นโยบายและแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานปลัดกระทรวงศึกษาธิการ

ประกาศสำนักงานปลัดกระทรวงศึกษาธิการ
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานปลัดกระทรวงศึกษาธิการ พ.ศ ๒๕๕๙

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ สำนักงานปลัดกระทรวงศึกษาธิการโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานปลัดกระทรวงศึกษาธิการ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงศึกษาธิการ พ.ศ.๒๕๕๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๔

๓.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๕ - ๑๓

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๔.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบายโดยกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสำนักงานปลัดกระทรวงศึกษาธิการ

(๓) กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ของสำนักงานปลัดกระทรวงศึกษาธิการ เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

/(๔) กำหนดให้...

(๔) กำหนดให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงศึกษาธิการ เป็นผู้รับผิดชอบในการติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะและคำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

(๕) มีการทบทวนและปรับปรุงนโยบาย และแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง

๔.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย โดยจะต้องครอบคลุมเนื้อหาอย่างน้อย ดังนี้

- การเข้าถึงระบบสารสนเทศ
- การเข้าถึงระบบเครือข่าย
- การเข้าถึงระบบปฏิบัติการ
- การเข้าถึงระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application)

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน

มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และอยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

มีนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๕ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) อย่างน้อย ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

/ข้อ ๖ มีการบริหาร...

ข้อ ๖ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

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

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

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

ข้อ ๗ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘ มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

/(๑) การใช้บริการ...

(๑) การใช้บริการเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

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

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

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

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

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

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

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

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

/(๖) การจำกัด...

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๐ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึง สารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๑ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

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

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

/(๓) ในกรณี...

(๓) ในกรณีที่หน่วยงานไม่มีผู้ทำหน้าที่ในการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ให้ผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยสารสนเทศจากภายนอกดำเนินการดังกล่าว

ข้อ ๑๓ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๑๔ ให้ใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๕ เมษายน พ.ศ. ๒๕๕๙

(รองศาสตราจารย์กำจร ตติยกวี)
ปลัดกระทรวงศึกษาธิการ

ISO/IEC 27001:2013

ระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

Information Security Management System (ISMS)

รหัสเอกสาร:	MIS-1-PC-001
ชื่อเอกสาร:	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ (ICT Security Policy)
หมายเลขปรับปรุงเอกสาร:	1.1
วันที่เอกสารมีผลบังคับใช้:	
เจ้าของเอกสาร:	

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นสิ่งสำคัญสำหรับหน่วยงานที่เข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็วการติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของหน่วยงานที่เชื่อมต่อในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ และการมีเว็บไซต์เป็นของหน่วยงานสำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่างๆ เป็นต้น ทั้งนี้ระบบเครือข่ายดังกล่าว แม้จะมีประโยชน์และอำนวยความสะดวกก็ตาม แต่ในขณะเดียวกันก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตราย หรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเครือข่ายคอมพิวเตอร์เปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอกทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการโจมตีทางระบบเครือข่ายเพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้นผู้ใช้งานและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารจึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและชื่อถือได้ และมาตรา 7 แนวนโยบายและแนวปฏิบัติตามมาตรา 5 ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย สำนักงานปลัดกระทรวงศึกษาธิการ จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ของสำนักงานปลัดกระทรวงศึกษาธิการ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จากทุกหน่วยและต้องดำเนินการอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานปลัดกระทรวงศึกษาธิการ จึงหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของสำนักงานปลัดกระทรวงศึกษาธิการทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงศึกษาธิการต่อไป

สำนักงานปลัดกระทรวงศึกษาธิการ

สารบัญ

หน้า

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ สำนักงานปลัดกระทรวงศึกษาธิการ

1 วัตถุประสงค์

1.1 เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงานปลัดกระทรวงศึกษาธิการตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

1.2 เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้แก่บุคลากรและผู้ปฏิบัติงานในการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน รวมทั้งการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

1.3 เพื่อให้มีกระบวนการสำรองข้อมูลสารสนเทศ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถกู้คืนระบบได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจของหน่วยงาน

1.4 เพื่อให้มีการตรวจประเมินการรักษาความมั่นคงปลอดภัยสารสนเทศและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

1.5 เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจ และส่งเสริมให้มีการอบรม ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรและบุคคลที่เกี่ยวข้อง

2 หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัย และเชื่อถือได้ สำนักงานปลัดกระทรวงศึกษาธิการ จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ สำนักงานปลัดกระทรวงศึกษาธิการ เพื่อรักษาความมั่นคงปลอดภัยข้อมูลและระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นเครื่องมือที่สำคัญในการปฏิบัติงานและการบริหารราชการต่อไป

3 เป้าหมายการรักษาความมั่นคงปลอดภัยสารสนเทศ สำนักงานปลัดกระทรวงศึกษาธิการ

3.1 ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของหน่วยงาน

3.2 มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิด หรือฝ่าฝืนนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งติดตาม และตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

3.3 เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

3.4 เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาหาความรู้เพิ่มเติมอย่างต่อเนื่อง

3.5 ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี

3.6 หน่วยงานด้านสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึงข้อมูล และอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

4 ขอบเขตของนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ สำนักงานปลัดกระทรวงศึกษาธิการ

นโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ สำนักงานปลัดกระทรวงศึกษาธิการ จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศให้สอดคล้อง และเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งนโยบายออกเป็นส่วนๆ ดังต่อไปนี้

หมวดที่ 1	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
หมวดที่ 2	โครงสร้างความมั่นคงปลอดภัยสารสนเทศ
หมวดที่ 3	ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล
หมวดที่ 4	การบริหารจัดการสินทรัพย์
หมวดที่ 5	การเข้ารหัส
หมวดที่ 6	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
หมวดที่ 7	ความมั่นคงปลอดภัยในการดำเนินงาน
หมวดที่ 8	ความมั่นคงปลอดภัยในการสื่อสารข้อมูล
หมวดที่ 9	การจัดหา การพัฒนาและการบำรุงรักษาระบบ
หมวดที่ 10	ความสัมพันธ์กับผู้ให้บริการภายนอก
หมวดที่ 11	การบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

หมวดที่ 12 ความสอดคล้องในการปฏิบัติต่อข้อกำหนด

หมวดที่ 13 การบริหารจัดการความเสี่ยง

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. **“หน่วยงาน”** หมายความว่า หน่วยงานในสังกัดสำนักงานปลัดกระทรวงศึกษาธิการ ทั้งในส่วนกลางและส่วนภูมิภาค จำนวน 16 หน่วยงาน ดังนี้

    1) สำนักงานส่งเสริมการศึกษานอกระบบและการศึกษาตามอัธยาศัย

    2) สำนักงานคณะกรรมการส่งเสริมการศึกษาเอกชน

    3) สำนักงานคณะกรรมการข้าราชการครูและบุคลากรทางการศึกษา

    4) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.

    5) กลุ่มพัฒนาระบบบริหาร สป.

    6) สำนักนโยบายและยุทธศาสตร์ สป.

    7) สำนักอำนวยการ สป.

    8) สำนักความสัมพันธ์ต่างประเทศ สป.

    9) สำนักนิติการ สป.

    10) หน่วยตรวจสอบภายใน สป.

    11) กลุ่มตรวจสอบภายในระดับกระทรวง

    12) สำนักตรวจราชการและติดตามประเมินผล สป.

    13) สถาบันพัฒนาครู คณาจารย์ และบุคลากรทางการศึกษา

    14) สำนักการลูกเสือ ยุวกาชาด และกิจการนักเรียน สป.

    15) สำนักส่งเสริมกิจการการศึกษา

    16) สำนักงานรัฐมนตรี

2. **“หน่วยงานด้านสารสนเทศ”** หมายความว่า หน่วยงานในสังกัดสำนักงานปลัดกระทรวงศึกษาธิการที่รับผิดชอบดูแลระบบสารสนเทศและระบบเครือข่าย ซึ่งประกอบด้วย

    1) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

    2) กลุ่มพัฒนาระบบเทคโนโลยี สำนักงานคณะกรรมการส่งเสริมการศึกษาเอกชน

    3) กลุ่มแผนงาน สำนักงานส่งเสริมการศึกษานอกระบบและการศึกษาตามอัธยาศัย

    4) กลุ่มเทคโนโลยีและสารสนเทศการบริหารงานบุคคล สำนักงานคณะกรรมการข้าราชการครูและบุคลากรทางการศึกษา

3. **“ระบบคอมพิวเตอร์”** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

4. **“ระบบเครือข่าย”** หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

5. **“สิทธิของผู้ใช้งาน”** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

6. **“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ”** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

7. **“ความมั่นคงปลอดภัยด้านสารสนเทศ”** หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และ ความน่าเชื่อถือ (Reliability)

8. **“เหตุการณ์ด้านความมั่นคงปลอดภัย** (Information Security Event)” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

9. **“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด”** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

10. **“ระบบอินทราเน็ต (Intranet)”** หมายความว่าระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

11. **“ระบบอินเทอร์เน็ต (Internet)”** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

12. **“ระบบสารสนเทศ (Information Technology System)”** หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

13. **“เครื่องคอมพิวเตอร์”** หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

