ความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ตาม

แผนการจัดการความรู้ ประจำปีงบประมาณ พ.ศ. 2555

ประเด็นยุทธศาสตร์ที่ 4

การเสริมสร้างองค์ความรู้ด้านเศรษฐกิจอุตสาหกรรมและพัฒนาองค์กร

โดย

คณะทำงานจัดทำความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มิถุนายน 2555

คำนำ

ด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่น ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ภาครัฐนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย โดยเห็นความสำคัญที่จะนำกฎหมาย ข้อบังคับต่าง ๆ มาบังคับใช้ ทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำ เพื่อช่วยให้ระบบสารสนเทศของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

ในส่วนของสำนักงานเศรษฐกิจอุตสาหกรรม โดยศูนย์สารสนเทศเศรษฐกิจอุตสาหกรรมได้ดำเนินการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศ โดยจัดทำแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ที่มีกำหนดการปรับปรุงเป็นประจำทุกปี ทำให้ระบบสารสนเทศของสำนักงานฯ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

เพื่อให้ระบบสารสนเทศของสำนักงานเศรษฐกิจอุตสาหกรรม มีความสอดคล้องตามกฎหมาย ข้อบังคับต่าง ๆ คณะทำงานจัดทำความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศ จึงได้ศึกษาแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ เพื่อประเมินความสอดคล้องตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2555 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเรื่องแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2555

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

หน้า

บทที่ 1

ทำความเข้าใจประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

1.1 นิยามศัพท์ตามกฎหมายฉบับนี้

(1) ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

(2) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(3) สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

(4) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(5) ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(6) เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์ อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(7) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(8) คำนิยาม (อื่น) – สามารถเพิ่มได้ตามความจำเป็น และสอดคล้องกับความต้องการขององค์กร

1.2 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

1.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(1) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(2) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(3) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(4) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติ ให้เป็นปัจจุบันอยู่เสมอ

1.4 ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อย ครอบคลุมตามข้อ 1.5 – 1.13

1.5 ข้อกำหนดในการเข้าถึงและควบคุมการใช้งานสารสนเทศ

ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(2) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

(3) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

1.6 ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

1.7 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(2) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(3) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(4) การบริหารจัดการรหัสผ่านสาหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

1.8 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยการล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(3) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk

and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(4) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544

1.9 การควบคุมการเข้าถึงเครือข่าย

ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(2) การยืนยันตัวบุคคลสาหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(3) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(4) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(5) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(6) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(7) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

1.10 การควบคุมการเข้าถึงระบบปฏิบัติการ

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(2) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(3) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(4) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(5) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(6) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

1.11 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(1) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้ กำหนดไว้

(2) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

(3) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(4) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ

แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

1.12 การจัดทำระบบสำรอง

หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

(1) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(2) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(3) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(4) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(5) สาหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

1.13 การกำหนดความรับผิดชอบที่ชัดเจน

หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

บทที่ 2
ประเมินความสอดคล้องกับระบบที่มีอยู่

ด้วยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 มีจุดมุ่งหมายให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ ควรจัดทำเอกสารอย่างน้อย 4 ฉบับ ดังนี้

1. นโยบายในการรักษาความมั่นคงปลอดภัย
2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
3. แผนสำรองระบบสารสนเทศ
4. แผนเตรียมความพร้อมกรณีฉุกเฉิน

ดังนั้น คณะทำงานจัดทำความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงได้ศึกษาข้อมูลสารสนเทศของ สศอ.จากแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ประจำปี 2555 เพื่อใช้ประกอบการประเมินความสอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

2.1 ประเมินความสอดคล้องกับระบบที่มีอยู่

การประเมินสถานะปัจจุบันของระบบสารสนเทศของสำนักงานเศรษฐกิจอุตสาหกรรม เปรียบเทียบกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 คณะทำงานจัดทำความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศฯ ได้ใช้แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานภาครัฐ[1]

---

[1]แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานภาครัฐ ภาคผนวก
ตามมาตรา 7 ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 โดยแบบประเมินดังกล่าว สามารถ Download จากเว็บไซต์

กระทรวง ICT http://www.mict.go.th และเว็บไซต์คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ http://www.etcommission.go.th

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานภาครัฐ เป็นการตรวจสอบการดำเนินงานของหน่วยงานว่ามีการดำเนินงานครบถ้วนตามข้อกำหนดในประกาศหรือไม่ โดยแบบประเมินฯ เป็นการ Check List การดำเนินงานตามประกาศ ดังนั้น เพื่อความเข้าใจวิธีการประเมินตามแบบประเมินดังกล่าว จึงได้แสดงคำอธิบายวิธีการประเมิน/การตรวจสอบรายละเอียดการดำเนินงานดังนี้

<u>ศึกษาวิธีการประเมินตามแบบประเมิน</u>

1. ให้ตรวจสอบเบื้องต้นก่อนว่า องค์กรได้มีการดำเนินการในแต่ละหัวข้อไปแล้วบ้างหรือไม่

2. หาก (คิดว่า) มี ให้บันทึก “ผ่าน” ในช่อง “หน่วยงานประเมินตนเอง” ไว้พลางก่อน

<u>ตรวจสอบรายละเอียดการดำเนินงาน</u>

1. ตรวจสอบว่า องค์กรมีการประกาศนโยบายหรือแนวปฏิบัติ” ในเรื่องที่ได้check ไว้แล้วหรือไม่

2. กรณี “มีการจัดทำประกาศใด ๆ” ไว้แล้ว ให้ตรวจสอบความครบถ้วนตามข้อกำหนดในประกาศ

3. บันทึกชื่อเอกสารอ้างอิงในแบบประเมิน หน้าแรก หัวข้อ “เอกสารประกอบการพิจารณา”

4. ใช้แบบประเมินเป็นเครื่องมือ Check List โดยระบุข้อมูลอ้างอิง ดังนี้

- ชื่อเอกสาร (ประกาศ/ข้อปฏิบัติ/คู่มือการทำงาน)
- หัวข้อที่เกี่ยวข้อง
- เลขหน้าของเอกสาร
- สรุปสาระสั้น ๆ พอเข้าใจ
- หากประกาศไม่ได้ใช้ข้อความตรงตามประกาศแต่มีการดำเนินงานที่สอดคล้องให้ระบุเหตุผล ประกอบการพิจารณา

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
1	**กำหนดนิยาม**		
	(1) ผู้ใช้งาน	ผ่าน	หน้าที่ 15 การกำหนดสิทธิผู้ใช้
	(2) สิทธิของผู้ใช้งาน	ผ่าน	หน้าที่ 15 การกำหนดสิทธิผู้ใช้, การกำหนดขอบเขตการเข้าถึงข้อมูล
	(3) สินทรัพย์	ไม่ผ่าน	
	(4) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	ไม่ผ่าน	
	(5) ความมั่นคงปลอดภัยด้านสารสนเทศ	ไม่ผ่าน	
	(6) เหตุการณ์ด้านความมั่นคงปลอดภัย	ไม่ผ่าน	
	(7) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	ไม่ผ่าน	
	(8) คำนิยามอื่น ๆ ตามความต้องการขององค์กร	ไม่ผ่าน	
2	**หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้**		
	(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	ผ่าน	หน้า 30 ข้อ 3.6 นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ หน้า 32 ข้อ 3.8 นโยบายความมั่นคงปลอดภัยของเครือข่าย หน้า 26 หมวด 6 ว่าด้วยซอฟต์แวร์และลิขสิทธิ์

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(2) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่าง ต่อเนื่อง	ผ่าน	หน้า 34 ข้อ 3.9 นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล หน้า 35 แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ
	(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ	ผ่าน	ตั้งคณะทำงานฯ เพื่อจัดทำแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ รายปี
3	**หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการดังต่อไปนี้**		
	(1) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	ผ่าน	หน้า 23 นโยบายความมั่นคงปลอดภัย
	(2) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้	ผ่าน	- ผู้บริหาร สศอ. ลงนามให้ความเห็นชอบแผนบริหารความเสี่ยงฯ ปี 2555 - เวียนแผนบริหารความเสี่ยงให้หน่วยงานภายใน สศอ. รับทราบ - จัดสัมมนาชี้แจงนโยบายความมั่นคงปลอดภัยสารสนเทศ สศอ.

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(3) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน	ผ่าน	หน้า 15 การกำหนดสิทธิ์เข้าใช้งานระบบฐานข้อมูลและระบบงานต่าง ๆ
	(4) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ	ผ่าน	ตั้งคณะทำงานฯ เพื่อจัดทำแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ รายปี
4	**ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหา อย่างน้อยครอบคลุมตามข้อ 5 - 15**	ผ่าน	หน้า 23 นโยบายความมั่นคงปลอดภัย
5	**ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อยดังนี้**		
	(1) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย	ผ่าน	หน้า 15 การกำหนดสิทธิ์เข้าใช้งานระบบฐานข้อมูลและระบบงานต่าง ๆ
	(2) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ	ผ่าน	หน้า 15 การกำหนดสิทธิ์เข้าใช้งานระบบฐานข้อมูลและระบบงานต่าง ๆ

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(3) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับ - ประเภทของข้อมูล - ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล - รวมทั้งระดับชั้นการเข้าถึง - เวลาที่ได้เข้าถึง - และช่องทางการเข้าถึง	ไม่ผ่าน	
6	**ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย**	ไม่ผ่าน	
7	**ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ผ่าน	หน้า 12 ข้อ 2) การจัดให้มีการอบรมให้ความรู้ด้านคอมพิวเตอร์

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม	ผ่าน	หน้า 12 ข้อ 2) การจัดให้มีการอบรมให้ความรู้ด้านคอมพิวเตอร์
	(1) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว	ผ่าน	หน้า 12 ข้อ 2) การควบคุมและการกำหนดสิทธิให้แก่ผู้ใช้งาน และ ข้อ 3) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่าน (password)
	(2) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง	ผ่าน	หน้า 15 การกำหนดสิทธิ์เข้าใช้งานระบบฐานข้อมูลและระบบงานต่าง ๆ
	(3) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม	ผ่าน	ข้อ 3) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่าน (password)

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(4) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้	ไม่ผ่าน	
8	**ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ไม่ผ่าน	หน้า 15 การกำหนดสิทธิ์เข้าใช้งานระบบฐานข้อมูลและระบบงานต่าง ๆ แต่ไม่มีการกำหนดหน้าที่รับผิดชอบเรื่อง - การเปิดเผย การล่วงรู้ - การลักลอบทำสำเนาข้อมูลสารสนเทศ - การลักขโมยอุปกรณ์ประมวลผลสารสนเทศ
	(1) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน
	(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(3) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน
	(4) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.2544	ไม่ผ่าน	
9	**ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**		
	(1) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน หน้า 23 นโยบายความมั่นคง

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษา

ความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทาง
อิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(2) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน
	(3) การระบุอุปกรณ์บนเครือข่าย ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน
	(4) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย	ผ่าน	หน้า 32 ข้อ 3.8 นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
	(5) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ	ผ่าน	หน้า 32 ข้อ 3.8 นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(6) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง	ผ่าน	หน้า 32 ข้อ 3.8 นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
	(7) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ	ผ่าน	หน้า 32 ข้อ 3.8 นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
10	**ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อยดังนี้**		
	(1) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(2) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน
	(3) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ	ผ่าน	หน้า 23 นโยบายความมั่นคง หมวด 1 ว่าด้วยการพิสูจน์ตัวตน
	(4) การใช้งานโปรแกรมอรรถประโยชน์ ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว	ผ่าน	หน้า 26 หมวด 6 ว่าด้วยซอฟต์แวร์และลิขสิทธิ์
	(5) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)	ผ่าน	หน้า 30 ข้อ 3.6 นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(6) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง	ผ่าน	หน้า 30 ข้อ 3.6 นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
11	**ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้**		
	(1) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ	ผ่าน	หน้า 30 ข้อ 3.6 นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
	(2) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่	ไม่ผ่าน	

	และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)		

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน / ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(3) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่	ไม่ผ่าน	
	(4) การปฏิบัติงานจากภายนอกสำนักงาน ต้องกำหนดข้อปฏิบัติแผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน	ไม่ผ่าน	
12	**หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรองตามแนวทางต่อไปนี้**		
	(1) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม	ผ่าน	หน้า 35 แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ
	(2) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ	ผ่าน	หน้า 35 แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ ไม่ ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(3) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์	ผ่าน	หน้า 35 แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ
	(4) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ (โปรดระบุความถี่)	ผ่าน	หน้า 35 แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ
	(5) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน	ผ่าน	หน้า 35 แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ
13	**หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง เป็นผู้รับผิดชอบต่อความเสี่ยงฯ**	ผ่าน	แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555

บทที่ 3

กำหนดแนวทางปฏิบัติให้สอดคล้องตามกฎหมาย

3.1 ความรู้ในการกำหนดนโยบายด้านความมั่นคงปลอดภัยของสารสนเทศ

ในบทที่ 2 การประเมินความสอดคล้องกับระบบที่มีอยู่ ได้แสดงวิธีการประเมินสถานะปัจจุบันของระบบสารสนเทศของสำนักงานเศรษฐกิจอุตสาหกรรม เปรียบเทียบกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 โดยใช้แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานภาครัฐ ตามมาตรา 7 ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่ง ผลการประเมินสามารถสรุปได้ ดังนี้

1. ไม่ผ่าน

<u>การตรวจสอบในเบื้องต้น</u>

สำนักงานเศรษฐกิจอุตสาหกรรม ไม่ได้มีการดำเนินการในหัวข้อนั้น ๆ

2. ผ่าน

<u>การตรวจสอบในเบื้องต้น</u>

สำนักงานเศรษฐกิจอุตสาหกรรม ได้มีการดำเนินการในหัวข้อนั้น ๆ

<u>ตรวจสอบรายละเอียดการดำเนินงาน</u>

สำนักงานเศรษฐกิจอุตสาหกรรม ได้มีการดำเนินการในหัวข้อนั้น ๆ <u>แต่ไม่มี</u>การประกาศนโยบายหรือแนวปฏิบัติในแต่ละหัวข้อ ทำให้ไม่สอดคล้องตามกฎหมาย

จากข้อสรุปดังกล่าวข้างต้นนั้น สามารถสรุปได้ว่า สำนักงานเศรษฐกิจอุตสาหกรรม ได้มีการดำเนินการในหัวข้อนั้น ๆ แต่ไม่ได้จัดทำนโยบายหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ จึงไม่สอดคล้องตามตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ดังนั้น คณะทำงานจัดทำความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศฯ จึงได้ศึกษา ค้นคว้าความรู้ในการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ที่สอดคล้องตามกฎหมาย ซึ่ง ได้แสดงรายละเอียด ดังนี้

แนวนโยบาย/และแนวปฏิบัติ (ประกาศของคณะกรรมการ)

1. กำหนดคำนิยาม อาจอ้างอิงตามประกาศ หรือ อธิบายขอบเขตที่เกี่ยวข้อง ดังนี้

(1) ผู้ใช้งาน - ผู้ใช้งานในองค์กร หมายถึงใครบ้าง

(2) สิทธิของผู้ใช้งาน - สิทธิในการใช้งานที่อะไรบ้าง ผู้ใช้งานในองค์กรมีสิทธิใดบ้าง

(3) สินทรัพย์ - สินทรัพย์ที่เกี่ยวข้องหมายรวมถึงอะไรบ้าง

(4) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ - การเข้าถึง หรือควบรวมการใช้งานสารสนเทศ หมายรวมถึงอะไรบ้าง

(5) ความมั่นคงปลอดภัยด้านสารสนเทศ - ความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรหมายรวมถึงอะไรบ้าง

(6) เหตุการณ์ด้านความมั่นคงปลอดภัย - เหตุการณ์ที่เกิดขึ้นแล้ว หรือ เหตุการณ์ที่เคยเกิดขึ้นจริงและมีการดำเนินงานแล้ว

(7) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด - สถานการณ์ที่อาจยังไม่เกิดขึ้นจริง หรือ คาดว่าจะเกิดขึ้น และมีมาตรการเตรียมรองรับเพื่อป้องกันและแก้ไขปัญหาที่จะเกิดขึ้น

(8) คำนิยาม (อื่น) - นิยามอื่น ๆ ที่องค์กรเห็นสมควร

2. หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ต้องระบุหลักฐานว่ามีการจัดทำนโยบายเพื่อควบคุมการเข้าถึงและการใช้งานสารสนเทศที่เป็นเป้าหมาย **<u>อย่างน้อย</u>** ต้องครอบคลุม 4 เรื่อง ดังนี้

(1.1) การเข้าถึงระบบสารสนเทศ

(1.2) การเข้าถึงระบบเครือข่าย

(1.3) การเข้าถึงระบบปฏิบัติการ

(1.4) การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นฯ

(2) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่าง ต่อเนื่อง

ต้องแสดงหลักฐานว่ามีการจัดทำเอกสารอย่างน้อย 2 เรื่อง คือ

(2.1) การสำรองข้อมูล เพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน

(2.2) การจัดทำแผนเตรียมความพร้อม โดยระบุเป็นนโยบายข้อหนึ่งขององค์กรด้วย

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ต้องแสดงหลักฐานว่ามีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยระบุความถี่ของการดำเนินงานเป็นนโยบายข้อหนึ่งขององค์กรด้วย

3. หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(1) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ต้องแสดงหลักฐานว่ามีการจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายในข้อ 2 ทุกข้อ

(2) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(2.1) ต้องแสดงหลักฐานว่าจะมีการประกาศนโยบายโดยวิธีใด

(2.2) หรือระบุเป็นข้อหนึ่งของนโยบายด้วยว่า ต้องประกาศ และประกาศโดยวิธีใดบ้าง

(3) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(3.1) ต้องระบุหน้าที่ความรับผิดชอบตามสายบังคับบัญชา ตั้งแต่ CIO จนถึงผู้ปฏิบัติ

(3.2) ระบุรายละเอียดในทางปฏิบัติ ที่เกี่ยวข้องกับ นโยบายข้อ 2 ในแนวปฏิบัติเฉพาะแต่ละด้านด้วย

(4) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ต้องระบุว่ามีระยะเวลาในการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอย่างไร มีความถี่อย่างไร และระบุเป็นนโยบายข้อหนึ่งขององค์กร

4. ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ 5 - 15

ระบุแนวปฏิบัติทั้งหมดที่เกี่ยวข้อง สามารถระบุ Scope กว้างได้

5. ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

ต้องแสดงหลักฐานว่ามีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลอย่างไร

<u>แนวปฏิบัติ</u>

(ก) จำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน

(ข) กำหนดกลุ่มผู้ใช้งาน

(ค) กำหนดสิทธิของกลุ่มผู้ใช้งาน

(2) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

ต้องแสดงหลักฐานว่ามีการกำหนดสิทธิอย่างไร ให้การอนุญาตอย่างไร หรือมีการมอบอำนาจในเรื่องใดบ้าง

<u>แนวปฏิบัติ</u>

(ก) กำหนดสิทธิของแต่ละกลุ่มที่เกี่ยวข้อง เช่น อ่านอย่างเดียว, สร้างข้อมูล, ป้อนข้อมูล, แก้ไข, อนุมัติ, ไม่มีสิทธิ์

(ข) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ

(3) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับ

(3.1) ประเภทของข้อมูล

(3.2) ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

(3.3) รวมทั้งระดับชั้นการเข้าถึง

(3.4) เวลาที่ได้เข้าถึง

(3.5) และช่องทางการเข้าถึง

<u>มาตรการ</u>

ต้องแสดงหลักฐานว่ามีการกำหนดในเรื่องอย่างไร

(ก) ประเภทของข้อมูล แบ่งอย่างไร

(ข) ลำดับความสำคัญ หรือลาดับชั้นความลับของข้อมูล มีอะไรบ้าง

(ค) ระดับชั้นการเข้าถึง มีอะไรบ้าง

(ง) เวลาที่ได้เข้าถึง มีช่วงใดบ้าง

(จ) และช่องทางการเข้าถึง มีกี่ช่องทาง อะไรบ้าง

<u>แนวปฏิบัติ</u>

(ก) จัดทำบัญชีทรัพย์สิน/ทะเบียนทรัพย์สิน

(ข) หลักการ “ตามความจำเป็นที่ต้องรู้”

(ค) แนวทางการปกป้องข้อมูล

(ง) การบังคับใช้เส้นทางเครือข่าย

(จ) แนวทางการเชื่อมโยงเครือข่าย

6. ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

<u>มาตรการ</u>

การจัดทำข้อปฏิบัติสำหรับการใช้งานสารสนเทศตามภารกิจ ให้คำนึงถึงเรื่องต่อไปนี้

(ก) การควบคุมการเข้าถึงสารสนเทศ

(ข) การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

<u>การอ้างอิงอย่างน้อยควรเกี่ยวข้องกับเรื่องต่อไปนี้</u>

(ก) แนวทางการควบคุมการเข้าถึงระบบสารสนเทศ

(ข) สิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศ

(ค) หลักการ “ตามความจำเป็นที่ต้องรู้”

7. ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

ต้องแสดงหลักฐานว่ามีการกำหนดในเรื่องต่อไป อย่างไร

(ก) บริหารจัดการการเข้าถึงของผู้ใช้งาน

(ข) การฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training)

(1) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

ต้องแสดงหลักฐานว่ามีการกำหนด หลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) หรือไม่อย่างไร

(2) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

<u>มาตรการ</u>

(ก) ต้องแสดงขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน

(ข) ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ

(ค) ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ

<u>แนวทางปฏิบัติ</u>

(ก) กำหนดขั้นตอนปฏิบัติ ครอบคลุมเรื่องต่อไปนี้

- ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
- จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้เท่าที่จำเป็น
- มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือความต้องการทางธุรกิจ
- จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย
- มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบงาน
- มีการเพิกถอนสิทธิ เมื่อมีการลาออก เปลี่ยนตำแหน่ง หรือย้าย
- มีการตรวจสอบและทบทวนบัญชีผู้ใช้งานอย่างสม่ำเสมอ

(ข) เจ้าของระบบงาน ทำหน้าที่อนุมัติการเข้าถึง

(ค) ต้องระวังการสมรู้ร่วมคิด เกี่ยวกับการให้สิทธิ

(ง) อนุญาตการใช้ระบบ เมื่อได้รับอนุมัติแล้ว

(3) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

<u>มาตรการ</u>

ต้องแสดงรายละเอียดว่ามีการควบคุมและจำกัดการใช้งานสิทธิ (การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ) อย่างไร

<u>แนวทางปฏิบัติ</u>

(ก) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(ข) มีการกำหนดระดับสิทธิในการเข้าถึงระบบงานที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

