ประกาศสำนักงานสถิติแห่งชาติ

เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงานสถิติแห่งชาติ พ.ศ. ๒๕๖๒

ด้วย สำนักงานสถิติแห่งชาติ มีบทบาทและอำนาจหน้าที่ตามพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ ในฐานะเป็นหน่วยงานกลางของรัฐ เกี่ยวกับการดำเนินการด้านสถิติของประเทศ บริหารจัดการสถิติและสารสนเทศของชาติอย่างเป็นระบบเพื่อการพัฒนา และเสริมสร้างศักยภาพการแข่งขัน โดยการจัดทำสำมะโนหรือสำรวจด้วยตัวอย่าง การอำนวยการเพื่อให้ได้ฐานข้อมูลทางด้านเศรษฐกิจสังคม เทคโนโลยีสารสนเทศ และอื่นๆ ของประเทศ รวมทั้งการให้ความร่วมมือและประสานงานกับองค์กรระหว่างประเทศในงานเกี่ยวกับสถิติ ปัจจุบัน สำนักงานสถิติแห่งชาติ นำระบบคอมพิวเตอร์เครือข่าย และวิธีการทางอิเล็กทรอนิกส์มาใช้ในกระบวนการบริหารจัดการระบบสถิติ กระบวนการผลิตข้อมูลสถิติ กระบวนการให้บริการข้อมูลสถิติและสารสนเทศ เพื่อให้เกิดประสิทธิภาพสูงสุดในการปฏิบัติงาน

อาศัยอำนาจตามความใน มาตรา ๕ และ มาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกอบประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และ ที่แก้ไขเพิ่มเติม พ.ศ. ๒๕๕๖ สำนักงานสถิติแห่งชาติ จึงได้จัดทำประกาศฉบับนี้ขึ้น เพื่อเป็นแนวทางให้ทุกภาคส่วนขององค์กรนำไปปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความเชื่อถือต่อผู้ใช้ข้อมูลและสารสนเทศ โดยมีเนื้อหาสาระดังต่อไปนี้

ข้อ ๑. ในประกาศนี้

๑) “สำนักงานสถิติแห่งชาติ” หมายความว่า หน่วยงานภายในสังกัด สำนักงานสถิติแห่งชาติ รวมถึงสำนักงานสถิติจังหวัด

๒) “กระบวนการสถิติ” หมายความว่า กระบวนการที่สร้างคุณค่า และกระบวนการสนับสนุน

๓) “กระบวนการที่สร้างคุณค่า” หมายความว่า กระบวนการผลิตข้อมูลสถิติ กระบวนการให้บริการข้อมูลสถิติ กระบวนการบริหารจัดการระบบสถิติ

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) “สินทรัพย์” 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) “สารสนเทศสถิติ” หมายความว่า ข้อมูลที่ได้จากการประมวลผลหรือวิเคราะห์ด้วยระเบียบวิธีสถิติ

๒๐) “ข้อมูลสถิติ” หมายความว่า ข้อมูลที่ได้จากการดำเนินการเกี่ยวกับสถิติตามหลักวิชาการ ประกอบด้วย ข้อมูลดิบ ข้อมูลระดับย่อย ข้อมูลเฉพาะบุคคล

๒๑) “ข้อมูลดิบ” หมายความว่า ข้อมูลจากแบบสอบถามของโครงการสำมะโน/สำรวจต่างๆ ของสำนักงานสถิติแห่งชาติที่อยู่ในรูปอิเล็กทรอนิกส์ และยังมิได้ประมวลผล

๒๒) “ข้อมูลระดับย่อย” หมายความว่า ข้อมูลดิบทั้งหมดที่ผ่านการตรวจสอบความถูกต้อง ความครบถ้วน และความแนบนัยของข้อมูลไว้เรียบร้อยแล้ว พร้อมที่จะนำไปใช้ในการประมวลผลเป็นสถิติต่อไป

๒๓) “ข้อมูลเฉพาะบุคคล” หมายความว่า ข้อมูลของบุคคล หรือนิติบุคคล ห้างหุ้นส่วนสามัญ หรือคณะบุคคล ซึ่งเป็นเจ้าของข้อมูลที่ได้ให้ข้อมูลหรือกรอกแบบสอบถามให้แก่สำนักงานสถิติแห่งชาติ

๒๔) “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลของบุคคลธรรมดา เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

๒๕) “ระบบคอมพิวเตอร์” หมายความว่า เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่ต่อพ่วงรวมถึงซอฟต์แวร์ที่ใช้งาน

๒๖) “ระบบเครือข่าย” หมายความว่า ระบบเครือข่ายระยะไกล ระบบเครือข่ายภายใน NGX ระบบเครือข่ายไร้สาย

๒๗) “ระบบเครือข่าย NGX” หมายความว่า ระบบคอมพิวเตอร์เครือข่ายภายในแบบใช้สายและไร้สาย ของศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา อาคารรัฐประศาสนภักดี (อาคาร B) ซึ่งจัดการโดยบริษัท ทีโอที จำกัด (มหาชน)

๒๘) “ระบบเครือข่าย GIN” หมายความว่า ระบบคอมพิวเตอร์เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ

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

๓๐) “การเข้าถึงหรือควบคุมการใช้งานข้อมูลและการใช้สารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือ ข้อมูล หรือ ระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับผู้ติดต่อราชการ ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๓๑) “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ

รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๓๒) "การรักษาความลับ (Confidentiality)" หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์ จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

๓๓) "การรักษาความครบถ้วน (Integrity)" หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

๓๔) "การรักษาสภาพพร้อมใช้งาน (Availability)" หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

๓๕) "เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า การเกิดเหตุการณ์ หรือสภาพของบริการที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๓๖) "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๓๗) "ผู้ดูแลระบบ" หมายความว่า ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย ผู้ดูแลระบบความมั่นคงปลอดภัย ผู้ดูแลระบบโปรแกรมประยุกต์ ผู้ดูแลระบบฐานข้อมูล ผู้ดูแลระบบสารสนเทศ ผู้ดูแลระบบสำรองข้อมูล

๓๘) "ผู้ดูแลระบบคอมพิวเตอร์" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบคอมพิวเตอร์แม่ข่าย

๓๙) "ผู้ดูแลระบบเครือข่าย" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบคอมพิวเตอร์เครือข่าย

๔๐) "ผู้ดูแลระบบความมั่นคงปลอดภัย" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ

๔๑) "ผู้ดูแลระบบโปรแกรมประยุกต์" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการโปรแกรมประยุกต์

๔๒) "ผู้ดูแลระบบฐานข้อมูล" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบฐานข้อมูล

๔๓) "ผู้ดูแลระบบสำรองข้อมูล" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบสำรองข้อมูลและกู้คืน

๔๔) "ผู้ดูแลระบบสารสนเทศ" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบสารสนเทศ

๔๕) “วิธีการแบบปลอดภัย” หมายความว่า วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

๔๖) “ธุรกรรมทางอิเล็กทรอนิกส์” หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน

๔๗) “ธุรกรรม” หมายความว่า การกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนด

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

๔๙) “การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์” หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

๕๐) “การแปลงข้อมูล” หมายความว่า การแปลงข้อมูลจากเอกสารเข้าระบบอิเล็กทรอนิกส์ด้วยวิธีการ Key เข้าระบบหรือ Scan เป็นไฟล์ภาพเข้าระบบ

๕๑) “ผู้บริหารระดับสูงสุด” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานสถิติแห่งชาติ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย ตัดสินใจ และแนะนำแนวทางการดำเนินงานของสำนักงานสถิติแห่งชาติ

ข้อ ๒. กำหนดให้ผู้อำนวยการสำนักงานสถิติแห่งชาติ เป็นผู้รับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๓. ให้มีหมวดของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จำนวน ๑๑ หมวด และให้มีการปรับปรุงให้สอดคล้องกับภารกิจและเป็นปัจจุบันอยู่เสมอในทุก ๒ ปี ดังนี้

หมวดที่ ๑ การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อให้ระบบความมั่นคงปลอดภัยด้านสารสนเทศ รองรับกับภารกิจและกระบวนงานของสำนักงานสถิติแห่งชาติ มีความน่าเชื่อถือ มีคุณสมบัติ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และ การรักษาสภาพพร้อมใช้งาน (Availability)

หมวดที่ ๒ โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อกำหนดความรับผิดชอบและข้อตกลงการดำเนินงานในกิจกรรมระบบความมั่นคงปลอดภัยด้านสารสนเทศ ของเจ้าหน้าที่สำนักงานสถิติแห่งชาติและผู้สนับสนุนจากภายนอก

หมวดที่ ๓ การบริหารจัดการทรัพย์สินสารสนเทศ

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อปกป้องให้ทรัพย์สินสารสนเทศมีสภาพความพร้อมในการใช้งาน ไม่เกิดความเสียหายเป็นอุปสรรคต่อการดำเนินงาน

หมวดที่ ๔ การสร้างความมั่นคงปลอดภัยด้านบุคลากร

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อเป็นการป้องกันความเสียหายที่เกิดจากบุคลากรภายในหรือจากภายนอกเป็นสำคัญ

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบงานคอมพิวเตอร์

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อการจัดการช่องทางสื่อสารและระบบคอมพิวเตอร์ให้มีความปลอดภัยรองรับกับการใช้งาน

หมวดที่ ๗ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อควบคุมการเข้าถึงของผู้ใช้ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบความมั่นคงปลอดภัย โปรแกรมประยุกต์ ไฟล์ข้อมูล ระบบฐานข้อมูล และ การทำลายข้อมูลและสื่ออิเล็กทรอนิกส์

หมวดที่ ๘ การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อรับมือกับภัยธรรมชาติ ภัยบนระบบเครือข่าย และภัยอื่นๆ ที่อาจสร้างความเสียหายกับทรัพย์สินสารสนเทศ อย่างเป็นขั้นตอน