14. **“เครื่องแม่ข่าย”** หมายความว่า เครื่องหรือโปรแกรมคอมพิวเตอร์ซึ่งทำงานให้บริการ ในระบบเครือข่ายแก่ลูกข่าย (ซึ่งให้บริการผู้ใช้อีกทีหนึ่ง) เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเซิร์ฟเวอร์นี้ควรจะมีประสิทธิภาพสูง มีความเสถียร สามารถให้บริการแก่ผู้ใช้ได้เป็นจำนวนมาก

15. **“ข้อมูลคอมพิวเตอร์”** หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

16. **“สารสนเทศ (Information)”** หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

17. **“ผู้บังคับบัญชา”** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานปลัดกระทรวงศึกษาธิการ

18. **“ผู้ใช้งาน”** หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน และให้หมายความรวมถึงผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

19. **“ผู้ดูแลระบบ (System Administrator)”** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

20. **“หน่วยงานภายนอก”** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

21. **“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร”** หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

(1) พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

(2) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

(3) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

22. **“สินทรัพย์”** หมายความว่า ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

23. **“จดหมายอิเล็กทรอนิกส์ (E-mail)”** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

24. **“รหัสผ่าน (Password)”** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

25. **“บัญชีผู้ใช้บริงาน (Account)”** หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

26. **“โปรแกรมประสงค์ร้าย (Malware)”** หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

27. **“ชื่อเครื่องคอมพิวเตอร์ (Computer Name)”** หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

28. **“สื่อบันทึกพกพา”** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

29. **“ปุ่มกดง่าย (Shortcut)”** หมายความว่า เครื่องมือที่ช่วยในการเรียกใช้โปรแกรมได้อย่างรวดเร็วและสามารถเข้าถึงโปรแกรมหรือแฟ้มข้อมูลที่ต้องการได้ทันที ซึ่งผู้ใช้สามารถลบหรือสร้างใหม่ได้

30. **“ไบออส (BIOS)”** หมายความว่า ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนเมนบอร์ดของเครื่องคอมพิวเตอร์ทำหน้าที่ควบคุมขั้นตอนการบู๊ตและการทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนเมนบอร์ด

31. **“การตั้งค่าระบบ (Configuration)”** หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

32. **“เลขที่อยู่ไอพี (IP Address)”** หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข 4 ส่วนหรือ 6 ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

33. **“เลขที่อยู่ไอพีสาธารณะ (Public IP Address)”** หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงานหรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

34. **“แบนด์วิดท์ (Bandwidth)”** หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

35. **“ชื่อผู้ใช้ (Username)”** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

36. **“ลงบันทึกเข้า (Login)”** หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้ เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

37. **“ลงบันทึกออก (Logout)”** หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

38. **“อัพเดท (Update)”** หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

39. **“ช่องโหว่ (Vulnerability)”** หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

40. **“ไฟล์ที่สามารถประมวลผลได้ (Executable file)”** หมายความว่า ไฟล์โปรแกรมที่สามารถเรียกใช้งานได้ทันที เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe ในขณะที่ไฟล์ข้อมูลอื่นๆ จะเป็นไฟล์ข้อมูลประกอบ

41. **“การเข้ารหัส (Encryption)”** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

42. **“อุปกรณ์กระจายสัญญาณ (Access Point)”** หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

43. **“SSID (Service Set Identifier)”** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

44. **“โดยปริยาย (Default)”** หมายความว่า ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้าและนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้งาน

45. **“WEP (Wired Equivalent Privacy)”** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

46. **“WPA (Wi-Fi Protected Access)”** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

47. **“Wireless LAN Client”** หมายความว่า เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE 802.11

48. **“MAC Address (Media Access Control Address)”** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

49. **“ไฟร์วอลล์ (Firewall)”** หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

50. **“VPN (Virtual Private Network)”** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ - ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

51. **“Web Server”** หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่างๆ

52. **“ชื่อโดเมนย่อย (Sub Domain Name)”** หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ "ที่อยู่เว็บไซต์" แทนก็ได้

53. **“อุปกรณ์จัดเส้นทาง (Router)”** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

54. **“อุปกรณ์กระจายสัญญาณข้อมูล (Switch)”** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

55. **“การพิสูจน์ยืนยันตัวตน (Authentication)”** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

56. **“แผนผังระบบเครือข่าย (Network Diagram)”** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

57. **“Command Line”** หมายความว่า บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

58. **“Firewall Log”** หมายความว่า การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

59. **“DOD 5220.22-M”** หมายความว่า การลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับและใช้งานกับกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้ ซึ่งทำการลบข้อมูล 3 รอบ รอบแรกด้วยข้อมูลแบบสุ่ม รอบที่สองด้วยบิตที่ตรงกันข้าม รอบสุดท้ายด้วยข้อมูลไบต์สุ่ม

60. **“ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (Internal IT Auditor)”** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรับผิดชอบให้สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log)

61. **“ผู้ตรวจสอบระบบสารสนเทศจากหน่วยงานภายนอก (External IT Auditor)”** หมายความว่า ผู้ที่ได้รับมอบหมายจากหน่วยงานให้มีสิทธิในการตรวจสอบระบบสารสนเทศหรือระบบเครือข่ายของหน่วยงาน

62. **“เวลาอ้างอิงสากล (Stratum 0)”** หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

63. **“ข้อมูลจราจรทางคอมพิวเตอร์ (Log)”** หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

64. **“ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO)”** หมายความว่า ปลัดกระทรวงศึกษาธิการ

หมวดที่ 1
นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ

ผู้บริหารจัดให้มีและควบคุมให้มีการพัฒนานโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยนโยบายต้องมีองค์ประกอบดังนี้

1.1.1 วัตถุประสงค์ ขอบเขต และหน้าที่ความรับผิดชอบ

1.1.2 ข้อความในนโยบายต้องไม่ขัดต่อกฎหมาย ระเบียบและข้อปฏิบัติของหน่วยงาน

1.1.3 มีการทบทวน และการอนุมัตินโยบายและแนวทางการปฏิบัติก่อนทำการประกาศใช้ ซึ่งรายละเอียดผู้มีอำนาจลงนามการอนุมัติเอกสารเป็นไปตามขั้นตอนการปฏิบัติการควบคุมเอกสาร (MIS-2-PR-001)

1.1.4 มีการสื่อสารไปยังบุคลากร หน่วยงานภายนอก และผู้ที่เกี่ยวข้องหลังการอนุมัติและประกาศใช้นโยบายและแนวปฏิบัติ

1.2 การทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ

1.2.1 ผู้บริหารจัดให้มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อให้คงความถูกต้องและความเหมาะสมอย่างน้อยปีละหนึ่งครั้ง

หมวดที่ 2
โครงสร้างความมั่นคงปลอดภัยสารสนเทศ

2.1 โครงสร้างภายในองค์กร

2.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

บทบาทและหน้าที่ความรับผิดชอบของคณะกรรมการที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยจะมีการเสนอแต่งตั้งคณะกรรมการและคณะทำงาน ประกอบด้วย คณะกรรมการนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ คณะกรรมการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และคณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

2.1.2.หลักการแบ่งแยกหน้าที่ความรับผิดชอบ

(1) หน้าที่ในการบริหารจัดการระบบและการจัดการเครือข่ายต้องแยกออกจากกัน

(2) ไม่ให้บุคคลเดียวกันทำงานที่สำคัญๆ ในกระบวนการเดียวกัน เพื่อป้องกันการทุจริตและการได้รับสิทธิมากเกินไป

2.1.3 การติดต่อกับหน่วยงาน

คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จะต้องมีรายชื่อและเบอร์ติดต่อของหน่วยงานที่มีอำนาจในการบังคับใช้กฎหมาย หน่วยงานด้านกฎระเบียบ ผู้ให้บริการทางด้านข้อมูลและผู้ให้บริการทางด้านโทรคมนาคม เพื่อการสื่อสารอย่างมีประสิทธิภาพเมื่อเกิดเหตุฉุกเฉิน

2.1.4 การติดต่อกับผู้ที่อยู่ในแวดวงการรักษาความปลอดภัยและผู้เชี่ยวชาญด้านความปลอดภัย

(1) หน่วยงานต้องสมัครเป็นสมาชิกการแจ้งเตือนข่าวสารด้านความปลอดภัยจากผู้ค้า เพื่อช่วยเป็นข้อมูลในการบริหารจัดการช่องโหว่จากผลิตภัณฑ์ของผู้ค้า

(2) หน่วยงานต้องติดต่อกับผู้ที่อยู่ในแวดวงด้านการรักษาความปลอดภัยและผู้เชี่ยวชาญด้านความปลอดภัยและสมาคมวิชาชีพทางด้านความปลอดภัย เพื่อรับทราบข่าวความเคลื่อนไหว รวมทั้งข้อมูลแนวทางในการปฏิบัติทางด้านความปลอดภัยที่ได้รับความนิยม

2.1.5 ความมั่นคงปลอดภัยสำหรับสารสนเทศในการบริหารโครงการ

หน่วยงานต้องระบุหัวข้อและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในทุกโครงการที่เกิดขึ้นไม่ว่าจะเกี่ยวข้องกับเทคโนโลยีสารสนเทศหรือไม่