(ค) การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(ง) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

(4) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

<u>มาตรการ</u>

(ก) ต้องระบุเกี่ยวกับกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

<u>แนวทางปฏิบัติ</u>

(ก) ต้องมีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(ข) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(ค) หลีกเลี่ยงการใช้ e-mail ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(ง) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(จ) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์ที่ซื้อจากผู้ผลิต

(ฉ) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(ช) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ ตามระยะเวลาที่กำหนดไว้

<u>มาตรการ</u>

(ก) ต้องระบุเกี่ยวกับการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด

<u>แนวทางปฏิบัติ</u>

(ก) มีกระบวนการทบทวนสิทธิการเข้าถึงระบบงานของผู้ใช้งาน

(ข) ต้องทบทวนสิทธิ ตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลง เช่น เลื่อน ย้าย สิ้นสุดการจ้าง

(ค) ทบทวนสิทธิสาหรับผู้มีสิทธิในระดับสูง ด้วยความถี่มากกว่าผู้ใช้งานทั่วไป

(ง) บันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่ได้ทำการทบทวน เพื่อใช้ในการตรวจสอบภายหลัง

8. ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

ต้องแสดงหลักฐานในการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน ให้ครอบคลุมเรื่องดังนี้

(ก) ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(ข) การเปิดเผย การล่วงรู้

(ค) การลักลอบทำสำเนาข้อมูลสารสนเทศ

(ง) การลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

(1) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

มาตรการ

ต้องกำหนดวิธีปฏิบัติในการเลือกรหัสผ่านและการใช้งานรหัสผ่าน

แนวทางปฏิบัติ

(ก) ผู้ใช้งานรหัสผ่านต้องปฏิบัติ ดังนี้

- ตั้งรหัสที่ยากต่อการเดา
- ไม่เปิดเผยรหัสผ่าน
- จัดเก็บรหัสผ่านไว้ในสถานที่ปลอดภัย
- เปลี่ยนรหัสผ่านทันที เมื่อทราบว่า รหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้
- มีความยาวขั้นต่ำตามที่กำหนด
- ใช้เทคนิคส่วนตัวที่ง่ายต่อการจำ
- ไม่ตั้งจากคำในพจนานุกรม
- ไม่ตั้งจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน
- เปลี่ยนรหัสตามรอบระยะเวลาที่กำหนดไว้
- ผู้ดูแลระบบต้องเปลี่ยนรหัส ถี่กว่าผู้ใช้งานทั่วไป
- หลีกเลี่ยงการใช้รหัสผ่านเดิม
- เปลี่ยนรหัสผ่านชั่วคราวทันที ครั้งแรกที่ล็อกอินเข้าระบบ
- ไม่กำหนดให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่าน
- ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
- หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

มาตรการ

ผู้ใช้งานต้องตระหนักและเอาใจใส่ต่อการป้องกันอุปกรณ์ขององค์กรในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

แนวทางปฏิบัติ

(ก) กำหนดพนักงานป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

(ข) ต้องมีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(ค) ต้องสร้างความตระหนักให้พนักงานเข้าใจในมาตรการป้องกัน

(ง) พนักงานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(จ) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานมาช่วงระยะเวลาหนึ่ง และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(ฉ) ต้องล็อคอุปกรณ์คอมพิวเตอร์สำคัญเมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

(3) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

<u>มาตรการ</u>

ต้องมีการควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญ ให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่าง ๆ เช่น

(ก) การจัดการบริเวณล้อมรอบ

(ข) การควบคุมการเข้า-ออก

(ค) การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก

(ง) การวางอุปกรณ์

(จ) ระบบและอุปกรณ์สนับสนุนการทำงาน

<u>แนวทางปฏิบัติ</u>

(ก) ต้องกำหนดมาตรการป้องกันทรัพย์สินขององค์กร

(ข) การป้องกันต้องสอดคล้องกับแนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ

(ค) การป้องกันต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ

(ง) การป้องกันต้องสอดคล้องกับวัฒนธรรมองค์กร

(จ) กำหนดการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

<u>โดยมีขอบเขตการป้องกัน</u> ดังนี้

(ก) พนักงานทุกคนต้องปฏิบัติการป้องกันทรัพย์สิน

(ข) ออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

(ค) จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

(ง) ใช้กุญแจล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน

(จ) ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน

(ฉ) ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

(ช) ป้องกันให้ไม่ให้ผู้อื่นใช้อุปกรณ์ ต่อไปนี้ โดยไม่ได้รับอนุญาต

- กล้องดิจิตอล
- เครื่องสำเนาเอกสาร
- เครื่องสแกนเอกสาร

(ซ) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(4) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.2544

(4.1) ต้องแสดงหลักฐานว่ากำหนดเรื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวดอย่างไร มีอะไรบ้าง

(4.2) ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ สำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่มีความสำคัญยิ่งยวด

9. ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ที่เกี่ยวข้องกับการป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

(1) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

มาตรการ

(ก) ต้องแสดงหลักฐานว่ามีระบบสารสนเทศอะไรบ้างที่ต้องควบคุมการเข้าถึง

(ข) ต้องแสดงข้อปฏิบัติที่กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

แนวปฏิบัติ

ต้องระบุได้ว่า เครือข่ายใด หรือบริการใดที่อนุญาตให้มีการใช้งานได้บ้าง

(2) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

มาตรการ

ต้องแสดงข้อปฏิบัติ/กระบวนการที่ช่วยยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

แนวปฏิบัติ

(ก) ตรวจสอบผู้ใช้ทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล

(ข) ควบคุมการเชื่อมต่อผ่านสารโทรศัพท์สู่ระบบภายใน

(3) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

มาตรการ

ต้องแสดงวิธีการ/กระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง

แนวปฏิบัติ

(ก) กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

(ข) ควบคุมการใช้งานอย่างเหมาะสม

(ค) จำกัดผู้ใช้ที่สามารถเข้าใช้อุปกรณ์ได้

(4) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

มาตรการ

ต้องแสดงขั้นตอน/หลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ดังนี้

(ก) การเข้าถึงทางกายภาพ

(ข) การเข้าถึงทางเครือข่าย

แนวปฏิบัติ

(ก) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(ข) ต้องมีการควบคุมการใช้งานช่องทางดังกล่าวอย่างเหมาะสม

(ค) จำกัดผู้ใช้ที่สามารถเข้าใช้ช่องทางดังกล่าว

(5) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

มาตรการ

ต้องระบุข้อมูลเกี่ยวกับการแบ่งแยกเครือข่าย สำหรับกลุ่มต่าง ๆ

<u>แนวปฏิบัติ</u>

ระบุการแบ่งแยกเครือข่ายย่อย โดยพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคง และระดับความสำคัญของข้อมูลบนเครือข่าย เช่น

(ก) กลุ่มของบริการสารสนเทศ

(ข) กลุ่มผู้ใช้งาน

(ค) กลุ่มของระบบสารสนเทศ

(6) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

<u>มาตรการ</u>

ต้องแสดงขั้นตอน/หลักเกณฑ์ในการควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงในแต่ละกลุ่มที่เกี่ยวข้อง

<u>แนวปฏิบัติ</u>

(ก) มีการตรวจสอบการเชื่อมต่อเครือข่าย

(ข) จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

(ค) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(ง) มีระบบการตรวจรับผู้บุกรุกทั้งในระดับเครือข่าย และระดับแม่ข่าย

(จ) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

(7) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

<u>มาตรการ</u>

ต้องแสดงขั้นตอน/หลักเกณฑ์ในการจัดเส้นทางบนเครือข่าย ดังนี้

(ก) ให้มีการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ

(ข) ต้องสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

<u>แนวปฏิบัติ</u>

(ก) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

(ข) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(ค) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการเข้าใช้บริการเครือข่าย

๑๐. ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ที่เกี่ยวข้องกับการป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

(1) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

มาตรการ

ต้องแสดงขั้นตอนปฏิบัติในเรื่องดังนี้

(ก) การเข้าใช้งานที่มั่นคงปลอดภัย

(ข) การเข้าถึงระบบปฏิบัติการ

(ค) ต้องแสดงวิธีการยืนยันตัวตน

<u>แนวปฏิบัติ</u>

(ก) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(ข) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(ค) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(ง) แสดงข้อความเตือน “อนุญาตเฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิเข้าใช้งาน”

(จ) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

(2) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

<u>มาตรการ</u>

ต้องแสดงขั้นตอน/หลักเกณฑ์ ดังนี้

(ก) กำหนดข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน

(ข) กำหนดขั้นตอนในการยืนยันตัวตนของผู้ใช้งาน

<u>แนวปฏิบัติ</u>

(ก) ผู้ใช้ต้องมีรหัสผู้ใช้

(ข) การอนุญาตให้ใช้รหัสผู้ใช้ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

(ค) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card หรือ การตรวจสอบคุณลักษณะเฉพาะตัวของบุคคล (Biometric)

(3) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

<u>มาตรการ</u>

ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ ในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบหรือ อัตโนมัติ

<u>แนวปฏิบัติ</u>

หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้ที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(4) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

<u>มาตรการ</u>

ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ในการใช้งานโปรแกรมอรรถประโยชน์ โดยครอบคลุมเรื่องดังนี้

(ก) ป้องกันการละเมิด

(ข) หลีกเลี่ยงมาตรการความมั่นคงปลอดภัย

<u>แนวปฏิบัติ</u>

กำหนดมาตรการควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

(ก) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(ข) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(ค) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(ง) การเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(จ) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(5) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

มาตรการ

ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ ให้ยุติการใช้งานระบบสารสนเทศ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง

แนวปฏิบัติ

(ก) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(ข) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

(6) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

มาตรการ

ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

แนวปฏิบัติ

ต้องกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง โดย ต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

11. ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้ ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ที่เกี่ยวข้องกับการป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(1) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

มาตรการ

ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน หรือบุคลากร โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(2) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์

คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

(2.1) ต้องแสดงให้เห็นว่า หน่วยงานที่ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กรหรือไม่ อย่างไร

(2.2) ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ ในการแยกระบบดังกล่าวออกจากระบบอื่น ๆ

(2.3) ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ ในการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

(2.4) ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ ในการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(3) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ ในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(4) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ต้องแสดงข้อปฏิบัติ/แผนงาน และขั้นตอนปฏิบัติ สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

12. หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

ต้องแสดงเอกสารหลักฐาน ในการจัดทำระบบสำรองสาหรับระบบสารสนเทศที่กำหนดไว้

(1) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(1.1) ต้องแสดงขั้นตอน/หลักเกณฑ์ในการคัดเลือกระบบสารสนเทศ

(1.2) ต้องแสดงขั้นตอน/หลักเกณฑ์ในการจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

(2) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(2.1) ต้องแสดงแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(2.2) ต้องแสดงมาตรการ/กระบวนการปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(3) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องแสดงรายละเอียดการกำหนดหน้าที่และความรับผิดชอบของบุคลากรในเรื่องต่อไปนี้

(3.1) ระบบสารสนเทศ

(3.2) ระบบสำรอง

(3.3) การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(4) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ (โปรดระบุความถี่)

ต้องแสดงกระบวนการ/หลักเกณฑ์ในการทดสอบสภาพพร้อมใช้งานในเรื่องดังต่อไปนี้

(4.1) ระบบสารสนเทศ

(4.2) ระบบสำรอง

(4.3) ระบบแผนเตรียมพร้อมกรณีฉุกเฉิน

(5) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ต้องแสดงให้เห็นความถี่ของการปฏิบัติ ในการปฏิบัติแต่ละเรื่องดังนี้

