ่านระบบอินเตอร์เน็ตได้ตลอด ๒๔ ชั่วโมง สำหรับผู้ใช้ทั่วไปและผู้ใช้แบบสมาชิก

๘) จัดแบ่งลำดับชั้นความปลอดภัยของข้อมูล ดังนี้

(๑) “ชั้นความปลอดภัยระดับต่ำ” หมายถึง ข้อมูลที่บันทึกภายในสื่ออิเล็กทรอนิกส์ที่มีความสำคัญน้อย

(๒) “ชั้นความปลอดภัยระดับปานกลาง” หมายถึง ข้อมูลที่บันทึกภายในสื่ออิเล็กทรอนิกส์ที่มีความสำคัญปานกลาง

(๓) “ชั้นความปลอดภัยระดับสูง” หมายถึง ข้อมูลที่บันทึกภายในสื่ออิเล็กทรอนิกส์ที่มีความสำคัญมากที่สุด

๖. ให้บันทึกความเสียหายจากการใช้งานทรัพย์สินสารสนเทศลงในแบบบันทึกโดยมีข้อมูลดังต่อไปนี้

๑) วัน/เวลา

๒) หมายเลขครุภัณฑ์

๓) ความเสียหายที่เกิดขึ้น

๔) สาเหตุ

๕) ผลกระทบ

๗. ให้มีการจัดการเข้าถึงตามระดับชั้นความลับดังต่อไปนี้

๑) ให้มีการลงทะเบียนผู้ใช้งานเพื่อควบคุมสิทธิ มีการจำกัดข้อมูลที่สำคัญ และฟังก์ชันของระบบ ได้แก่ สิทธิที่สามารถแก้ไขข้อมูล สิทธิการสร้างข้อมูล สิทธิการอ่านข้อมูล สิทธิการส่งออกข้อมูล สิทธิการอ่านข้อมูลเฉพาะสดมภ์

๒) ให้กำหนดรหัสผู้ใช้และรหัสผ่าน และมอบสิทธิการใช้ระบบงานตามลำดับชั้นของข้อมูล โดยมีการควบคุมด้วยเมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบงานที่สอดคล้องกับนโยบายการควบคุมการเข้าถึง

๓) ใช้ระบบการเข้ารหัสข้อมูลที่มีความสำคัญหรือมีชั้นความลับในระบบงานที่เป็นความลับ

หมวด ๕ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงทรัพย์สินสารสนเทศขององค์กรให้กับผู้มีสิทธิใช้งานให้เป็นไปตามหน้าที่ความรับผิดชอบ เพื่อป้องกันความเสียหายที่เกิดขึ้นจากการใช้งานโดยขาดการควบคุม จนอาจสร้างความเสียหายต่อระบบสารสนเทศขององค์กรหรือกระทบต่อการปฏิบัติงานประจำวัน

แนวทางปฏิบัติ

๑. ให้มีการควบคุมการเข้าถึงทรัพย์สินสารสนเทศของผู้ใช้เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีแนวปฏิบัติในการควบคุมการเข้าถึงระบบคอมพิวเตอร์ การเข้าถึงระบบปฏิบัติการ การเข้าถึงระบบเครือข่าย การเข้าถึงคอมพิวเตอร์ลูกข่าย การเข้าถึงระบบสารสนเทศ การเข้าถึงโปรแกรมประยุกต์ การเข้าถึงระบบฐานข้อมูล การเข้าถึงไฟล์ข้อมูล การเข้าถึงการใช้งานจดหมายอิเล็กทรอนิกส์ และการเข้าถึงเอกสารและสื่อเก็บข้อมูล

๒) ให้มีการจัดทำทะเบียนควบคุมทรัพย์สินสารสนเทศที่สำคัญขององค์กร และมีการตรวจสอบสภาพและการมีอยู่ของทรัพย์สินสารสนเทศเหล่านั้นเป็นประจำทุกปี

๓) ให้มีการลงทะเบียนผู้ใช้งานภายในและผู้ใช้งานภายนอกแบบสมาชิกก่อนการใช้งานระบบสารสนเทศ

๒. ให้มีการจัดการสิทธิของผู้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการลงทะเบียนผู้ใช้งาน (User Registration) เป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการลงทะเบียน โดยผู้ใช้งานต้องลงทะเบียนตามแบบที่ผู้จัดการระบบกำหนด และมีการลงนามรับทราบในเงื่อนไขพร้อมให้ผู้บังคับบัญชาลงนามรับรองการใช้งาน

(๒) ในแบบลงทะเบียนผู้ใช้งานต้องประกอบด้วยข้อมูลดังต่อไปนี้เป็นอย่างน้อย

๒.๑ ชื่อ/นามสกุล

๒.๒ หมายเลขบัตรประชาชนหรือบัตรทางราชการ

๒.๓ สังกัด

๒.๔ เบอร์ติดต่อ

๒.๕ กลุ่มผู้ใช้ (ข้าราชการ สมาชิก ทั่วไป)

๒.๖ บริการที่ขอใช้งาน

๒.๗ วันหมดอายุ

๒.๘ เงื่อนไขข้อกำหนดการใช้งาน

๒.๙ ผู้รับรอง

๒) ให้มีการจัดการทะเบียนผู้ใช้งานให้เป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีทะเบียนคุมผู้ใช้งานเพื่อใช้ในการตรวจสอบการใช้งานในภายหลังต้องประกอบด้วยข้อมูลดังต่อไปนี้เป็นอย่างน้อย

๑.๑ ชื่อ/นามสกุล

๑.๒ หมายเลขบัตรประชาชนหรือบัตรทางราชการ

๑.๓ สังกัด

๑.๔ เบอร์ติดต่อ

๑.๕ รหัสผู้ใช้

๑.๖ รหัสผ่าน

๑.๗ สิทธิการใช้งาน

๑.๘ วันหมดอายุ

(๒) ให้จัดเก็บทะเบียนผู้ใช้งานอย่างปลอดภัยโดยมีการเข้ารหัสไฟล์และเป็นเอกสารที่เป็นความลับห้ามเปิดเผยต่อบุคคลภายนอกหรือบุคคลที่ไม่เกี่ยวข้อง

(๓) ให้ใช้วิธีการจัดการสิทธิการเข้าถึง (User Management) เป็นไปตามข้อกำหนดดังต่อไปนี้

๓.๑ ใช้การควบคุมแบบกลุ่ม (Group-Based) และหน้าที่ (Role-Based) สำหรับควบคุมการเข้าถึงระบบสารสนเทศ

๓.๒ ใช้การควบคุมแบบรายบุคคล (Identity-Based) ควบคุมการเข้าถึงระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์

๓.๓ ให้มีการมอบสิทธิการใช้งานให้กับผู้ใช้งานเป็นรายบุคคล เป็นความลับ และป้องกันการปฏิเสธความรับผิดชอบของผู้ใช้งานได้

๓) ให้มีการทบทวนสิทธิการใช้งานของผู้ใช้งาน (Review of User Access Right) เป็นประจำทุกปีเป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้หน่วยงานการเจ้าหน้าที่ หรือผู้บังคับบัญชาแจ้งไปยังผู้จัดการระบบหากผู้ใช้งานลาออกหรือพ้นสภาพจากการเป็นเจ้าหน้าที่สำนักงานสถิติแห่งชาติ

(๒) ทบทวนสิทธิประจำปีการเข้าถึงทรัพย์สินสารสนเทศของผู้ใช้งานใน ๑๔ หมวด

(๓) ให้ยกเลิกสิทธิการใช้งานออกจากระบบทะเบียนและในระบบที่เกี่ยวข้องหากพบเงื่อนไขของผู้ใช้งานดังนี้

๓.๑ ไม่มีการใช้งานเกิน ๖ เดือน

๓.๒ ไม่สามารถติดต่อยืนยันการใช้งานจากผู้ใช้งานโดยตรงนั้นได้ในระยะเวลา ๓ เดือน

๓. ให้มีการพิสูจน์ตัวตนผู้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดทำบัญชีชื่อผู้ใช้งาน (User Account) แบบรายกลุ่มและรายบุคคล และการกำหนดสิทธิ (Authorization) ในการเข้าถึงข้อมูลหรือระบบงานตามสิทธิที่ได้รับอนุมัติ

๒) ให้มีการบันทึกการใช้งาน (Accountability) โดยการบันทึกรายละเอียดของการใช้ระบบและการใช้งานต่าง ๆ เพื่อตรวจสอบว่าผู้ใช้งานได้เข้ามากระทำการใดบ้างในระบบ

๓) ผู้ใช้งานต้องพิสูจน์ตัวตนทุกครั้งในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสถิติแห่งชาติ ด้วยชื่อผู้ใช้และรหัสผ่านเป็นอย่างน้อย และต้องเป็นแบบปลอดภัยโดยต้องเข้ารหัสข้อมูล

๔) ให้ใช้โปรโตคอลที่ปลอดภัยในกระบวนการพิสูจน์ตัวตนของผู้ใช้ในการใช้งาน

๕) ให้มีฐานข้อมูลผู้ใช้งานกลาง (LDAP) ที่เก็บข้อมูลผู้ใช้และรหัสผ่านโดยมีการเข้ารหัสให้ปลอดภัย

๖) ให้จัดทำข้อตกลงกับผู้ใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบหากเกิดความเสียหายอันจะเกิดขึ้นจากการใช้งาน

๔. การบริหารจัดการรหัสผ่าน (User Password Management)

๑) มีการจำกัดระยะเวลาการใช้งานรหัสผ่านของผู้ใช้งานระบบ โดยจะต้องเปลี่ยนรหัสผ่านทันทีเมื่อเริ่มแรกเข้าสู่ระบบ และต้องเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

๒) กำหนดให้ผู้ใช้งานสามารถกำหนดรหัสผ่านของตนเองได้ โดยจัดทำช่องรับข้อมูล (Confirmation) ที่ทำการรับค่ารหัสผ่านเพื่อป้อนเข้าสู่ระบบซ้ำอีกครั้ง ระบบต้องทำการตรวจสอบว่าตรงกับค่าที่กรอกมาก่อนหน้านี้ จึงสามารถทำการเปลี่ยนแปลงรหัสผ่านในระบบได้

๓) มีระบบบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานแบบอัตโนมัติ ซึ่งผู้ใช้งานต้องกำหนดรหัสผ่านมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน ช่วยให้ผู้ใช้งานสามารถกำหนดรหัสผ่านที่มีคุณภาพได้

๔) ผู้ดูแลระบบต้องจัดส่งรหัสผ่าน (Password) ชั่วคราวด้วยวิธีการรัดกุมและปลอดภัย ไม่ส่งผ่านบุคคลที่สาม ด้วยการใส่ซองปิดผนึกไม่สามารถมองเห็นได้

๕) กำหนดให้การป้อนรหัสผ่าน ต้องปกปิดหรือไม่แสดงบนหน้าจอขณะที่ทำการป้อนรหัสผ่าน

๖) กำหนดให้ผู้ใช้งานป้อนรหัสผู้ใช้และรหัสผ่านในการใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

๗) กำหนดให้เข้ารหัสผ่านบนไฟล์ (Password Protection) หรือการทำข้อมูลนิรนาม (Anonymization) หรือการบดบังข้อมูล (Data Masking) หรือการทำข้อมูลแฝง (Pseudonymization) ตามความเหมาะสมของการใช้งานข้อมูลหรือตามนโยบายของการดำเนินงานโครงการ

๕. การใช้งานรหัสผ่าน (Password)

๑) ผู้ใช้งานต้องเก็บรหัสผ่านเป็นความลับ และต้องไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบ

๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และเปลี่ยนรหัสผ่านที่ยากต่อการเดาของผู้อื่น

๓) ผู้ใช้งานต้องไม่พิมพ์รหัสผ่านขณะที่มีผู้อื่นเห็นการพิมพ์

๔) ผู้ใช้งานต้องไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ หรือไม่เก็บรักษารหัสผ่านไว้ในสถานที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย

๕) ผู้ใช้งานต้องไม่ใช้รหัสผ่านเดียวกันกับระบบอื่น ๆ

๖) ผู้ใช้งานต้องไม่นำรหัสผ่านเดิมที่เคยใช้มาแล้วมาใช้ซ้ำอีก

๗) ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที หากพบว่ารหัสผ่านของตนถูกล็อค หรือมีปัญหาโดยไม่ทราบสาเหตุ

๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหากทราบว่ารหัสผ่านของตนเองถูกเปิดเผยให้ผู้อื่นล่วงรู้

๙) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๖. การกำหนดรหัสผ่าน

๑) ไม่นำ ชื่อ นามสกุลของผู้ใช้งาน หรือบุคคลในครอบครัว หรือบุคคลที่มีความใกล้ชิด หรือหมายเลขโทรศัพท์ หรือ วันเดือนปีเกิด มากำหนดเป็นรหัสผ่าน

๒) ต้องกำหนดรหัสผ่านโดยให้ประกอบด้วย ตัวอักษร อักขระพิเศษ และตัวเลข ซึ่งง่ายในการจดจำแต่ยากในการคาดเดา

๓) ไม่กำหนดรหัสผ่านที่เป็นคำอยู่ในพจนานุกรม หรือชื่อสถานที่

๗. ให้มีการควบคุมการป้องกันทรัพย์สินสารสนเทศในระหว่างที่ไม่ได้ใช้งาน (Clear Desk and Clear Screen Policy) เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้ตั้งค่าข้อกำหนดการปิดหน้าจอและล็อคหน้าจอด้วยรหัสผ่านเครื่องคอมพิวเตอร์ หากระบบไม่ได้รับการโต้ตอบจากผู้ใช้งานภายในเวลา ๑๕ นาที

๒) ให้ตั้งค่าข้อกำหนดการปิดการเชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย อุปกรณ์ความมั่นคงปลอดภัย หากผู้ใช้งานขาดการโต้ตอบจากระบบภายในเวลา ๑๕ นาที

๓) ให้ตั้งค่ายุติการใช้งานโปรแกรมประยุกต์ หากผู้ใช้ว่างเว้นการใช้ภายในเวลา ๑๕ นาที

๘. ให้มีการควบคุมการเข้าถึงระบบคอมพิวเตอร์ในศูนย์คอมพิวเตอร์ เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ โดยจัดทำประกาศความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์

๒) ให้มีการควบคุมการเข้าถึงตัวเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย อุปกรณ์ความมั่นคงปลอดภัย ผ่านแบบบันทึกขอแก้ไขและต้องได้รับอนุมัติจากผู้ที่ได้รับมอบอำนาจ

๙. ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้จัดทำทะเบียนรายชื่อโปรแกรมที่ยินยอมให้ติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ลูกข่าย และให้มีการตรวจสอบการละเมิดการใช้โปรแกรมนอกเหนือจากที่กำหนด

๒) ให้กำหนดเฉพาะเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบปฏิบัติการและให้ใช้โปรโตคอลที่มีการเข้ารหัสในการเข้าถึง

๓) ให้ทำทะเบียนคุมรายชื่อผู้ใช้ระบบปฏิบัติการและจำแนกสิทธิการใช้งานตามหน้าที่ของผู้ใช้งาน

๔) ให้มีการตรวจสอบและประเมินบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำทุกปี

๕) ให้มีการปรับปรุงช่องโหว่ของระบบปฏิบัติการให้มีความเข้มแข็งอย่างต่อเนื่อง

๖) ให้ผู้ดูแลระบบเครื่องคอมพิวเตอร์เก็บรักษารหัสผ่านไว้เป็นความลับและให้เปลี่ยนรหัสผ่านใหม่ในทุก ๆ ๒ เดือน และเป็นรหัสผ่านที่มีความเข้มแข็ง

๗) ให้มีการควบคุมการติดตั้งโปรแกรมอรรถประโยชน์ (Use of System Utilities) ลงบนเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันการละเมิดลิขสิทธิ์ และป้องกันการหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย ที่อาจทำให้ระบบเกิดช่องโหว่ในการเข้าถึงตามกระบวนการบริหารจัดการเปลี่ยนแปลง และให้มีระบบการป้องกันโหลดไฟล์จากอินเทอร์เน็ตที่อาจทำความเสียหายต่อระบบความมั่นคงจากภายนอกด้วยโปรแกรมตรวจกรอง (Web Filtering)

๘) ให้มีการควบคุมระยะเวลาการใช้งานระบบปฏิบัติการเพื่อป้องกันการใช้งานจากผู้ประสงค์ร้าย

๙) ให้กำหนดสภาพแวดล้อมของระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) กำหนดเวลาของเครื่องให้เป็นมาตรฐานสากลเพื่อการตรวจสอบเหตุการณ์ด้านความมั่นคง

(๒) มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์และตรวจสอบความทันสมัยของฐานข้อมูลไวรัสคอมพิวเตอร์

๑๐. ให้มีการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ตามข้อกำหนดดังต่อไปนี้

๑) มีการควบคุมอุปกรณ์เครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) อุปกรณ์เครือข่ายต้องติดตั้งอยู่ในตู้ มีการจัดเก็บ MAC Address และหมายเลขไอพี (IP Address) เพื่อใช้ในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network)

(๒) ให้มีการปิดพอร์ตและบริการบนระบบเครือข่ายที่ไม่มีความจำเป็นในการใช้งาน เพื่อป้องกันการนำอุปกรณ์เครือข่ายจากภายนอกมาเชื่อมต่อเพื่อกระจายสัญญาณ (Remote Diagnostic and Configuration Port Protection)

(๓) มีการกำหนดหมายเลขไอพีของเครือข่ายออกเป็นกลุ่ม (VLAN) แยกจากกันเพื่อควบคุมสิทธิการใช้งาน

(๔) ไม่อนุญาตทำการเข้าถึงจากระยะไกลผ่านระบบเครือข่ายสำหรับอุปกรณ์ที่สำคัญ

๒) ให้มีการควบคุมการเข้าถึงเครือข่ายแบบสายสัญญาณภายใน ตามข้อกำหนดดังนี้

(๑) ให้ลงทะเบียนเครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์พกพาในการใช้งานระบบเครือข่าย และมีการตรวจสอบและจัดเก็บ MAC Address ของเครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์พกพาที่เข้าเชื่อมต่อระบบเครือข่ายเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย

(๒) ให้ผู้ดูแลระบบเครือข่ายจัดทำทะเบียนพอร์ตการใช้งานและรายละเอียดของอุปกรณ์เครือข่ายและโครงสร้างการเชื่อมต่อของระบบเครือข่าย

(๓) ให้มีการติดตามตรวจสอบเครื่องคอมพิวเตอร์ลูกข่าย มีการตั้งค่าข้อกำหนดเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย ปีละ ๑ ครั้ง

(๔) ให้มีการควบคุมการใช้งานในระดับพอร์ต (Port Security) เป็นอย่างน้อย

(๕) ให้จัดการระบบเครือข่ายออกเป็นโซนหรือ Segment ดังนี้

๕.๑ ให้แบ่งแยกเครือข่ายภายในและเครือข่ายภายนอกออกจากกันด้วยอุปกรณ์ Firewall

๕.๒ ให้แบ่งแยกเครือข่ายออกเป็น ๕ โซน ดังนี้

๕.๒.๑ Internet Zone เป็นเครือข่ายการเข้าถึงสำหรับสารสนเทศบริการผู้ใช้ทางอินเทอร์เน็ต

๕.๒.๒ Core Stat Zone เป็นเครือข่ายสำหรับสารสนเทศระบบประมวลผลข้อมูล และเข้าถึงเฉพาะผู้มีสิทธิเฉพาะเท่านั้น

๕.๒.๓ GIN Zone เป็นเครือข่ายสำหรับระบบสารสนเทศสนับสนุนสำนักงานสถิติจังหวัด และเข้าถึงเฉพาะผู้มีสิทธิเฉพาะเท่านั้น

๕.๒.๔ MIS Zone เป็นเครือข่ายสำหรับระบบสารสนเทศเพื่อการบริหารและจัดการในองค์กร และเข้าถึงเฉพาะผู้มีสิทธิเฉพาะเท่านั้น

๕.๒.๕ Infra Zone เป็นเครือข่ายสำหรับการจัดการระบบไอที และเข้าถึงเฉพาะผู้มีสิทธิเฉพาะเท่านั้น

๓) การควบคุมการเข้าถึงระบบเครือข่ายแบบไร้สาย (Wireless LAN Access Control) ให้มีความมั่นคงปลอดภัยตามข้อกำหนดดังนี้

(๑) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานจะต้องลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๒) ผู้ดูแลระบบต้องดำเนินการลงทะเบียนผู้ใช้งานดังนี้

๒.๑ ลงทะเบียนและกำหนดสิทธิผู้ใช้งาน การเข้าถึงระบบเครือข่ายไร้สาย เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๒ ให้มีระบบการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่านโดยวิธีที่ปลอดภัยของผู้ใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

๒.๓ ให้มีการแบ่งกลุ่มผู้ใช้เครือข่ายไร้สายออกเป็นแบบจำกัดระยะเวลาการใช้งานสำหรับบุคคลภายนอก (Tickets) และแบบบุคลากร (Employee) สำหรับเจ้าหน้าที่สำนักงานสถิติแห่งชาติ

๒.๔ ต้องลงทะเบียนอุปกรณ์ที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๒.๕ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒.๖ ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาติดตั้งใช้งานและกำหนดให้ซ่อน SSID (Service Set Identifier) เพื่อความปลอดภัย

๒.๗ เปลี่ยนค่ารหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและกำหนดรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถคาดเดาหรือเจาะรหัสได้โดยง่าย

๒.๘ กำหนดค่าใช้ WPA2 (Wi-Fi Protected Access 2) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับ เพื่อความปลอดภัย

๒.๙ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้สามารถเข้าใช้ระบบเครือข่ายไร้สายได้

๒.๑๐ ควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๒.๑๑ กำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๒.๑๒ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทันที

๒.๑๓ ให้มีการตรวจสอบและจัดเก็บ MAC Address ของเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์พกพา (โน้ตบุ๊ก สมาร์ทโฟน แท็บเล็ตคอมพิวเตอร์) ที่เข้าเชื่อมต่อระบบเครือข่ายเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย

๔) การเข้าถึงระบบเครือข่ายจากระยะไกล (User Authentication for External Communication) ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกสำนักงานสถิติแห่งชาติ สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงานสถิติแห่งชาติได้ ตามข้อกำหนด ดังนี้

(๑) กำหนดให้การเชื่อมต่อ Remote Access จะต้องใช้ช่องทางเชื่อมต่อผ่านระบบ Secure Sockets Layer Virtual Private Network (SSL VPN) ในการเข้าถึงทรัพย์สินสารสนเทศภายใน เมื่ออยู่ภายนอกสำนักงานสถิติแห่งชาติ

(๒) ก่อนจะกำหนดสิทธิของผู้ใช้งานในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นกับสำนักงานสถิติแห่งชาติ และต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานเป็นลายลักษณ์อักษร

(๓) การเข้าสู่ระบบของสำนักงานสถิติแห่งชาติ ผู้ใช้งานจะต้องพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่าน ด้วยวิธีการเข้ารหัสเพื่อความปลอดภัย

(๔) อุปกรณ์ที่ใช้ในการเชื่อมต่อเข้าสู่ระบบต้องมีการติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็น ได้แก่ ซอฟต์แวร์ป้องกันไวรัส ไฟร์วอลล์ (Firewall) เป็นต้น

(๕) ให้กำหนดสิทธิการเข้าถึงระบบสารสนเทศตามความจำเป็นในหน้าที่และความรับผิดชอบในการทำงาน

๕) การเข้าถึงเครือข่ายอินเทอร์เน็ต ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการลงทะเบียนการใช้บริการเครือข่ายอินเทอร์เน็ต และจดหมายอิเล็กทรอนิกส์ก่อนการใช้งาน และแนบคำแนะนำการใช้งานอย่างปลอดภัยให้ผู้ใช้งานได้รับทราบไปพร้อมกัน

(๒) ให้มีการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่านโดยวิธีที่ปลอดภัยของผู้ใช้งานเพื่อป้องกันการปฏิเสธความรับผิดชอบ