2.2 อุปกรณ์แบบพกพา

2.2.1 นโยบายสำหรับอุปกรณ์แบบพกพา

(1) การป้องกันด้านกายภาพ

ก) อุปกรณ์ใดๆ ที่ต้องนำไปใช้ในกิจกรรมของหน่วยงานภายนอกสถานที่ ต้องได้รับการอนุมัติจากผู้บริหาร โดยอุปกรณ์ดังกล่าวต้องมีการควบคุมด้านความมั่นคงปลอดภัยในระดับเดียวกับอุปกรณ์ที่ใช้ภายในสำนักงาน

ข) ต้องมีการป้องกันหรือการล็อคอุปกรณ์พกพา และคอมพิวเตอร์พกพาอย่างเหมาะสมเมื่อไม่ได้ใช้งานภายในสำนักงาน

ค) บุคลากรต้องไม่วางอุปกรณ์ไว้ในที่สาธารณะโดยที่ไม่มีคนดูแล บุคลากรมีหน้าที่รับผิดชอบในดูแลและป้องกันอุปกรณ์ต่างๆ ที่ได้รับ

ง) อุปกรณ์ที่จะนำไปใช้ภายนอกสำนักงานต้องมีการเข้ารหัสลับของดิสก์ (Disk encryption)

จ) ต้องปฏิบัติตามคู่มือการป้องกันอุปกรณ์ที่ได้รับจากผู้ผลิตตลอดเวลา เช่น การป้องกันจากการเข้าใกล้สนามแม่เหล็กไฟฟ้า

(2) การป้องกันด้านตรรกะ

ก) อุปกรณ์พกพาต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต

ข) มีการบังคับใช้มาตรการการเข้าถึงในระดับไบออส (BIOS) สำหรับคอมพิวเตอร์พกพา

ค) ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

ง) ต้องติดตั้งซอฟต์แวร์ป้องกันคอมพิวเตอร์ไวรัส (Antivirus) บนอุปกรณ์พกพา และทำการปรับปรุงข้อมูลไวรัส (Virus Pattern) ให้ทันสมัยอยู่เสมอ

จ) ต้องทำการสำรองข้อมูลสารสนเทศที่อยู่ในอุปกรณ์พกพาบนเครื่องคอมพิวเตอร์แม่ข่าย หรือหากจำเป็นสามารถสำรองข้อมูลสารสนเทศบนสื่อบันทึกพกพา

ฉ) ข้อมูลสารสนเทศสำรองบนสื่อบันทึกพกพาต้องได้รับการป้องกันตามมาตรฐานการจัดประเภทข้อมูล การจัดทำป้ายและการจัดการกับข้อมูล

ช) ข้อมูลสารสนเทศสำรองบนสื่อบันทึกพกพาต้องถูกลบ หรือทำลายอย่างปลอดภัยตามมาตรฐานการกำจัดสื่อเมื่อไม่ได้ใช้งาน

หมวดที่ 3
ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล

3.1 การปฏิบัติงานในหน่วยงาน

3.1.1 หน้าที่ความรับผิดชอบของผู้บริหารของหน่วยงาน

(1) ต้องสรุปย่อเกี่ยวกับบทบาท หน้าที่ความรับผิดชอบ และความคาดหวังในการรักษาความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรทุกคน รวมถึงผู้รับจ้างก่อนเริ่มต้นทำงาน

(2) ผู้ใช้งานทุกคน รวมถึงผู้ใต้บังคับบัญชาต้องได้รับการอบรมและแจ้งถึงข้อมูลใหม่ๆ เช่น นโยบาย กระบวนการต่างๆ ซึ่งรวมไปถึงข้อกำหนดด้านความปลอดภัย มาตรการทางด้านการดำเนินงาน และการใช้อุปกรณ์ประมวลผลสารสนเทศเป็นประจำทุกปี

(3) ต้องทำการประกาศใช้ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศต่างๆ ที่เหมาะสม (นโยบาย, มาตรฐาน, แนวทางปฏิบัติ หรือกระบวนการ) กับหน่วยงานภายนอกก่อนเริ่มทำงาน

3.1.2 การสร้างความตระหนักรู้ การให้ความรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

(1) จัดฝึกอบรมการปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

(2) ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

3.1.3 กระบวนการทางวินัย

หากพบว่ามีการกระทำผิดระเบียบและนโยบายด้านความมั่นคงปลอดภัยของหน่วยงาน ให้ปฏิบัติตามข้อบังคับของ สป. โดยต้องมีการสอบสวนและให้ความเป็นธรรมต่อบุคลากรก่อนดำเนินการกระบวนการทางวินัย

หมวดที่ 4
การบริหารจัดการสินทรัพย์

4.1 หน้าที่ความรับผิดชอบต่อสินทรัพย์

4.1.1 บัญชีรายการสินทรัพย์

ผู้บริหารจัดให้มีการจัดทำบัญชีรายการสินทรัพย์ทั้งหมดที่อยู่ภายใต้ขอบเขตการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

(1) สินทรัพย์ทั้งหมดที่เกี่ยวข้องกับการดำเนินงานจะต้องได้รับการจัดเก็บในรายการสินทรัพย์ โดยครอบคลุมถึงสินทรัพย์ประเภทต่างๆ ดังนี้ ต่อไปนี้ ข้อมูล เครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ และอุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และอุปกรณ์เครือข่าย ซอฟต์แวร์ และโปรแกรมที่ใช้สนับสนุนการปฏิบัติงาน

(2) ต้องทำการทบทวนบัญชีรายการสินทรัพย์เป็นประจำทุกปี

(3) สินทรัพย์ทางกายภาพต้องทำการติดป้ายระบุ

(4) การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของหน่วยงานจะต้องกำหนดโดยเจ้าหน้าที่ของหน่วยงานด้านสารสนเทศเท่านั้น

4.1.2 กรรมสิทธิ์ของสินทรัพย์

สินทรัพย์ทุกประเภทต้องมีผู้ดูแลและกำหนดชื่อผู้เป็นเจ้าของ โดยเจ้าของสินทรัพย์อาจเป็นบุคคลหรือหน่วยงานก็ได้ ในกรณีที่กำหนดให้กรรมสิทธิ์ของสินทรัพย์เป็นของหน่วยงาน ความรับผิดชอบต่อสินทรัพย์ดังกล่าวจะตกเป็นของหัวหน้าหน่วยงานนั้นๆ

4.1.3 การใช้สินทรัพย์อย่างเหมาะสม

(1) การใช้ระบบสารสนเทศในการดำเนินงาน

ผู้ใช้งานต้องใช้ข้อมูลในระบบสารสนเทศในการดำเนินงานอย่างระมัดระวัง ผู้ใช้งานต้องพิจารณาถึงความเหมาะสมและความสำคัญของข้อมูลก่อนการนำข้อมูลเข้าสู่ระบบสารสนเทศ

ระบบสารสนเทศในการดำเนินงานครอบคลุมถึงบริการไฟล์และสิ่งพิมพ์ ปฏิทินอิเล็กทรอนิกส์ และอินทราเน็ต (Intranet)

(2) การใช้งานทั่วไป ผู้ใช้งานต้องปฏิบัติดังต่อไปนี้

ก) ข้อมูล ข้อความ และเอกสารใดๆ ที่จัดเก็บไว้ในระบบสารสนเทศขององค์กรให้ถือเป็นสินทรัพย์ขององค์กร

ข) การใช้งานสินทรัพย์จะทำได้เฉพาะบุคลากรหรือผู้ที่ได้รับอนุญาตเท่านั้น

ค) ต้องใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานอย่างมีประสิทธิภาพ และเกิดประโยชน์สูงสุดแก่ทางราชการ

ง) การใช้งานจะต้องไม่เป็นการขัดขวางประสิทธิภาพในการปฏิบัติงานภายในองค์กร

จ) ไม่ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

ฉ) ไม่อนุญาตให้รับหรือส่งไฟล์ที่เป็นการละเมิดกฎหมาย หรือนโยบายขององค์กร

ช) บุคคลภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

(3) ผู้ใช้งานจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ ดังต่อไปนี้

ก) แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

ข) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

ค) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

ง) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

จ) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

ฉ) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

ช) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ ตามข้อ (3)

ซ) ผู้ใช้งานจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามข้อ (3) ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

(4) ผู้ใช้งานจะต้องไม่กระทำการดังต่อไปนี้

ก) เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

ข) นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

ค) เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

ง) กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

จ) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

ฉ) กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

ช) กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

ซ) จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามข้อ (4)

4.2 การจัดประเภทของข้อมูล

เพื่อกำหนดแนวปฏิบัติในการกำหนดระดับชั้นข้อมูลตามลำดับความสำคัญและความร้ายแรงหากมีการสูญเสีย/ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

4.2.1 ประเภทของข้อมูล

ข้อมูลทั้งหมดจะต้องได้รับการแยกประเภทออกตามระดับชั้นความลับและตามความจำเป็นในการใช้ในการปฏิบัติงาน ดังนี้

(1) การจำแนกระดับชั้นความลับจะต้องเป็นไปตามเอกสาร MIS-2-SD-001 แนวทางในการจัดประเภทข้อมูล และการจัดการข้อมูล