หมวดที่ ๙ การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อเตรียมความพร้อม กู้คืนระบบคอมพิวเตอร์ การสำรองข้อมูล การกู้คืนข้อมูล หรือ กำหนดทางเลือกใช้ศูนย์คอมพิวเตอร์สำรอง ให้ระบบสารสนเทศกลับมาดำเนินการได้ในเวลาที่รวดเร็ว

หมวดที่ ๑๐ การจัดหา การพัฒนา และการบำรุงรักษา

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาควบคุมการจัดหา การติดตั้ง การพัฒนาโปรแกรมประยุกต์ และการบำรุงรักษาระบบเพื่อให้มีสภาพพร้อมใช้งานตลอดเวลา

หมวดที่ ๑๑ การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบายและข้อกำหนด

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการตรวจสอบและประเมินระบบความมั่นคงปลอดภัยด้านสารสนเทศ จากหน่วยตรวจสอบภายใน หรือหน่วยตรวจสอบภายนอก

ข้อ ๔. ให้มีแนวปฏิบัติในแต่ละหมวด พร้อมทั้งระเบียบการใช้งานที่เกี่ยวกับงานความมั่นคงปลอดภัยด้านสารสนเทศ และบทลงโทษที่เหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวปฏิบัติ ระเบียบการใช้งาน อย่างเป็นลายลักษณ์อักษร พร้อมกับประกาศให้เจ้าหน้าที่สำนักงานสถิติแห่งชาติรับทราบโดยทั่วกัน

ข้อ ๕. ส่งเสริมและสนับสนุนให้มีการนำแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ และระเบียบการใช้งานทรัพย์สินสารสนเทศ บังคับใช้ในองค์กรอย่างจริงจัง และ ให้มีคณะกรรมการด้านความมั่นคงและปลอดภัยด้านสารสนเทศ หรือ คณะกรรมการเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อกำกับและติดตามงานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

ข้อ ๖. ส่งเสริมและสนับสนุนให้มีการกำกับดูแลระบบสารสนเทศที่ดี (IT Governance) การจัดการความเสี่ยงด้านไอที (IT Risk) และการปฏิบัติตามกฎหมาย (Compliance) ระเบียบ การควบคุมภายใน

ข้อ ๗. ส่งเสริมและสนับสนุนให้ทุกส่วนงานของสำนักงานสถิติแห่งชาติใช้วิธีการแบบปลอดภัยในกระบวนการสถิติทั้งในกระบวนการสร้างที่สร้างคุณค่า และกระบวนการสนับสนุน

ข้อ ๘. ส่งเสริมและสนับสนุนให้มีการนำเทคโนโลยีด้านความมั่นคงปลอดภัยที่จำเป็นมาติดตั้งใช้งาน เพื่อสร้างความเข้มแข็งให้เพียงพอต่อการป้องกันภัยร้ายบนระบบเครือข่ายทั้งสำนักงานสถิติแห่งชาติและสำนักงานสถิติจังหวัด

ข้อ ๙. ส่งเสริมและสนับสนุนให้มีการซ้อมแผนฉุกเฉินจากเหตุการณ์อันไม่พึงประสงค์ ประกอบด้วย เพลิงไหม้ น้ำท่วม และภัยคุกคามจากระบบเครือข่ายอินเทอร์เน็ตเป็นประจำ เพื่อเตรียมความพร้อมหากเกิดเหตุการณ์ฉุกเฉินและไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้

ข้อ ๑๐. ส่งเสริมและสนับสนุนให้กลุ่มตรวจสอบภายในสามารถตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศในระดับเบื้องต้นที่เกี่ยวกับระเบียบการใช้งาน และใช้ผู้ตรวจสอบจากภายนอกในการตรวจสอบความครบถ้วนของระบบความมั่นคงปลอดภัย

ข้อ ๑๑. ส่งเสริมให้มีการเผยแพร่ความรู้ และ จัดการอบรมความรู้ความเข้าใจของเจ้าหน้าที่ ให้ตระหนักในภัยร้ายและการร่วมมือในการปกป้องภัยร้ายประเภทต่างๆ ที่อาจเกิดขึ้น

ข้อ ๑๒. ส่งเสริมให้บุคลากรที่ดูแลและจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศได้รับการอบรมและมีความรู้ความสามารถผ่านเกณฑ์มาตรฐานที่ยอมรับ

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ เดือน มีนาคม พ.ศ. ๒๕๖๒

(นายภุชพงค์ โนดไธสง)
ผู้อำนวยการสำนักงานสถิติแห่งชาติ

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒

ด้วยข้อมูลสถิติและสารสนเทศสถิติของสำนักงานสถิติแห่งชาติ มีการจัดเก็บด้วยวิธีการทางอิเล็กทรอนิกส์ ถือเป็นทรัพย์สินสารสนเทศหลักขององค์กรที่ต้องมีวิธีการจัดการให้มีความปลอดภัย ถูกต้องและน่าเชื่อถือ และด้วยปัญหาภัยคุกคามด้านความมั่นคงปลอดภัยด้านสารสนเทศที่มีต่อระบบสารสนเทศขององค์กรมีแนวโน้มเพิ่มมากขึ้น มีหลายปัจจัยทั้งจากภายนอกและภายในซึ่งอาจสร้างความเสียหายต่อทรัพย์สินสารสนเทศและภาพพจน์ของสำนักงานสถิติแห่งชาติจนนำไปสู่การขาดความน่าเชื่อถือต่อผู้ใช้ข้อมูลสถิติและสารสนเทศสถิติ ประกอบกับมาตรา ๑๕ ในพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ ระบุไว้ว่าบรรดาข้อมูลเฉพาะบุคคลหรือเฉพาะรายที่ได้มา ต้องถือเป็นความลับโดยเคร่งครัด สำนักงานสถิติแห่งชาติจึงได้จัดทำแนวปฏิบัติให้สอดคล้องกับนโยบายเพื่อเป็นแนวทางในการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานให้มีประสิทธิภาพ

หมวดที่ ๑

การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

วัตถุประสงค์

เพื่อให้การจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศมีคุณสมบัติการรักษาความลับ (Confidentiality) ความครบถ้วน (Integrity) และการรักษาสภาพความพร้อมใช้งาน (Availability) การดำเนินการจึงต้องมีวงจรการบริหารแบบคุณภาพ (PDCA) กำกับการดำเนินงาน ประกอบด้วย การวางแผน (Plan) การปฏิบัติตามแผน (Do) การตรวจสอบ (Check) และ การปรับปรุงแก้ไข (Act)

แนวทางปฏิบัติ

๑. ให้มีการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยในกระบวนการสถิติพร้อมระบุวิธีการแบบปลอดภัยในกระบวนการสถิติ ทั้งกระบวนการที่สร้างคุณค่า และกระบวนการสนับสนุน เพื่อใช้เป็นกรอบการดำเนินงานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๒. การจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศต้องไม่ส่งผลกระทบต่อผู้รับบริการ

๓. ให้กำหนดกิจกรรมการบริหารระบบความมั่นคงปลอดภัย (Information Security Management System) เพื่อใช้เป็นกระบวนการการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

๑) กิจกรรมในการวางแผนมีข้อกำหนด ดังนี้

(๑) ให้จัดทำ ทบทวน ปรับปรุง นโยบาย แนวปฏิบัติตามข้อกำหนดในนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศ ๑๑ หมวด และสถาปัตยกรรมระบบความมั่นคงปลอดภัยอย่างสม่ำเสมอทุก ๒ ปี เพื่อให้สอดคล้องกับความต้องการของกระบวนการ

สถิติ สภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศที่เปลี่ยนแปลง และข้อบังคับของกฎหมาย

(๒) ให้วางแผนการปรับปรุงเทคโนโลยีด้านความมั่นคงปลอดภัยสารสนเทศ และกำหนดในแผนแม่บทเทคโนโลยีสารสนเทศสำนักงานสถิติแห่งชาติ

(๓) ให้วางแผนการประเมินผลด้วยตนเองอย่างสม่ำเสมอเพื่อติดตามความครบถ้วนการดำเนินงานในกระบวนการการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

๒) กิจกรรมการปฏิบัติตามแผนมีข้อกำหนด ดังนี้

(๑) ให้ประกาศให้ทุกภาคส่วนของสำนักงานสถิติแห่งชาติได้รับทราบถึง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ ๑๑ หมวด รวมทั้งระเบียบการใช้งานทรัพย์สินสารสนเทศ ให้ทราบทั่วกัน

(๒) ให้นำข้อกำหนดในแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ ๑๑ หมวด มาดำเนินงาน โดยให้มีการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นเป็นประจำวัน และการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ

(๓) ให้รายงานให้ผู้บริหารได้รับทราบเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศขึ้นในสำนักงานสถิติแห่งชาติ

(๔) ให้เผยแพร่ข้อมูล และให้ความรู้กับบุคลากรให้รู้ทันภัยร้ายและตระหนักในความมั่นคงปลอดภัยด้านสารสนเทศเป็นประจำอย่างสม่ำเสมอ

(๕) ให้ประสานความร่วมมือกับหน่วยงานภายนอกทั้งในและต่างประเทศเพื่อรู้เท่าทันในภัยคุกคามบนระบบเครือข่ายที่อาจเกิดขึ้น

๓) กิจกรรมการตรวจสอบมีข้อกำหนด ดังนี้

(๑) ให้ประเมินความเสี่ยงและจัดการกับความเสี่ยงที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญเป็นประจำอย่างสม่ำเสมอ โดยมีขั้นตอน การระบุปัจจัยที่มีผลทำให้เกิดความเสี่ยง และการระบุความเสี่ยงที่มีโอกาสเกิดขึ้น (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการบริหารจัดการกับความเสี่ยง (Risk Management)

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

(๓) ให้ทดสอบแผนการจัดการเหตุการณ์ที่ไม่คาดฝันเป็นประจำอย่างสม่ำเสมอ

(๔) ให้ตรวจสอบพฤติกรรมการใช้งานของผู้ใช้เป็นประจำสม่ำเสมอและแจ้งเตือนให้รับทราบ และควบคุมการใช้งานที่สร้างความเสียหายต่อผู้ใช้ในการปฏิบัติราชการและการให้บริการต่อผู้รับบริการ

