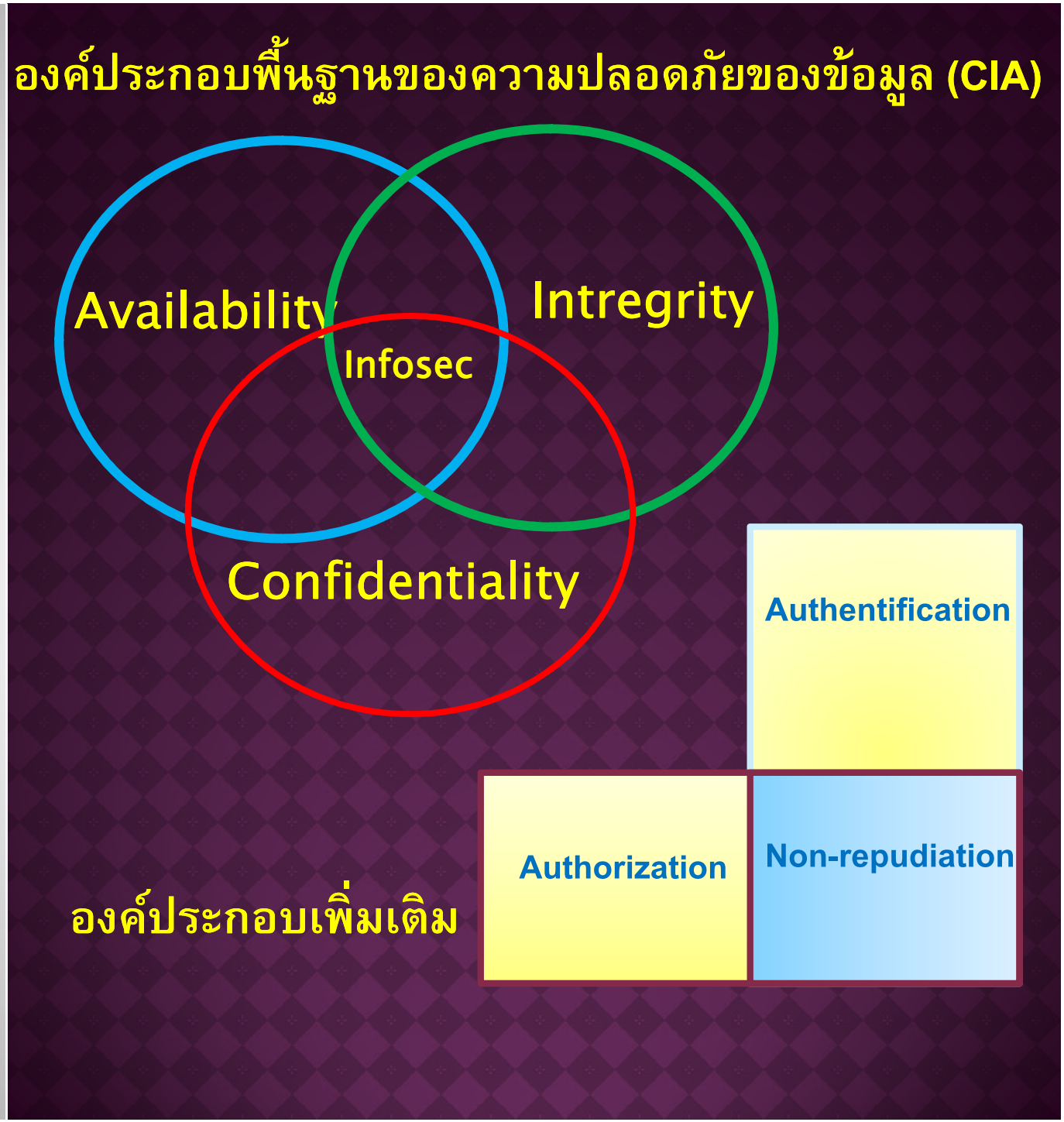
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ร่วมกับคณะอนุกรรมการความมั่นคงปลอดภัย ภายใต้คณะกรรมการ
ธุรกรรมทางอิเล็กทรอนิกส์

หัวข้อการบรรยาย

- มาตรการที่สอดคล้องกับหลักการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล
- ข้อแนะนำในการเตรียมการดำเนินงาน
- ข้อแนะนำในการจัดทำนโยบาย
- ข้อแนะนำในการจัดทำแนวปฏิบัติ
- ข้อแนะนำในการจัดทำคำนิยาม
- ประเด็นเทคนิคในการคุ้มครองข้อมูลส่วนบุคคล

มาตรการที่สอดคล้องกับหลักการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล



ความสอดคล้องกับหลักการ CIA

หลักการสำคัญ	ข้อกำหนดตามประกาศที่เกี่ยวข้อง
(๑) **การธำรงไว้ซึ่งความลับ (Confidentiality)**	ข้อ ๘ ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) ข้อ ๙ ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) ข้อ ๑๐ ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