(2) เจ้าของข้อมูลจะต้องเป็นผู้กำหนดระดับชั้นความลับของข้อมูลที่ตนเป็นเจ้าของ

4.2.2 การจัดทำป้าย

ข้อมูลจะต้องได้รับการจัดทำป้ายและจัดการในแง่ของการจัดเก็บ การขนส่ง การประมวลผล และการทำลายทิ้ง โดยเป็นไปตามเอกสาร MIS-2-SD-001 แนวทางในการจัดประเภทข้อมูล และการจัดการข้อมูล

ข้อมูลที่ไม่สามารถติดป้ายได้ เช่น ไฟล์อิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์ จะต้องมีวิธีปฏิบัติปฏิบัติให้สอดคล้องกับระดับชั้นความลับสูงสุดที่มีในเครื่อง โดยไม่จำเป็นต้องติดป้าย

4.2.3 การจัดการสินทรัพย์

(1) สื่อบันทึกข้อมูลจะต้องได้รับการจัดประเภทของข้อมูลตามระดับความลับสูงสุดของข้อมูลในนั้น

(2) การเปิดเผยหรือเผยแพร่ข้อมูลจะต้องสอดคล้องกับข้อกำหนดที่ระบุไว้ในเอกสาร MIS-2-SD-001 แนวทางในการจัดประเภทข้อมูล และการจัดการข้อมูล

4.3 การจัดการสื่อบันทึก

4.3.1 การบริหารจัดการสื่อบันทึกพกพา

การบริหารจัดการสื่อบันทึกพกพาต้องเป็นไปตามเอกสาร MIS-2-SD-002 มาตรฐานการกำจัดสื่อบันทึกข้อมูล

4.3.2 การกำจัดสื่อบันทึก

(1) การกำจัดสื่อบันทึกให้ปฏิบัติตามเอกสาร MIS-2-SD-002 มาตรฐานการกำจัดสื่อบันทึกข้อมูล

(2) ต้องกำหนดอายุการใช้งานของสื่อบันทึกเพื่อให้ทราบกำหนดระยะเวลาที่ต้องมีการทำลาย

(3) ต้องลบข้อมูลเป็นการถาวร และต้องทำลายสื่อบันทึกเพื่อป้องกันการกู้คืนข้อมูลในสื่อบันทึก หรือนำสื่อบันทึกกลับมาใช้ใหม่

(4) หน่วยงานภายนอกที่จัดจ้างเพื่อทำลายสื่อบันทึกจะต้องมีการเซ็นสัญญาไม่เปิดเผยความลับข้อมูล

(5) ต้องเก็บบันทึกข้อมูลที่สำคัญก่อนทำลายสื่อบันทึกทุกครั้ง

หมวดที่ 5
การเข้ารหัส

5.1 มาตรการเข้ารหัส

กำหนดให้มีนโยบายในการควบคุมการเข้ารหัสหากมีความจำเป็นต้องใช้เทคโนโลยีดังกล่าวในการรักษาความถูกต้องสมบูรณ์ของข้อมูล และพิสูจน์ยืนยันผู้รับ-ส่ง

5.1.1 นโยบายการใช้มาตรการเข้ารหัส

ต้องมีการป้องกันกุญแจเข้ารหัสลับ (Encryption Key) ด้วยการใช้รหัสผ่าน (Password) หรือวิธีการอื่นที่เทียบเท่า และต้องไม่เก็บในที่เปิดเผยหรือเห็นได้ชัด ในกรณีของกุญแจเข้ารหัสส่วนบุคล ควรเก็บใน tamper-evident cryptographic key server หรืออย่างน้อยควรถูกเข้ารหัส

5.1.2 การบริหารจัดการกุญแจ

ต้องควบคุมให้มีการใช้กุญแจเข้ารหัส ดังนี้

(1) การบริหารจัดการกุญแจนั้นสำหรับจัดการกุญแจเข้ารหัสที่มีการแทรกแซงโดยมนุษย์

(2) หากการเข้ารหัสลับถูกใช้งานกับอุปกรณ์เฉพาะที่เพื่อทำการป้องกันข้อมูล การบริหารจัดการกุญแจเข้ารหัสลับต้องทำอย่างเป็นทางการ

(3) กิจกรรมที่เกี่ยวข้องกับการบริหารจัดการกุญแจเข้ารหัสลับต้องถูกบันทึกสำหรับการตรวจสอบ

(4) มีการเปลี่ยนกุญแจเข้ารหัสอย่างสม่ำเสมอ

(5) มีการเปลี่ยนกุญแจเข้ารหัส และทำลายรหัสเก่าเมื่อมีเหตุต้องสงสัยว่ามีบุคคลที่ไม่ได้รับอนุญาตรู้รหัสดังกล่าว

หมวดที่ 6
ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

6.1 พื้นที่การรักษาความมั่นคงปลอดภัยสารสนเทศ (Secure areas)

กำหนดให้พื้นที่ทางกายภาพมีการออกแบบเพื่อป้องกันการเข้าถึง ทำลาย ก่อกวน หรือแทรกแซง โดยไม่ได้รับอนุญาต

6.1.1 อาณาเขตการรักษาความปลอดภัยทางกายภาพ

(1) จะต้องกำหนดพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยให้ชัดเจน

(2) ต้องมีการจัดทำแผนผังที่ตั้งอาคารที่ใช้เป็นพื้นที่ในการปฏิบัติการ

(3) ประตูและหน้าต่างที่อยู่ในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย จะต้องทำจากวัสดุที่แข็งแรง เพื่อป้องกันการบุกรุกจากภายนอก

(4) จะต้องมีการควบคุมการเข้าออกพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย

6.1.2 การควบคุมการเข้าออกพื้นที่

(1) ให้หน่วยงานด้านสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(2) บุคลากรที่ได้รับสิทธิในการเข้าออกพื้นที่จะต้องเข้ากระบวนการลงทะเบียนและเพิกถอนสิทธิผู้ใช้งาน และจะได้รับการบันทึกลายนิ้วมือ (Fingerprint Scan) เพื่อใช้ในการเข้าออกพื้นที่

(3) ต้องมีการบันทึกรายละเอียดของผู้เข้าเยี่ยมทุกคนในสมุดบันทึกการเข้าเยี่ยม และผู้เข้าเยี่ยมต้องมีบัตรแสดงตนว่าเป็นผู้เข้าเยี่ยม และทำการคืนบัตรผ่านทันทีเมื่อเสร็จการเข้าเยี่ยม

6.1.3 การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงานและอุปกรณ์ต่างๆ

(1) อาคารหรือพื้นที่ที่มีการดำเนินการที่เป็นความลับหรือสำคัญ (เช่น ห้องคอมพิวเตอร์) ต้องไม่สามารถรุกล้ำเข้าไปได้ และแสดงวัตถุประสงค์ของพื้นที่ไว้เท่าที่จำเป็น ต้องไม่มีป้ายหรือรายชื่อแสดงให้เห็นเด่นชัดว่าพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยอยู่ที่ใด นอกจากนั้นในพื้นที่ดังกล่าวต้องจะมีระดับการป้องกันที่เหมาะสมและต้องมีการควบคุมการผ่านเข้าออก

(2) ในระหว่างช่วงที่ไม่มีผู้ดูแล ต้องห้ามผ่านเข้าออกห้องทำงานหรือห้องที่มีระบบประมวลผลข้อมูล โดยต้องล็อคประตูและหน้าต่าง

(3) ต้องหลีกเลี่ยงการวางอุปกรณ์เทคโนโลยีสารสนเทศไว้ในพื้นที่ส่วนกลาง

(4) สถานที่ปฏิบัติงานไม่ควรมีทางเข้าและทางออกมากนัก

6.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม

(1) ห้องคอมพิวเตอร์ต้องมีการควบคุมการเข้าออกอย่างเข้มงวด และตั้งอยู่ในพื้นที่ที่ปลอดภัยจากภัยทางธรรมชาติ เช่น ดินถล่ม หรือน้ำท่วม เป็นต้น

(2) สถานที่ปฏิบัติงานต้องมีอุปกรณ์ดับเพลิงที่เหมาะสม ในพื้นที่ที่มีความอ่อนไหวเป็นพิเศษควรพิจารณาติดตั้งระบบดับเพลิงอัตโนมัติ FM 200 หรือเทียบเท่าด้วย

(3) ต้องทำการบำรุงรักษาพื้นที่โดยทั่วไปอย่างสม่ำเสมอเพื่อกำจัดขยะที่อาจติดไฟได้

6.1.5 การทำงานในพื้นที่การรักษาความมั่นคงปลอดภัย

(1) ต้องมีผู้ติดตามบุคคล หรือหน่วยงานภายนอกที่เข้าพื้นที่ เพื่อป้องกันการดำเนินการที่ไม่ได้รับอนุญาต

(2) ต้องปิดล็อคประตูห้องที่ไม่มีการใช้งาน ปิดประตูและหน้าต่างทุกครั้งที่เลิกงาน หรือเมื่อไม่มีผู้ดูแล

(3) ไม่อนุญาตให้นำอุปกรณ์ถ่ายภาพ วิดีโอ อุปกรณ์บันทึกเสียง หรืออุปกรณ์บันทึกอื่นๆ เข้ามาภายในบริเวณดังกล่าว เว้นแต่จะได้รับอนุญาต