(5.1) ระบบสารสนเทศ

(5.2) ระบบสำรอง

(5.3) ระบบแผนเตรียมพร้อมกรณีฉุกเฉิน

13. หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ต้องแสดงให้เห็นว่าถึงความรับผิดชอบโดยตรงของผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐ และเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

บทที่ 4

ทำความเข้าใจประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ของหน่วยงานของรัฐ พ.ศ. 2553

4.1 นิยามศัพท์ตามกฎหมายฉบับนี้

1. ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่นการศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

2. ผู้ควบคุมข้อมูลส่วนบุคคล หมายความว่า ผู้ซึ่งมีหน้าที่รับผิดชอบในการเก็บรวบรวม ควบคุมการใช้และการเปิดเผยข้อมูลส่วนบุคคลตามประกาศนี้

4.2 นโยบายการคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานของรัฐกำหนดนโยบายและข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ ดังต่อไปนี้

1. ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังนี้

(1) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

การจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้มีขอบเขตจำกัด และใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี

(2) คุณภาพของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานของรัฐตามกฎหมาย

(3) การระบุวัตถุประสงค์ในการเก็บรวบรวม

ให้บันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลในขณะที่มีการรวบรวมและจัดเก็บ รวมถึงการนำข้อมูลนั้นไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลให้จัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

(4) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้

(5) การรักษาความมั่นคงปลอดภัย

ให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ

(6) การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

ให้มีการเปิดเผยการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคลและจัดให้มีวิธีการที่สามารถตรวจดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคลวัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

(7) การมีส่วนร่วมของเจ้าของข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอภายในระยะเวลาอันสมควรตามวิธีการในรูปแบบ รวมถึงค่าใช้จ่าย (ถ้ามี) ตามสมควร

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูลผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ ตามกฎหมาย

ให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใด ๆ เกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน

(8) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามมาตรการที่กำหนดไว้ข้างต้นเพื่อให้การดำเนินงานตามแนวนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้

4.3 ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ

หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการและให้มีรายการอย่างน้อย ดังนี้

1. ข้อมูลเบื้องต้น ประกอบด้วย

(ก) ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด

(ข) รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์

(ค) ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ เช่นการ

แจ้งล่วงหน้าให้เจ้าของข้อมูลทราบก่อน 15 วัน โดยการส่งทางจดหมายอิเล็กทรอนิกส์หรือประกาศไว้ในหน้าแรกของเว็บไซต์ เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น

การขอความยินยอมจากเจ้าของข้อมูลนั้น ให้มีความชัดเจนว่าหน่วยงานของรัฐขอรับความยินยอมเพื่อวัตถุประสงค์ใด

4.4 การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐที่ทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์หรือผ่านรูปแบบของการกรอกข้อความทางกระดาษแล้วนำมาแปลงข้อความเข้าระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่น ให้แสดงรายละเอียดของการรวบรวมข้อมูลเป็นชนิด ประเภทรวมถึงข้อมูลที่จะไม่จัดเก็บและข้อมูลที่รวบรวมและจัดเก็บนั้นจะนำไปใช้ตามวัตถุประสงค์ใด โดยลักษณะหรือด้วยวิธีการที่ทำให้เจ้าของข้อมูลได้ทราบ ทั้งนี้ การรวบรวมและจัดเก็บข้อมูลนั้น ให้ทำเป็นประกาศหรือแจ้งรายละเอียดให้เจ้าของข้อมูลทราบ

ให้หน่วยงานของรัฐที่จัดบริการผ่านทางเว็บไซต์ แสดงรายละเอียดของการรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานนั้น รวมถึงการใช้ข้อมูลซึ่งอย่างน้อยต้องระบุว่าอยู่ในส่วนใดของเว็บไซต์หรือในเว็บเพจใดที่มีการรวบรวมและจัดเก็บข้อมูล และให้มีรายละเอียดอย่างแจ้งชัดถึงวิธีการในการรวบรวมและจัดเก็บข้อมูล เช่น การจัดเก็บโดยให้มีการลงทะเบียน หรือการกรอกแบบสอบถาม เป็นต้น

ให้หน่วยงานของรัฐรวบรวม จัดเก็บและใช้ข้อมูลส่วนบุคคลจัดทำรายละเอียด ดังต่อไปนี้

(ก) การติดต่อระหว่างหน่วยงานของรัฐ

ให้หน่วยงานของรัฐซึ่งจะติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์บอกกล่าวให้ผู้ใช้บริการทราบล่วงหน้า ทั้งนี้ ผู้ใช้บริการอาจแจ้งความประสงค์ให้ติดต่อโดยวิธีการอื่นได้

(ข) การใช้คุกกี้ (Cookies)

ให้หน่วยงานของรัฐระบุบนเว็บไซต์สำหรับการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคลว่าผู้ใช้บริการจะใช้คุกกี้เพื่อวัตถุประสงค์และประโยชน์ใด และให้สิทธิที่จะไม่รับการต่อเชื่อมคุกกี้ได้

(ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information)

ให้หน่วยงานของรัฐมีเว็บไซต์สำหรับการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร เช่น เพศ อายุ อาชีพ ที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ระบุถึงวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วย และให้ชี้แจงวัตถุประสงค์ของการใช้ข้อมูลดังกล่าว รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

(ง) บันทึกผู้เข้าชมเว็บ (Log Files)

ให้หน่วยงานของรัฐซึ่งจัดบริการเว็บไซต์ที่มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติ เช่น หมายเลขไอพี (IP Address) เว็บไซต์ที่เข้าออกก่อนและหลัง และประเภทของโปรแกรมบราวเซอร์ (Browser) ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้ ระบุวิธีการรวบรวมและจัดเก็บ

ข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล และให้ชี้แจงวัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

(จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกว่า “จะให้หรือไม่ให้” ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่น ในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์

4.5 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางจัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวโดยมิชอบ รวมถึงการป้องกันการกระทำใดที่จะมีผลทำให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งาน ซึ่งหน่วยงานของรัฐพึงดำเนินการ ดังนี้

(ก) สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ

(ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงานหรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด

(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง

(ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐหรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจนเช่น หมายเลขบัตรเดบิตหรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น

(จ) ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม

บทที่ 5
ประเมินความสอดคล้องกับระบบที่มีอยู่

ด้วยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 มีจุดมุ่งหมายให้หน่วยงานคำนึงถึงการรักษาความเป็นส่วนตัวหรือคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย ความน่าเชื่อถือและมีการคุ้มครองข้อมูลส่วนบุคคล

โดยทั่วไป หลักการที่ต้องคำนึงถึงเกี่ยวกับนโยบายคุ้มครองข้อมูลส่วนบุคคล มีดังนี้

1. การเปิดเผยข้อมูล

2. ลูกค้าหรือผู้ใช้บริการจะต้องมีทางเลือกในการให้ข้อมูล รวมถึงอนุญาตให้นำข้อมูลนั้นไปใช้งานได้ และยังสามารถป้องกันไม่ให้นำข้อมูลฯ ไปขายต่อ หรือเผยแพร่ข้อมูลในรูปแบบใดที่สามารถระบุตัวตนของลูกค้าหรือผู้ใช้บริการ

3. ลูกค้าหรือผู้ใช้บริการ จะต้องสามารถเข้าถึงข้อมูลส่วนตัวที่เก็บรักษา เพื่อแก้ไขข้อมูลให้ถูกต้องได้

4. เว็บไซต์ที่ให้บริการ จะต้องมีระบบรักษาความมั่นคงปลอดภัยอย่างเพียงพอ

ดังนั้น คณะทำงานจัดทำความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงได้ศึกษาข้อมูลสารสนเทศของ สศอ.จากแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ประจำปี 2555 เพื่อใช้ประกอบการประเมินความสอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

5.1 ประเมินความสอดคล้องกับระบบที่มีอยู่

การประเมินสถานะปัจจุบันของระบบสารสนเทศของสำนักงานเศรษฐกิจอุตสาหกรรม เปรียบเทียบกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 คณะทำงานจัดทำความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศฯ ได้ใช้แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ตามมาตรา ๗ ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 โดยแบบประเมินดังกล่าว สามารถ Download จากเว็บไซต์กระทรวง ICT http://www.mict.go.th และเว็บไซต์คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ http://www.etcommission.go.th

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ[2] เป็นการตรวจสอบการดำเนินงานของหน่วยงานว่ามีการ

ดำเนินงานครบถ้วนตามข้อกำหนดในประกาศหรือไม่ โดยแบบประเมินฯ เป็นการ Check List การดำเนินงานตามประกาศ ดังนั้น เพื่อความเข้าใจวิธีการประเมินตามแบบประเมินดังกล่าว จึงได้แสดงคำอธิบายวิธีการประเมิน/การตรวจสอบรายละเอียดการดำเนินงาน ดังนี้

<u>ศึกษาวิธีการประเมินตามแบบประเมิน</u>

1. ให้ตรวจสอบเบื้องต้นก่อนว่า องค์กรได้มีการดำเนินการในแต่ละหัวข้อไปแล้วบ้างหรือไม่

2. หาก (คิดว่า) มี ให้บันทึก “ผ่าน” ในช่อง “หน่วยงานประเมินตนเอง” ไว้พลางก่อน

<u>ตรวจสอบรายละเอียดการดำเนินงาน</u>

1. ตรวจสอบว่า องค์กรมีการประกาศนโยบายหรือแนวปฏิบัติ” ในเรื่องที่ได้check ไว้แล้วหรือไม่

2. กรณี “มีการจัดทำประกาศใด ๆ” ไว้แล้ว ให้ตรวจสอบความครบถ้วนตามข้อกำหนดในประกาศ

3. บันทึกชื่อเอกสารอ้างอิงในแบบประเมิน หน้าแรก หัวข้อ “เอกสารประกอบการพิจารณา”

4. ใช้แบบประเมินเป็นเครื่องมือ Check List โดยระบุข้อมูลอ้างอิง ดังนี้

- ชื่อเอกสาร (ประกาศ/ข้อปฏิบัติ/คู่มือการทำงาน)
- หัวข้อที่เกี่ยวข้อง
- เลขหน้าของเอกสาร
- สรุปสาระสั้น ๆ พอเข้าใจ
- หากประกาศไม่ได้ใช้ข้อความตรงตามประกาศแต่มีการดำเนินงานที่สอดคล้อง ให้ระบุเหตุผล ประกอบการพิจารณา

---

[2]แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานภาครัฐ ภาคผนวก

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
1	**ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังนี้**		
	(1) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด	ไม่ผ่าน	
	(2) คุณภาพของข้อมูลส่วนบุคคล	ไม่ผ่าน	
	(3) การระบุวัตถุประสงค์ในการเก็บรวบรวม	ไม่ผ่าน	
	(4) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้	ไม่ผ่าน	
	(5) การรักษาความมั่นคงปลอดภัย	ไม่ผ่าน	
	(6) การเปิดเผยเกี่ยวกับการดำ เนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล	ไม่ผ่าน	
	(7) การมีส่วนร่วมของเจ้าของข้อมูล	ไม่ผ่าน	
	(8) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล	ไม่ผ่าน	