(๓) ให้มีการจัดทำรายงานพฤติกรรมการใช้งานให้ผู้บริหารได้รับทราบอย่างสม่ำเสมอ

(๔) ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น

(๕) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่อระบบเครือข่ายของสำนักงาน ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

(๖) ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

(๗) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

(๘) ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

(๙) ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

(๑๐) ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

(๑๑) หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้วควรออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

(๑๒) ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

๖) ให้มีวิธีการแบบปลอดภัยในการแลกเปลี่ยนข้อมูลระหว่างเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) การโอนไฟล์ข้อมูลระหว่างเครื่องต้องใช้โปรโตคอลที่สามารถเข้ารหัสก่อนส่งผ่านข้อมูล

(๒) การแลกเปลี่ยนข้อมูลบริการแบบเว็บเซอร์วิส (Web Service) โปรโตคอลที่ใช้ในการส่งผ่านข้อมูลระหว่างระบบแบบอัตโนมัตินั้น ต้องมีการเข้ารหัสก่อนส่งผ่านข้อมูลด้วยวิธีการ XML Encryption

๗) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ทั้งแบบใช้สายและไร้สายเป็นตามข้อกำหนดดังต่อไปนี้

(๑) ผู้ดูและระบบมีการตรวจสอบและจำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อทางเครือข่ายตามนโยบายการเข้าถึง

(๒) มีการระบุอุปกรณ์และเครื่องมือที่ใช้ในการเชื่อมต่อทางเครือข่าย ต้องไม่นำอุปกรณ์กระจายสัญญาณ ได้แก่ ฮับ (Hub) สวิตช์ (Switch) อุปกรณ์ค้นหาเส้นทาง (Router) และอุปกรณ์ไวเลสแลน (Wireless LAN) มาเชื่อมต่อเข้ากับระบบเครือข่าย ก่อนได้รับอนุญาตจากผู้ดูแลระบบเครือข่าย

(๓) ไม่เปลี่ยนชื่อเครื่องคอมพิวเตอร์ ไม่เปลี่ยนสายสัญญาณในการเชื่อมต่อที่ได้ระบุไว้ในข้อกำหนดของการเชื่อมต่อ ไม่เปลี่ยนหมายเลขไอพี (IP Address) ของเครือข่ายไปจากที่ผู้ดูแลเครือข่ายกำหนด

(๔) มีการควบคุมบริการบนเครือข่ายที่สามารถเชื่อมต่อได้เฉพาะที่อนุญาตเท่านั้น

๘) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศบนเครือข่ายเป็นไปตามนโยบายการควบคุมการเข้าถึง ตามข้อกำหนดดังต่อไปนี้

(๑) มีการกำหนดมาตรการใช้เส้นทางบนเครือข่าย และจำกัดสิทธิเข้าใช้บริการ ให้สามารถเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้เท่านั้น

(๒) ให้มีระบบ Redundant บนอุปกรณ์เครือข่ายหลัก เพื่อการใช้งานที่ต่อเนื่อง กรณีที่อุปกรณ์หลักตัวใดตัวหนึ่งไม่สามารถทำงานได้ ระบบจะทำการเปลี่ยนเส้นทางบนเครือข่ายให้โดยอัตโนมัติ

๑๑. ให้มีการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ลูกข่าย ตามข้อกำหนดดังต่อไปนี้

๑) ให้ตั้งรหัสผู้ใช้และรหัสผ่านก่อนการเข้าใช้งานเครื่องคอมพิวเตอร์ลูกข่าย

๒) ให้ตั้งการควบคุมหน้าจอด้วยรหัสผู้ใช้และรหัสผ่านก่อนการเข้าใช้งานหลังจากมีการหยุดใช้งานไปแล้ว ๕ นาที

๓) ให้มีการควบคุมการแชร์ไฟล์ข้อมูลบนระบบเครือข่ายอย่างปลอดภัย

๔) ให้มีการควบคุมการตั้งค่าและการเปลี่ยนแปลงข้อกำหนดของเครื่องคอมพิวเตอร์ลูกข่าย

๕) ให้มีการควบคุมการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ลูกข่าย

๖) ให้มีการปิดช่องโหว่ระบบปฏิบัติการของเครื่องคอมพิวเตอร์เมื่อตรวจพบ

๑๒. ให้มีการควบคุมการเข้าถึงระบบสารสนเทศ ตามข้อกำหนดดังต่อไปนี้

๑) ให้จัดทำทะเบียนระบบสารสนเทศขององค์กร และปรับปรุงให้ทันสมัยเป็นประจำทุกปี

๒) ให้มีการควบคุมการใช้งานระบบสารสนเทศที่เป็นภารกิจหลัก และมีผลต่อองค์กรโดยตรงที่ใช้งานภายใน ประกอบด้วย ระบบบันทึกข้อมูล ระบบประมวลผลข้อมูล โดยการกำหนดสิทธิของผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓) ให้มีการควบคุมทางกายภาพของระบบ และไม่อนุญาตใช้งานผ่านระบบเครือข่ายระยะไกล

๔) ให้ผู้จัดการระบบสารสนเทศกำหนดสิทธิของผู้ใช้งานโปรแกรมประยุกต์ ตามบทบาทและหน้าที่ของผู้ใช้

๕) ให้ผู้จัดการระบบสารสนเทศตรวจสอบสิทธิของผู้ใช้งานในระบบงานเป็นประจำสม่ำเสมอ

๑๓. ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์ (Application and Information Access Control) ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการลงทะเบียนโปรแกรมประยุกต์และตรวจสอบความครบถ้วนในแบบลงทะเบียนโปรแกรมประยุกต์

๒) ให้มีการควบคุมโปรแกรมประยุกต์ที่มีความสำคัญหรือมีความเสี่ยงสูงไว้ในองค์ประกอบที่มั่นคงปลอดภัย โดยแบ่งแยกด้วยอุปกรณ์ไฟร์วอลล์ (Firewall) และจำกัดการเข้าถึงเฉพาะกลุ่มผู้ใช้ที่มีสิทธิเท่านั้น

๓) ผู้ดูแลระบบต้องจำกัดระยะเวลา (Limitation of Connection Time) ในการเชื่อมต่อการใช้งานระบบสารสนเทศหรือโปรแกรมประยุกต์ที่มีความเสี่ยงและความสำคัญสูง ดังนี้

(๑) กำหนดให้การเชื่อมต่อในแต่ละครั้งได้ไม่เกิน ๒ ชั่วโมง ต่อการพิสูจน์ตัวตนเข้าใช้งาน

(๒) ต้องตัดการเชื่อมต่อเมื่อใช้งานเกินระยะเวลาที่กำหนด

(๓) ต้องตรวจสอบยืนยันตัวตนใหม่ทุกครั้ง ทุกช่วงเวลาที่กำหนด

๔) ให้จำแนกโปรแกรมประยุกต์ที่ให้บริการผู้ใช้ภายนอก และโปรแกรมประยุกต์ที่ใช้งานภายในองค์กร

๕) ให้มีการเก็บรายละเอียดการเข้าใช้งานของผู้ใช้เพื่อใช้ในการตรวจสอบการใช้งานประจำปี

๑๔. ให้มีการควบคุมระบบฐานข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) ให้ผู้จัดการฐานข้อมูลกำหนดสิทธิและจัดทำทะเบียนผู้ใช้งานฐานข้อมูลและปรับปรุงให้ทันสมัย

๒) ให้ตรวจสอบช่องโหว่ของระบบฐานข้อมูลและดำเนินการปรับปรุงเป็นประจำสม่ำเสมอ

๓) ให้มีระบบการตรวจสอบการเข้าถึงระบบฐานข้อมูลที่มีความสำคัญต่อการปฏิบัติงานเพื่อการอ้างอิงในภายหลัง โดยต้องมีรายละเอียดเกี่ยวกับรหัสผู้ใช้และวันเวลาที่เข้าถึง

๔) ห้ามใช้ชื่อผู้ใช้ที่สิทธิสูงสุด (DBA) ของระบบฐานข้อมูลใช้ในการเชื่อมต่อในโปรแกรมประยุกต์

๕) ให้มีการควบคุมไฟล์ที่กำหนดข้อมูลการเชื่อมต่อระบบฐานข้อมูลของโปรแกรมประยุกต์

๖) ให้มีการปกปิดข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายที่ได้จากกระบวนการสถิติ มิให้สามารถระบุได้ว่าข้อมูลนั้น ๆ เป็นของบุคคลใด หรือ นิติบุคคลใด หรือ คณะใด

๑๕. ให้มีการควบคุมไฟล์ข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเข้าถึงไฟล์ข้อมูลหรือแก้ไขไฟล์ข้อมูลที่ได้จากกระบวนงานที่มีสถานะเป็นไฟล์ข้อมูลดิบ ไฟล์ข้อมูลระดับย่อย ไฟล์ข้อมูลส่วนบุคคล และไฟล์ข้อมูลเฉพาะบุคคลหรือเฉพาะราย เฉพาะผู้ที่ได้รับอนุญาตให้เข้าถึงเท่านั้น และให้มีการเข้ารหัสไฟล์ข้อมูล หากมีความจำเป็นกรณีที่ให้บุคคลภายนอกเป็นผู้ดำเนินการจัดเก็บข้อมูลและมีการจัดเก็บข้อมูลไปไว้บนระบบคอมพิวเตอร์ที่มิใช่ระบบคอมพิวเตอร์สำนักงานสถิติแห่งชาติ จะต้องจัดทำเป็นข้อห้ามเปิดเผยข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายขึ้นไว้เป็นหลักฐานทั้งสองฝ่าย

๒) ให้มีการควบคุมไฟล์ข้อมูลที่มีเนื้อหาและมีระดับชั้นความลับให้สอดคล้องกับระเบียบสำนักงานสถิติแห่งชาติ ว่าด้วยแนวทางปฏิบัติเกี่ยวกับเอกสารที่มีข้อมูลที่เป็นความลับตามพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐

๓) ให้มีการควบคุมการแก้ไขข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายเท่าที่จำเป็นโดยเจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการแก้ไขข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายเท่านั้น และต้องมีการบันทึกรายละเอียดการปรับแก้ไขข้อมูลส่วนบุคคล ได้แก่

(๑) การได้รับอนุมัติจากผู้มีอำนาจ

(๒) การประมวลผล

(๓) การบันทึกการแก้ไขเปลี่ยนแปลง

(๔) การแจ้งผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงทราบ

๔) ให้มีการจัดทำทะเบียนข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายให้ทันสมัยอยู่เสมอ โดยมีรายละเอียดประกอบด้วย ชื่อ โครงการ ชื่อไฟล์/ชื่อฐานข้อมูล สื่ออิเล็กทรอนิกส์ที่ใช้เก็บ ชื่อเครื่องคอมพิวเตอร์ วันเดือนปี ที่เก็บ

๑๖. ให้มีการควบคุมการเข้าถึงเอกสารและสื่อเก็บข้อมูลอิเล็กทรอนิกส์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมเอกสารการปฏิบัติราชการ ดังนี้

(๑) เอกสารการปฏิบัติราชการของสำนักงานสถิติแห่งชาติ ให้ปฏิบัติตามระเบียบการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

(๒) เอกสารที่ปฏิบัติงานในการจัดการระบบไอซีที ประกอบด้วย เอกสารรหัสผ่าน เอกสารเชิงระบบคอมพิวเตอร์และเครือข่ายที่มีหมายเลขไอพีปรากฏ เอกสารข้อกำหนดของระบบคอมพิวเตอร์และเครือข่าย ห้ามนำไปเปิดเผยต่อบุคคลภายนอก มีการจัดเก็บให้ปลอดภัยหากเป็นไฟล์ให้มีการเข้ารหัสป้องกัน

(๓) คู่มือหรือเอกสารที่ใช้ในการปฏิบัติงานและมีเนื้อหาสำคัญและหากถูกเปิดเผยอาจทำความเสียหายต่อระบบสารสนเทศได้ให้มีข้อกำกับการนำไปใช้อย่างชัดเจน

๒) ให้มีการควบคุมการแปลงข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะราย โดยเจ้าหน้าที่ผู้มีหน้าที่ความรับผิดชอบในการแปลงข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายเข้าระบบอิเล็กทรอนิกส์เท่านั้น