(4) ไม่อนุญาตให้ใช้อุปกรณ์เชื่อมต่อเคลื่อนที่ (เช่น โมเด็ม) ในขณะที่เชื่อมต่อกับเครือข่ายขององค์กร

(5) การสื่อสารให้บุคลากรได้ทราบเกี่ยวกับลูกค้าหรือปัญหาภายในจะต้องทำในกรณีที่บุคลากรนั้นจำเป็นต้องใช้ข้อมูลในการปฏิบัติงานเท่านั้น

6.1.6 พื้นที่รับส่งของ

(1) การนำสิ่งของเข้าไปส่งในห้องคอมพิวเตอร์จะต้องมีการเตรียมการล่วงหน้า และมีการลงทะเบียนก่อนนำเข้ามาในอาคาร

(2) วัสดุที่นำเข้ามาจะต้องผ่านการตรวจสอบว่ามีอันตรายหรือไม่ ก่อนทำการเคลื่อนย้ายจากพื้นที่ขนถ่ายไปยังจุดที่จะมีการใช้งาน

(3) ต้องมีการตรวจสอบถึงอันตราย และการงัดแงะของสิ่งของที่เข้ามาก่อนทำการส่งสิ่งของนั้นออกจากพื้นที่คอยไปยังพื้นที่ที่ต้องการ

6.2 อุปกรณ์และสินทรัพย์

6.2.1 การจัดตั้งและป้องกันอุปกรณ์

(1) ต้องใช้ชั้นวางอุปกรณ์ (Server Rack) สำหรับวางเซิร์ฟเวอร์และอุปกรณ์เครือข่ายที่สำคัญ

(2) ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

6.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน

(1) อุปกรณ์ทุกชนิดต้องได้รับการป้องกันจากฟิวส์ไฟฟ้า หรือเครื่องตัดกระแสไฟฟ้าที่เหมาะสม

(2) อุปกรณ์ต้องได้รับการป้องกันจากไฟกระชาก

(3) ต้องปฏิบัติตามรายละเอียดการทำงานของอุปกรณ์ และข้อกำหนดด้านสภาพแวดล้อมที่ได้รับจากผู้ผลิตเมื่อใช้งานในพื้นที่ปฏิบัติงาน

(4) ควรใช้ระบบปรับอากาศเพื่อสร้างสภาพแวดล้อมที่เหมาะสมให้กับอุปกรณ์ต่างๆ

6.2.3 ความมั่นคงปลอดภัยของสายเคเบิ้ล

(1) สายเคเบิ้ลเครือข่ายที่ใช้ในการวางระบบต้องมีการป้องกันทางแม่เหล็กไฟฟ้า

(2) สายเคเบิ้ลที่มีข้อมูลวิ่งผ่านต้องมีการป้องกันจากการดักจับข้อมูลหรือความเสียหาย

(3) ต้องแยกสายไฟทั้งหมดออกจากสายเคเบิ้ลเพื่อป้องกันการรบกวน

(4) สายสื่อสาร และสายไฟฟ้าต้องได้รับการป้องกันทางกายภาพจากความเสียหาย

(5) ต้องติดป้ายเพื่อระบุต้นทางและปลายทางของสายเคเบิ้ลที่ใช้เชื่อมต่ออุปกรณ์เทคโนโลยีสารสนเทศ

6.2.4 การบำรุงรักษาอุปกรณ์

(1) ต้องทำการบำรุงรักษาระบบควบคุมสภาพแวดล้อมและอุปกรณ์ต่างๆ ตามคำแนะนำที่ผู้ผลิตระบุไว้ รวมทั้งในระหว่างปิดระบบเพื่อบำรุงรักษาตามแผน

(2) ต้องทำการบันทึกงานซ่อมบำรุงอุปกรณ์ทั้งหมดที่เกิดขึ้น

(3) เฉพาะบุคลากรที่ผ่านการฝึกอบรมและได้รับอนุญาตเท่านั้นที่จะสามารถทำการซ่อมบำรุงระบบและอุปกรณ์ต่างๆ ในกรณีที่ใช้บริการซ่อมบำรุงจากผู้ค้าจากภายนอก จะต้องกำหนดเงื่อนไขในการบำรุงรักษาอย่างละเอียด

6.2.5 การนำสินทรัพย์ออกนอกหน่วยงาน

(1) การเคลื่อนย้ายสินทรัพย์โดยไม่ได้รับอนุญาตอาจนำไปสู่ปัญหาการขโมยสินทรัพย์ ซึ่งส่งผลให้เกิดความไม่พร้อมใช้งาน การสูญเสียความลับของข้อมูลได้ ดังนั้นในการเคลื่อนย้ายอุปกรณ์ ข้อมูล และซอฟต์แวร์ จะต้องได้รับการอนุญาตอย่างเป็นทางการจากหัวหน้างาน และต้องมีการเก็บบันทึกการอนุญาตดังกล่าวด้วย

(2) การเคลื่อนย้ายอุปกรณ์ใดๆ ต้องสามารถติดตามได้ และต้องมีการเก็บรักษาข้อมูลไว้

6.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และสินทรัพย์ที่ใช้ภายนอกหน่วยงาน

(1) เมื่อมีการนำอุปกรณ์และสื่อที่เคลื่อนย้ายได้ออกไปใช้นอกหน่วยงาน จะต้องมีการป้องกันโดยยึดตามนโยบายการใช้คอมพิวเตอร์แบบเคลื่อนที่และการปฏิบัติงานจากนอกสถานที่

(2) ในกรณีที่ต้องการนำอุปกรณ์ที่ไม่สามารถพกพาออกไปใช้ภายนอกหน่วยงาน ต้องได้รับการอนุมัติก่อน

(3) อุปกรณ์พกพา หมายรวมถึงอุปกรณ์ใดๆของหน่วยงาน หรือส่วนตัวที่สามารถพกพา และสามารถเก็บหรือประมวลผลข้อมูลของหน่วยงานได้

6.2.7 ความมั่นคงปลอดภัยในการกำจัดอุปกรณ์ที่ไม่ใช้แล้วหรือการนำอุปกรณ์กลับมาใช้ใหม่

(1) หากทำการกำจัดอุปกรณ์ที่ไม่ใช้แล้ว หรือนำอุปกรณ์กลับมาใช้อย่างไม่ถูกต้อง อาจเกิดผลกระทบด้านความมั่นคงปลอดภัยกับหน่วยงานเนื่องจากข้อมูลภายในอุปกรณ์ต่าง ดังนั้นหน่วยงานต้องทำการลบสื่อบันทึกก่อนทำการกำจัดอุปกรณ์ใดๆ

(2) สื่อบันทึกที่อยู่ในอุปกรณ์ที่ต้องการกำจัดหรือนำกลับมาใช้ใหม่ต้องได้รับการตรวจเพื่อยืนยันว่าข้อมูลสำคัญต่างๆ และซอฟต์แวร์ลิขสิทธิ์ได้ถูกลบ หรือบันทึกข้อมูลทับ โดยไม่สามารถกู้คืนและนำกลับมาใช้ได้

6.2.8 อุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

ให้หน่วยงานด้านสารสนเทศกำหนดมาตรการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแลดังต่อไปนี้

(1) ผู้ใช้งานออกจากระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน หรือไม่อยู่หน้าจอเป็นเวลานาน

(2) ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

(3) ผู้ใช้งานล๊อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่มีดูแล

(4) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกันการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

(5) เมื่อไม่มีผู้ใช้งานระบบสารสนเทศ ระบบจะยุติการใช้งานระบบสารสนเทศทันที

6.2.9 นโยบายในการเก็บโต๊ะทำงานและปิดหน้าจอ

(1) บุคลากรต้องมั่นใจว่าไม่มีเอกสารสำคัญ หรือสื่อบันทึกดิจิตอลต่างๆ เช่น แผ่นซีดี เทปบันทึกข้อมูล วางไว้บนโต๊ะทำงานเมื่อจบการทำงานในแต่ละวัน หรือเมื่อไม่มีผู้ดูแลโต๊ะทำงานเป็นระยะเวลาหนึ่ง โดยให้จัดการตามประเภทข้อมูลที่กำหนดในแนวทางในการจัดประเภทข้อมูล และการจัดการข้อมูล

(2) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screensaver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน (สูงสุด 10 นาที) หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(3) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

หมวดที่ 7
ความมั่นคงปลอดภัยในการดำเนินงาน

7.1 กระบวนการดำเนินงานและหน้าที่ความรับผิดชอบ

7.1.1 การบริหารจัดการการเปลี่ยนแปลง

การเปลี่ยนแปลงใดๆ ในระบบขั้นตอนการปฏิบัติงานจะต้องสอดคล้องกับ MIS-2-PR-005 ขั้นตอนปฏิบัติการดำเนินงานเพื่อบริหารการเปลี่ยนแปลง (Change Management Procedure) โดยต้องมีแนวปฏิบัติดังนี้

(1) มีการขออนุมัติการเปลี่ยนแปลงก่อนดำเนินการทุกครั้ง

(2) หลีกเลี่ยงการดำเนินงานในช่วงเวลาที่มีการใช้งานเป็นจำนวนมากเพื่อหลีกเลี่ยงผลกระทบที่อาจเกิดขึ้นกับผู้ใช้