๔) การปรับปรุงแก้ไขมีข้อกำหนด ดังนี้

(๑) ให้มีการตรวจสอบและประเมินระบบความมั่นคงปลอดภัยด้านสารสนเทศเป็นประจำอย่างสม่ำเสมอและให้นำผลการตรวจสอบและการประเมินมาใช้ในกิจกรรมวางแผนเพื่อปรับปรุงระบบความมั่นคงปลอดภัยด้านสารสนเทศต่อไป

(๒) ให้ทบทวนและวิเคราะห์ช่องว่างการบริหารระบบความมั่นคงปลอดภัย (Gap Analysis)

หมวดที่ ๒
โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร

วัตถุประสงค์

เพื่อกำหนดผู้รับผิดชอบในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศและการดำเนินงานในกิจกรรมที่เกี่ยวเนื่อง ซึ่งประกอบด้วยผู้รับผิดชอบหลักที่เป็นเจ้าหน้าที่ของสำนักงานสถิติแห่งชาติ และผู้สนับสนุนจากภายนอก

แนวทางปฏิบัติ

๑. กำหนดให้ผู้อำนวยการสำนักงานสถิติแห่งชาติ เป็นผู้รับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ให้คณะกรรมการด้านความมั่นคงปลอดภัยด้านสารสนเทศ หรือคณะกรรมการเทคโนโลยีสารสนเทศ ทำหน้าที่ในการทบทวน ปรับปรุง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๓. ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทำหน้าที่ในการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ และกำหนดสถาปัตยกรรมระบบความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับภารกิจของสำนักงานสถิติแห่งชาติ

๔. ให้สำนักงานสถิติจังหวัดทำหน้าที่ในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติจังหวัดให้สอดคล้องกับภารกิจของสำนักงานสถิติจังหวัดใน ๖ หมวด ประกอบด้วย

หมวดที่ ๓ การบริหารจัดการทรัพย์สินสารสนเทศ

หมวดที่ ๔ การสร้างความมั่นคงปลอดภัยด้านบุคลากร

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบงานคอมพิวเตอร์

หมวดที่ ๗ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ

หมวดที่ ๙ การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง

๕. ให้กลุ่มนิติการทำหน้าที่ประสานงานการดำเนินงานทางทางคดีหากมีการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือพระราชบัญญัติอื่น

๖. ให้กลุ่มการเจ้าหน้าที่ทำหน้าที่ในการแจ้งรายชื่อบุคลากรของสำนักงานสถิติแห่งชาติที่ลาออกให้ศูนย์เทคโนโลยีและสารสนเทศรับทราบเป็นรายเดือน เพื่อใช้ในการยกเลิกสิทธิผู้ใช้งานออกจากระบบการใช้งาน

๗. ให้กลุ่มตรวจสอบภายในทำหน้าที่ในการบริหารและจัดการระบบการตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติ

๘. ให้มีการจัดทำข้อตกลงการปกปิดข้อมูลและห้ามเปิดเผยข้อมูลที่เป็นความลับสำหรับผู้สนับสนุนจากภายนอกที่เข้ามาดำเนินงานติดตั้ง งานบำรุงรักษา และงานที่มีความเกี่ยวเนื่องกับระบบความมั่นคงปลอดภัยด้านสารสนเทศ

๙. ให้ผู้รับผิดชอบในระบบแลกเปลี่ยนข้อมูลจัดทำข้อตกลงการปกปิดข้อมูล การดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง สำหรับหน่วยงานภายนอกที่สำนักงานสถิติแห่งชาติได้นำไปติดตั้งตามกระทรวงต่างๆ

๑๐. ให้ผู้ดูแลระบบซึ่งประกอบด้วย ผู้ดูแลระบบสารสนเทศ ผู้ดูแลโปรแกรมประยุกต์ ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสำรองข้อมูล ทำหน้าที่ในการบริหารจัดการระบบตามหน้าที่ที่ได้รับมอบหมายและปฏิบัติตามข้อกำหนดในแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนงานที่เกี่ยวเนื่อง

๑๑. ให้มีคณะกรรมการประสานงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่ออำนวยการและประสานการดำเนินงานเมื่อเกิดภัยพิบัติในภาวะวิกฤต

๑๒. ให้มีคณะทำงานตอบสนองต่อภัยพิบัติด้านสารสนเทศ เพื่อจัดทำแผนสร้างความต่อเนื่องและสนับสนุนการกู้คืนระบบสารสนเทศให้กลับสู่ภาวะปกติ

๑๓. สำหรับในภารกิจที่ไม่ปรากฏผู้รับผิดชอบและหน้าที่ไว้เป็นการเฉพาะและมีเหตุต้องจัดการกับภารกิจนั้น ให้แต่งตั้งคณะทำงานเฉพาะขึ้นมาเพื่อดำเนินการแทน

๑๔. ให้ศูนย์/ สำนักงานเลขานุการกรม/กอง/สำนักงานสถิติจังหวัด นำแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศไปใช้ในการปฏิบัติงานประจำ

หมวดที่ ๓
การบริหารจัดการทรัพย์สินสารสนเทศ

วัตถุประสงค์

เพื่อจัดการทรัพย์สินสารสนเทศของสำนักงานสถิติแห่งชาติ ประกอบด้วย ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบความมั่นคงปลอดภัย ระบบงานคอมพิวเตอร์ เอกสาร ข้อมูลสารสนเทศ และทรัพย์สินอื่นๆ ให้มีความพร้อมต่อการใช้ในการปฏิบัติงานและการให้บริการ

แนวทางปฏิบัติ

๑. ให้จัดทำระเบียบการใช้งานทรัพย์สินสารสนเทศอย่างเป็นลายลักษณ์อักษรและประกาศให้ผู้ใช้งานได้รับทราบถึงวิธีการใช้งานที่ถูกต้อง ข้อห้าม และบทลงโทษหากมีการฝ่าฝืนหรือละเมิดการใช้งาน

๒. ให้จัดทำทะเบียนสินทรัพย์และปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอทุกปี โดยต้องมีข้อมูลดังนี้

๑) หมายเลขครุภัณฑ์

๒) ประเภทครุภัณฑ์

๓) ผู้ครอบครองหรือผู้ดูแล

๔) สถานที่ใช้งาน

๕) ระดับความสำคัญ

๖) มูลค่าการจัดหา

๗) วิธีการเก็บรักษา

๘) การควบคุมการใช้งาน

๓. ให้จัดการสินทรัพย์ เครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล ระบบความมั่นคงปลอดภัย ระบบงานคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้ทำข้อตกลงการใช้ทรัพย์สินสารสนเทศก่อนการใช้งานให้เป็นไปตามระเบียบการใช้งานทรัพย์สินสารสนเทศ

๒) ให้ทำระบบการยืม/คืน ทรัพย์สินสารสนเทศที่สำคัญในการปฏิบัติงานภายนอกเพื่อตรวจสอบและป้องกันความเสียหาย

๓) ให้มีการควบคุมการเคลื่อนย้ายสินทรัพย์ที่ต้องนำออกไปภายนอกและการนำทรัพย์สินจากภายนอกเข้ามาใช้งานภายในองค์กร

๔. ให้จัดการสินทรัพย์ 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 ข้อมูลและสารสนเทศสถิติ ในรูปข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดทำทะเบียนข้อมูลและเอกสารที่สำคัญที่ต้องมีชั้นความลับในการควบคุมและกำหนดใช้วิธีการจัดการและควบคุม ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๒) ให้มีการจำแนกทะเบียนเอกสารที่สำคัญดังต่อไปนี้

(๑) เปิดเผยต่อสาธารณะ เฉพาะสมาชิก หรือเฉพาะกลุ่ม

(๒) ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

(๓) ระดับชั้นการเข้าถึง

(๔) เวลาที่ได้เข้าถึง

(๕) ช่องทางการเข้าถึง

๓) ให้มีการจำแนกทะเบียนข้อมูลดังต่อไปนี้

(๑) ประเภทของข้อมูลสถิติ แบ่งเป็น ข้อมูลดิบ ข้อมูลระดับย่อย และข้อมูลเฉพาะบุคคล

(๒) ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

(๓) ระดับชั้นการเข้าถึง

(๔) เวลาที่ได้เข้าถึง

(๕) ช่องทางการเข้าถึง

๖. ให้บันทึกความเสียหายจากการใช้งานทรัพย์สินสารสนเทศลงในแบบบันทึกโดยมีข้อมูลดังต่อไปนี้

๑) วัน/เวลา

๒) หมายเลขครุภัณฑ์

๓) ความเสียหายที่เกิดขึ้น

๔) สาเหตุ

๕) ผลกระทบ

๗. ให้มีการจัดการการเข้าถึงตามระดับชั้นความลับดังต่อไปนี้

๑) ให้มีการลงทะเบียนผู้ใช้งานเพื่อควบคุมสิทธิ มีการจำกัดข้อมูลที่สำคัญ และฟังก์ชั่นของระบบได้แก่ สิทธิที่สามารถแก้ไขข้อมูล สิทธิการลบข้อมูล สิทธิการอ่านข้อมูลทั้งหมด สิทธิการส่งออกข้อมูล และสิทธิการอ่านข้อมูลเฉพาะสดมภ์ เป็นต้น

๒) ให้กำหนดรหัสผู้ใช้และรหัสผ่าน และมอบสิทธิการใช้ระบบงานตามลำดับชั้นของข้อมูลโดยมีการควบคุมด้วยเมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชั่นต่างๆ ของระบบงานที่สอดคล้องกับนโยบายการควบคุมการเข้าถึง

๓) กำหนดช่องทางการเข้าถึงข้อมูลที่มีชั้นความลับปานกลางในระบบอินทราเน็ตที่เป็นระบบปิดภายในตลอด ๒๔ ชั่วโมง สำหรับผู้ใช้งานภายใน