๓) ให้มีการควบคุมสื่อเก็บข้อมูลภายนอกที่สามารถนำมาเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์ที่มีไฟล์ข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะราย

๔) ให้มีการควบคุมการทำลายข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะราย โดยเจ้าหน้าที่ที่ได้รับมอบหมาย ดังนี้

(๑) ข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายที่จัดเก็บในรูปแบบเอกสาร ให้ดำเนินการตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และระเบียบ สำนักงานสถิติแห่งชาติ ว่าด้วยแนวทางปฏิบัติเกี่ยวกับเอกสารที่มีข้อมูลที่เป็นความลับตามพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐

(๒) ข้อมูลส่วนบุคคลที่จัดเก็บในรูปแบบสื่ออิเล็กทรอนิกส์ ให้มีการลบหรือทำลายข้อมูลแบบถาวรอย่างปลอดภัย โดยให้เป็นไปตามคู่มือแนวทางการทำลายข้อมูลและสื่ออิเล็กทรอนิกส์ ที่กำหนดขึ้น

๑๗. ให้มีการควบคุมการแลกเปลี่ยนข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายระหว่างหน่วยงาน โดยต้องบันทึกและจัดเก็บข้อมูลดังต่อไปนี้

๑) ข้อมูลการขออนุญาตเข้าใช้ระบบ

๒) ข้อมูลการเข้า - ออก ของผู้มีสิทธิในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

๓) รายละเอียดการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล

๔) รายละเอียดข้อมูลที่ใช้ในการจัดเก็บ

๑๘. ให้มีการควบคุมการให้สิทธิพิเศษในการเข้าถึงข้อมูลส่วนบุคคลสำหรับผู้บริหารระดับสูงของหน่วยงานเป็นกรณีเฉพาะ โดยให้กำหนดระยะเวลาในการเข้าถึงครั้งละไม่เกิน ๑ สัปดาห์ และหากมีความต้องการใช้งานต่อให้ขยายเวลาได้ครั้งละไม่เกิน ๑ สัปดาห์ และเมื่อครบกำหนดเวลาและไม่มีความประสงค์ใช้งานอีกต่อไป ให้ทำการยกเลิกสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายนั้น

๑๙. ให้มีการควบคุมการจัดเก็บข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายประเภทอื่นที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลและสารสนเทศอย่างชัดเจน ได้แก่ หมายเลขบัตรเดบิตหรือบัตรเครดิต หมายเลขประจำตัวประชาชนหรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศของบุคคลซึ่งอายุไม่เกินสิบแปดปี ด้วยวิธีการโดยเฉพาะและเหมาะสม

๒๐. ให้มีการควบคุมระบบที่ไวต่อการถูกรบกวน ตามข้อกำหนดดังต่อไปนี้

๑) ระบบที่มีความไวต่อการถูกรบกวนที่ต้องควบคุมประกอบด้วย

(๑) ระบบบันทึกข้อมูลผ่านเว็บ

(๒) ระบบบริการข้อมูลระดับย่อย

(๓) ระบบแลกเปลี่ยนข้อมูล

๒) การกำหนดบริเวณที่ต้องมีการรักษาความปลอดภัย

(๑) กำหนดและจำแนกพื้นที่ใช้งานสารสนเทศตามสิทธิการเข้าถึงโดยแยกพื้นที่ออกเป็นห้องที่สามารถควบคุมการเข้า - ออกได้ ได้แก่ ห้องคอมพิวเตอร์ เป็นต้น

(๒) กำหนดให้มีผู้รับผิดชอบในการควบคุมบริเวณที่ต้องมีการรักษาความปลอดภัย

๓) การควบคุมการเข้า – ออกสถานที่ และการเข้า - ออกห้องคอมพิวเตอร์

(๑) ให้มีระบบวงจรปิดเพื่อตรวจสอบหากเกิดปัญหา

(๒) ให้มีระบบตรวจสอบลายนิ้วมือการเข้าถึงห้องคอมพิวเตอร์

(๓) ให้จัดทำประกาศเพื่อควบคุมพื้นที่และข้อปฏิบัติการใช้ห้องคอมพิวเตอร์

(๔) ผู้ที่อยู่ในข่ายของการควบคุมประกอบด้วย ผู้ดูแลศูนย์คอมพิวเตอร์โดยตรง ผู้จัดการระบบ ผู้สนับสนุนจากภายนอก และบุคคลภายนอกที่ใช้พื้นที่

(๕) ให้มีการตรวจสอบการเข้า - ออกเป็นประจำทุกเดือน

๔) การกำหนดระดับการควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

(๑) ควบคุมในระดับสูงสุด ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการฐานข้อมูลและฐานข้อมูลทะเบียนกลาง (LDAP)

(๒) ควบคุมในระดับสูง ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการโปรแกรมประยุกต์และ Middleware

(๓) ควบคุมในระดับปานกลาง ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการเว็บ

๕) การกำหนดระดับการควบคุมระบบคอมพิวเตอร์เครือข่าย

(๑) ควบคุมในระดับสูงสุด ประกอบด้วยระบบเครือข่ายแบบไร้สาย

(๒) ควบคุมในระดับสูง ประกอบด้วยระบบเครือข่ายภายใน ห้ามมีการเชื่อมต่อไปใช้ยังสถานที่อื่นที่ไม่ใช่พื้นที่ของหน่วยงาน

๖) การกำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(๑) อุปกรณ์ที่ใช้ในการสื่อสาร หรือปฏิบัติงานจากภายนอกหน่วยงาน ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ และมีการอัพเดทระบบปฏิบัติการให้มีความมั่นคงปลอดภัย

(๒) การเข้าถึงระบบโดยการปฏิบัติงานจากภายนอกต้องขออนุมัติการใช้งานจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเปิดสิทธิให้ปฏิบัติงานจากภายนอกได้

(๓) ผู้ปฏิบัติงานจากภายนอก ต้องปฏิบัติงานในที่ปลอดภัย และงดการใช้เครือข่ายสาธารณะเพื่อเข้าถึงระบบสารสนเทศขององค์กร

๗) การพิสูจน์ตัวตนจากภายนอก

(๑) กำหนดรหัสผู้ใช้และรหัสผ่านเพื่อเข้าระบบงานและให้มีการพิสูจน์ตัวตนของผู้ใช้ข้อมูลในแต่ละระบบและแต่ละชั้นความลับ

(๒) กำหนดช่องทางการเข้าถึงเฉพาะวิธีการแบบปลอดภัยด้วยระบบ Virtual Private Network

๒๑. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ (Mobile Computing) กำหนดแนวปฏิบัติและมาตรการเพื่อปกป้องระบบสารสนเทศ ซึ่งจากความเสี่ยงของการ ใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติดังนี้

๑) การป้องกันอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ครอบคลุมการใช้งาน อุปกรณ์สื่อสารประเภทพกพา ได้แก่ โน้ตบุ๊ก สมาร์ทโฟน แท็บเล็ต คอมพิวเตอร์หรืออุปกรณ์อื่นใดในลักษณะเดียวกันนี้ โดยกำหนดให้มีการป้องกันการเชื่อมต่อของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เข้ากับเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต

๒) ผู้ใช้งานจะต้องยืนยันตัวตนก่อนการเข้าใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ด้วยรหัสผ่าน หรือการสแกนใบหน้า หรือการสแกนลายนิ้วมือ

๓) ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ของตนเอง

๒๒. การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ตามข้อกำหนดดังนี้

๑) ควบคุมพอร์ตการเข้าถึงเฉพาะพอร์ตที่ใช้งานเท่านั้น

๒) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่างๆ ภายในหน่วยงาน

๓) การเข้าถึงระบบสารสนเทศภายในให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกโดยมีรายละเอียดดังนี้

(๓.๑) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน

(๓.๒) รายละเอียดและลักษณะของระบบงาน

(๓.๓) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก

(๓.๔) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

๔) การเข้าสู่ระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการยืนยันตัวตน (Authentication) ด้วยชื่อผู้ใช้ และรหัสผ่าน

๕) ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

๖) ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

๒๓. การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : E-Mail) ดังนี้

๑) กำหนดให้ผู้ใช้งานต้องสามารถเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อได้รับรหัสผ่านครั้งแรก (Default Password) และเปลี่ยนรหัสผ่านใหม่ทุก ๓ เดือน

๒) ในขณะที่ผู้ใช้งานใส่รหัสผ่านให้แสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษร เช่น '*'

๓) ระบบจดหมายอิเล็กทรอนิกส์จะออกจากระบบ (Log out) เพื่อตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบภายในระยะเวลา ๓๐ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

๔) ผู้ใช้งานควรหลีกเลี่ยงการตั้งค่าให้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๕) ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ ไม่ให้เกิดความเสียหายต่อหน่วยงาน ได้แก่ การละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์รวมทั้งไม่ อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของหน่วยงาน

๖) ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ

๗) หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งาน E-Mail โดยไม่ได้รับอนุญาต

๘) ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ ที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๙) ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพ หรือรับ - ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมหรือข้อมูลอันอาจทำให้เสียชื่อเสียง หรือข้อมูลทำให้เกิดความแตกแยกผ่านทางจดหมายอิเล็กทรอนิกส์

๑๐) ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองอย่างสม่ำเสมอ และควรลบจดหมายอิเล็กทรอนิกส์ ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่บนจดหมายอิเล็กทรอนิกส์

หมวด ๖ การเข้ารหัสข้อมูล (Cryptography)

วัตถุประสงค์

เพื่อกำหนดให้มีการเข้ารหัสอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันการเปิดเผยความลับของข้อมูล การปลอมแปลงข้อมูลและรักษาไว้ซึ่งความสมบูรณ์ถูกต้องของข้อมูลโดยมีการกำหนด แนวปฏิบัติและมาตรการเข้ารหัสข้อมูล รวมถึงการบริหารจัดการกุญแจรหัสข้อมูล (Cryptography key)

แนวทางปฏิบัติ

๑. การเข้ารหัสผ่านบนไฟล์ (Password Protection) การทำข้อมูลนิรนาม (Anonymization) การบดบังข้อมูล (Data Masking) และการทำข้อมูลแฝง (Pseudonymization) จะไม่ถือว่าเป็นการเข้ารหัสภายใต้หมวดนี้

๒. นโยบายและแนวปฏิบัตินี้มีผลครอบคลุมถึงการพัฒนาระบบสารสนเทศ การจัดเก็บข้อมูลในฐานข้อมูลบนระบบการจัดการฐานข้อมูล (Database Management System) แต่ไม่รวมถึงการจัดเก็บข้อมูลแบบไฟล์ (File Storage) บนเครื่องแม่ข่ายหรือเครื่องลูกข่ายที่ใช้งานส่วนบุคคล เช่น File Sharing Server เว้นแต่การเก็บข้อมูลแบบไฟล์นั้นจะเป็นการจัดเก็บบนฐานข้อมูลหรือสื่อบันทึกที่สามารถเข้ารหัสข้อมูลได้ทั้งหมด เช่น Hardware Encryption

๓. ข้อมูลอ่อนไหวที่กำหนดโดยหน่วยงาน หรือ เจ้าของโครงการ ที่รับผิดชอบโดยตรงกับข้อมูล ซึ่งอาจกำหนดให้มีการเข้ารหัส (Encryption) ด้วยวิธีการอัลกอริทึมที่เป็นมาตรฐาน

๔. ไม่อนุญาตให้มีการคิดค้นหรือพัฒนาอัลกอริทึมในการเข้ารหัสที่แตกต่างไปจากมาตรฐานสากลที่นำมาใช้บนข้อมูลสารสนเทศของ สสช. เว้นแต่มีเหตุจำเป็นที่เกี่ยวข้องกับความมั่นคงแห่งรัฐ ที่จำเป็นต้องใช้อัลกอริทึมที่แตกต่างไปจากมาตรฐานสากล โดยเป็นการสั่งการจากผู้บริหารระดับสูงสุด หรือหน่วยงานที่มีอำนาจ