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
ตามมาตรา 7 ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
2	**ให้หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ และให้มีรายการอย่างน้อยดังนี้**		
	(1) ข้อมูลเบื้องต้น ประกอบด้วย (ก) ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด (ข) รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์ (ค) ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้ง ตามวิธีการและภายในกำหนดเวลาที่ประกาศ	ไม่ผ่าน	

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(2) การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล ให้หน่วยงานของรัฐรวบรวม จัดเก็บและใช้ข้อมูลส่วนบุคคล จัดทำรายละเอียด ดังต่อไปนี้ (ก) การติดต่อระหว่างหน่วยงานของรัฐ (ข) การใช้คุกกี้ (Cookies) (ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (ง) บันทึกผู้เข้าชมเว็บไซต์ (Log Files) (จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกว่า “จะให้หรือไม่ให้” ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์	ไม่ผ่าน	
	(3) การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น	ไม่ผ่าน	
	(4) การรวมข้อมูลจากที่มาหลายๆ แห่ง	ไม่ผ่าน	
	(5) การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล	ไม่ผ่าน	

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(6) การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ	ไม่ผ่าน	
	(7) การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน	ไม่ผ่าน	
	(8) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งหน่วยงานของรัฐพึงดำเนินการ ดังนี้ (ก) สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่น คงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรม ในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ (ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด	ผ่าน	หน้า 12 ข้อ 2) การจัดให้มีการอบรมให้ความรู้ด้านคอมพิวเตอร์ หน้า 15 การกำหนดสิทธิ์ผู้ใช้

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง (ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน (จ) ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่น คงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม	ผ่าน	มีการทบทวนแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ เป็นประจำทุกปี หน้า 23 นโยบายความมั่นคงปลอดภัย

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของรัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
	(9) การติดต่อกับเว็บไซต์เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูล ติดต่อผ่านทางออนไลน์ด้วย ข้อมูลติดต่อที่หน่วยงานของรัฐควรจะระบุเอาไว้อย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้ (ก) ชื่อและที่อยู่ (ข) หมายเลขโทรศัพท์ (ค) หมายเลขโทรสาร (ง) ที่อยู่จดหมายอิเล็กทรอนิกส์	ไม่ผ่าน	
3	**ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้หลักการตามข้อ 1 และข้อ 2 สำหรับหน่วยงานของรัฐที่ได้รับทรัสต์มาร์คจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกทรัสต์มาร์ค (Trust Mark) ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองทรัสต์มาร์คดังกล่าวต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์**	ไม่ผ่าน	

แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง	
		ผ่าน/ไม่ผ่าน	อ้างอิง แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ สศอ. ปี 2555 หน้า... / ระบุเหตุผล (ถ้ามี)
4	ให้หน่วยงานของรัฐกำหนดชื่อเรียกนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ให้ชัดเจน และในกรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ซึ่งจะมีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย	ไม่ผ่าน	

บทที่ 6

กำหนดแนวทางปฏิบัติให้สอดคล้องตามกฎหมาย

6.1 ความรู้ในการกำหนดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ในบทที่ 5 การประเมินความสอดคล้องกับระบบที่มีอยู่ ได้แสดงวิธีการประเมินสถานะปัจจุบันของระบบสารสนเทศของสำนักงานเศรษฐกิจอุตสาหกรรม เปรียบเทียบกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 โดยใช้แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ตามมาตรา 7 ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่ง ผลการประเมินสามารถสรุปได้ ดังนี้

๑. ไม่ผ่าน

<u>การตรวจสอบในเบื้องต้น</u>

สำนักงานเศรษฐกิจอุตสาหกรรม ไม่ได้มีการดำเนินการในหัวข้อนั้น ๆ

๒. ผ่าน

<u>การตรวจสอบในเบื้องต้น</u>

สำนักงานเศรษฐกิจอุตสาหกรรม ได้มีการดำเนินการในหัวข้อนั้น ๆ

<u>ตรวจสอบรายละเอียดการดำเนินงาน</u>

สำนักงานเศรษฐกิจอุตสาหกรรม ได้มีการดำเนินการในหัวข้อนั้น ๆ <u>แต่ไม่มี</u>การประกาศนโยบายหรือแนวปฏิบัติในแต่ละหัวข้อ ทำให้ไม่สอดคล้องตามกฎหมาย

จากข้อสรุปดังกล่าวข้างต้นนั้น สามารถสรุปได้ว่า สำนักงานเศรษฐกิจอุตสาหกรรม ได้มีการดำเนินการในหัวข้อนั้น ๆ แต่ไม่ได้จัดทำนโยบายหรือแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ จึงไม่สอดคล้องตามตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ดังนั้น คณะทำงานจัดทำความรู้เรื่องความมั่นคงปลอดภัยของสารสนเทศฯ จึงได้ศึกษา ค้นคว้าความรู้ในการกำหนดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ที่สอดคล้องตามกฎหมาย ซึ่ง ได้แสดงรายละเอียด ดังนี้

รูปแบบของนโยบาย และแนวปฏิบัติ

<u>ข้อแนะนำในการเขียนนโยบาย</u>

1. ให้สั้น กระชับได้ใจความ และสามารถเข้าใจได้โดยง่าย เช่นเดียวกันกับองค์ประกอบอื่นๆ ของเว็บไซต์ของหน่วยงาน เพื่อให้สมาชิกทุกคนทั้งภายนอกและภายในหน่วยงานสามารถเข้าใจได้อย่างชัดเจน

2. องค์ประกอบแต่ละข้อที่ปรากฏ ควรมีความหมายเป็นไปตามหลักการของประกาศฯ

3. จากข้อ (2) นโยบายควรจะต้องกำหนดขึ้นจากข้อมูลที่เป็นจริง สอดคล้องกับวัตถุประสงค์ของหน่วยงาน ซึ่งจะต้องได้รับการกำหนดขึ้นก่อนที่จะมีการดำเนินงาน โดยการกำหนดกลวิธีในการปฏิบัติไว้กว้าง ๆ เพื่อให้ผู้ปฏิบัติสามารถพิจารณาตีความแล้วนำไปปฏิบัติตามความสามารถ สอดคล้องกับสภาวการณ์ในขณะนั้นๆ และเหมาะสมกับความเป็นจริง และนโยบายที่ดีควรจะต้องครอบคลุมไปถึงงานที่กำลังจะดำเนินการในระยะเวลาอันใกล้กับงานที่จะต้องดำเนินการในอนาคตมีความสอดคล้องและต่อเนื่องกัน

สรุปว่า นโยบายที่ดีจะช่วยให้สามารถปฏิบัติงานได้อย่างถูกทิศทาง ง่าย และมีประสิทธิภาพมากยิ่งขึ้น ช่วยให้ผู้ปฏิบัติสามารถกำหนดแนวปฏิบัติและตัดสินใจในภารกิจที่ตนเองรับผิดชอบได้ด้วยตนเอง

แนวปฏิบัติ ควรเขียนให้สอดคล้องกับนโยบายที่กำหนดไว้ ซึ่งจะต้องวิเคราะห์และกำหนดความสำคัญตามความเป็นไปได้ ตามความรับผิดชอบของทุกหน่วยงานย่อย (ถ้ามี) โดยมีความชัดเจนที่สามารถนำไปปฏิบัติตามได้

ประเด็นการพิจารณา การกำหนดสาระสำคัญในประกาศ ควรมีอะไรบ้าง

<u>ชื่อประกาศ</u>

สิ่งแรกที่ต้องบอกให้ผู้ใช้บริการ / ผู้ที่เกี่ยวข้องได้รับรู้ก่อน คือ นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนี้ เป็นของหน่วยงานไหน เว็บไซต์อะไร

<u>ข้อแนะนำ</u>

นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ <u>ชื่อหน่วยงาน</u>

<u>คำนำ วัตถุประสงค์ ขอบเขตเบื้องต้น</u>

เกริ่นถึงอำนาจหน้าที่ ภารกิจของหน่วยงานที่มีการให้บริการตามกฎหมาย ซึ่งอาจรวมถึงวัตถุประสงค์ ขอบเขตเบื้องต้นของนโยบายและแนวปฏิบัติ ด้วยก็ได้

<u>ข้อแนะนำ</u>

- <u>ชื่อหน่วยงาน</u> เป็นหน่วยงานที่มีภารกิจในด้าน….. และบริการ…… โดยมีการให้บริการตามภารกิจด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนั้นจึงมีนโยบายที่จะ-กล่าวถึงขอบเขตเบื้องต้น เช่น จัดเก็บ ใช้หรือเผยแพร่ข้อมูลส่วนบุคคลที่ได้มาจาก…-- การลงทะเบียนขอใช้บริการผ่านทางอิเล็กทรอนิกส์…จึงจัดทำ

นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการที่ติดต่อเข้ามายังเว็บไซต์ของ ชื่อหน่วยงาน เพื่อคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ....

- ชื่อหน่วยงาน ให้ความสำคัญถึงสิทธิ ข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ดังนั้นจึงได้จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์กับ ชื่อหน่วยงาน ทราบถึงรายละเอียด --กล่าวถึงขอบเขตเบื้องต้น เช่น การตรวจสอบถึงพฤติกรรมของการสืบค้นข้อมูลของผู้ใช้บริการ --

นโยบาย ระบุองค์ประกอบของนโยบายของหน่วยงานในเรื่องนี้ว่า มีกี่ส่วน มีองค์ประกอบเรื่องอะไรบ้าง (ตามหลักการทั้ง 8 ข้อ)

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

การจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้มีขอบเขตจำกัด และใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี

ข้อแนะนำ

ชื่อหน่วยงาน มีการจัดเก็บ รวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการฯ โดยนำข้อมูลไปใช้เพื่อวัตถุประสงค์ในการดำเนินงานของ ชื่อหน่วยงาน ตามที่กฎหมายกำหนด ในกรณีที่ ชื่อหน่วยงาน ประสงค์จะใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการเพื่อวัตถุประสงค์อื่น ชื่อหน่วยงาน จะแจ้งความประสงค์ให้ท่านทราบและขอความยินยอมจากท่าน และข้อมูลส่วนบุคคลที่ ชื่อหน่วยงาน ได้รับ จัดเก็บ รวบรวม เช่น .....

2. คุณภาพของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานของรัฐตามกฎหมาย

ข้อแนะนำ

ชื่อหน่วยงาน มีการรวบรวมและจัดเก็บข้อมูลส่วนบุคคลเพื่อประโยชน์ต่อการดำเนินงานตามภารกิจของ ชื่อหน่วยงาน โดยเน้นความครบถ้วน ถูกต้องและเป็นปัจจุบันของข้อมูล

3. การระบุวัตถุประสงค์ในการเก็บรวบรวม

ให้บันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล ในขณะที่มีการเก็บรวบรวมและจัดเก็บ รวมถึงการนำข้อมูลนั้นไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลให้จัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

ข้อแนะนำ

ข้อมูลส่วนบุคคลของผู้ใช้บริการ ชื่อหน่วยงาน จะถูกเก็บรวบรวมตามหลักเกณฑ์ที่ ชื่อหน่วยงาน กำหนด โดยเจ้าหน้าที่ที่เกี่ยวข้องจะมีการบันทึกวัตถุประสงค์ของการจัดเก็บ รวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการฯ ไว้อย่างชัดเจน และกำหนดให้มีการบันทึกการแก้ไขเพิ่มเติม หากมีการเปลี่ยนแปลงวัตถุประสงค์ในการจัดเก็บข้อมูล

4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นกรณีที่กฎหมายกำหนดให้กระทำได้

ข้อแนะนำ

ชื่อหน่วยงาน จะไม่เปิดเผยข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล ยกเว้นการเปิดเผยข้อมูลตามที่กฎหมายกำหนดให้กระทำได้หรือตามที่กำหนดไว้ในนโยบายเรื่องการเปิดเผยเกี่ยวกับการดำเนินงาน แนวปฏิบัติและแนวนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

5. การรักษาความมั่นคงปลอดภัย

ให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ

ข้อแนะนำ

ชื่อหน่วยงาน มีระบบรักษาความมั่นคงปลอดภัยที่มีมาตรฐานเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เพื่อป้องกันมิให้ข้อมูลสูญหาย ถูกนำไปใช้อย่างผิดๆ เปลี่ยนแปลงแก้ไขหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

ให้มีการเปิดเผยการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคลและจัดให้มีวิธีการที่สามารถตรวจสอบดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคล วัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

ข้อแนะนำ

ชื่อหน่วยงาน จะใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการเพียงเท่าที่จำเป็น เพื่อใช้ในการติดต่อการให้บริการ ประชาสัมพันธ์ หรืออื่นๆ ตามกิจการ กิจกรรมของ ชื่อหน่วยงาน เท่านั้น โดย ชื่อหน่วยงาน ได้มีการดำเนินการตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งหากผู้ใช้บริการมีข้อสงสัยในรายละเอียด สามารถติดต่อกับ ชื่อหน่วยงาน ได้ตามที่อยู่ที่ปรากฏในข้างท้ายประกาศฉบับนี้

7. การมีส่วนร่วมของเจ้าของข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอภายในระยะเวลาอันสมควรตามวิธีการในรูปแบบ รวมถึงค่าใช้จ่าย (ถ้ามี) ตามสมควรห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ ตามกฎหมายให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บความถูกต้อง หรือการกระทำใดๆ เกี่ยวกับเจ้าของข้อมูลไว้เป็นหลักฐาน

ข้อแนะนำ

กรณีที่ ชื่อหน่วยงาน ได้รับคำร้องขอจากเจ้าของข้อมูล ชื่อหน่วยงาน จะเปิดเผยรายละเอียดของข้อมูลส่วนบุคคลให้เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ ตามกฎหมาย ทราบภายในระยะเวลาที่เหมาะสม หลังจากที่ ชื่อหน่วยงาน ได้ตรวจสอบหลักฐานที่เชื่อถือได้ซึ่งเจ้าของข้อมูลได้แสดงต่อ ชื่อหน่วยงาน แล้วทั้งนี้ ในกรณีที่ ชื่อหน่วยงาน ปฏิเสธการให้ข้อมูลส่วนบุคคลใดๆ ชื่อหน่วยงาน จะจัดทำคำชี้แจงแจ้งให้เจ้าของข้อมูลทราบ และจะบันทึกคำคัดค้านเพื่อเก็บไว้เป็นหลักฐาน

8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามมาตรการที่กำหนดไว้ข้างต้นเพื่อให้การดำเนินงานตามแนวนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้

ข้อแนะนำ

ชื่อหน่วยงาน กำหนดให้เจ้าหน้าที่ พนักงานทุกคนที่จัดเก็บข้อมูลส่วนบุคคลต้องให้ความสำคัญและรับผิดชอบในการจัดเก็บและคุ้มครองข้อมูลส่วนบุคคลที่ตนจัดเก็บตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้

แนวปฏิบัติ ควรเขียนให้สอดคล้องกับนโยบายที่กำหนดไว้และสอดคล้องตามประกาศคณะกรรมการฯ ข้อ 3

1. ข้อมูลเบื้องต้น

ข้อมูลเบื้องต้น

- ชื่อนโยบายฯ
- รายละเอียดขอบเขตการบังคับใช้ วัตถุประสงค์

ต้องบอกว่า ข้อมูลส่วนบุคคลและการดำเนินการของบุคคลใดบ้าง ที่จะตกอยู่ในบังคับของนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ในประกาศนี้

ข้อแนะนำ

- แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ ชื่อหน่วยงาน
- ตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ชื่อหน่วยงาน ได้กำหนดขอบเขตเอาไว้ว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้ ใช้กับการดำเนินการใดๆ ของ ชื่อหน่วยงาน ต่อข้อมูลส่วนบุคคลที่ ชื่อหน่วยงาน เก็บรวบรวมหรือได้รับมาเท่านั้น ซึ่งข้อมูลดังกล่าว รวมถึงข้อมูลที่ผู้ใช้บริการใช้บริการของ ชื่อหน่วยงาน ด้วย ซึ่งข้อมูลส่วนบุคคลคือ ข้อมูลที่ระบุตัวบุคคลของผู้ใช้บริการได้เช่นเดียวกับชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์ของผู้ใช้บริการ ทั้งนี้ข้อมูลส่วนบุคคลในที่นี้ ไม่ได้รวมถึงข้อมูลที่สาธารณชน

สามารถเข้าถึงได้เป็นการทั่วไป และยังได้ระบุขอบเขตของนโยบายฯ ดังกล่าวเพิ่มเติมว่า ไม่ใช้กับแนวปฏิบัติต่อข้อมูลส่วนบุคคลของหน่วยงานอื่นที่ ชื่อหน่วยงาน มิได้เกี่ยวข้องหรือสามารถควบคุมได้ และไม่ใช้บังคับกับแนวปฏิบัติของบุคคลที่มิได้เป็นเจ้าหน้าที่หรือพนักงานของ ชื่อหน่วยงาน หรือที่ ชื่อหน่วยงาน ไม่มีอำนาจควบคุมดูแล

- การแจ้งให้ทราบถึงการเปลี่ยนแปลงของนโยบายการคุ้มครองข้อมูลส่วนบุคคลต้องระบุไว้ในประกาศให้ผู้ใช้บริการได้ทราบว่า หากจะมีการเปลี่ยนแปลงนโยบายฯ จะใช้วิธีการใดในการแจ้งให้ผู้ใช้บริการทราบ

- ในกรณีที่มีการเปลี่ยนแปลงนโยบายในการคุ้มครองข้อมูลส่วนบุคคล จะมีการประกาศแจ้งให้ทราบผ่านทางหน้าเว็บไซต์ของ ชื่อหน่วยงาน ล่วงหน้าเป็นเวลา 30 วัน

- ชื่อหน่วยงาน และเว็บไซต์อาจทำการปรับปรุงหรือแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ได้แจ้งให้ท่านทราบล่วงหน้า ทั้งนี้เพื่อความเหมาะสมและความมีประสิทธิภาพในการให้บริการ ดังนั้นจึงขอแนะนำให้ผู้ใช้บริการอ่านนโยบายการคุ้มครองข้อมูลส่วนบุคคลทุกครั้งที่ใช้บริการ

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ชื่อหน่วยงาน ใช้มาตั้งแต่วันที่ ….. และปรับปรุงล่าสุดเมื่อวันที่ …….

2. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

หน่วยงานจะต้องให้รายละเอียดว่า หน่วยงานเก็บรวบรวมข้อมูลอะไรบ้างผ่านทางเว็บไซต์ หรือผ่านการกรอกข้อความทางกระดาษแล้วนำมาแปลงเป็นข้อมูลอิเล็กทรอนิกส์ และข้อมูลที่ถูกเก็บรวบรวมมานั้น จะถูกใช้ไปอย่างไร โดยควรแจ้งให้ชัดถึงวิธีในการเก็บ เช่น เก็บโดยการลงทะเบียนผ่านทางเว็บไซต์ หรือการกรอกแบบฟอร์มต่างๆ เป็นต้น รายละเอียดดังนี้

- การติดต่อระหว่างหน่วยงานของรัฐ (การติดต่อจากทางเว็บไซต์)
- การใช้คุกกี้ (Cookies)
- การเก็บข้อมูลสถิติเกี่ยวกับประชากร (ข้อมูลพื้นฐานบุคคล)
- บันทึกเข้าออก (Log Files)
- ข้อมูลที่เก็บเป็นข้อมูลที่ต้องให้เลือกได้ว่า “จะให้หรือไม่ให้” ก็ได้

ก. การติดต่อระหว่างหน่วยงานของรัฐ

ถ้าหน่วยงานจะส่งการติดต่อใดๆ ไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ หน่วยงานจะต้องบอกให้ผู้ใช้บริการได้รู้ตัวก่อนล่วงหน้า โดยต้องบอกรายละเอียดว่า กรณีใดบ้างที่จะติดต่อไป เช่น ทางอีเมล์ โทรศัพท์ จดหมาย นอกจากนี้ หากหน่วยงานมีการใช้ข้อมูลร่วมกับหน่วยงาน/ บุคคลภายนอก และหน่วยงานหรือบุคคลภายนอกนั้นอาจจะติดต่อไปยังผู้ใช้บริการ กรณีนี้ก็ต้องระบุเอาไว้ด้วย

ข. การใช้คุกกี้ (Cookies)

หากเว็บไซต์มีการใช้คุกกี้ ก็ต้องระบุเอาไว้ด้วย และต้องบอกด้วยว่าคุกกี้ดังกล่าวเชื่อมโยง เก็บรวบรวมข้อมูลเกี่ยวกับข้อมูลส่วนบุคคลด้วยหรือไม่ก็

ค. การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information)

ในกรณีที่เว็บไซต์มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชาการ เช่น เพศ อายุ อาชีพ ต้องระบุการเก็บรวบรวมข้อมูลดังกล่าวไว้ในนโยบายด้วย และต้องบอกด้วยว่าเอาข้อมูลดังกล่าวไปใช้อย่างไร มีการให้บุคคลอื่นร่วมใช้ข้อมูลดังกล่าวด้วยหรือไม่

ง. บันทึกผู้เข้าชมเว็บ (Log Files)

ในกรณีที่เว็บไซต์มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติเช่น IP Address เว็บไซต์ที่เข้าออกก่อนและหลัง ประเภทของบราวเซอร์ ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลส่วนบุคคลได้ ระบุวิธีการจัดเก็บ และชี้แจงวัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

จ.ข้อมูลที่เก็บเป็นข้อมูลที่ต้องให้ หรือเลือกได้ว่าจะให้ หรือไม่ให้ก็ได้

ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกว่า “จะให้หรือไม่ให้” ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่พึงประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์

ข้อแนะนำ

- การเก็บรวบรวมข้อมูลส่วนบุคคลของ ชื่อหน่วยงาน ผ่านทางการลงทะเบียนหรือการกรอกแบบฟอร์มนั้น ข้อมูลที่จำเป็นต้องกรอกลงไปได้แก่ ชื่อ ชื่อสกุล หมายเลขประจำตัวประชาชน ที่อยู่ อีเมล์ หมายเลขโทรศัพท์ โดยข้อมูลเหล่านี้จำเป็นต่อการประมวลผลและการดำเนินงานตามภารกิจการให้บริการของ ชื่อหน่วยงาน ส่วนข้อมูลอื่นๆ นอกจากนี้ ผู้ใช้บริการมีสิทธิเลือกที่จะให้หรือไม่ให้ก็ได้ ซึ่งข้อมูลต่างๆ เหล่านี้ ชื่อหน่วยงาน จะใช้เพื่อปรับปรุงการให้บริการที่ดีขึ้นต่อไป