๔) กำหนดช่องทางการเข้าถึงข้อมูลที่มีชั้นความลับปานกลางในระบบเชื่อมโยงสื่อสารข้อมูลหน่วยงานภาครัฐตลอด ๒๔ ชั่วโมง สำหรับสำนักงานสถิติจังหวัด

๕) กำหนดช่องทางการเข้าถึงข้อมูลที่ไม่มีชั้นความลับผ่านระบบอินเตอร์เน็ตได้ตลอด ๒๔ ชั่วโมง สำหรับผู้ใช้ทั่วไปและผู้ใช้แบบสมาชิก

๖) ใช้ระบบการเข้ารหัสข้อมูลที่มีความสำคัญหรือมีชั้นความลับในระบบงานที่เป็นความลับ

หมวดที่ ๔
การสร้างความมั่นคงปลอดภัยด้านบุคลากร

วัตถุประสงค์

เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดจากบุคลากรเป็นสำคัญ โดยให้มีการแจ้งระเบียบการใช้งานทรัพย์สินสารสนเทศก่อนทำหน้าที่และการให้ความรู้และตระหนักถึงภัยร้ายเพื่อไม่ตกเป็นผู้กระทำความผิดสร้างความเสียหายให้เกิดกับองค์กรและผู้อื่นโดยขาดความระมัดระวัง รวมทั้งการยกเลิกสิทธิและเรียกคืนสินทรัพย์ที่ใช้งานในหน้าที่กลับคืนเมื่อพ้นหน้าที่ความรับผิดชอบ

แนวทางปฏิบัติ

๑. ให้มีการชี้แจงความรับผิดชอบ และการอบรมให้กับเจ้าหน้าที่ที่เข้าใหม่ของสำนักงานสถิติแห่งชาติ ให้สามารถใช้งานทรัพย์สินสารสนเทศได้อย่างปลอดภัย และรับทราบระเบียบการใช้งานทรัพย์สินสารสนเทศ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ให้มีการชี้แจงการรักษาความลับข้อมูลเฉพาะบุคคลหรือเฉพาะราย ในพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ มิให้ถูกเปิดเผยไม่ว่าด้วยวิธีการใดก็ตามให้กับเจ้าหน้าที่ที่เข้าใหม่ได้รับทราบ

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

๔. ให้มีการป้องกันการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลโดยมิชอบ โดยข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลของสำนักงานสถิติแห่งชาติที่ได้มาตามอำนาจหน้าที่ที่บัญญัติไว้ในพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ จะได้รับการคุ้มครองตามบทบัญญัติในมาตรา ๑๔ ถึงมาตรา ๑๖ หากผู้ใดฝ่าฝืนจะต้องได้รับโทษตามบทบัญญัติในมาตรา ๒๐ แห่งพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ และในการปฏิบัติงานจะต้องปฏิบัติตามระเบียบอื่นๆ ได้แก่ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ระเบียบสำนักงานสถิติแห่งชาติว่าด้วยการดำเนินการต่อเรื่องร้องเรียน พ.ศ. ๒๕๕๕ และระเบียบสำนักงานสถิติแห่งชาติว่าด้วยการใช้งานทรัพย์สินสารสนเทศ พ.ศ. ๒๕๕๗

๕. ให้มีการอบรมให้กับเจ้าหน้าที่ประจำให้มีองค์ความรู้และความตระหนักในด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่องเป็นประจำอย่างสม่ำเสมอ เพื่อมิให้ตกเป็นผู้กระทำความผิดตามกฎหมายหรือละเมิดระเบียบที่สำนักงานสถิติแห่งชาติประกาศใช้งาน

๖. ให้มีการทบทวนสิทธิของผู้ใช้ระบบสารสนเทศเป็นประจำทุกปี ดังต่อไปนี้

๑) ยกเลิกสิทธิของผู้ใช้งานระบบสารสนเทศ หรือบริการพื้นฐานทั้งหมด ในกรณีพ้นสภาพจากการเป็นเจ้าหน้าที่สำนักงานสถิติแห่งชาติ และมีการทบทวนสิทธิการใช้งานระบบสารสนเทศ ตามรายชื่อที่กลุ่มการเจ้าหน้าที่แจ้ง เมื่อมีการปรับเปลี่ยนหน้าที่หรือพ้นจากหน้าที่ความรับผิดชอบ

๒) เรียกคืนทรัพย์สินสารสนเทศทั้งหมด สำหรับบุคคลที่ไม่มีสิทธิการใช้งานได้แก่ เครื่องคอมพิวเตอร์ บัตรประจำตัว เป็นต้น

หมวดที่ ๕
การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อควบคุมความปลอดภัยด้านกายภาพและสิ่งแวดล้อมซึ่งอาจเกิดความเสียหายต่อทรัพย์สินสารสนเทศที่สำคัญ ในบริเวณที่มีทรัพย์สินสารสนเทศติดตั้งใช้งานอยู่ ได้แก่ ศูนย์คอมพิวเตอร์ ห้องฝึกอบรม โต๊ะทำงาน เพื่อป้องกันการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

แนวทางปฏิบัติ

๑. ให้ตรวจสอบและเฝ้าระวังศูนย์คอมพิวเตอร์ หรือ ห้องคอมพิวเตอร์ดังต่อไปนี้

๑) ให้จัดทำประกาศรักษาความมั่นคงปลอดภัยที่เป็นพื้นที่ควบคุมในการเข้าถึงและเฝ้าระวังศูนย์คอมพิวเตอร์

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

๓) ให้มีระบบเก็บบันทึกการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายหรือพื้นที่เฝ้าระวังจากบุคคลภายนอก โดยในบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้า-ออก

๔) ให้มีการตรวจสอบสภาพความสมบูรณ์ของระบบสายไฟฟ้าและอุปกรณ์ให้มีสภาพพร้อมใช้งานและไม่เป็นอันตรายต่อการเกิดเพลิงไหม้

๕) ให้ติดตั้งอุปกรณ์เตือนไฟไหม้ ได้แก่ เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

๖) ให้มีถังดับเพลิงเพื่อใช้สำหรับดับเพลิงในเบื้องต้น และต้องมีการตรวจสอบ อย่างสม่ำเสมอ

๒. ให้ตรวจสอบและเฝ้าระวังการใช้งานผู้เข้าร่วมประชุมจากภายนอกที่นำเครื่องคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายภายในองค์กรทั้งในแบบใช้สายและไร้สาย ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ที่ใช้ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์และทันสมัย

๒) ไม่มีการติดตั้งโปรแกรมตรวจจับรหัสผ่านหรือโปรแกรมประสงค์ร้าย

๓. ให้ตรวจสอบและเฝ้าระวังเครื่องคอมพิวเตอร์ในห้องอบรม ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์และทันสมัย

๒) ให้บันทึกความเสียหายที่เกิดขึ้นจากการใช้งานของผู้อบรม

๓) ให้จัดทำประกาศการใช้เครื่องคอมพิวเตอร์หรือซอฟต์แวร์สำหรับบุคคลภายนอกที่เข้ารับการฝึกอบรมในหลักสูตรต่างๆ

๔. ให้ตรวจสอบและเฝ้าระวังเครื่องคอมพิวเตอร์ในห้องบริการข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์และทันสมัย

๒) ให้บันทึกความเสียหายที่เกิดขึ้นจากการใช้บริการของผู้ใช้

๓) ให้มีการควบคุมสื่อเก็บข้อมูลภายนอกที่นำมาเชื่อมต่อกับเครื่องคอมพิวเตอร์

๔) ให้จัดทำประกาศการใช้เครื่องคอมพิวเตอร์หรือซอฟต์แวร์สำหรับบุคคลภายนอกที่เข้าใช้บริการข้อมูลและสารสนเทศ

๕. ให้ตรวจสอบและเฝ้าระวังพื้นที่ต้องห้าม ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเข้าถึงบุคคลภายนอกเข้าภายในด้วยระบบควบคุมและติดตั้งกล้องวงจรปิดในจุดที่สำคัญ

๒) ให้มีการตรวจสอบการทำงานของอุปกรณ์ในระบบกล้องวงจรปิดสามารถทำงานได้เป็นปกติและสามารถบันทึกภาพได้ตลอดเวลา

หมวดที่ ๖
การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบงานคอมพิวเตอร์

วัตถุประสงค์

เพื่อเป็นการวางแผนและการจัดการระบบสื่อสารและระบบคอมพิวเตอร์แม่ข่าย 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 กำหนดระดับคุณภาพของการให้บริการ ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีข้อกำหนดเกณฑ์คุณภาพการให้บริการ (SLA) จากผู้ให้บริการ

(๒) ให้จัดทำข้อตกลงระหว่างผู้ให้บริการระบบสื่อสารข้อมูลให้มีการจัดการช่องสัญญาณด้วยวิธีการแบบปลอดภัย และ ให้มีการจัดทำรายงานปริมาณการใช้งานช่องสัญญาณเป็นรายเดือน

๓. ให้จัดการความปลอดภัยบนระบบเครือข่าย ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเชื่อมต่ออุปกรณ์เข้ากับระบบเครือข่ายทั้งแบบใช้สายและไร้สาย

๒) ให้เก็บข้อมูลและรายละเอียดข้อกำหนดของการเชื่อมต่อและสำรองข้อมูลไว้ และมีแผนการกู้คืนหากระบบเครือข่ายไม่สามารถใช้งานได้

๓) ให้ตรวจสอบสแกนช่องโหว่ของระบบเครือข่าย เครื่องคอมพิวเตอร์ อุปกรณ์ความมั่นคงโปรแกรมประยุกต์ 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) ตรวจสอบกฎของการควบคุม (Firewall Policy) เป็นไปตามการจัดการระบบที่ดี

(๒) ควบคุมบริการเฉพาะที่กำหนดเพื่อป้องกันการใช้บริการที่ไม่อนุญาตใช้งาน ที่เป็นอันตรายต่อระบบเครือข่าย

(๓) การปรับเปลี่ยนกฎของการควบคุมต้องไม่ทำให้ระบบความมั่นคงปลอดภัยขององค์กรลดลงหรือมีความเสี่ยงต่อการสูญเสียบริการ