๕. การเข้ารหัสต้องไม่ขัดหรือแย้งต่อกฎหมาย ทั้งกฎหมายของไทย และกฎหมายในพื้นที่ที่ข้อมูลถูกจัดเก็บ ประมวลผล ไม่ว่าการจัดเก็บหรือประมวลผลนั้นจะผ่านระบบสารสนเทศหรือไม่ก็ตาม

๖. ไม่อนุญาตให้ใช้อัลกอริทึมในการเข้ารหัสที่ถูกประกาศโดยหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศในระดับสากลหรือที่เป็นที่น่าเชื่อถือ ว่าเป็นอัลกอริทึมที่ไม่แข็งแรง หรือสามารถถูกถอดรหัส (Decryption) ด้วยวิธีการที่ไม่เกี่ยวเนื่องจากการใช้กุญแจรหัสโดยปกติ ได้ในเวลาอันรวดเร็ว

๗. การเข้ารหัสข้อมูลสารสนเทศที่ไม่จำเป็นต้องมีการถอดรหัสอีก เช่น รหัสผ่าน ให้ใช้อัลกอริทึมที่ไม่สามารถถอดรหัสย้อนกลับได้ ตัวอย่างเช่น การเข้ารหัสข้อมูล (Hashing)

๘. ข้อมูลส่วนบุคคล แต่ไม่รวมถึงข้อมูลของเจ้าหน้าที่ สสช. ที่ใช้เพื่อการบริหารงานบุคคลหรือปฏิบัติภารกิจภายในหน่วยงาน ต้องได้รับการเข้ารหัสบนระบบฐานข้อมูล กรณีการเข้ารหัสเป็นการเข้ารหัสที่มีกุญแจรหัสประเภท (Private Key) ให้จัดส่งกุญแจรหัสแก่หน่วยงานที่เกี่ยวข้องโดยตรงกับข้อมูล หรือผู้ที่ได้รับมอบหมาย

๙. ไม่ให้มีการเปิดเผย ส่งต่อ หรือเปลี่ยนแปลง แก้ไข กุญแจรหัส เว้นแต่หน่วยงานที่เกี่ยวข้องโดยตรงกับข้อมูล หรือผู้ที่ได้รับมอบหมาย หรือผู้บังคับบัญชาตามสายงานอนุมัติเป็นลายลักษณ์อักษร

๑๐. หน่วยงานที่เกี่ยวข้องโดยตรงกับข้อมูล หรือผู้ที่ได้รับมอบหมายจัดทำบัญชีรายการกุญแจรหัสที่ใช้โดยไม่พิจารณาว่าผู้ดูแลระบบจะมีกุญแจรหัสหรือไม่

๑๑. มาตรการที่ดำเนินการบนชุดข้อมูลที่มีการเข้ารหัส ต้องดำเนินการในลักษณะเดียวกันกับกุญแจรหัสประเภท Private Key ด้วย เช่น มาตรการสำรองข้อมูล การสื่อสารและส่งต่อข้อมูล การระบุชั้นความลับข้อมูล

๑๒. กุญแจรหัสประเภท Private Key จะมีระดับชั้นความลับไม่ต่ำกว่าข้อมูลที่ถูกเข้ารหัสเสมอ

๑๓. การแก้ไข เปลี่ยนแปลงกุญแจรหัสจะต้องดำเนินการอย่างรัดกุม เพราะอาจจะกระทบต่อข้อมูลเดิมที่เคยถูกเข้ารหัสไว้แล้วด้วยกุญแจรหัสเดิม

๑๔. การเข้ารหัสกุญแจรหัส (Key encrypts key) ให้พิจารณาดำเนินการตามระดับชั้นความลับของสารสนเทศ หรือเมื่อไม่สามารถยืนยันการจัดการกุญแจรหัสเดิมได้อย่างมีประสิทธิภาพเมื่อมีการเปลี่ยนแปลง ทั้งนี้ให้เป็นดุลยพินิจของหน่วยงานที่เกี่ยวข้องโดยตรงกับข้อมูล

๑๕. การเข้ารหัสในระดับเครือข่าย (encryption-base secure network protocol) ให้อ้างอิงตามมาตรการของเทคโนโลยีเครือข่ายและการสื่อสารของระบบสารสนเทศที่หน่วยงานเลือกใช้ โดยต้องสอดรับกับแนวปฏิบัติภายในหมวดนี้

หมวด ๗ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security)

วัตถุประสงค์

เพื่อควบคุมความปลอดภัยด้านกายภาพและสิ่งแวดล้อมซึ่งอาจเกิดความเสียหายต่อทรัพย์สินสารสนเทศที่สำคัญ ในบริเวณที่มีทรัพย์สินสารสนเทศติดตั้งใช้งานอยู่ ได้แก่ ศูนย์คอมพิวเตอร์ ห้องฝึกอบรม โต๊ะทำงาน เพื่อป้องกันการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

แนวทางปฏิบัติ

๑. ให้ตรวจสอบและเฝ้าระวังศูนย์คอมพิวเตอร์ หรือ ห้องคอมพิวเตอร์ ดังต่อไปนี้

๑) ให้จัดทำประกาศรักษาความมั่นคงปลอดภัยที่เป็นพื้นที่ควบคุมในการเข้าถึงและเฝ้าระวังศูนย์คอมพิวเตอร์

๒) ให้จัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายไว้ในศูนย์คอมพิวเตอร์หรือในพื้นที่ที่มีการป้องกันหรือควบคุมเพียงพอ และต้องกำหนดสิทธิการเข้า - ออกศูนย์คอมพิวเตอร์แต่เฉพาะเจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ เจ้าหน้าที่ดูแลระบบ และบุคคลที่มีหน้าที่เกี่ยวข้อง ทั้งนี้ ให้รวมถึงระบบไฟฟ้า ระบบไฟฟ้าสำรอง ระบบปรับอากาศ ระบบระบายอากาศ ระบบเครือข่าย และระบบดับเพลิง

๓) ให้มีระบบเก็บบันทึกการเข้า – ออกห้องคอมพิวเตอร์แม่ข่าย หรือพื้นที่เฝ้าระวังจากบุคคลภายนอก โดยในบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้า - ออก

๔) ให้มีการตรวจสอบสภาพความสมบูรณ์ของระบบสายไฟฟ้าและอุปกรณ์ให้มีสภาพพร้อมใช้งานและไม่เป็นอันตรายต่อการเกิดเพลิงไหม้

๕) ให้ติดตั้งอุปกรณ์เตือนไฟไหม้ ได้แก่ เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

๖) ให้มีถังดับเพลิงเพื่อใช้สำหรับดับเพลิงในเบื้องต้น และต้องมีการตรวจสอบอย่างสม่ำเสมอ

๒. ให้ตรวจสอบและเฝ้าระวังการใช้งานผู้เข้าร่วมประชุมจากภายนอกที่นำเครื่องคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายภายในองค์กรทั้งในแบบใช้สายและไร้สาย ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ที่ใช้ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ทันสมัย

๒) ไม่ติดตั้งโปรแกรมตรวจจับรหัสผ่านหรือโปรแกรมประสงค์ร้าย

๓. ให้ตรวจสอบและเฝ้าระวังเครื่องคอมพิวเตอร์ในห้องอบรม ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ทันสมัย

๒) ให้บันทึกความเสียหายที่เกิดขึ้นจากการใช้งานของผู้อบรม

๓) ให้จัดทำประกาศการใช้เครื่องคอมพิวเตอร์ หรือซอฟต์แวร์สำหรับบุคคลภายนอกที่เข้ารับการฝึกอบรมในหลักสูตรต่าง ๆ

๔. ให้ตรวจสอบและเฝ้าระวังเครื่องคอมพิวเตอร์ในห้องบริการข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ทันสมัย

๒) ให้บันทึกความเสียหายที่เกิดขึ้นจากการใช้บริการของผู้ใช้

๓) ให้มีการควบคุมสื่อเก็บข้อมูลภายนอกที่นำมาเชื่อมต่อกับเครื่องคอมพิวเตอร์

๔) ให้จัดทำประกาศการใช้เครื่องคอมพิวเตอร์ หรือซอฟต์แวร์สำหรับบุคคลภายนอกที่เข้าใช้บริการข้อมูลและสารสนเทศ

๕. ให้ตรวจสอบและเฝ้าระวังพื้นที่ต้องห้าม ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเข้าถึงพื้นที่ภายในของบุคคลภายนอกด้วยระบบควบคุมและติดตั้งกล้องวงจรปิดในจุดที่สำคัญ

๒) ให้มีการตรวจสอบการทำงานของอุปกรณ์ในระบบกล้องวงจรปิดให้สามารถทำงานได้เป็นปกติ และสามารถบันทึกภาพได้ตลอดเวลา

หมวด ๘ ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operations Security)

วัตถุประสงค์

เพื่อเป็นการวางแผน การจัดการระบบสื่อสาร และระบบคอมพิวเตอร์แม่ข่าย ลูกข่าย ให้สามารถใช้งานได้ตลอดเวลาลดความเสี่ยงของความล้มเหลวของระบบ

แนวทางปฏิบัติ

๑. ให้มีการวิเคราะห์และวางแผนเพื่อรองรับปริมาณการใช้งาน ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการวางแผนและการจัดการระบบสื่อสารและระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วงให้สามารถรองรับปริมาณการใช้งาน การเก็บข้อมูล และการให้บริการของผู้ใช้

๒) ให้มีการวิเคราะห์สถาปัตยกรรมการเชื่อมต่อที่สอดคล้องกับโปรแกรมประยุกต์และผู้ใช้งาน ปลายทางเพื่อกำหนดเส้นทางการส่งผ่านข้อมูลที่มีประสิทธิภาพและปลอดภัย

๒. ให้มีขั้นตอนการปฏิบัติงานการจัดการระบบเครือข่ายและระบบคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้ผู้รับผิดชอบในการจัดการระบบเครือข่ายและระบบคอมพิวเตอร์ ดำเนินการตามข้อกำหนดดังต่อไปนี้

(๑) ให้ผู้ดูแลระบบเครือข่ายและระบบคอมพิวเตอร์จัดทำคู่มือการจัดการระบบเครือข่าย

(๒) ให้ผู้ดูแลระบบเครือข่ายและระบบคอมพิวเตอร์ดำเนินการตรวจสอบระบบเครือข่ายเป็นประจำ

(๓) ให้ผู้ดูแลระบบเครือข่ายและระบบคอมพิวเตอร์ใช้มาตรฐานการบริหารงานไอที (ITIL) ในการปฏิบัติงานดูแลระบบงานคอมพิวเตอร์ประจำวัน

๒) ให้ผู้รับผิดชอบในการให้บริการช่องสื่อสาร กำหนดระดับคุณภาพของการให้บริการตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีข้อกำหนดเกณฑ์คุณภาพการให้บริการ (SLA) จากผู้ให้บริการ

(๒) ให้จัดทำข้อตกลงระหว่างผู้ให้บริการระบบสื่อสารข้อมูลให้มีการจัดการช่องสัญญาณด้วยวิธีการแบบปลอดภัย และให้มีการจัดทำรายงานปริมาณการใช้งานช่องสัญญาณเป็นรายเดือน

๓. ให้จัดการความปลอดภัยบนระบบเครือข่าย ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเชื่อมต่ออุปกรณ์เข้ากับระบบเครือข่ายทั้งแบบใช้สายและไร้สาย

๒) ให้เก็บข้อมูล รายละเอียดข้อกำหนดของการเชื่อมต่อ การสำรองข้อมูล และมีแผนการกู้คืนหากระบบเครือข่ายไม่สามารถใช้งานได้

๓) ให้ตรวจสอบสแกนช่องโหว่ของระบบเครือข่าย เครื่องคอมพิวเตอร์ อุปกรณ์ความมั่นคง โปรแกรมประยุกต์ ระบบฐานข้อมูล เป็นประจำทุกปี และให้มีการปรับแก้ให้อยู่ในระดับที่ปลอดภัย

๔) ให้ติดตั้งอุปกรณ์ป้องกันการโจมตีจากระบบเครือข่าย ประกอบด้วย อุปกรณ์ป้องกันการโจมตีและตรวจจับผู้บุกรุกบนเครือข่าย (IPS/IDS) อุปกรณ์ควบคุมบริการบนเครือข่าย (Firewall) อุปกรณ์ควบคุมบริการ (Security Gateway) และระบบป้องกันไวรัสคอมพิวเตอร์ โดยคำนึงถึงความจำเป็นและความสามารถในการจัดการระบบ