ความสอดคล้องกับหลักการ CIA

หลักการสำคัญ	ข้อกำหนดตามประกาศที่เกี่ยวข้อง (ต่อ)
(๑) **การธำรงไว้ซึ่งความลับ (Confidentiality)**	ข้อ ๑๑ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)

ความสอดคล้องกับหลักการ CIA

หลักการสำคัญ	ข้อกำหนดตามประกาศที่เกี่ยวข้อง
(๒) **ความถูกต้องครบถ้วน (Integrity)**	ข้อ ๕ ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ข้อ ๖ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) ข้อ ๗ ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

ความสอดคล้องกับหลักการ CIA

หลักการสำคัญ	ข้อกำหนดที่เกี่ยวข้อง
(๓) ความพร้อมใช้หรือสภาพพร้อมใช้งาน (Availability)	ข้อ ๑๒ หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ข้อ ๑๓ หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อแนะนำในการเตรียมจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อแนะนำในการเตรียมการ

เอกสารที่เกี่ยวข้อง

- นโยบายในการรักษาความมั่นคงปลอดภัย
- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
- แผนสำรองระบบสารสนเทศ
- แผนเตรียมความพร้อมกรณีฉุกเฉิน
- คำสั่งแต่งตั้งผู้รับผิดชอบตามนโยบายและแนวปฏิบัติ

ข้อแนะนำในการเตรียมการ

พิจารณาสาระสำคัญ

- ประเด็นหลัก ๓ ข้อตาม พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
- ประเด็นหลักที่เกี่ยวกับการเข้าถึง ๔ ด้าน ตามประกาศฯ กำหนด
- ประเด็นหลักเกี่ยวกับการสำรอง และแผนเตรียมความพร้อมฉุกเฉินตามที่ประกาศฯ กำหนด
- ประเด็นหลักที่เกี่ยวกับการตรวจประเมินความเสี่ยง ตามที่ประกาศฯ กำหนด

แนวปฏิบัติกลาง ๆ ที่สำคัญของทุกหน่วยงาน

- การลงทะเบียนผู้ใช้งาน
- การบริหารรหัสผ่าน
- การใช้งานรหัสผ่าน
- การบริหารจัดการสิทธิ์

สภาพความเป็นจริงของหน่วยงาน

- ต้องระวังการเข้าถึงสารสนเทศ
- ต้องระวังการเข้าถึงเครือข่าย
- ต้องระวังการเข้าถึงระบบปฏิบัติการ
- ต้องระวังการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

การบริหารจัดการสิทธิ์

ควรคำนึงถึงความสัมพันธ์ระหว่างสถานะของผู้ใช้งาน และสิทธิ์ที่เกี่ยวข้อง เช่น

- สิทธิในการอ่านอย่างเดียว
- สิทธิในการสร้าง / บันทึกข้อมูล
- สิทธิในการแก้ไขเปลี่ยนแปลงข้อมูล
- สิทธิในการลบข้อมูล
- สิทธิในการอนุญาตสิทธิให้บุคคลอื่น ๆ ได้

ทั้งนี้ขึ้นอยู่กับหน้าที่ของผู้ใช้งานในแต่ละระดับที่เกี่ยวข้อง ซึ่งต้องกำหนดคำนิยามให้ชัดเจน

หน่วยงานต้องทำการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานแต่ละกลุ่มอย่างสม่ำเสมอ

เริ่มระดมความเห็นร่วมกันในการกำหนดนโยบายและแนวปฏิบัติของหน่วยงาน

ข้อแนะนำ
ในการจัดทำเอกสารนโยบาย

ชื่อประกาศ

คำนำ / อ้างอิงอำนาจตามกฎหมาย

ระบุวัตถุประสงค์ / ขอบเขตนโยบาย

ระบุองค์ประกอบของนโยบาย มีกี่ส่วน เรื่องอะไรบ้าง เช่น

๑. การบริหารจัดการของผู้บริหาร
๒. ขอบเขตการใช้งานคอมพิวเตอร์/เครือข่ายสำหรับผู้ใช้
๓. การบริหารจัดการนโยบายและแนวปฏิบัติ
๔. ด้านบุคลากร
๕. การเผยแพร่ข้อมูล

ประกาศ ณ วันที่

ลงนามผู้ประกาศ

อย่างน้อยควรมี
เนื้อหาตามประกาศ
ข้อ ๒(๑) (๒)(๓)
ข้อ ๓(๑)(๒)(๓)(๔)
และ ข้อ ๑๔

ข้อ ๒ หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

<u>ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้</u>

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการ ด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