๗) ให้จัดการอุปกรณ์ควบคุมบริการ (Security Gateway) ตามข้อกำหนดดังต่อไปนี้

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

(๒) ให้มีระบบเฝ้าติดตามการใช้งานอินเทอร์เน็ต ตามข้อกำหนดดังต่อไปนี้

๒.๑ ติดตั้งระบบเฝ้าติดตามการแพร่ระบาดไวรัสบนอินเทอร์เน็ต (Web Gateway) เพื่อติดตามสถานการณ์การภัยร้ายของไวรัสบนอินเทอร์เน็ต

๒.๒ ติดตั้งระบบกรองเว็บที่เป็นอันตราย (URL Filtering) เพื่อควบคุมการเข้าถึงข้อมูลที่ไม่เหมาะสมและป้องกันการใช้โปรโตคอลที่สร้างความเสียหายต่อระบบเครือข่ายและ มีเนื้อหาไม่เหมาะสมและเป็นอันตรายต่อองค์กร

๒.๓ ตรวจสอบและติดตามพฤติกรรมการใช้งานที่ละเมิดต่อระเบียบการใช้งานทรัพย์สินสารสนเทศของสำนักงานสถิติแห่งชาติ

๘) ให้จัดเก็บข้อมูลเพื่อการตรวจสอบระบบเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ตั้งเวลาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ด้านความมั่นคงทุกเครื่อง โดยอิงกับเวลามาตรฐานกลางของโลก

(๒) จัดเก็บข้อมูลจราจรระบบเครือข่ายและโปรแกรมประยุกต์ที่ให้บริการ เพื่อการวิเคราะห์และตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยและเป็นไปตามกฎหมายที่กำหนด

๔. ให้มีการจัดการระบบงานคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดการระบบคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการตรวจสอบสภาพของตัวเครื่องและอุปกรณ์เป็นประจำวัน

(๒) ให้มีการตรวจสอบสภาพของระบบสนับสนุนห้องศูนย์คอมพิวเตอร์เป็นประจำวัน

(๓) ให้มีการเฝ้าติดตามการให้บริการเป็นประจำวัน

(๔) ให้มีการตรวจสอบค้นหาช่องโหว่ของระบบปฏิบัติการเป็นประจำเพื่อให้เท่าทันในภัยร้ายที่เกิดขึ้นบนระบบเครือข่าย

(๕) ให้มีการจัดการโปรแกรมประยุกต์ที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อกำหนด ดังต่อไปนี้

๕.๑ โปรแกรมประยุกต์บนเว็บที่ให้บริการบนระบบเครือข่ายอินเทอร์เน็ตต้องมีการตรวจสอบและให้เป็นไปตามมาตรฐาน OWASP หรือมาตรฐานสากลอื่นๆ

๕.๒ โปรแกรมประยุกต์ที่ใช้งานบนเว็บต้องใช้พอร์ตมาตรฐาน HTTP (๘๐) และ HTTPS (๔๔๓) เท่านั้น

๕.๓ ให้มีการควบคุมช่วงอายุการใช้งาน (Session) และ ช่วงเวลาในการเข้าถึงเพื่อป้องกันภัยร้ายจากโปรแกรม

๒) ให้มีการจัดการระบบคอมพิวเตอร์ลูกข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ให้จัดทำข้อกำหนดการติดตั้งโปรแกรมและข้อกำหนดการเชื่อมต่อ ที่ส่งผลเสียต่อระบบเครือข่ายขององค์กร

(๒) ให้มีการควบคุมโปรแกรมการติดตั้งของลูกข่ายเฉพาะที่ใช้ในการปฏิบัติงานและไม่ใช้เพื่อเป็นเครื่องให้บริการต่อผู้ใช้

๓) ให้มีการจัดการระบบป้องกันไวรัสเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามข้อกำหนดดังต่อไปนี้

(๑) ตรวจสอบความทันสมัยของฐานข้อมูลไวรัสคอมพิวเตอร์เป็นประจำสม่ำเสมอ

(๒) ติดตามเครื่องคอมพิวเตอร์ที่ขาดการปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์ให้ทันสมัย

(๓) ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้มีการทำงานเป็นปกติ

(๔) รายงานการติดไวรัสคอมพิวเตอร์ของเครื่องคอมพิวเตอร์ลูกข่าย พร้อมทั้งรายละเอียดข้อมูลของไวรัสคอมพิวเตอร์ที่แพร่กระจายในองค์กร

หมวดที่ ๗
การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงทรัพย์สินสารสนเทศขององค์กรให้กับผู้มีสิทธิใช้งานให้เป็นไปตามหน้าที่ความรับผิดชอบ เพื่อป้องกันความเสียหายที่เกิดขึ้นจากการใช้งานโดยขาดการควบคุม จนอาจสร้างความเสียหายต่อระบบสารสนเทศขององค์กรหรือกระทบต่อการปฏิบัติงานประจำวัน

แนวทางปฏิบัติ

๑. ให้มีการควบคุมการเข้าถึงทรัพย์สินสารสนเทศของผู้ใช้เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีแนวปฏิบัติในการควบคุมการเข้าถึงระบบคอมพิวเตอร์ การเข้าถึงระบบปฏิบัติการ การเข้าถึงระบบเครือข่าย การเข้าถึงคอมพิวเตอร์ลูกข่าย การเข้าถึงระบบสารสนเทศ การเข้าถึงโปรแกรมประยุกต์ การเข้าถึงระบบฐานข้อมูล การเข้าถึงไฟล์ข้อมูล และการเข้าถึงเอกสารและสื่อเก็บข้อมูล

๒) ให้มีการจัดทำทะเบียนควบคุมทรัพย์สินสารสนเทศที่สำคัญขององค์กร และมีการตรวจสอบสภาพและการมีอยู่ของทรัพย์สินสารสนเทศเหล่านั้นเป็นประจำทุกปี

๓) ให้มีการลงทะเบียนผู้ใช้งานภายในและผู้ใช้งานภายนอกแบบสมาชิกก่อนการใช้งานระบบสารสนเทศ

๒. ให้มีการจัดการสิทธิของผู้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการลงทะเบียนผู้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการลงทะเบียน โดยผู้ใช้งานต้องลงทะเบียนตามแบบที่ผู้จัดการระบบกำหนดและมีการลงนามรับทราบในเงื่อนไขพร้อมให้ผู้บังคับบัญชาลงนามรับรองการใช้งาน

(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) ให้ใช้วิธีการจัดการสิทธิการเข้าถึงเป็นไปตามข้อกำหนดดังต่อไปนี้

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

๓.๒ ใช้การควบคุมแบบรายบุคคล (Identity-Based) ควบคุมการเข้าถึงระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์

๓.๓ ให้มีการมอบสิทธิการใช้งานให้กับผู้ใช้งานเป็นรายบุคคล เป็นความลับ และป้องกันการปฏิเสธความรับผิดชอบของผู้ใช้งานได้

๓) ให้มีการทบทวนสิทธิการใช้งานผู้ใช้งานเป็นประจำทุกปีเป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้หน่วยงานการเจ้าหน้าที่ หรือผู้บังคับบัญชาแจ้งไปยังผู้จัดการระบบหากผู้ใช้งานลาออกหรือพ้นสภาพจากการเป็นเจ้าหน้าที่สำนักงานสถิติแห่งชาติ

(๒) ทบทวนสิทธิประจำปีการเข้าถึงทรัพย์สินสารสนเทศของผู้ใช้งานใน ๙ หมวดข้างต้น

(๓) ให้ยกเลิกสิทธิการใช้งานออกจากระบบทะเบียนและในระบบหากพบเงื่อนไขของผู้ใช้งานดังนี้

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

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

๕. การใช้งานรหัสผ่าน

๑) ผู้ใช้งานต้องเก็บรหัสผ่านเป็นความลับ และต้องไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบ

๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราวและเปลี่ยนรหัสผ่านที่ยากต่อการเดาของผู้อื่น

๓) ผู้ใช้งานต้องไม่พิมพ์รหัสผ่านขณะที่มีผู้อื่นเห็นการพิมพ์

๔) ผู้ใช้งานต้องไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ หรือ ไม่เก็บรักษารหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย

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, สัญลักษณ์, และตัวเลข ซึ่งง่ายในการจดจำแต่ยากในการเดาของคนอื่น

๓) ไม่กำหนดรหัสผ่านที่เป็นคำอยู่ในพจนานุกรม หรือ ชื่อสถานที่

๗. ให้มีการควบคุมการป้องกันทรัพย์สินสารสนเทศในระหว่างที่ไม่ได้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

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) ให้ผู้ดูแลระบบเครื่องคอมพิวเตอร์เก็บรักษารหัสผ่านไว้เป็นความลับและให้เปลี่ยนรหัสผ่านใหม่ในทุกๆ ๒ เดือนและเป็นรหัสผ่านที่มีความเข้มแข็ง

๗) ให้มีการควบคุมการติดตั้งโปรแกรมอรรถประโยชน์ลงบนเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันการละเมิดลิขสิทธิ และป้องกันการหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย ที่อาจทำให้ระบบเกิดช่องโหว่ในการเข้าถึงตามกระบวนการบริหารจัดการเปลี่ยนแปลง และให้มีระบบการป้องกันโหลดไฟล์จากอินเทอร์เน็ตที่อาจทำความเสียหายต่อระบบความมั่นคงจากภายนอกด้วยโปรแกรมตรวจกรอง (Web Filtering)

๘) ให้มีการควบคุมระยะเวลาการใช้งานระบบปฏิบัติการเพื่อป้องกันการใช้งานจากผู้ประสงค์ร้าย

๙) ให้กำหนดสภาพแวดล้อมของระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) กำหนดเวลาของเครื่องให้เป็นมาตรฐานสากลเพื่อการตรวจสอบเหตุการณ์ด้านความมั่นคง

(๒) มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์และตรวจสอบความทันสมัยของฐานข้อมูลไวรัสคอมพิวเตอร์