(3) ประเมินผลกระทบจากการเปลี่ยนแปลงและกำหนดแผนสำรอง (Fallback Plan) เพื่อใช้กู้คืนหากการดำเนินงานไม่สัมฤทธิ์ผล

7.1.2 การบริหารจัดการทรัพยากรสารสนเทศ

(1) ทรัพยากรคอมพิวเตอร์และระบบสารสนเทศ

ก) ต้องมีการวางแผนระดับความต้องการทรัพยากรคอมพิวเตอร์ก่อนทำการเพิ่มระบบคอมพิวเตอร์เพื่อให้มั่นใจว่าขนาดของระบบที่ใช้งานอยู่เพียงพอที่จะรองรับปริมาณการใช้งานที่เพิ่มขึ้น

ข) ต้องมีการเฝ้าระวังการใช้งานคอมพิวเตอร์เพื่อลดโอกาสความล้มเหลวที่จะเกิดขึ้น ต้องระบุการใช้งานอุปกรณ์หลักเพื่อทำการเฝ้าระวังที่รวมถึงปริมาณงานของ CPU การใช้งานหน่วยความจำ และการใช้งานดิสก์เก็บข้อมูล

ค) ต้องกำหนดระดับเตือนภัย และระดับวิกฤตของการใช้ทรัพยากร และทำการวัดเปรียบเทียบสมรรถนะ

- ในกรณีที่การใช้ทรัพยากรถึงระดับเตือนภัย องค์กรต้องสำรวจหาทางเลือกอื่นๆ เพื่อลดการใช้งานทรัพยากร
- ในกรณีที่การใช้ทรัพยากรถึงระดับวิกฤต องค์กรต้องตัดสินใจเพื่อให้มีทรัพยากรเพียงพอตามที่ต้องการ

(2) ทรัพยากรในระบบเครือข่าย

ก) ต้องทำการระบุและปฏิบัติตามกระบวนการในการเฝ้าระวัง ดูแนวโน้ม และการวางแผนระดับความต้องการทรัพยากรของปริมาณการใช้งานระบบเครือข่ายและอุปกรณ์ระบบเครือข่ายเป็นประจำ

ข) ข้อมูลเครือข่ายทั้งหมด เช่น การตั้งค่า, กฎ, การควบคุมการเข้าถึง, ตารางการจัดเส้นทาง (routing table) ต้องได้รับการป้องกันจากการเข้าถึงที่ไม่ได้รับอนุญาต การปรับแต่ง การลบและการทุจริต

ค) ต้องมีการเฝ้าระวังเครือข่ายในส่วนของการใช้งานแบนด์วิดท์ และมีการจัดการบริการให้เหมาะสมกับการดำเนินงาน

ง) ต้องมีการกำหนดระดับเตือนภัยและระดับวิกฤตของการใช้งานเครือข่าย และทำการเปรียบเทียบกับเกณฑ์นี้

- ในกรณีที่การใช้งานถึงระดับเตือนภัย องค์กรต้องสำรวจหาทางเลือกอื่นๆ เพื่อลดการใช้งาน
- ในกรณีที่การใช้งานถึงระดับวิกฤต องค์กรต้องตัดสินใจเพื่อให้มีทรัพยากรเพียงพอตามที่ต้องการ

7.1.3 การแบ่งแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงานจริงออกจากกัน

(1) ต้องแยกซอฟต์แวร์สภาพแวดล้อมในการพัฒนา การทดสอบ และการปฏิบัติงานให้อยู่ในโดเมนหรือไดเร็กทอรี่ที่ต่างกันออกไป

2) ระบบพัฒนา และระบบที่ให้บริการต้องไม่ใช้หน่วยประมวลผลเดียวกัน

7.2 การป้องกันโปรแกรมประสงค์ร้าย

7.2.1 มาตรการป้องกันโปรแกรมประสงค์ร้าย (Malware)

(1) เครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

(2) ผู้ใช้งานต้องทำการอัพเดท (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

(3) ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

(4) หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์อื่นๆ

(5) ก่อนการใช้งานสื่อบันทึกพกพา ต้องมีการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware)

(6) ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ (Information) ผ่านทางระบบเครือข่ายผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง

(7) ผู้ใช้งานต้องทำการตรวจสอบไฟล์ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันโปรแกรมประสงค์ร้าย (Malware) เป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

7.3 การสำรองข้อมูล

7.3.1 ต้องจัดทำสำเนาข้อมูลและซอฟต์แวร์และทำการเก็บโดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

7.3.2 ต้องมีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติต้องแยกตามระบบสารสนเทศแต่ละระบบ

7.3.3 ต้องจัดเก็บข้อมูลสำรองในสื่อเก็บข้อมูล และจัดทำรายการบันทึกให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองต้องจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ในสถานที่จัดทำระบบสำรอง และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

7.4 การบันทึกข้อมูลเหตุการณ์ (Logging) และการเฝ้าระวัง

7.4.1 การบันทึกเหตุการณ์ (Event Logging)

(1) ต้องมีการระบุและตกลงถึงข้อมูลที่ต้องทำการบันทึก โดยจะต้องประกอบไปด้วยข้อมูลอย่าง ดังต่อไปนี้

ก) รหัสประจำตัวผู้ใช้

ข) วันที่และช่วงเวลาที่เข้าใช้งานและออกจากการใช้งาน

ค) เครื่องคอมพิวเตอร์ อุปกรณ์ หรือตำแหน่งที่ใช้ในการเข้าใช้งาน หากสามารถระบุได้

ง) บันทึกการพยายามเข้าใช้งานระบบทั้งที่ประสบความสำเร็จและที่ถูกปฏิเสธ

จ) บันทึกการพยายามเข้าใช้งานโปรแกรมทั้งที่ประสบความสำเร็จและที่ถูกปฏิเสธ หากสามารถทำได้

7.4.2 การป้องกันบันทึกข้อมูล

ต้องมีการป้องกันบันทึกข้อมูลการใช้งานจากการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและต้องมีการบันทึกการเข้าใช้งานบันทึกข้อมูลการใช้งานด้วย

7.4.3 บันทึกการดำเนินการของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ

(1) กิจกรรมต่างๆของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องได้รับการเฝ้าระวัง และต้องแจ้งให้ทั้งสองส่วนทราบ ซึ่งรวมไปถึง การเข้า-ออกจากระบบ ฟังก์ชั่นการบริหารจัดการไฟล์ ฟังก์ชั่นหลักฐานการตรวจสอบ

(2) ต้องทำการสำรองข้อมูล และเก็บรักษาข้อมูลการปฏิบัติงานไว้เพื่อการสืบสวน ข้อมูลการปฏิบัติงานต้องได้รับการปกป้องจากการทุจริต

(3) ต้องมีการบันทึกการใช้งานผ่านสิทธิพิเศษของผู้ดูแลระบบ

(4) ต้องมีการบันทึกการบริหารจัดการผู้ใช้งานจัดทำโดยผู้ดูแลระบบ

7.4.4 การตั้งเวลาให้ตรงกัน

ต้องมีการตั้งเวลาของระบบทั้งหมดให้ตรงกันเพื่อช่วยในการวิเคราะห์ลำดับการเกิดขึ้นของเหตุการณ์

7.5 การควบคุมซอฟต์แวร์ปฏิบัติการ

7.5.1 การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ

(1) ต้องงกำหนดรายการซอฟต์แวร์ที่ใช้ในองค์กร

(2) ห้ามนำซอฟต์แวร์ที่ไม่ได้รับอนุญาตมาใช้ในองค์กร

(3) ห้ามดาวน์โหลดโปรแกรมต่างๆ และแจ้งให้ทุกคนในองค์กรทราบและปฏิบัติตามอย่างเคร่งครัด

(4) การปรับปรุงรายการซอฟต์แวร์ดำเนินงานซึ่งสนับสนุนหน้าที่สำคัญต่างๆ ต้องกระทำโดยเจ้าหน้าที่ที่ได้รับแต่งตั้งเท่านั้น และต้องบันทึกความเคลื่อนไหวทั้งหมดของรายการโปรแกรมที่ใช้ในการดำเนินงาน

7.6 การบริหารจัดการช่องโหว่ทางเทคนิค

7.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค

(1) ต้องจัดกลุ่มช่องโหว่ต่างๆที่ระบุไว้ตามระดับภัยคุกคาม และทำการปิดช่องโหว่ตามกรอบเวลาและความสำคัญของระบบ

ก) ระดับวิกฤต ภายใน 1 เดือน

ข) ระดับสูง ภายใน 2 เดือน

ค) ระดับกลาง ภายใน 3 เดือน

ง) ระดับเตือนภัย ขึ้นอยู่กับดุลยพินิจของเจ้าของระบบ

(2) การปิดช่องโหว่ต้องได้รับการประเมิน การทดสอบ และการประเมินผลก่อนทำการติดตั้ง เพื่อให้เกิดประสิทธิภาพและลดผลกระทบที่อาจเกิดขึ้น

(3) ต้องทำการปิดช่องโหว่ของซอฟต์แวร์ที่สามารถลด หรือกำจัดจุดอ่อนด้านความมั่นคงปลอดภัยได้