๕) ให้จัดการอุปกรณ์ป้องกันการโจมตีและตรวจจับผู้บุกรุกบนเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ให้ตรวจสอบฐานข้อมูลการตรวจจับเป็นประจำสม่ำเสมอ

(๒) ให้เฝ้าติดตามสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดจากการตรวจจับเป็นประจำทุกวัน

๖) ให้จัดการอุปกรณ์ควบคุมบริการบนเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ตรวจสอบกฎการควบคุม (Firewall Policy) เป็นไปตามการจัดการระบบที่ดี

(๒) ควบคุมบริการเฉพาะที่กำหนดเพื่อป้องกันการใช้บริการที่ไม่อนุญาตใช้งานที่เป็นอันตรายต่อระบบเครือข่าย

(๓) การปรับเปลี่ยนกฎของการควบคุมต้องไม่ทำให้ระบบความมั่นคงปลอดภัยขององค์กรลดลงหรือมีความเสี่ยงต่อการสูญเสียบริการ

๗) ให้จัดการอุปกรณ์ควบคุมบริการ (Security Gateway) ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีระบบเฝ้าติดตามการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Gateway) เพื่อกำจัด Spam Mail และติดตามสถานการณ์โจมตีของระบบจดหมายอิเล็กทรอนิกส์

(๒) ให้มีระบบเฝ้าติดตามการใช้งานอินเทอร์เน็ต ตามข้อกำหนดดังต่อไปนี้

๒.๑ ติดตั้งระบบเฝ้าติดตามการแพร่ระบาดไวรัสบนอินเทอร์เน็ต (Web Gateway) เพื่อติดตามสถานการณ์ภัยร้ายของไวรัสบนอินเทอร์เน็ต

๒.๒ ติดตั้งระบบกรองเว็บที่เป็นอันตราย (URL Filtering) เพื่อควบคุมการเข้าถึงข้อมูลที่ไม่เหมาะสมและป้องกันการใช้โปรโตคอลที่สร้างความเสียหายต่อระบบเครือข่าย มีเนื้อหาไม่เหมาะสม และเป็นอันตรายต่อองค์กร

๒.๓ ตรวจสอบและติดตามพฤติกรรมการใช้งานที่ละเมิดต่อระเบียบการใช้งานทรัพย์สินสารสนเทศของสำนักงานสถิติแห่งชาติ

๘) ให้จัดเก็บข้อมูลเพื่อการตรวจสอบระบบเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ตั้งเวลาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ด้านความมั่นคงทุกเครื่องโดยอิงกับเวลามาตรฐานกลางของโลก

(๒) จัดเก็บข้อมูลจราจรระบบเครือข่ายและโปรแกรมประยุกต์ที่ให้บริการ เพื่อการวิเคราะห์และตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยและเป็นไปตามกฎหมายที่กำหนด

๔. ให้มีการจัดการระบบงานคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดการระบบคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการตรวจสอบสภาพของตัวเครื่องและอุปกรณ์เป็นประจำวัน

(๒) ให้มีการตรวจสอบสภาพของระบบสนับสนุนห้องศูนย์คอมพิวเตอร์เป็นประจำวัน

(๓) ให้มีการเฝ้าติดตามการให้บริการเป็นประจำวัน

(๔) ให้มีการตรวจสอบค้นหาช่องโหว่ของระบบปฏิบัติการเป็นประจำเพื่อให้เท่าทันในภัยร้ายที่เกิดขึ้นบนระบบเครือข่าย

(๕) ให้มีการจัดการโปรแกรมประยุกต์ที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

๕.๑ โปรแกรมประยุกต์บนเว็บที่ให้บริการบนระบบเครือข่ายอินเทอร์เน็ตต้องมีการตรวจสอบและให้เป็นไปตามมาตรฐาน OWASP หรือมาตรฐานสากลอื่น ๆ

๕.๒ โปรแกรมประยุกต์ที่ใช้งานบนเว็บต้องใช้พอร์ตมาตรฐาน HTTP (80) และ HTTPS (443) เท่านั้น

๕.๓ ให้มีการควบคุมช่วงอายุการใช้งาน (Session) และช่วงเวลาในการเข้าถึงเพื่อป้องกันภัยร้ายจากโปรแกรม

๒) ให้มีการจัดการระบบคอมพิวเตอร์ลูกข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ให้จัดทำข้อกำหนดการติดตั้งโปรแกรมและข้อกำหนดการเชื่อมต่อ ที่ส่งผลเสียต่อระบบเครือข่ายขององค์กร

(๒) ให้มีการควบคุมโปรแกรมการติดตั้งของลูกข่ายเฉพาะที่ใช้ในการปฏิบัติงานและไม่ใช้เพื่อเป็นเครื่องให้บริการต่อผู้ใช้

๓) ให้มีการจัดการระบบป้องกันไวรัสเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ตรวจสอบความทันสมัยของฐานข้อมูลไวรัสคอมพิวเตอร์เป็นประจำสม่ำเสมอ

(๒) ติดตามเครื่องคอมพิวเตอร์ที่ขาดการปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์ให้ทันสมัย

(๓) ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้มีการทำงานเป็นปกติ

(๔) รายงานการติดไวรัสคอมพิวเตอร์ของเครื่องคอมพิวเตอร์ลูกข่าย พร้อมทั้งรายละเอียดข้อมูลของไวรัสคอมพิวเตอร์ที่แพร่กระจายในองค์กร

หมวด ๙ ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)

วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยข้อมูลและสารสนเทศบนระบบเครือข่าย และอุปกรณ์คอมพิวเตอร์ โดยมีการกำหนดการบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย และการถ่ายโอน ข้อมูลและสารสนเทศ รวมถึงข้อกำหนดในการรักษาความลับ หรือการไม่เปิดเผยความลับซึ่งมีผลบังคับใช้กับเจ้าหน้าที่ขององค์กร รวมถึงบุคคลภายนอก

แนวทางปฏิบัติ

๑. ห้ามมิให้สื่อสารข้อมูลชั้นความลับ ข้อมูลอ่อนไหว และข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการปฏิบัติภารกิจ ผ่านโปรแกรมสื่อสาร สื่อสังคมออนไลน์ แพลตฟอร์มสาธารณะ หรือสื่ออื่นใด ที่ไม่ได้กำหนดและอนุญาตจาก สสช. โดยเด็ดขาด เว้นแต่การสื่อสารนั้นเป็นการสื่อสารตามภารกิจ ข้อมูลสาธารณะอันเป็นสาธารณประโยชน์ หรือเกี่ยวข้องกับภารกิจของ สสช. หรือเป็นการสื่อสารตรงถึงผู้ที่เกี่ยวข้องกับข้อมูลดังกล่าว เช่น เจ้าของข้อมูลส่วนบุคคล ผู้ร้องเรียน

๒. จัดส่งข้อมูลสารสนเทศผ่านระบบ ไฟล์ดิจิทัล (Digital file) สื่อสิ่งพิมพ์ (Hardcopy) หรือการเชื่อมต่อบูรณาการฐานข้อมูล กับหน่วยงานภายนอกที่ไม่ใช่ภาครัฐ ต้องจัดให้มีการลงนามข้อตกลงด้านการรักษาความลับ (Non-Disclosure Agreement : NDA) เว้นแต่ได้มีการลงนามความร่วมมือ (Memorandum of Understanding : MOU) และข้อตกลงการรักษาความลับเป็นส่วนหนึ่งของเอกสารดังกล่าว

๓. จัดให้มีข้อตกลงด้านการรักษาความลับกับหน่วยงานภายนอกที่เป็นผู้รับจ้าง ที่ปรึกษา ผู้รับเหมาที่ สสช. เป็นผู้ว่าจ้างตรง และเข้าถึงข้อมูลชั้นความลับของ สสช.

๔. จัดให้มีมาตรการทางเทคโนโลยีด้านความมั่นคงปลอดภัยสารสนเทศบนเครือข่ายของ สสช. และจัดให้มีการแบ่งเครือข่ายภายในตามระดับความสำคัญของระบบสารสนเทศ โดยพิจารณาถึงระดับชั้นความลับของข้อมูลสารสนเทศที่ระบบสารสนเทศประมวลผลหรือจัดเก็บ มาตรการด้านความมั่นคงปลอดภัยทางเครือข่ายต้องสะท้อนให้เห็นถึงการป้องกัน ตรวจจับ และตอบสนองต่อเหตุภัยคุกคามไซเบอร์ทางเครือข่ายได้อย่างมีประสิทธิภาพ

๕. จัดทำแผนผังเครือข่าย (Network diagram) ที่มีข้อมูลเพียงพอต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบนระบบเครือข่าย

๖. อุปกรณ์บนระบบเครือข่าย และอุปกรณ์ที่เป็นจุดเชื่อมต่อเครือข่ายของ สสช. ต้องได้รับการตรวจทานการตั้งค่า (Configuration) อย่างเหมาะสม

๗. ไม่อนุญาตให้มีการดำเนินกิจกรรมใด ๆ ที่จะส่งผลกระทบให้เกิดการเชื่อมต่อระบบเครือข่ายของ สสช. กับระบบเครือข่ายภายนอก (Network bridge) โดยไม่ได้รับการอนุมัติเป็นลายลักษณ์อักษร

๘. การเชื่อมต่อเครือข่ายของ สสช. ต้องผ่านกลไกการระบุตัวตนผู้ใช้งาน ไม่ว่าจะเป็นเจ้าหน้าที่ของ สสช. หรือบุคลากรภายนอก การระบุตัวตนดังกล่าวสามารถตรวจสอบย้อนกลับ (Audit trail) และจัดเก็บบันทึก (Log) ให้ไม่น้อยกว่า ๙๐ วัน หรือต้องสอดคล้องกับ ระยะเวลาการจัดเก็บบันทึกจราจรคอมพิวเตอร์ขององค์กร

๙. ไม่อนุญาตให้ใช้ Port, Service หรือช่องทางการเชื่อมต่อที่ไม่ปลอดภัย และไม่แนะนำให้มีการใช้ Default port การใช้งานที่เป็นลักษณะคำขอชั่วคราว (Request) เพื่อให้บรรลุวัตถุประสงค์ของการดำเนินโครงการ หรือกิจกรรมใด ต้องกำหนดระยะเวลาให้ชัดเจน และได้รับการอนุมัติเป็นลายลักษณ์อักษร

๑๐. ปิดการใช้งานการเชื่อมต่อที่ตัวอุปกรณ์เครือข่ายทุกประเภทที่ไม่ได้ใช้งาน โดยเฉพาะในบริเวณสำนักงานที่บุคคลภายนอกสามารถเข้าถึงได้

๑๑. จัดให้มีมาตรการเฝ้าระวังภัยคุกคามทางเครือข่ายด้วยเทคโนโลยีที่ทันสมัย สามารถตรวจสอบได้ในระดับ Deep package inspection หากเป็นไปได้ต้องมีเทคโนโลยีป้องกันในระดับ Application เช่น Web Application Firewall (WAF) และมีการใช้เปิดตัวกรองการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม (Web Filtering)

๑๒. อุปกรณ์เฝ้าระวังทางเครือข่ายควรมีเทคโนโลยี Threat Intelligence ที่สามารถปรับปรุงฐานข้อมูลภัยคุกคามจากแหล่งข้อมูลที่น่าเชื่อถือได้

๑๓. ต้องจัดให้มีมาตรการแจ้งเตือนภัยคุกคามทางเครือข่ายหรือพฤติการณ์ผิดปกติของการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายของ สสช. หรือเรียกตรวจสอบเครื่องคอมพิวเตอร์ดังกล่าว เพื่อให้มั่นใจว่าไม่พบการติด Malware ที่ส่งผลให้มีการใช้งานภายในเครือข่าย

๑๔. เมื่อมีการเชื่อมต่อบูรณาการข้อมูลระบบระหว่างระบบสารสนเทศภายใน สสช. กับระบบสารสนเทศภายนอกที่กำหนดจากหมายเลข IP Address ได้ ต้องกำหนดหมายเลข IP Address ต้นทางและเป้าหมายในการติดต่อสื่อสาร รวมถึงบริการ (Service) ที่จำเป็นเท่านั้น และใช้หลักการตั้งค่า Deny by default เสมอ