๑๐. ให้มีการควบคุมการเข้าถึงระบบเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ตามข้อกำหนดดังต่อไปนี้

๑) มีการควบคุมอุปกรณ์เครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) อุปกรณ์เครือข่ายต้องติดตั้งอยู่ในตู้ มีการจัดเก็บ Mac Address และหมายเลขไอพี (IP Address) เพื่อใช้ในการระบุอุปกรณ์บนเครือข่าย

(๒) ให้มีการปิดพอร์ตและบริการบนระบบเครือข่ายที่ไม่มีความจำเป็นในการใช้งาน เพื่อป้องกันการนำอุปกรณ์เครือข่ายจากภายนอกมาเชื่อมต่อเพื่อกระจายสัญญาณ

(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) การเข้าถึงเครือข่ายแบบไร้สาย ตามข้อกำหนด ดังนี้

(๑) ให้มีการลงทะเบียนเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์พกพาในการใช้งานระบบเครือข่ายไร้สาย และมีการตรวจสอบและจัดเก็บ Mac Address ของเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์พกพาที่เข้าเชื่อมต่อระบบเครือข่ายเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย

(๒) ให้มีระบบการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่านโดยวิธีที่ปลอดภัยของผู้ใช้งานเพื่อป้องกันการปฏิเสธความรับผิดชอบ

(๓) ให้มีการแบ่งกลุ่มผู้ใช้เครือข่ายไร้สายออกเป็นแบบจำกัดระยะเวลาการใช้งานสำหรับบุคคลภายนอก (Tickets) และแบบบุคลากร (Employee) สำหรับเจ้าหน้าที่สำนักงานสถิติแห่งชาติ

๔) การเข้าถึงระบบเครือข่ายจากระยะไกล ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกสำนักงานสถิติแห่งชาติ สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงานสถิติแห่งชาติได้ ตามข้อกำหนด ดังนี้

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

(๒) ก่อนจะกำหนดสิทธิของผู้ใช้งานในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นกับสำนักงานสถิติแห่งชาติ และต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานเป็นลายลักษณ์อักษร

(๓) การเข้าสู่ระบบของสำนักงานสถิติแห่งชาติ ผู้ใช้งานจะต้องพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่าน ด้วยวิธีการเข้ารหัสเพื่อความปลอดภัย

(๔) อุปกรณ์ที่ใช้ในการเชื่อมต่อเข้าสู่ระบบต้องมีการติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็น ได้แก่ ซอฟต์แวร์ป้องกันไวรัส ไฟร์วอล เป็นต้น

(๕) ให้กำหนดสิทธิการเข้าถึงระบบสารสนเทศตามความจำเป็นในหน้าที่และความรับผิดชอบในการทำงาน

๕) การเข้าถึงเครือข่ายอินเทอร์เน็ต ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการลงทะเบียนการใช้บริการเครือข่ายอินเทอร์เน็ต และจดหมายอิเล็กทรอนิกส์ก่อนการใช้งาน และแนบคำแนะนำการใช้งานอย่างปลอดภัยให้ผู้ใช้งานได้รับทราบไปพร้อมกัน

(๒) ให้มีการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่านโดยวิธีที่ปลอดภัยของผู้ใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

(๓) ให้มีการจัดทำรายงานพฤติกรรมการใช้งานให้ผู้บริหารขององค์กรได้รับทราบอย่างสม่ำเสมอ

๖) ให้มีวิธีการแบบปลอดภัยในการแลกเปลี่ยนข้อมูลระหว่างเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) การโอนไฟล์ข้อมูลระหว่างเครื่องต้องใช้โปรโตคอลที่สามารถเข้ารหัสก่อนส่งผ่านข้อมูล

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

๗) การควบคุมการเชื่อมต่อทางเครือข่าย ทั้งแบบใช้สายและไร้สายเป็นตามข้อกำหนดดังต่อไปนี้

(๑) ผู้ดูและระบบมีการตรวจสอบและจำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อทางเครือข่ายตามนโยบายการเข้าถึง

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

(๓) ไม่เปลี่ยนชื่อเครื่องคอมพิวเตอร์ ไม่เปลี่ยนสายสัญญาณในการเชื่อมต่อที่ได้ระบุไว้ในข้อกำหนดของการเชื่อมต่อ ไม่เปลี่ยนหมายเลขไอพี (IP Address) ของเครือข่ายไปจากที่ผู้ดูแลเครือข่ายกำหนด

(๔) มีการควบคุมบริการบนเครือข่ายที่สามารถเชื่อมต่อได้เฉพาะที่อนุญาตเท่านั้น

๘) การควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศบนเครือข่าย เป็นไปตามนโยบายการควบคุมการเข้าถึง 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 โดยการกำหนด

สิทธิของผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓) ให้มีการควบคุมทางกายภาพของระบบ และไม่อนุญาตใช้งานผ่านระบบเครือข่ายระยะไกล

๔) ให้ผู้จัดการระบบสารสนเทศกำหนดสิทธิของผู้ใช้งานโปรแกรมประยุกต์ ตามบทบาทและหน้าที่ของผู้ใช้

๕) ให้ผู้จัดการระบบสารสนเทศตรวจสอบสิทธิของผู้ใช้งานในระบบงานเป็นประจำสม่ำเสมอ

๑๓. ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการลงทะเบียนโปรแกรมประยุกต์และตรวจสอบความครบถ้วนในแบบลงทะเบียนโปรแกรมประยุกต์

๒) ให้มีการควบคุมโปรแกรมประยุกต์ที่มีความสำคัญหรือมีความเสี่ยงสูงไว้ในองค์ประกอบที่มั่นคงปลอดภัย โดยแบ่งแยกด้วยอุปกรณ์ไฟร์วอล (Firewall) และจำกัดการเข้าถึงเฉพาะกลุ่มผู้ใช้ที่มีสิทธิเท่านั้น

๓) ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อการใช้งานระบบสารสนเทศหรือโปรแกรมประยุกต์ที่มีความเสี่ยงและความสำคัญสูง ดังนี้

(๑) กำหนดให้การเชื่อมต่อในแต่ละครั้งได้ไม่เกิน ๒ ชั่วโมง ต่อการพิสูจน์ตัวตนเข้าใช้งาน

(๒) ต้องตัดการเชื่อมต่อเมื่อใช้งานเกินระยะเวลาที่กำหนด

(๓) ต้องตรวจสอบยืนยันตัวตนใหม่ทุกครั้ง ทุกช่วงเวลาที่กำหนด

๔) ให้จำแนกโปรแกรมประยุกต์ที่ให้บริการผู้ใช้ภายนอก และโปรแกรมประยุกต์ที่ใช้งานภายในองค์กร

๕) ให้มีการเก็บรายละเอียดการเข้าใช้งานของผู้ใช้เพื่อใช้ในการตรวจสอบการใช้งานประจำปี

๑๔. ให้มีการควบคุมระบบฐานข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) ให้ผู้จัดการฐานข้อมูลกำหนดสิทธิและจัดทำทะเบียนผู้ใช้งานฐานข้อมูลและปรับปรุงให้ทันสมัย

๒) ให้ตรวจสอบช่องโหว่ของระบบฐานข้อมูลและดำเนินการปรับปรุงเป็นประจำสม่ำเสมอ

๓) ให้มีระบบการตรวจสอบการเข้าถึงระบบฐานข้อมูลที่มีความสำคัญต่อการปฏิบัติงาน เพื่อการอ้างอิงในภายหลัง โดยต้องมีรายละเอียดเกี่ยวกับรหัสผู้ใช้และวันเวลาที่เข้าถึง

๔) ห้ามใช้ชื่อผู้ใช้ที่สิทธิสูงสุด (DBA) ของระบบฐานข้อมูลใช้ในการเชื่อมต่อในโปรแกรมประยุกต์

๕) ให้มีการควบคุมไฟล์ที่กำหนดข้อมูลการเชื่อมต่อระบบฐานข้อมูลของโปรแกรมประยุกต์

๖) ให้มีการปกปิดข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลที่ได้จากกระบวนการสถิติ มิให้สามารถระบุได้ว่าข้อมูลนั้น ๆ เป็นของบุคคลใด หรือ นิติบุคคลใด หรือ คณะใด

๑๕. ให้มีการควบคุมไฟล์ข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเข้าถึงไฟล์ข้อมูลหรือแก้ไขไฟล์ข้อมูลที่ได้จากกระบวนงานที่มีสถานะเป็นไฟล์ข้อมูลดิบ ไฟล์ข้อมูลระดับย่อย ไฟล์ข้อมูลส่วนบุคคลและไฟล์ข้อมูลเฉพาะบุคคล เฉพาะผู้ที่ได้รับอนุญาตให้เข้าถึงเท่านั้น และให้มีการเข้ารหัสไฟล์ข้อมูลหากมีความจำเป็น

กรณีที่ให้บุคคลภายนอกเป็นผู้ดำเนินการจัดเก็บข้อมูลและมีการจัดเก็บข้อมูลไปไว้บนระบบคอมพิวเตอร์ที่มิใช่ระบบคอมพิวเตอร์สำนักงานสถิติแห่งชาติ จะต้องจัดทำเป็นข้อห้ามเปิดเผยข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลขึ้นไว้เป็นหลักฐานทั้งสองฝ่าย

๒) ให้มีการควบคุมไฟล์ข้อมูลที่มีเนื้อหาและมีระดับชั้นความลับให้สอดคล้องกับระเบียบสำนักงานสถิติแห่งชาติ ว่าด้วยแนวทางปฏิบัติเกี่ยวกับเอกสารที่มีข้อมูลที่เป็นความลับตามพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ พ.ศ. ๒๕๖๑

๓) ให้มีการควบคุมการแก้ไขข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลเท่าที่จำเป็น โดยเจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการแก้ไขข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลเท่านั้น และต้องมีการบันทึกรายละเอียดการปรับแก้ไขข้อมูลส่วนบุคคล ได้แก่