(4) ถ้าไม่สามารถทำการปิดช่องโหว่ตามกรอบเวลาที่กำหนดไว้ได้ ต้องทำการพิจารณาถึงมาตรการควบคุมต่างๆ เหล่านี้

ก) ทำการปิดบริการที่เกี่ยวข้องกับช่องโหว่เหล่านั้น

ข) ปรับ หรือเพิ่มการควบคุมการเข้าถึงที่ไฟร์วอลล์

ค) เพิ่มการเฝ้าระวังเพื่อตรวจจับ หรือป้องกันการจู่โจม

ง) เพิ่มการตระหนักรู้ถึงช่องโหว่

จ) ทำการปิดช่องโหว่ในระบบสำคัญที่มีความสำคัญรองลงมา

7.6.2 ข้อจำกัดการติดตั้งซอฟต์แวร์

(1) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(2) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานได้ เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงานด้านสารสนเทศหรือผู้ที่ได้รับมอบหมาย

หมวดที่ 8
ความมั่นคงปลอดภัยในการสื่อสารข้อมูล

8.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย

8.1.1 ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษรแล้ว

8.1.2 ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน เป็นต้น

8.1.3 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

8.1.4 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือสินทรัพย์ทางปัญญา

8.1.5 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

8.1.6 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

8.1.7 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

8.2 การถ่ายโอนข้อมูลสารสนเทศ

8.2.1 นโยบายและกระบวนการในการการถ่ายโอนข้อมูลสารสนเทศ

(1) การแลกเปลี่ยนข้อมูลสารสนเทศในองค์กร

การแลกเปลี่ยนข้อมูลสารสนเทศภายในองค์กรจะต้องปฏิบัติตามเอกสาร MIS-2-SD-001 แนวทางในการจัดประเภทข้อมูล และการจัดการข้อมูล

(2) การแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กร

เจ้าหน้าที่ที่เกี่ยวข้องในกางกับการจัดทำข้อกำหนดเกี่ยวกับการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กรต้อง ประเมินความเสี่ยงของในการเข้ามาใช้ข้อมูลจากโดยหน่วยงานภายนอก โดยพิจารณาประเด็นต่างๆ ดังต่อไปนี้

ก) รูปแบบของการเข้าถึงข้อมูลสารสนเทศ

ข) ประเภทของข้อมูลสารสนเทศที่ต้องการใช้ในการแลกเปลี่ยน

ค) มาตรฐานทางเทคนิคในการบันทึกและอ่านข้อมูลสารสนเทศ ตลอดจนซอฟต์แวร์ที่เกี่ยวข้อง

ง) ข้อมูลหรือซอฟต์แวร์ที่ต้องการจะส่ง หรือมาตรการ/กระบวนการในการแลกเปลี่ยนสื่อบันทึกข้อมูล

จ) มาตรการอื่นๆ ที่จำเป็นในการป้องกันข้อมูลที่สำคัญ เช่น การใช้กุญแจในการเข้ารหัสข้อมูล เป็นต้น

ฉ) ทบทวนมาตรการ (Control) ตามที่ได้กำหนดไว้สำหรับการเข้าออกสถานที่ตลอดจนการเข้าถึงระบบ หากมีความจำเป็นอาจเพิ่มมาตรการเพื่อลดความเสี่ยงที่มีแนวโน้มว่าจะเกิดขึ้น ทั้งนี้มาตรการทั้งหมดต้องได้รับการวางแผนและนำมาใช้อย่างเป็นทางการต่อไป

(3) ต้องมีสัญญาหรือข้อตกลงเพื่อระบุความรับผิดชอบของฝ่ายที่รับข้อมูล รวมทั้งระบุมาตรฐานในบรรจุเอกสารหรือข้อมูล และการส่งอย่างชัดเจน

(4) หน่วยงานภายนอกทั้งหมดต้องเข้าร่วมลงนามในสัญญาที่ว่าด้วยข้อกำหนดด้านความมั่นคงปลอดภัยในการแลกเปลี่ยนข้อมูลสารสนเทศ รวมถึง

ก) การจัดส่งข้อมูล และ/หรือ ซอฟต์แวร์

ข) การจัดการแลกเปลี่ยนสื่อบันทึกข้อมูล

8.2.2 การส่งข้อความแบบอิเล็กทรอนิกส์

(1) มิให้ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

(2) การส่งข้อความ รูปภาพ หรือวัสดุใดๆ ซึ่งองค์กรเห็นว่าเป็นสิ่งผิดกฎหมาย สร้างความอับอาย คุกคาม ก้าวร้าว สร้างความเกลียดชังหรือสนับสนุนให้มีการดำเนินการซึ่งถือเป็นความผิดทางอาญา สร้างความวุ่นวายให้กับพลเรือนหรือเป็นการละเมิดกฎหมายใดๆ

(3) ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งาน และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

(4) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

(5) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ต้องระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

(6) จดหมายอิเล็กทรอนิกส์ (e-mail) ทุกฉบับต้องระบุถ้อยความการรักษาความลับข้อมูล และถ้อยความการปฏิเสธความรับผิดของข้อมูลภายในจดหมายอิเล็กทรอนิกส์ (e-mail)

8.2.3 ข้อตกลงในการรักษาความลับ

หน่วยงานภายนอกจะต้องลงนามในสัญญาการรักษาข้อมูลที่เป็นความลับสำหรับหน่วยงานภายนอก

หมวดที่ 9
การจัดหา การพัฒนาและการบำรุงรักษาระบบ

9.1 ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

9.1.1 การวิเคราะห์ และการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

(1) ข้อกำหนดด้านความปลอดภัยต้องมีการระบุในระหว่างขั้นตอนการกำหนดความต้องการของผู้ใช้งาน

(2) ข้อกำหนดด้านความปลอดภัยขั้นต่ำควรประกอบด้วยด้านต่างๆ ต่อไปนี้

ก) การระบุและการตรวจสอบยืนยันตัวบุคคลของผู้ใช้งาน

ข) การควบคุมการเข้าถึงและการอนุญาตให้ใช้งาน

ค) การป้องกันความลับและความสมบูรณ์ครบถ้วนของรายการเปลี่ยนแปลงหรือข้อมูล

ง) ข้อกำหนดการตรวจสอบ

จ) ข้อกำหนดของกฎหมาย หน่วยงานกำกับดูแล และการปฏิบัติให้เป็นไปตามกฎหมาย

9.2 ความมั่นคงปลอดภัยในกระบวนการพัฒนาและสนับสนุน

9.2.1 ข้อจำกัดในการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Software Package)

(1) ห้ามมิให้มีการเปลี่ยนแปลงใดๆ บนซอฟต์แวร์สำเร็จรูป

(2) หากต้องทำการเปลี่ยนแปลงใดๆ บนซอฟต์แวร์สำเร็จรูป ต้องทำการประเมินถึงผลกระทบของการเปลี่ยนแปลงซอฟต์แวร์

(3) ต้องได้รับการยินยอมจากผู้ให้บริการก่อนทำการเปลี่ยนแปลงใดๆ เพื่อป้องกันการละเมิดสิทธิทางปัญญา

(4) การเปลี่ยนแปลงซอฟต์แวร์มาตรฐานตามความต้องการของผู้ซื้อต่อ จะต้องได้รับการสนับสนุนจากผู้ให้บริการ

9.2.2 การทดสอบเพื่อตรวจรับระบบสารสนเทศ

(1) จะต้องมีเกณฑ์ในการตรวจรับระบบสารสนเทศทุกระบบที่มีการพัฒนาขึ้นมาใหม่หรือมีการปรับปรุงประสิทธิภาพเพิ่มเติม โดยเกณฑ์ที่ใช้ในการตรวจรับจะต้องเป็นเกณฑ์ที่กำหนดอย่างละเอียด ผ่านการอนุมัติ มีการจัดทำเป็นลายลักษณ์อักษร และผ่านการทดสอบการใช้งานแล้ว

(2) ทีมผู้พัฒนาระบบต้องไม่เป็นผู้ทำการทดสอบเพื่อตรวจรับระบบสารสนเทศ

9.3 ข้อมูลสำหรับการทดสอบระบบสารสนเทศ

9.3.1 การป้องกันข้อมูลสำหรับการทดสอบระบบสารสนเทศ

ต้องได้รับการอนุญาตก่อนนำสำเนาข้อมูลปฏิบัติการไปใช้ในการทดสอบระบบสารสนเทศทุกครั้ง

หมวดที่ 10
ความสัมพันธ์กับผู้ให้บริการภายนอก

10.1 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก

10.1.1 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

ข้อตกลงกับบุคคลภายนอกจะต้องระบุถึงการให้ความสำคัญกับความปลอดภัยที่เกี่ยวข้องดังต่อไปนี้

(1) การจัดหมวดหมู่ข้อมูลและการจัดการกับข้อมูล

(2) ระดับเป้าหมายของการให้บริการที่ยอมรับได้

(3) ความรับผิดของทั้งสองฝ่าย

(4) การป้องกันสิทธิในทรัพย์สินทางปัญญา (IPR) และลิขสิทธิ์ของงานที่ทำร่วมกัน

(5) การจัดหาการควบคุมการเข้าเข้าใช้งานทั้งแบบเข้ามาใช้ถึงตัวเครื่องและแบบผ่านทางระบบเครือข่าย (รวมถึงการเข้าใช้งานแบบพิเศษ)