หมวด ๑๐ การจัดหา การพัฒนา และการบำรุงรักษา
(Information System Acquisition Development and Maintenance)

วัตถุประสงค์

เพื่อให้การจัดหาหรือพัฒนาระบบสารสนเทศ รวมถึงที่มีอยู่ให้มีความปลอดภัยสำหรับการใช้งานจริง โดยพิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นพื้นฐานสำคัญ ป้องกันการผิดพลาด การสูญหาย การเปลี่ยนแปลงแก้ไขซอฟต์แวร์และโปรแกรมประยุกต์โดยไม่ได้รับอนุญาต การป้องกันความลับ และให้มั่นใจว่าโครงการต่าง ๆ หรือนโยบายต่าง ๆ ที่จัดทำขึ้นนั้น สร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สารสนเทศ และดูแลรักษาให้สารสนเทศมีความมั่นคงปลอดภัยอยู่เสมอ

แนวทางปฏิบัติ

๑. ให้มีมาตรการควบคุมการว่าจ้างพัฒนาระบบ (Outsource Software Development) กรณีมีการจ้างเหมาดำเนินการพัฒนา บำรุงรักษาระบบสารสนเทศและเครือข่าย เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยด้านสารสนเทศ (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาเป็นลายลักษณ์อักษร อย่างน้อยเป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้ใช้วิธีการในการพัฒนาชุดคำสั่งตามมาตรฐาน OWASP หรือมาตรฐาน CWE ที่มีกระบวนการควบคุมการนำเข้าข้อมูล การแสดงผล การควบคุม การประมวลผล เป็นอย่างน้อย

(๒) ให้มีการทดสอบการสแกนหาช่องโหว่ของโปรแกรมประยุกต์ และหากพบช่องโหว่จะต้องดำเนินการปิดช่องโหว่ที่ปรากฏให้หมด

(๓) ให้ใช้วิธีการทางวิศวกรรมซอฟต์แวร์ในการพัฒนาโปรแกรมตามมาตรฐาน ISO/IEC 29110

(๔) กำหนดให้มีการจัดทำแผนงานและขั้นตอนการดำเนินงานที่เกี่ยวกับการพัฒนาระบบสารสนเทศ การติดตั้งระบบคอมพิวเตอร์และอุปกรณ์ การทดสอบระบบหลังการติดตั้ง และแผนการบริหารความเสี่ยง โดยจะต้องนำเสนอแผนฯ ทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้กับผู้ที่รับผิดชอบงานโครงการ

(๕) ให้มีเกณฑ์ในการตรวจรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ รวมทั้งต้องตรวจสอบและทดสอบระบบโดยละเอียด ก่อนที่จะตรวจรับและติดตั้งใช้งานจริง

๒) ให้มีข้อกำหนดการเปลี่ยนแปลงแก้ไขระบบสารสนเทศให้เป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ระบบสารสนเทศหรือเปลี่ยนแปลงโครงสร้างฐานข้อมูล ตามแบบคำขอให้แก้ไข โดยจะต้องมาจากผู้มีสิทธิและต้องได้รับการอนุมัติจากผู้มีอำนาจ รวมถึงมีการบันทึกรายละเอียดการแก้ไขจากผู้สนับสนุนภายนอกทุกครั้ง

(๒) ให้เข้าถึงได้เฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมีการควบคุมหรือตรวจสอบอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

(๓) ให้มีมาตรการควบคุมป้องกันการรั่วไหลของสารสนเทศขององค์กร หากมีความจำเป็นต้องใช้ข้อมูลจริงในการทดสอบระบบ จะต้องเป็นข้อมูลเฉพาะบางส่วน หรือข้อมูลที่ไม่สำคัญ และจะต้องได้รับอนุมัติจากผู้ที่รับผิดชอบแล้วเท่านั้น

๒. ให้มีมาตรการควบคุมผู้สนับสนุนจากภายนอก ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการกำหนดเกณฑ์การคัดเลือกผู้สนับสนุนจากภายนอกที่มีคุณภาพ มีขั้นตอนการปฏิบัติงานที่ดีเป็นที่เชื่อถือ

๒) ให้มีการกำหนดเกณฑ์การตรวจสอบประวัติพนักงานจ้างบำรุงรักษา พัฒนาระบบงาน

๓) ให้ผู้สนับสนุนจากภายนอกที่จะเข้ามาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์จะต้องขอความเห็นชอบจากผู้รับผิดชอบหรือผู้ดูแลระบบก่อนทุกครั้ง และการดำเนินงานทุกครั้งจะต้องอยู่ในความดูแลของผู้รับผิดชอบหรือผู้ดูแลระบบ

๔) ผู้สนับสนุนจากภายนอกจะได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ลูกข่ายเฉพาะที่อนุญาตให้เข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายเพื่อแก้ไขซอฟต์แวร์เท่านั้น

๕) ให้มีการลงนามในสัญญาการจ้างการพัฒนาระบบ การไม่เปิดเผยข้อมูลที่เป็นความลับและงานที่มีความเกี่ยวเนื่องกับระบบความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

๖) กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ

๗) ให้ผู้สนับสนุนจากภายนอกจัดทำรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางการแก้ไข

๘) ผู้สนับสนุนจากภายนอกจะต้องปฏิบัติตามข้อกำหนดและระเบียบของสำนักงานสถิติแห่งชาติอย่างเคร่งครัด และเมื่อสิ้นสุดโครงการผู้สนับสนุนจากภายนอกจะถูกยกเลิกสิทธิทั้งหมดทันที

๙) กรณีการนำเครื่องคอมพิวเตอร์ออกไปซ่อมบำรุงภายนอกสำนักงานสถิติแห่งชาติและในเครื่องคอมพิวเตอร์นั้นมีข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะรายให้มีการทำข้อตกลงว่าด้วยการไม่เปิดเผยข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลหรือเฉพาะราย

๓. ให้มีการบำรุงรักษาระบบและเฝ้าติดตามคุณภาพการใช้งาน ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการบำรุงรักษาระบบสนับสนุนห้องศูนย์คอมพิวเตอร์ ประกอบด้วย ระบบสำรองไฟฟ้า ระบบดับเพลิง ระบบตรวจจับควันไฟ ระบบปรับอากาศ ระบบตรวจจับการรั่วซึมของน้ำ ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย และระบบความมั่นคงปลอดภัย อย่างต่อเนื่องเป็นประจำทุกปี

๒) ให้ผู้ดูแลระบบทำการปรับปรุงคู่มือการจัดการระบบ คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องให้มีความถูกต้องและทันสมัยตลอดเวลา

๓) ให้เฝ้าติดตามการใช้งานของทรัพยากรในระบบ และติดตามคุณภาพการให้บริการเป็นรายระบบ และหากพบให้ปรับปรุงให้มีค่าเป็นไปตามที่กำหนดไว้

๔. ให้มีมาตรการเข้ารหัสมาใช้ในการรับ - ส่งข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) การตรวจสอบสิทธิของผู้ใช้งานในหน้าเว็บ

๒) โปรแกรมประยุกต์และบริการบนเครือข่ายอินเทอร์เน็ตที่ต้องการความปลอดภัย

๓) การโอนไฟล์ข้อมูลระหว่างเครื่องที่มีข้อมูลที่ต้องปกปิด

๕. ให้มีมาตรการควบคุมไฟล์ข้อมูลที่ถูกเปลี่ยนแปลง ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดการและควบคุมสิทธิการเข้าถึงและแก้ไขไฟล์ข้อมูล

๒) ให้มีการวิเคราะห์ไฟล์ที่เปลี่ยนแปลงมีผลกระทบต่อการบริการอื่นหรือไม่

๓) ให้มีการสำรองไฟล์ข้อมูลที่จะถูกเปลี่ยนแปลงในทุกครั้งก่อนดำเนินการเปลี่ยนแปลง เพื่อใช้ในการกู้คืนในภายหลัง

๖. ให้มีการตรวจสอบช่องโหว่ (Vulnerability) ของระบบสารสนเทศเป็นประจำ ตามข้อกำหนดดังต่อไปนี้

๑) การตรวจสอบช่องโหว่ของระบบเครือข่าย ช่องโหว่ของระบบคอมพิวเตอร์แม่ข่าย และช่องโหว่ของโปรแกรมประยุกต์

๒) ให้มีการปรับแก้เพื่อปิดช่องโหว่ที่ตรวจพบและเป็นภัยที่อันตรายต่อระบบโดยเร็ว

หมวด ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

วัตถุประสงค์

เพื่อเป็นการคุ้มครองทรัพย์สินขององค์กรที่ผู้ให้บริการภายนอกสามารถเข้าถึงได้ รวมถึงการควบคุมผู้ให้บริการ Outsource จึงจำเป็นต้องมีมาตรการควบคุมดูแลการให้บริการของผู้ให้บริการภายนอกเหล่านั้น เพื่อให้มั่นใจว่าการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยของข้อมูลเป็นไปตามสัญญาหรือข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่ได้กำหนดไว้

แนวทางปฏิบัติ

๑. ภายใต้สัญญาบริการกับผู้ให้บริการภายนอกต้องปรากฏ

๑.๑ ข้อตกลงการรักษาความลับ ไม่ว่าจะเป็นส่วนหนึ่งของสัญญา หรือเป็นสัญญาประกอบ หรือเป็นสัญญาแยกออกมา โดยเงื่อนไขการรักษาความลับต้องครอบคลุมระยะเวลาไม่ต่ำกว่าระยะเวลาของสัญญาบริการ

๑.๒ ข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่สอดรับกับผลการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ของกระบวนการทางภารกิจของ สสช. ที่สัญญาบริการนั้นมีผลกระทบ หรือเป็นส่วนสนับสนุนที่สำคัญ

๑.๓ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing Agreement) ในกรณีที่บริการดังกล่าวมีการ เก็บ รวบรวม ใช้ เปิดเผย ซึ่งข้อมูลส่วนบุคคลที่ผู้ให้บริการรายดังกล่าวเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data processor)

๑.๔ ลิขสิทธิ์และสิทธิอันเกิดจากผลงานสร้างสรรค์ภายใต้สัญญาจ้างหรือสัญญาบริการ ต้องกำหนดผู้เป็นเจ้าของลิขสิทธิ์ ลักษณะสิทธิการใช้ เงื่อนไขการใช้สิทธิ (Terms and Conditions) เว้นแต่มีเอกสารแยกออกมาที่ได้ครอบคลุมประเด็นดังกล่าวแล้ว เช่น Subscription agreement, User agreement

๑.๕ กำหนดความรับผิดความเสียหายที่เกิดจากเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดจากความบกพร่อง ชำรุด หรือความผิดพลาดของผู้รับจ้าง โดยให้พิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคลที่ สสช. เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) ด้วย

๒. ความสามารถในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สามารถเป็นเกณฑ์หนึ่งในการประเมินสมรรถนะและคัดเลือกของผู้รับยื่นข้อเสนอ เช่น การพิจารณามาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงานที่ยื่นข้อเสนอ เว้นแต่เกณฑ์การพิจารณาดังกล่าวจะขัดหรือแย้งต่อระเบียบการจัดซื้อจัดจ้างภาครัฐ

๓. จัดให้หน่วยงานที่เกี่ยวข้องกับสัญญาบำรุงรักษา พิจารณาประเมินสมรรถนะการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอก ตามระดับความเสี่ยงและระดับชั้นความลับของข้อมูลสารสนเทศที่ผู้ให้บริการภายนอกรายนั้นเข้าถึง

๔. สำหรับบริการ Cloud Service ต้องพิจารณาถึงขีดความสามารถของผู้ให้บริการที่เหมาะสมระดับสัญญาบริการ และการวางแผนจัดการหลังจากเลิกใช้บริการ (Exit Plan) ตลอดจนมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการได้รับการรับรอง