(๑) การได้รับอนุมัติจากผู้มีอำนาจ

(๒) การประมวลผล

(๓) การบันทึกการแก้ไขเปลี่ยนแปลง

(๔) การแจ้งผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงทราบ

๔) ให้มีการจัดทำทะเบียนข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลให้ทันสมัยอยู่เสมอ 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) ให้มีการควบคุมการแปลงข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคล โดยเจ้าหน้าที่ผู้มีหน้าที่ความรับผิดชอบในการแปลงข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลเข้าระบบอิเล็กทรอนิกส์เท่านั้น

๓) ให้มีการควบคุมสื่อเก็บข้อมูลภายนอกที่สามารถนำมาเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์ที่มีไฟล์ข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคล

๔) ให้มีการควบคุมการทำลายข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคล โดยเจ้าหน้าที่ที่ได้รับมอบหมาย ดังนี้

(๑) ข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลที่จัดเก็บในรูปแบบเอกสาร ให้ดำเนินการตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และระเบียบสำนักงานสถิติแห่งชาติ ว่าด้วยแนวทางปฏิบัติเกี่ยวกับเอกสารที่มีข้อมูลที่เป็นความลับตามพระราชบัญญัติสถิติ พ.ศ.๒๕๕๐ พ.ศ. ๒๕๖๑

(๒) ข้อมูลส่วนบุคคลที่จัดเก็บในรูปแบบสื่ออิเล็กทรอนิกส์ ให้มีการลบหรือทำลายข้อมูลแบบถาวรอย่างปลอดภัย โดยให้เป็นไปตามคู่มือแนวทางการทำลายข้อมูลและสื่ออิเล็กทรอนิกส์ ที่กำหนดขึ้น

๑๗. ให้มีการควบคุมการแลกเปลี่ยนข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลระหว่างหน่วยงาน โดยต้องบันทึกและจัดเก็บข้อมูลดังต่อไปนี้

๑) ข้อมูลการขออนุญาตเข้าใช้ระบบ

๒) ข้อมูลการเข้า-ออก ของผู้มีสิทธิในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

๓) รายละเอียดการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล

๔) รายละเอียดข้อมูลที่ใช้ในการจัดเก็บ

๑๘. ให้มีการควบคุมการให้สิทธิพิเศษในการเข้าถึงข้อมูลส่วนบุคคลสำหรับผู้บริหารระดับสูงของหน่วยงานเป็นกรณีเฉพาะ โดยให้กำหนดระยะเวลาในการเข้าถึงครั้งละไม่เกิน ๑ สัปดาห์ และหากมีความต้องการใช้งานต่อให้ขยายเวลาได้ครั้งละไม่เกิน ๑ สัปดาห์ และเมื่อครบกำหนดเวลาและไม่มีความประสงค์ใช้งานอีกต่อไป ให้ทำการยกเลิกสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลนั้น

๑๙. ให้มีการควบคุมการจัดเก็บข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลประเภทอื่นที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน ได้แก่ หมายเลขบัตรเดบิตหรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ ของบุคคลซึ่งอายุไม่เกินสิบแปดปี ด้วยวิธีการโดยเฉพาะและเหมาะสม

๒๐. ให้มีการควบคุมระบบที่ไวต่อการรบกวน ตามข้อกำหนดดังต่อไปนี้

๑) ระบบที่มีความไวต่อการถูกรบกวนที่ต้องควบคุมประกอบด้วย

(๑) ระบบบันทึกข้อมูลผ่านเว็บ

(๒) ระบบบริการข้อมูลระดับย่อย

(๓) ระบบแลกเปลี่ยนข้อมูล

๒) การกำหนดบริเวณที่ต้องมีการรักษาความปลอดภัย

(๑) กำหนดและจำแนกพื้นที่ใช้งานสารสนเทศตามสิทธิการเข้าถึงโดยแยกพื้นที่ออกเป็นห้องที่สามารถควบคุมการเข้า-ออกได้ ได้แก่ ห้องคอมพิวเตอร์ เป็นต้น

(๒) กำหนดให้มีผู้รับผิดชอบในการควบคุมบริเวณที่ต้องมีการรักษาความปลอดภัย

๓) การควบคุมการเข้า-ออกสถานที่และการเข้า-ออกห้องคอมพิวเตอร์

(๑) ให้มีระบบวงจรปิดเพื่อตรวจสอบหากเกิดปัญหา

(๒) ให้มีระบบตรวจสอบลายนิ้วมือการเข้าถึงห้องคอมพิวเตอร์

(๓) ให้จัดทำประกาศเพื่อควบคุมพื้นที่และข้อปฏิบัติการใช้ห้อง

(๔) ผู้ที่อยู่ในข่ายของการควบคุมประกอบด้วย ผู้ดูแลศูนย์คอมพิวเตอร์โดยตรง ผู้จัดการระบบ ผู้สนับสนุนจากภายนอก และบุคคลภายนอกที่ใช้พื้นที่

(๕) ให้มีการตรวจสอบการเข้า-ออกเป็นประจำทุกเดือน

๔) การกำหนดระดับการควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

(๑) ควบคุมในระดับสูงสุด ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการฐานข้อมูลและฐานข้อมูลทะเบียนกลาง (LDAP)

(๒) ควบคุมในระดับสูง ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการโปรแกรมประยุกต์ และ Middle Ware

(๓) ควบคุมในระดับปานกลาง ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการเว็บ

๕) การกำหนดระดับการควบคุมระบบคอมพิวเตอร์เครือข่าย

(๑) ควบคุมในระดับสูงสุด ประกอบด้วยระบบเครือข่ายแบบไร้สาย

(๒) ควบคุมในระดับสูง ประกอบด้วยระบบเครือข่ายภายในห้ามมีการเชื่อมต่อไปใช้ยังสถานที่อื่นที่ไม่ใช่พื้นที่ของหน่วยงาน

๖) การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) ควบคุมพอร์ตการเข้าถึงเฉพาะพอร์ตที่ใช้งานเท่านั้น

(๒) ควบคุมการเข้าถึงแบบ Remote Access เฉพาะเครื่องคอมพิวเตอร์ลูกข่ายที่ถูกกำหนดสิทธิการเข้าถึงเท่านั้น

๗) การพิสูจน์ตัวตนจากภายนอก

(๑) กำหนดรหัสผู้ใช้และรหัสผ่านเพื่อเข้าระบบงานและให้มีการพิสูจน์ตัวตนของผู้ใช้ข้อมูลในแต่ละระบบและแต่ละชั้นความลับ

(๒) กำหนดช่องทางการเข้าถึงเฉพาะวิธีการแบบปลอดภัยด้วยระบบ Virtual Private Network

หมวดที่ ๘
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

วัตถุประสงค์

เพื่อให้มีแผนการจัดการหากเกิดสถานการณ์อันไม่พึงประสงค์และไม่คาดคิดกับระบบสารสนเทศ ได้แก่ ภัยจากการโจมตีบนระบบเครือข่ายอินเทอร์เน็ต หรือภัยจากเพลิงไหม้ ภัยจากธรรมชาติ หรือภัยอื่นๆ ให้ระงับได้อย่างรวดเร็ว เพื่อให้เกิดผลกระทบต่อระบบสารสนเทศของสำนักงานสถิติแห่งชาติให้น้อยที่สุด

แนวทางปฏิบัติ

๑. ให้มีการวิเคราะห์ กำหนด และทบทวนเหตุการณ์ที่เป็นภัยคุกคามต่อทรัพย์สินสารสนเทศที่สำคัญ ซึ่งนำไปสู่ความเสียหายต่อระบบสารสนเทศ จนส่งผลกระทบต่อการดำเนินงานตามภารกิจขององค์กร โดยให้จัดทำแผนการจัดการเหตุการณ์ภัยที่ไม่พึงประสงค์เป็นไปตามลำดับความสำคัญและความน่าจะเป็นที่จะเกิดขึ้น

๒. ในจัดทำแผนจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ 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. ให้มีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะผิดปกติผ่านระบบเครือข่าย และรายงานจุดอ่อน ช่องโหว่ที่ตรวจพบโดยเร่งด่วน โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

๑) ความพยายามในการบุกรุกผ่านระบบเครือข่าย

๒) การใช้งานในลักษณะผิดปกติ

๓) การใช้งานที่มีการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๔. ให้มีการซ้อมแผนและฝึกอบรมเผชิญเหตุสำหรับแผนป้องกันไฟไหม้เป็นประจำทุกปีหรือในความถี่ที่เหมาะสม และนำมาปรับปรุงการดำเนินงานอย่างต่อเนื่อง

หมวดที่ ๙
การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง

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 หรือวิธีปฏิบัติในการสำรองข้อมูลโดยต้องมีองค์ประกอบตามข้อกำหนดดังต่อไปนี้

(๑) ข้อมูลที่ต้องสำรอง

(๒) ความถี่ในการสำรอง

(๓) ประเภทสื่อบันทึก (Media)

(๔) จำนวนที่ต้องสำรอง (Copy)

(๕) ขั้นตอนและวิธีการสำรองโดยละเอียด

(๖) สถานที่และวิธีการเก็บรักษาสื่อสำรองให้ปลอดภัย

(๗) การเฝ้าติดตามตรวจสอบผลการสำรองข้อมูล

๓) ให้มีการบันทึกการปฏิบัติงาน (Log Book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าว พร้อมทั้งรายงานอย่างสม่ำเสมอ

(๑) ให้มีการติดฉลากที่มีรายละเอียดเกี่ยวกับข้อมูลในสื่อบันทึกไว้บนสื่อบันทึกข้อมูลสำรองไว้ให้ชัดเจน เพื่อให้สามารถค้นหาข้อมูลได้โดยเร็วและเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

(๒) ให้จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่จัดเก็บดังกล่าวต้องให้มีระบบควบคุมการเข้า-ออก และระบบป้องกันความเสียหายของข้อมูลด้วย

(๓) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย อาทิ การเก็บอุปกรณ์และซอฟต์แวร์ ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกไว้