(6) สิทธิในการตรวจสอบความรับผิดชอบตามสัญญาหรือการตรวจสอบที่ดำเนินการโดยบุคคลที่สาม

(7) การเกี่ยวข้องของบุคคลภายนอกโดยกับผู้รับจ้างช่วงอื่น

(8) ข้อกำหนดในการเก็บรักษาไว้ซึ่งรายชื่อของผู้ที่ได้รับอนุญาตใช้บริการ และสิทธิอื่นๆ

(9) สิทธิในการเฝ้าระวังและยกเลิกกิจกรรมของผู้ใช้

(10) ข้อกำหนดในการทำสำเนา และเปิดเผยข้อมูลองค์กร

(11) การคืน หรือการทำลายข้อมูลต่างๆเมื่อสัญญาจบสิ้น

(12) ข้อกำหนดในการป้องกันซอฟต์แวร์ประสงค์ร้าย

10.1.2 ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อตกลงกับผู้ให้บริการภายนอกต้องรวมความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

หมวดที่ 11
การบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

11.1 การบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ และการปรับปรุง

11.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ

ต้องมีการกำหนดขั้นตอนการจัดการเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อจัดการเหตุการณ์ในหลายๆ ลักษณะที่เกิดขึ้น

(1) ระบบข้อมูลขัดข้อง และไม่สามารถใช้บริการได้

(2) โปรแกรมประสงค์ร้ายต่อระบบ

(3) การถูกโจมตีที่ทำให้เครื่องเป้าหมายไม่สามารถให้บริการได้

(4) ความผิดพลาดอันเป็นผลจากข้อมูลที่ไม่สมบูรณ์หรือไม่ถูกต้อง

(5) การล่วงละเมิดความลับและความครบถ้วนสมบูรณ์ของข้อมูล

(6) การใช้ระบบข้อมูลโดยมิชอบ

11.1.2 การเก็บรวบรวมหลักฐาน

อาจต้องมีการเก็บรักษาหลักฐานสนับสนุนอื่นๆ อาทิ จดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ดูแลการเข้าถึง ข้อยกเว้น ไฟร์วอลล์ และระบบตรวจจับการบุกรุก และหลักฐานที่เกี่ยวข้องอื่นๆ โดยวิธีการเก็บรวบรวมหลักฐานต้องสอดคล้องกับแนวปฏิบัติการจัดเก็บและจัดการกับหลักฐาน ตามเอกสาร MIS-2-SD-003

หมวดที่ 12
ความสอดคล้องในการปฏิบัติต่อข้อกำหนด

12.1 ความสอดคล้องในการปฏิบัติต่อข้อกำหนดทางกฎหมายและสัญญา

12.1.1 สิทธิในทรัพย์สินทางปัญญา

(1) ไม่คัดลอกโปรแกรมต่างๆ ที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(2) จัดให้มีการจัดซื้อซอฟต์แวร์จากส่วนกลางเพื่อควบคุมและบริหารจัดซื้อและการจัดเก็บ และรักษาเอกสารการอนุญาตใช้ในสิทธิต่างๆ

(3)สร้างรายการฐานข้อมูลของซอฟต์แวร์ที่ใช้ในองค์กรและมีการปรับปรุงรายการให้ถูกต้องสม่ำเสมอเพื่อทราบถึงรายการของซอฟต์แวร์ที่จำเป็นต้องใช้

(4) แต่งตั้งผู้รับผิดชอบเพื่อดูแลและป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์ในองค์กรและตรวจสอบอย่างสม่ำเสมอทุกปี

(5) เจ้าของระบบแต่ละรายต้องมั่นใจว่าระบบของตนเป็นไปตามข้อกำหนดของกฎหมายและหน่วยงานกำกับดูแลทั้งหมด ส่วนใดที่เบี่ยงเบนไปจากกฎหมายที่ใช้อยู่ในปัจจุบันต้องจัดทำเป็นเอกสารในเอกสารระบบ

12.1.2 การป้องกันบันทึกข้อมูล

(1) บันทึกข้อมูลที่มีความสำคัญขององค์กรต้องได้รับการป้องกันจากการสูญหาย การทำลายและการปลอมแปลง

(2) ต้องมีการระบุบันทึกข้อมูลตามประเภทของบันทึกข้อมูล ระยะเวลาการเก็บรักษา และประเภทของสื่อบันทึก

(3) ประเภทของบันทึกข้อมูลแบ่งเป็น ข้อมูลสำหรับการดำเนินงาน ข้อมูลการเงิน ข้อมูลส่วนบุคคล รหัสลับ ข้อมูลบันทึกเหตุการณ์ (logs)

(4) ประเภทของสื่อบันทึกแบ่งเป็น กระดาษ ไมโครฟิช (Microfiche) แผ่นเก็บข้อมูลประเภทแถบแม่เหล็ก (Magnetic) เช่น แผ่น Floppy Disk, Zip Disk หรือ Magnetic Tape หรือ แผ่นเก็บข้อมูลประเภทใช้แสง (Optical) เช่น CD-ROM, DVD-ROM เป็นต้น หรือ อุปกรณ์เก็บข้อมูลประเภทหน่วยความจำ (Memory) เช่น Flash Drive, Thumb Drive, Memory Stick เป็นต้น

(5) การเก็บรักษาและการควบคุมดูแลบันทึกข้อมูลองค์กรต้องทำตามระดับชั้นความลับข้อมูลที่กำหนดไว้และสอดคล้องตามเอกสาร MIS-2-SD-001 แนวทางในการจัดประเภทข้อมูล และการจัดการข้อมูล

12.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ

12.2.1 ต้องให้มีการทบทวนด้านความมั่นคงปลอดภัยข้อมูลโดยคณะกรรมการที่ สป. แต่งตั้ง และต้องมีการตรวจสอบความมั่นคงปลอดภัยของข้อมูลอย่างน้อยปีละครั้งเพื่อหาจุดที่ไม่เป็นไปตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ และ/หรือ กฎหมาย ประกาศ ระเบียบอื่นๆ ที่เกี่ยวข้อง

12.2.2 ผู้ตรวจสอบที่ได้รับมอบหมายให้ทำการตรวจสอบความมั่นคงปลอดภัยข้อมูลจะต้องไม่เป็นผู้ตรวจสอบงานของตนเอง และให้การปฏิบัติให้เป็นไปตามนโยบายและมาตรฐานด้านความปลอดภัย

12.2.3 หัวหน้างานจะต้องรับผิดชอบต่อบริการที่จัดทำโดยบุคลากรในทีมในด้านการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูล โดยมีความรับผิดชอบในการดูแล และหรือกำกับการทำงานของบุคลากรในทีมเพื่อให้เป็นไปตามนโยบาย ขั้นตอน และมาตรฐานด้านความปลอดภัยที่เกี่ยวข้อง ในกรณีที่เจอเหตุละเมิดด้านความมั่นคงปลอดภัยจากการปฏิบัติงานของลูกทีม ให้ดำเนินการร้องขอให้ทำการสอบสวน เพื่อให้เข้าสู่ขั้นตอนของกระบวนการแก้ไขปัญหา

12.2.4 หัวหน้างานต้องมีหน้าที่รับผิดชอบในการปฏิบัติตามข้อที่เกี่ยวข้องในนโยบายความมั่นคงปลอดภัย

12.2.5 การทบทวนความสอดคล้องทางเทคนิค ต้องมีการประเมินเครือข่ายและมาตรการความมั่นคงปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอโดยบุคลากรทางเทคนิคและด้านความมั่นคงปลอดภัยที่เหมาะสม เพื่อทดสอบว่าการควบคุมด้านความมั่นคงปลอดภัยต่างๆ เพียงพอต่อปัจจัยเสี่ยงล่าสุดต่างๆ

หมวดที่ 13
การบริหารจัดการความเสี่ยง

13.1 แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

ต้องมีการบริหารจัดการความเสี่ยงตามที่ โดยมีองค์ประกอบในการบริหารจัดการความเสี่ยงดังนี้

13.1.1 ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน เพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ผลที่ได้จากระเบียบวิธีการประเมินความเสี่ยงสามารถนำมาเปรียบเทียบและทำซ้ำได้

(1) ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

(2) ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

(3) ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

(4) ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

(5) ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

13.1.2 กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

13.1.3 การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

(1) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

(2) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

(3) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

13.1.4 ดำเนินการตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศของหน่วยงาน เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายในของหน่วยงาน ทั้งนี้ ผู้ตรวจต้องไม่มีส่วนเกี่ยวข้องและไม่มีส่วนได้ส่วนเสียกับงานที่ต้องการตรวจ

13.1.5 ในกรณีที่หน่วยงานไม่มีผู้ทำหน้าที่ในการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ให้ผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยสารสนเทศจากภายนอกดำเนินการดังกล่าว

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงศึกษาธิการ อาคารรัชมังคลาภิเษก ชั้น 4

โทร 0 2628 5643, 0 2281 9809 ต่อ 441-443

โทรสาร 0 2282 9241

www.mis.moe.go.th