- ผู้ใช้บริการอาจได้รับการร้องขอให้แจ้งข้อมูลส่วนบุคคลในเวลาใดๆ ที่ติดต่อกับ ชื่อหน่วยงาน และ ชื่อหน่วยงาน อาจมีการใช้งานข้อมูลส่วนบุคคลนี้ในหน่วยงาน และใช้ข้อมูลส่วนบุคคลนี้สอดคล้องกับนโยบายในการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ รวมทั้งอาจผนวกข้อมูลส่วนบุคคลนี้เข้ากับข้อมูลอื่นๆ เพื่อการดำเนินงานของหน่วยงาน และข้อมูลที่ผนวกเขาด้วยกันนี้ จะถือว่าเป็นข้อมูลส่วนบุคคลตราบเท่าที่ยังคงผนวกเข้าด้วยกันอยู่

- ชื่อหน่วยงาน จัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการที่ส่งเรื่องร้องเรียน / ติดต่อ ทางเว็บไซต์ โดย ชื่อหน่วยงาน จะจัดเก็บรวบรวมข้อมูลดังกล่าวไว้ เช่น ชื่อผู้ร้องเรียน อีเมล์ เบอร์ติดต่อ

- จัดเก็บข้อมูลหมายเลขไอพี แอดเดรส ของผู้ใช้บริการทุกท่านที่เข้าเยี่ยมชมเว็บของ ชื่อหน่วยงาน เพื่อใช้เป็นข้อมูลอ้างอิงต่อไป

- ชื่อหน่วยงาน จะใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการเพียงเท่าที่จำเป็น เช่น ชื่อ ชื่อสกุล ที่อยู่ อีเมล์ เบอร์โทรศัพท์ เพื่อใช้ในการติดต่อการให้บริการ ประชาสัมพันธ์ หรือให้ข้อมูลข่าวสารของ ชื่อหน่วยงาน เท่านั้น

- ในกรณีที่ ชื่อหน่วยงาน ว่าจ้างให้หน่วยงานอื่นดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการ เช่น การจัดทำ แปลงเอกสารเป็นข้อมูลอิเล็กทรอนิกส์ การทำสำเนาเอกสาร การส่งพัสดุไปรษณีย์ การวิเคราะห์ข้อมูลเชิงสถิติ ในกิจการหรือกิจกรรมของ ชื่อหน่วยงาน ชื่อหน่วยงาน จะกำหนดให้หน่วยงานที่ได้ว่าจ้างให้ดำเนินการต่างๆ ข้างต้น เก็บรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคลของผู้ใช้บริการ และกำหนดข้อห้ามมิให้นำข้อมูลส่วนบุคคลไปใช้นอกเหนือจากกิจการหรือกิจกรรมของ ชื่อหน่วยงาน

- ชื่อหน่วยงาน ขอแนะนำให้ผู้ใช้บริการตรวจสอบนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเว็บไซต์อื่นที่เชื่อมโยงจากเว็บไซต์ของ ชื่อหน่วยงาน เพื่อจะได้ทราบและเข้าใจว่าเว็บไซต์ดังกล่าวเก็บรวบรวม ใช้หรือดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านอย่างไร ทั้งนี้ ชื่อหน่วยงาน ไม่สามารถรับรองข้อความ หรือรับรองการดำเนินการตามที่ได้มีประกาศไว้ได้ และไม่ขอรับผิดชอบใดๆ หากเว็บไซต์เหล่านั้นไม่สามารถปฏิบัติการหรือดำเนินการใดๆ ตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ชื่อหน่วยงาน ที่ได้ประกาศไว้

- ชื่อหน่วยงาน จะติดต่อกับผู้ใช้บริการด้วยการส่งจดหมายอิเล็กทรอนิกส์ถึงสมาชิกใหม่เพื่อตรวจสอบชื่อผู้ใช้บริการและรหัสผ่าน ทั้งนี้ผู้ใช้บริการอาจแจ้งความประสงค์ให้ติดต่อด้วยวิธีการอื่นได้ในขณะที่ทำการลงทะเบียน

- ชื่อหน่วยงาน มีการใช้งานคุกกี้ (Cookies) เพื่อช่วยอำนวยความสะดวกของผู้ใช้บริการในการเข้าบริการของหน่วยงาน โดยคุกกี้เป็นไฟล์ข้อมูลขนาดเล็กที่ระบบบริการของเว็บ ชื่อหน่วยงาน ส่งไปยังโปรแกรมบราวเซอร์ของผู้ใช้บริการ เมื่อผู้ใช้บริการเข้าเยี่ยมชมเว็บไซต์หรือใช้บริการเว็บไซต์ของ ชื่อหน่วยงาน โดยคุกกี้เหล่านี้ช่วยให้การติดต่อระหว่างเครื่องคอมพิวเตอร์ของผู้ใช้บริการกับระบบของ ชื่อหน่วยงาน เป็นไปได้อย่างปกติ ซึ่งคุกกี้ดังกล่าวมิได้เก็บข้อมูลส่วนบุคคลของผู้ใช้บริการเว็บไซต์ของ ชื่อหน่วยงาน ไว้ อย่างไรก็ตามคุกกี้ทำให้ผู้ใช้บริการได้รับประโยชน์จากการให้บริการในลักษณะต่างๆ ของ ชื่อหน่วยงาน และ ชื่อหน่วยงาน แนะนำว่าผู้ใช้บริการควรปล่อยให้คุกกี้ทำงานไปตามปกติ

- ในกรณีที่ผู้ใช้บริการสมัครสมาชิก หรือใช้บริการอย่างใดอย่างหนึ่ง ชื่อหน่วยงาน อาจจะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพิ่มเติม ได้แก่ เพศ อายุ อาชีพ สิ่งที่โปรดปราน ความสนใจ หมายเลขบัตรเครดิต และที่อยู่ในการติดต่อเพื่อสะดวกในการแจ้งรายละเอียดต่างๆ เพื่อวัตถุประสงค์ภายในหน่วยงาน เช่น การตรวจสอบ การวิเคราะห์ข้อมูล เพื่อที่จะปรับปรุงระบบการให้บริการและติดต่อกับผู้ใช้บริการเพื่อส่งประกาศที่สำคัญ เปลี่ยนแปลงข้อกำหนด เงื่อนไขและนโยบายต่างๆ ของ ชื่อหน่วยงาน

- ชื่อหน่วยงาน กำหนดให้มีการเก็บบันทึกการเข้าออกเว็บไซต์ของ ชื่อหน่วยงาน เช่น IP Address ของผู้ใช้บริการทุกท่านที่เข้ามาใช้บริการ โดยผ่านระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้เป็นข้อมูลในการอ้างอิงต่อไป

- ชื่อหน่วยงาน เก็บรวบรวมข้อมูลเกี่ยวกับผู้ใช้บริการทุกครั้งที่เข้ามาใช้บริการในเว็บไซต์ของ ชื่อหน่วยงาน เช่น สถิติการจราจรในเว็บไซต์ (site traffic statistics) การเปิดหน้าเพจ (page view) ระบบปฏิบัติการ (operating system) ประเภทของบราวเซอร์ (browser) และไอพี แอดเดรส (IP address) ซึ่งข้อมูลเหล่านี้โดยทั่วไปจะไม่ระบุถึงตัวผู้ใช้บริการหรือสามารถเชื่อมโยงเกี่ยวพันกับผู้ใช้บริการ และเพื่อวัตถุประสงค์อื่นๆ ชื่อหน่วยงาน อาจเก็บรวบรวม รักษา หรือใช้ส่วนหนึ่งส่วนใดโดยที่ข้อมูลดังกล่าวไม่ได้ระบุถึงตัวผู้ใช้บริการ และไม่สามารถตามรอยได้ว่าเป็นของผู้ใช้บริการรายใด หากในกรณีที่ ชื่อหน่วยงาน เชื่อมโยงข้อมูลเหล่านี้กับข้อมูลผู้ใช้บริการอื่นๆ ข้อมูลดังกล่าวจะได้รับการปฏิบัติเหมือนกับข้อมูลส่วนบุคคลอื่นๆ ภายใต้นโยบายฉบับนี้

- เว็บไซต์ของ ชื่อหน่วยงาน จัดเก็บ/ใช้ Log Files เหมือนกับเว็บไซต์มาตรฐานทั่วๆ ไป ในที่นี้รวมไปถึง IP address, ประเภทของ browser, ผู้ให้บริการอินเทอร์เน็ต (ISP), หน้าเว็บอ้างอิง, คอมพิวเตอร์แพลตฟอร์ม, วัน/เวลา และจำนวนคลิ้กเพื่อวิเคราะห์แนวโน้ม และการจัดการบริหารเว็บไซต์ อีกทั้งเป็นการรวบรวมข้อมูลทั่วไปเชิงประชากรสำหรับการใช้งานโดยรวม ซึ่ง Log files ทั้งหมดจะไม่เชื่อมโยงกับข้อมูลส่วนบุคคล

- การจัดเก็บข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ของ ชื่อหน่วยงาน นั้น ชื่อหน่วยงาน มีการกำหนดว่าข้อมูลใดเป็นข้อมูลที่ต้องให้ ชื่อหน่วยงาน และข้อมูลใดเป็นข้อมูลที่ผู้ใช้บริการมีสิทธิเลือกว่าจะให้หรือไม่ให้ก็ได้ โดยแจ้งไว้ในขั้นตอนการกรอกข้อมูลแล้ว และในกรณีที่ผู้ใช้บริการไม่ประสงค์จะให้ข้อมูลกับ ชื่อหน่วยงาน ผ่านทางเว็บไซต์ ผู้ใช้บริการสามารถติดต่อ ชื่อหน่วยงาน ผ่านช่องทางการติดต่อสื่อสารอื่นๆ เช่น จดหมาย โทรศัพท์หรือติดต่อกับเจ้าหน้าที่ของ ชื่อหน่วยงาน โดยตรง เป็นต้น

- ในการลงทะเบียนหรือใช้บริการกับ ชื่อหน่วยงาน นั้น ขั้นตอนแรกผู้ใช้บริการจะต้องกรอกแบบฟอร์มการลงทะเบียนให้เรียบร้อยก่อน ซึ่งข้อมูลที่จำเป็นต้องกรอกลงไปได้แก่ข้อมูลดังต่อไปนี้ ชื่อ ชื่อสกุล หมายเลขบัตรประชาชน ที่อยู่ อีเมล์ และหมายเลขโทรศัพท์ โดยข้อมูลเหล่านี้จำเป็นต่อการประมวลผลของระบบที่ให้บริการตามที่ท่านใช้บริการ สำหรับข้อมูลอื่นๆ นอกจากนี้ ผู้ใช้บริการมีสิทธิเลือกที่จะให้หรือไม่ให้ก็ได้ เช่น งานอดิเรก สิ่งที่สนใจ เป็นต้น ซึ่งข้อมูลเหล่านี้นั้น ชื่อหน่วยงาน จะใช้เพื่อการพัฒนาการให้บริการที่ดีขึ้นแก่ผู้ใช้บริการ

3. การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

การเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ ที่มีการเชื่อมโยงให้ข้อมูลแก่หน่วยงานอื่น จะต้องมีการระบุการเชื่อมโยงดังกล่าวไว้ด้วย เพื่อช่วยให้ผู้ใช้บริการไม่เกิดความสับสนว่าหน่วยงานไหนที่เป็นผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ และหน่วยงานใดที่เป็นผู้มีกรรมสิทธิ์ในข้อมูลดังกล่าว- ใครคือผู้เก็บ ใคร