๓. ให้มีระบบทดสอบการกู้คืนข้อมูล เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดเตรียมเครื่องคอมพิวเตอร์แม่ข่ายเพื่อใช้ในการทดสอบการกู้คืนข้อมูลที่สำคัญ

๒) ให้ทดสอบการกู้คืนข้อมูลที่สำรองอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าข้อมูลรวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้ ตลอดจนขั้นตอนและวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

หมวดที่ ๑๐
การจัดหา การพัฒนา และการบำรุงรักษา

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) ให้ใช้วิธีการในการพัฒนาชุดคำสั่ง ตามมาตรฐาน OWASP หรือมาตรฐาน CWE TOP ๒๕ ที่มีกระบวนการควบคุมการนำเข้าข้อมูล การแสดงผล การควบคุมการประมวลผลเป็นอย่างน้อย

(๒) ให้มีการทดสอบการสแกนหาช่องโหว่ของโปรแกรมประยุกต์ และหากพบช่องโหว่จะต้องดำเนินการปิดช่องโหว่ที่ปรากฏให้หมด

(๓) ให้ใช้วิธีการทางวิศวกรรมซอฟต์แวร์ในการพัฒนาโปรแกรมตามมาตรฐาน ISO/IEC ๒๙๑๑๐

(๔) กำหนดให้มีการจัดทำแผนงานและขั้นตอนการดำเนินงานที่เกี่ยวกับการพัฒนาระบบสารสนเทศ การติดตั้งระบบคอมพิวเตอร์และอุปกรณ์ การทดสอบระบบหลังการติดตั้ง และแผนการบริหารความเสี่ยง โดยจะต้องนำเสนอแผนฯ ทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้กับผู้ที่รับผิดชอบงานโครงการ

(๕) ให้มีเกณฑ์ในการตรวจรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่นๆ รวมทั้งต้องตรวจสอบและทดสอบระบบโดยละเอียด ก่อนที่จะตรวจรับและติดตั้งใช้งานจริง

๒) ให้มีข้อกำหนดการเปลี่ยนแปลงแก้ไขระบบระบบสารสนเทศ เป็นไปตามข้อกำหนดดังต่อไปนี้

(๒) ให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ระบบงานสารสนเทศหรือเปลี่ยนแปลงโครงสร้างฐานข้อมูล ตามแบบคำขอให้แก้ไข โดยจะต้องมาจากผู้มีสิทธิ

และต้องได้รับการอนุมัติจากผู้มีอำนาจ รวมถึงมีการบันทึกรายละเอียดการแก้ไขจากผู้สนับสนุนจากภายนอกทุกครั้ง

(๓) ให้เข้าถึงได้เฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ต้องมีการควบคุมหรือตรวจสอบอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

(๔) ให้มีมาตรการควบคุมป้องกันการรั่วไหลของสารสนเทศขององค์กร หากมีความจำเป็นต้องใช้ข้อมูลจริงในการทดสอบระบบ จะต้องเป็นข้อมูลเฉพาะบางส่วน หรือข้อมูลที่ไม่สำคัญ และจะต้องได้รับอนุมัติจากผู้ที่รับผิดชอบแล้วเท่านั้น

๒. ให้มีมาตรการควบคุมผู้สนับสนุนจากภายนอก ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการกำหนดเกณฑ์การคัดเลือกผู้สนับสนุนจากภายนอกที่มีคุณภาพ มีขั้นตอนการปฏิบัติงานที่ดีเป็นที่เชื่อถือ

๒) ให้มีการกำหนดเกณฑ์การตรวจสอบประวัติพนักงานจ้างบำรุงรักษา พัฒนาระบบงาน

๓) ให้ผู้สนับสนุนจากภายนอกที่จะเข้ามาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์จะต้องขอความเห็นชอบจากผู้รับผิดชอบหรือผู้ดูแลระบบก่อนทุกครั้ง และการดำเนินงานทุกครั้งจะต้องอยู่ในความดูแลของผู้รับผิดชอบหรือผู้ดูแลระบบ

๔) ผู้สนับสนุนจากภายนอกจะได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ลูกข่ายเฉพาะที่อนุญาตให้เข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายเพื่อแก้ไขซอฟต์แวร์เท่านั้น

๕) ให้มีการลงนามในสัญญาการจ้างการพัฒนาระบบ การไม่เปิดเผยข้อมูลที่เป็นความลับ และงานที่มีความเกี่ยวเนื่องกับระบบความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

๖) กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อความคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ

๗) ให้ผู้สนับสนุนจากภายนอกจัดทำรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางการแก้ไข

๘) ผู้สนับสนุนจากภายนอกจะต้องปฏิบัติตามข้อกำหนดและระเบียบของสำนักงานสถิติแห่งชาติอย่างเคร่งครัด และเมื่อสิ้นสุดโครงการผู้สนับสนุนจากภายนอกจะถูกยกเลิกสิทธิทั้งหมดทันที

๙) กรณีการนำเครื่องคอมพิวเตอร์ออกไปซ่อมบำรุงภายนอกสำนักงานสถิติแห่งชาติและในเครื่องคอมพิวเตอร์นั้นมีข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคลให้มีการทำข้อตกลงว่าด้วยการไม่เปิดเผยข้อมูลส่วนบุคคลและข้อมูลเฉพาะบุคคล

๓. ให้มีการบำรุงรักษาระบบและเฝ้าติดตามคุณภาพการใช้งาน ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการบำรุงรักษาระบบสนับสนุนห้องศูนย์คอมพิวเตอร์ ประกอบด้วย ระบบสำรองไฟฟ้า ระบบดับเพลิง ระบบตรวจจับควันไฟ ระบบปรับอากาศ ระบบตรวจจับการรั่วซึมของน้ำ

ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย และระบบความมั่นคงปลอดภัย อย่างต่อเนื่องเป็นประจำทุกปี

๒) ให้ผู้ดูแลระบบทำการปรับปรุงคู่มือการจัดการระบบ คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องให้มีความถูกต้องและทันสมัยตลอดเวลา

๓) ให้เฝ้าติดตามการใช้งานของทรัพยากรในระบบและติดตามคุณภาพการให้บริการเป็นรายระบบ และหากพบให้ปรับปรุงให้มีค่าเป็นไปตามที่กำหนดไว้

๔. ให้มีมาตรการเข้ารหัสมาใช้ในการรับ/ส่งข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) การตรวจสอบสิทธิของผู้ใช้งานในหน้าเว็บ

๒) โปรแกรมประยุกต์และบริการบนเครือข่ายอินเทอร์เน็ตที่ต้องการความปลอดภัย

๓) การโอนไฟล์ข้อมูลระหว่างเครื่องที่มีข้อมูลที่ต้องปกปิด

๕. ให้มีมาตรการควบคุมไฟล์ข้อมูลที่ถูกเปลี่ยนแปลง ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดการและควบคุมสิทธิการเข้าถึงและแก้ไขไฟล์ข้อมูล

๒) ให้มีการวิเคราะห์ไฟล์ที่เปลี่ยนแปลงมีผลกระทบต่อการบริการอื่นหรือไม่

๓) ให้มีการสำรองไฟล์ข้อมูลที่จะถูกเปลี่ยนแปลงในทุกครั้งก่อนดำเนินการเปลี่ยนแปลงเพื่อใช้ในการกู้คืนในภายหลัง

๖. ให้มีการตรวจสอบช่องโหว่ (Vulnerability) ของระบบสารสนเทศเป็นประจำ ตามข้อกำหนดดังต่อไปนี้

๑) การตรวจสอบช่องโหว่ของระบบเครือข่าย ช่องโหว่ของระบบคอมพิวเตอร์แม่ข่าย และ ช่องโหว่ของโปรแกรมประยุกต์

๒) ให้มีการปรับแก้เพื่อปิดช่องโหว่ที่ตรวจพบและเป็นภัยที่อันตรายต่อระบบโดยเร็ว

หมวดที่ ๑๑
การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบายและข้อกำหนด

วัตถุประสงค์

เพื่อเป็นการตรวจสอบการนำนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งการใช้งานทรัพย์สินสารสนเทศของผู้ใช้งานเป็นไปตามระเบียบที่กำหนด โดยใช้กระบวนการตรวจสอบด้วยตนเองสำหรับผู้ปฏิบัติ การตรวจสอบจากหน่วยตรวจสอบภายในสำหรับผู้ใช้งาน และการตรวจสอบจากหน่วยตรวจสอบภายนอกในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

แนวทางปฏิบัติ

๑. ให้ผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยด้านสารสนเทศ ประเมินตนเองเพื่อนำมาสู่การปรับปรุงกระบวนงานให้มีความสมบูรณ์สูงสุดเป็นประจำทุกปี ตามข้อกำหนดดังนี้

๑) ประเมินตนเองด้วยแบบประเมินตนเองเพื่อวิเคราะห์ช่องว่าง (Gap)

๒) ประเมินตนเองด้วยการทดสอบการเจาะระบบ (Penetration Testing)

๒. ให้ผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยด้านสารสนเทศทำการประเมินตนเอง

๓. ให้หน่วยตรวจสอบภายในของสำนักงานสถิติแห่งชาติ ตรวจประเมินผู้ใช้งานมีการปฏิบัติตามระเบียบการใช้งานทรัพย์สินสารสนเทศและการนำแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศมาใช้ในการปฏิบัติงานเป็นประจำสม่ำเสมอในทุกๆ ๒ ปี

๔. ให้หน่วยตรวจสอบภายนอกตรวจประเมินระบบความมั่นคงปลอดภัยที่มีความซับซ้อนต้องใช้ความรู้ความเชี่ยวชาญเฉพาะเป็นประจำสม่ำเสมอในทุกๆ ๒ ปี

๕. ให้มีการตรวจสอบโดยหน่วยตรวจสอบภายในและหน่วยตรวจสอบภายนอกอย่างต่อเนื่องและให้นำผลการประเมินของหน่วยตรวจสอบมาใช้ในการวางแผนการปรับปรุงระบบความมั่นคงปลอดภัยด้านสารสนเทศในปีถัดไป