<u>ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้</u>

(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติ ให้เป็นปัจจุบันอยู่เสมอ

การจัดทำนโยบาย

ข้อกำหนดตามประกาศ	ข้อแนะนำ
(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้	•ต้องมีการประกาศนโยบาย ซึ่งลงนามโดยผู้บริหารของหน่วยงาน พร้อมทั้งให้ระบุวิธีการประกาศ และควรระบุไว้เป็นส่วนหนึ่งของนโยบาย •กรณีหน่วยงานมี “ผู้รับบริการทางอิเล็กทรอนิกส์” ต้องประกาศนโยบายและแนวปฏิบัติฯ ให้ผู้รับบริการทราบด้วย •หากหน่วยงานเห็นว่า “นโยบายและแนวปฏิบัติฯ” เป็นเรื่องลับ ไม่สามารถเปิดเผยได้ทั้งหมด ให้จัดทำเอกสาร “นโยบายและแนวปฏิบัติฯ (ฉบับผู้รับบริการ)” แยกส่วนที่สามารถเปิดเผยได้ขึ้นอีกฉบับ เพื่อแจ้งให้ผู้รับบริการทราบด้วย

การจัดทำนโยบาย

ข้อกำหนดตามประกาศ	ข้อแนะนำ
(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน	•ระบุผู้รับผิดชอบในฐานะการกำกับดูและให้มีการดำเนินงานตามประกาศ •ต้องระบุหน้าที่ความรับผิดชอบตามสายบังคับบัญชา ตั้งแต่ CIO จนถึงผู้ปฏิบัติ •ระบุรายละเอียดในทางปฏิบัติ ที่เกี่ยวข้องกับนโยบายข้อ ๒ ในแนวปฏิบัติเฉพาะแต่ละด้านด้วย

ข้อแนะนำ
การจัดทำแนวปฏิบัติ

เอกสารแนบท้ายประกาศ
เรื่อง.....

ส่วนที่ ๑
นโยบาย.....

วัตถุประสงค์

ผู้รับผิดชอบ

อ้างอิงมาตรฐาน

ข้อปฏิบัติ

๑).....

๑.๑).....

ข้อ ๔ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕ – ๑๕

ข้อ ๕ ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)

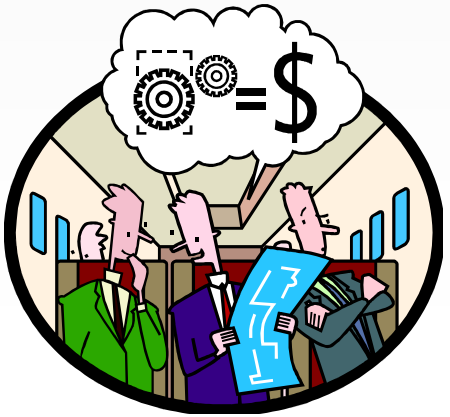
ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผล ข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบาย ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของ รัฐนั้น ๆ

(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือ ลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย



ข้อ ๗ ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

<u>โดยต้องมีเนื้อหาอย่างน้อย ดังนี้</u>

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

ข้อ ๗ (ต่อ)

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุม และจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้อง จัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

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

ข้อ ๘ ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยการล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

<u>โดยต้องมีเนื้อหาอย่างน้อย ดังนี้</u>

(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๙ ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

<u>โดยต้องมีเนื้อหาอย่างน้อย ดังนี้</u>

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

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

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

ข้อ ๙ (ต่อ)

โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

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

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

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐ ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

<u>โดยต้องมีเนื้อหาอย่างน้อย ดังนี้</u>

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

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

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

ข้อ ๑๐ (ต่อ)

โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

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

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)

<u>โดยต้องมีการควบคุม ดังนี้</u>

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

ข้อ ๑๑ (ต่อ)

โดยต้องมีการควบคุม ดังนี้

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

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๒ หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง

ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๓ หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

<u>โดยต้องมีเนื้อหาอย่างน้อย ดังนี้</u>

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ **ทั้งนี้ให้ผู้บริหารระดับสูงของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น**

ข้อ ๑๕ หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

ข้อแนะนำ

การกำหนดคำนิยาม

เอกสารแนบท้ายประกาศ
เรื่อง.....

ว่าด้วยคำนิยาม

ระบุรายการคำนิยามที่เกี่ยวข้องทั้งหมด

ผู้ใช้งาน .....

สิทธิ์ของผู้ใช้งาน.....

สินทรัพย์.....

และคำนิยามอื่น ๆ

ข้อ ๑ ในประกาศนี้

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

(๒) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๓) สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

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

ข้อ ๑ ในประกาศนี้

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

(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดง ให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือ มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์ อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

(๘) คำนิยาม (อื่น) - สามารถเพิ่มได้ตามความจำเป็น และสอดคล้องกับความ ขององค์กร

WEBSITE

เอกสารอ้างอิง

๑. ร่างมาตรฐานฯ การรักษาความมั่นคงในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เล่ม 1 ข้อกำหนด

http://ecec.nectec.or.th/node/25

๒. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เวอร์ชั่น ๒.๕

http://www.thaicert.org/paper/basic/Book_2.5_FullVersion.pdf


กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
Ministry of Information and Communication Technology

ขอบคุณ