เป็นผู้มีกรรมสิทธิ์ และใครจะเป็นผู้มีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัตินี้ และต้องกำหนดให้ชัดเจนว่าข้อมูลประเภทใดที่จะมีการใช้ร่วมกันกับหน่วยงานอื่น

ข้อแนะนำ

นอกจากเว็บไซต์ของ ชื่อหน่วยงาน แล้ว ชื่อหน่วยงาน ยังมีการเชื่อมโยงเว็บไซต์กับ ……. โดยให้ข้อมูลระหว่างกัน (ตามภารกิจของ ชื่อหน่วยงาน) และ ชื่อหน่วยงาน ยังมีการเชื่อมโยงข้อมูลกับเว็บไซต์ของหน่วยงานหรือองค์กรอื่นๆ ของรัฐ โดยการจัดเก็บ รวบรวม และรักษาความปลอดภัยของข้อมูลดังกล่าวที่เชื่อมโยงกันนั้น ชื่อหน่วยงาน ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลตามที่ประกาศไว้ และเนื่องจากแนวนโยบายและแนวปฏิบัติของหน่วยงานอื่นอาจมีความแตกต่างกัน ดังนั้น ชื่อหน่วยงาน ขอแนะนำให้ผู้ใช้บริการศึกษานโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานเหล่านั้นด้วย

4. การรวมข้อมูลจากที่มาหลาย ๆ แห่ง

ถ้าเว็บไซต์นำข้อมูลที่ได้รับมาโดยตรงจากผู้ใช้บริการไปรวมเข้ากับข้อมูลของลูกค้าที่ทางเว็บไซต์ได้รับมาจากบุคคลอื่น การดำเนินการลักษณะนี้จะต้องระบุไว้ในนโยบายและแนวปฏิบัติด้วย

ข้อแนะนำ

- ในบางกรณี ชื่อหน่วยงาน อาจจะนำข้อมูลส่วนบุคคลที่ผู้ใช้บริการให้ข้อมูลผ่านทางเว็บไซต์รวมเข้ากับข้อมูลที่ได้มาจากแหล่งอื่น เช่น ข้อมูลที่อยู่ปัจจุบันของผู้ใช้บริการ เป็นต้น ทั้งนี้เพื่อทำให้ข้อมูลของ ชื่อหน่วยงาน มีความครบถ้วนและถูกต้องเป็นปัจจุบัน และเพื่อทำให้ ชื่อหน่วยงาน สามารถให้บริการตามภารกิจและหน้าที่ของหน่วยงานได้อย่างดียิ่งขึ้น

5. การให้บุคคลอื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคล

ถ้ามีบุคคลอื่นที่จะเข้าถึงหรือใช้ข้อมูลที่หน่วยงานได้เก็บรวบรวมมาผ่านทางเว็บไซต์ ให้ระบุไว้ในนโยบายและแนวปฏิบัติด้วย โดยระบุไว้ด้วยว่าการให้เข้าถึง ใช้ หรือเปิดเผยข้อมูลดังกล่าว สอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานที่ดำเนินการดังกล่าว

ข้อแนะนำ

- ชื่อหน่วยงาน ไม่อนุญาตให้บุคคลอื่นเข้าถึงหรือใช้ข้อมูลที่ ชื่อหน่วยงาน เก็บรวบรวมมาจากเว็บไซต์

- ชื่อหน่วยงาน ใช้บริการการชำระเงินทางอิเล็กทรอนิกส์กับ xyz ในการดำเนินการเกี่ยวกับธุรกรรมทางการเงินทั้งหมด โดย xyz จะไม่จัดเก็บเอาข้อมูลส่วนบุคคลดังกล่าวไว้ ทั้งนี้ การให้ xyz เข้าถึงใช้ นั้นจะใช้เฉพาะงาน กิจกรรมที่เกี่ยวข้องเท่านั้น

- ข้อเพิ่มเติม กรณีที่มีการบังคับให้เปิดเผยข้อมูลตามกฎหมาย ตามหมายศาลหรือตามคำสั่งศาลนั้น ชื่อหน่วยงาน มีหน้าที่ที่จะต้องปฏิบัติตาม

6. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

กรณีที่หน่วยงานจะนำข้อมูลส่วนบุคคลไปดำเนินการอื่นๆ ที่นอกเหนือจากวัตถุประสงค์ของการรวบรวมที่ได้ระบุไว้

สิทธิของผู้ใช้บริการที่จะเลือกว่า จะให้หน่วยงานรวบรวม จัดเก็บหรือไม่ให้จัดเก็บ ใช้หรือไม่ให้ใช้ และเปิดเผยหรือไม่เปิดเผยข้อมูลดังกล่าว

ข้อแนะนำ

ในกรณีที่ ชื่อหน่วยงาน จะนำข้อมูลส่วนบุคคลที่ผู้ใช้บริการให้ข้อมูลไว้ไปใช้ในวัตถุประสงค์อื่นนอกเหนือจากที่ระบุไว้ จะต้องระบุไว้ในนโยบายฯ ถึงสิทธิของผู้ใช้บริการ ว่า ผู้ใช้บริการจะมีสิทธิในการคัดค้าน (Opt-out) ณ ขั้นตอนที่มีการขอข้อมูลส่วนบุคคลของผู้ใช้บริการเพื่อวัตถุประสงค์อื่นที่ไม่เกี่ยวข้องโดยตรงกับ ชื่อหน่วยงาน เพื่อให้ผู้ใช้บริการที่ไม่ต้องการให้ ชื่อหน่วยงาน เอาข้อมูลส่วนบุคคลของตนไปใช้ในสิ่งที่ไม่ตรงตามวัตถุประสงค์ของ ชื่อหน่วยงาน

อย่างไรก็ตาม สำหรับกรณีที่ผู้ใช้บริการได้ให้ข้อมูลต่างๆ ไว้แล้ว ก็ต้องสามารถให้ผู้ใช้บริการแจ้งยกเลิกได้ ในหัวข้อบอกเลิก (ถ้ามี) หรืออาจส่งจดหมายอิเล็กทรอนิกส์ไปแจ้ง

7. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

ให้หน่วยงานของรัฐ กำหนดวิธีการที่ผู้ใช้บริการเว็บไซต์สามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลเกี่ยวกับตนเองที่หน่วยงานองรัฐรวบรวมและจัดเก็บไว้ในเว็บไซต์ให้ถูกต้อง

ข้อแนะนำ

- ในกรณีที่ผู้ใช้บริการได้ให้ข้อมูลต่างๆ กับ ชื่อหน่วยงาน ผ่านทางเว็บไซต์ของ ชื่อหน่วยงาน และประสงค์จะแก้ไขหรือปรับปรุงข้อมูลดังกล่าวให้ถูกต้องหรือให้เป็นปัจจุบัน สามารถติดต่อ ชื่อหน่วยงาน ได้ทางช่องทางที่ระบุไว้

- ผู้ใช้บริการหรือสมาชิกสามารถเข้ามาตรวจสอบและแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลที่ได้ให้ไว้กับ ชื่อหน่วยงาน ได้ โดยไปที่หน้าเพจ ……My Account แล้วเลือกเมนู edit Profile

8. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ จัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล

ก) เสริมสร้างความสำนึกรับผิดชอบด้าน Security ให้แก่บุคลากร พนักงาน หรือลูกจ้างในหน่วยงาน ด้วยการเผยแพร่ข้อมูล ให้ความรู้ หรือฝึกอบรมเป็นประจำ

ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล ในแต่ละระดับชั้น ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ จัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล

ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง

ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมสำหรับข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดี หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของอย่างชัดเจน เช่น หมายเลขบัตรเครดิต หมายเลขประจำตัวประชาชน เชื้อชาติ ศาสนา สุขภาพ พฤติกรรมทางเพศ เป็นต้น

จ. นโยบายเกี่ยวกับข้อมูลส่วนบุคคลของเด็ก (ถ้ามี)

ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปี โดยใช้วิธีการโดยเฉพาะและเหมาะสม

ข้อแนะนำ

- ชื่อหน่วยงาน เสริมสร้างความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่พนักงาน เจ้าหน้าที่ของ ชื่อหน่วยงาน ด้วยการเผยแพร่ข้อมูลข่าวสาร การจัดอบรม และจัดสัมมนา

- ชื่อหน่วยงาน จำกัดการเข้าถึงข้อมูลส่วนบุคคลไว้ให้เฉพาะเจ้าหน้าที่ที่มีความจำเป็นต้องใช้ข้อมูลในการปฏิบัติงานในหน้าที่ ในแต่ละลำดับชั้น และจัดให้มีการการบันทึกและทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด นอกจากนี้ ในบางกรณี ชื่อหน่วยงาน จะใช้การเข้ารหัส SSL เพื่อรักษาความมั่นคงปลอดภัยในการส่งผ่านข้อมูล

- ชื่อหน่วยงาน จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง

- ชื่อหน่วยงาน กำหนดให้มีการใช้มาตรการในการรักษาความลับและความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญหรือเป็นข้อมูลที่อาจกระทบต่อความสงบเรียบร้อย และศีลธรรม อันดีของประชาชนซึ่งเป็นผู้ใช้บริการของ ชื่อหน่วยงาน

- ชื่อหน่วยงาน ไม่มีความตั้งใจที่จะเก็บรวบรวมข้อมูลจากบุคคลซึ่งอายุไม่เกิน 18 ปี หากทราบว่า ชื่อหน่วยงาน ได้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกิน 18 ปี จะดำเนินการเพื่อลบข้อมูลนั้นออกโดยเร็วที่สุดเท่าที่จะปฏิบัติได้

- เว็บไซต์ของ ชื่อหน่วยงาน เป็นเว็บไซต์สำหรับบุคคลทั่วไป ไม่ได้ออกแบบหรือมีเจตนาเพื่อเก็บข้อมูลส่วนบุคคลจากผู้เยาว์ จึงใคร่ขอให้พ่อแม่ผู้ปกครองดูแลผู้เยาว์ของท่านขณะเข้าเว็บไซต์

9. การติดต่อกับเว็บไซต์

เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย

(ก) ชื่อและที่อยู่

(ข) หมายเลขโทรศัพท์

(ค) หมายเลขโทรสาร

(ง) ที่อยู่จดหมายอิเล็กทรอนิกส์

ข้อแนะนำ

กรณีที่ผู้ใช้บริการมีข้อสงสัยหรือคำถามประการใดเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคลหรือกรณีที่ต้องการติดต่อใดๆ กับ ชื่อหน่วยงาน สามารถติดต่อได้ที่ .....อาคาร...ถนน ..... หมายเลขโทรศัพท์ โทรสาร อีเมล์

เอกสารอ้างอิง

หนังสือ

ศูนย์สารสนเทศเศรษฐกิจอุตสาหกรรม สำนักงานเศรษฐกิจอุตสาหกรรม**.**แผนบริหาร ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ประจำปี 2555**,** มีนาคม **255**5

แหล่งข้อมูลทาง Internet

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

http://www.etcommission.go.th

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=122&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.แนวทางการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=121&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.เรียนรู้จากประสบการณ์นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=120&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.สรุปผลการดำเนินงานเกี่ยวกับการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=119&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=118&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=91&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=92&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.แบบสอบถามหน่วยงานของรัฐ คำอธิบาย / คำชี้แจง ที่มีการดำเนินการตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=128&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=89&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=93&Itemid=11&lang=en

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล

http://www.etcommission.go.th/index.php?option=com_docman&task=doc_download&gid=21&Itemid=11&lang=en