๕. ในกรณีเป็นการจ้างพัฒนาระบบสารสนเทศ ผู้รับจ้างต้องจัดให้มีมาตรการด้านความมั่นคงปลอดภัยสารสนเทศอย่างเพียงพอ ในการกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ การออกแบบการพัฒนา การทดสอบ และการติดตั้ง ที่สอดรับกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สสช. โดยต้องพิจารณาประยุกต์ใช้ในขอบเขตที่ดำเนินการได้ตามความเหมาะสม เช่น การกำหนดมาตรการควบคุมคุณภาพรหัสผ่าน การเข้ารหัส การตรวจทานช่องโหว่ หรือการควบคุมการเปลี่ยนแปลงเวอร์ชั่นของระบบสารสนเทศ

๖. การดำเนินกิจกรรมใด ๆ ที่ก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่เป็นผลจากการปฏิบัติหน้าที่ของผู้ให้บริการภายนอกต้องตรวจทานก่อนการดำเนินการโดยผู้ดูแลระบบ

๗. เมื่อมีการสิ้นสุดการจ้างงาน หรือสิ้นสุดสัญญากับผู้ให้บริการภายนอก สสช. โดยผู้รับผิดชอบโครงการหรือคณะกรรมการตรวจรับโครงการ ต้องเรียกคืนทรัพย์สินสารสนเทศที่เป็นของ สสช. จากผู้ให้บริการภายนอก เว้นแต่การกระทำดังกล่าวไม่สามารถดำเนินการได้ ให้ผู้ที่เกี่ยวข้องดำเนินการตรวจสอบให้มั่นใจว่าได้มีการลบหรือทำลายข้อมูลสารสนเทศจากระบบสารสนเทศทั้งหมดแล้ว

หมวด ๑๒ การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้มีแผนการจัดการหากเกิดสถานการณ์อันไม่พึงประสงค์และไม่คาดคิดกับระบบสารสนเทศ ได้แก่ ภัยจากการโจมตีบนระบบเครือข่ายอินเทอร์เน็ต หรือภัยจากเพลิงไหม้ ภัยจากธรรมชาติ หรือภัยอื่น ๆ ให้ระงับได้อย่างรวดเร็ว เพื่อให้เกิดผลกระทบต่อระบบสารสนเทศของสำนักงานสถิติแห่งชาติให้น้อยที่สุด

แนวทางปฏิบัติ

๑. ให้มีการวิเคราะห์ กำหนด และทบทวนเหตุการณ์ที่เป็นภัยคุกคามต่อทรัพย์สินสารสนเทศที่สำคัญ ซึ่งนำไปสู่ความเสียหายต่อระบบสารสนเทศ จนส่งผลกระทบต่อการดำเนินงานตามภารกิจขององค์กร โดยให้จัดทำแผนการจัดการเหตุการณ์ภัยที่ไม่พึงประสงค์เป็นไปตามลำดับความสำคัญและความน่าจะเป็นที่จะเกิดขึ้น

๒. ให้จัดทำแผนจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ โดยต้องมีองค์ประกอบตามข้อกำหนดดังต่อไปนี้

๑) มีแผนการป้องกัน
   (๑) การวิเคราะห์การเกิดของสถานการณ์
   (๒) การกำหนดผู้รับผิดชอบต่อสถานการณ์
   (๓) การประเมินความเสียหายทรัพย์สินสารสนเทศ
   (๔) การกำหนดเครื่องมือในการดำเนินการ
   (๕) การให้ความรู้และการฝึกซ้อม
   (๖) การเตรียมการรับมือเหตุการณ์
   (๗) สถานที่ปฏิบัติงาน

๒) มีแผนการตรวจจับและเฝ้าระวัง
   (๑) ให้มีกระบวนการตรวจจับและเฝ้าระวัง
   (๒) กำหนดแบบฟอร์มที่ใช้จัดเก็บข้อมูล
   (๓) จัดเก็บข้อมูลเหตุการณ์ที่เกิดขึ้นลงในแบบฟอร์ม
   (๔) มีแผนการป้องกัน

๓) มีแผนการเผชิญเหตุ
   (๑) เครื่องมือในการปฏิบัติงาน
   (๒) การติดต่อสื่อสาร
   (๓) ขั้นตอนการปฏิบัติตามระดับความรุนแรงของเหตุการณ์

๔) มีแผนการสอบสวนและเก็บหลักฐาน
   (๑) การดำเนินคดีตามกฎหมาย
   (๒) การเก็บหลักฐานเพื่อการสอบสวน

๕) มีแผนการกู้คืนเพื่อกลับสู่สภาพเดิม

(๑) เครื่องมือการกู้คืนระบบ

(๒) ผู้รับผิดชอบในการกู้คืน

๓. ให้มีระบบตรวจสอบการบุกรุก และการใช้งานในลักษณะผิดปกติผ่านระบบเครือข่าย และรายงานจุดอ่อน ช่องโหว่ที่ตรวจพบโดยเร่งด่วน โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

๑) ความพยายามในการบุกรุกผ่านระบบเครือข่าย

๒) การใช้งานในลักษณะผิดปกติ

๓) การใช้งานที่มีการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๔. ให้มีการซ้อมแผนและฝึกอบรมเผชิญเหตุสำหรับแผนป้องกันไฟไหม้เป็นประจำทุกปีหรือในความถี่ที่เหมาะสม และนำมาปรับปรุงการดำเนินงานอย่างต่อเนื่อง

หมวด ๑๓ การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง (Government Continuity Management)

วัตถุประสงค์

เพื่อเป็นการเตรียมความพร้อมหากทรัพย์สินสารสนเทศขององค์กรได้รับความเสียหายจากสถานการณ์อันไม่พึงประสงค์ จนทำให้ระบบสารสนเทศและข้อมูลเสียหาย หรือหยุดทำงานไม่สามารถให้บริการได้ จึงต้องมีความพร้อมในการทำให้ระบบกลับมาใช้งานได้เช่นเดิม

แนวทางปฏิบัติ

๑. ให้จัดทำแผนสร้างความต่อเนื่องของการดำเนินงาน (Business Continuity Plan) โดยต้องมีองค์ประกอบตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการวิเคราะห์ผลกระทบของระบบสารสนเทศต่อภารกิจขององค์กร (Business Impact Analysis)

๒) ให้มีการระบุถึงเหตุการณ์ที่ต้องนำแผนฉุกเฉินมาใช้งาน

๓) ให้มีการกำหนดสถานการณ์ หรือลำดับความรุนแรงของปัญหา

๔) ให้มีการวิเคราะห์ทางเลือกใช้ศูนย์สำรองข้อมูล และสถานที่สำหรับใช้เป็นศูนย์สำรอง

๕) ให้มีการกำหนดหน้าที่ที่รับผิดชอบและผู้มีอำนาจในการตัดสินใจ รวมทั้งกำหนดช่องทางการติดต่อเมื่อมีเหตุการณ์เกิดขึ้น

๖) ให้กำหนดวิธีปฏิบัติโดยละเอียดเมื่อมีเหตุการณ์เกิดขึ้น

๗) ให้กำหนดวิธีปฏิบัติเพื่อโยกย้ายกิจกรรมไปยังสถานที่ชั่วคราว

๘) ให้กำหนดวิธีปฏิบัติภายหลังจากการโยกย้ายเพื่อกลับมาดำเนินการตามปกติ

๙) ให้มีการให้ความรู้และสร้างความตระหนักแก่บุคลากรที่เกี่ยวข้องกับแผนฉุกเฉิน

๑๐) ให้มีการทดสอบและปรับปรุงแผนต่อเนื่องปีละ ๑ ครั้ง เพื่อให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

๒. ให้มีระบบสำรองเป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้กำหนดวิธีปฏิบัติ หรือขั้นตอนในการสำรองข้อมูลให้ชัดเจน โดยระบุข้อมูลที่จะสำรอง ความถี่ในการสำรองข้อมูล สื่อที่ใช้ สถานที่เก็บ วิธีการเก็บรักษา และการนำมาใช้งาน

๒) ให้จัดทำนโยบาย ขั้นตอน หรือวิธีปฏิบัติในการสำรองข้อมูล (Back Up) โดยต้องมีองค์ประกอบตามข้อกำหนดดังต่อไปนี้

(๑) ข้อมูลที่ต้องสำรอง

(๒) ความถี่ในการสำรอง

(๓) ประเภทสื่อบันทึก (Media)

(๔) จำนวนที่ต้องสำรอง (Copy)

(๕) ขั้นตอนและวิธีการสำรองโดยละเอียด

(๖) สถานที่และวิธีการเก็บรักษาสื่อสำรองให้ปลอดภัย

(๗) การเฝ้าติดตามตรวจสอบผลการสำรองข้อมูล

(๘) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ดังนี้ ข้อมูลคอนฟิกกูเรชัน (Configuration) ของระบบฐานข้อมูล (Database) และซอฟต์แวร์ (Software) ของระบบสารสนเทศ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน หรือซอฟต์แวร์อื่น ๆ ที่สำคัญ

(๙) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยแบ่งเป็น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๓) ให้มีการบันทึกการปฏิบัติงาน (Log Book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวพร้อมทั้งรายงานอย่างสม่ำเสมอ

(๑) ให้จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่จัดเก็บดังกล่าวต้องให้มีระบบควบคุมการเข้า - ออก และระบบป้องกันความเสียหายของข้อมูลด้วย

(๒) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น การเก็บอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อที่บันทึกข้อมูลไว้

(๓) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องมีการรายงานข้อผิดพลาด (Fault logging) บันทึกข้อผิดพลาดและดำเนินการแก้ไขโดยทันที

๓. ให้มีระบบทดสอบการกู้คืนข้อมูล (Restore) เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดเตรียมเครื่องคอมพิวเตอร์แม่ข่ายเพื่อใช้ในการทดสอบการกู้คืนข้อมูลที่สำคัญ

๒) ให้ทดสอบการกู้คืนข้อมูลที่สำรองอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าข้อมูลรวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้ ตลอดจนขั้นตอนและวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

หมวด ๑๔ การปฏิบัติตามข้อกำหนด (Compliance)

วัตถุประสงค์

เพื่อเป็นการตรวจสอบการนำนโยบายและแนวปฏิบัติในการักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งการใช้งานทรัพย์สินสารสนเทศของผู้ใช้งานให้เป็นไปตามระเบียบที่กำหนด โดยใช้กระบวนการตรวจสอบด้วยตนเองสำหรับผู้ปฏิบัติ การตรวจสอบจากหน่วยตรวจสอบภายในสำหรับผู้ใช้งาน และการตรวจสอบจากหน่วยตรวจสอบภายนอกในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

แนวทางปฏิบัติ

๑. ให้ผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยด้านสารสนเทศ ประเมินตนเองเพื่อนำมาสู่การปรับปรุงกระบวนงานให้มีความสมบูรณ์สูงสุดเป็นประจำทุกปี ตามข้อกำหนดดังนี้

๑) ประเมินตนเองด้วยแบบประเมินตนเองเพื่อวิเคราะห์ช่องว่าง (Gap Analysis)

๒) ประเมินตนเองด้วยการทดสอบการเจาะระบบ (Penetration Testing)

๒. ให้ผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยด้านสารสนเทศทำการประเมินตนเอง

๓. ให้หน่วยตรวจสอบภายใน (Internal Auditor) ของสำนักงานสถิติแห่งชาติ ตรวจประเมินผู้ใช้งานมีการปฏิบัติตามระเบียบการใช้งานทรัพย์สินสารสนเทศ และการนำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาใช้ในการปฏิบัติงานเป็นประจำสม่ำเสมอในทุก ๆ ๒ ปี

๔. ให้หน่วยตรวจสอบภายนอก (External Auditor) ตรวจประเมินระบบความมั่นคงปลอดภัยที่มีความซับซ้อนต้องใช้ความรู้ความเชี่ยวชาญเฉพาะเป็นประจำสม่ำเสมอในทุก ๆ ๒ ปี

๕. ให้มีการตรวจสอบโดยหน่วยตรวจสอบภายใน และหน่วยตรวจสอบภายนอกอย่างต่อเนื่อง และให้นำผลการประเมินของหน่วยตรวจสอบมาใช้ในการวางแผนการปรับปรุงระบบความมั่นคงปลอดภัยด้านสารสนเทศในปีถัดไป