แนวทางการปฏิบัติด้านความมั่นคงปลอดภัย
ระบบเทคโนโลยีสารสนเทศ
กองกฎหมาย
กรมสนับสนุนบริการสุขภาพ

กองกฎหมาย

ธันวาคม ๒๕๖๕

แนวทางการปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
กองกฎหมาย กรมสนับสนุนบริการสุขภาพ

กองกฎหมาย ได้จัดทำนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศประจำปีงบประมาณ ๒๕๖๕ เพื่อให้ควบคุมการบริหารจัดการการปฏิบัติงานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกองกฎหมาย กรมสนับสนุนบริการสุขภาพ ให้เป็นไปได้อย่างมีประสิทธิภาพ จึงได้วางนโยบายและแนวทางปฏิบัติในการควบคุมการปฏิบัติงานด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยสาระสำคัญของนโยบายและแนวทางปฏิบัติฉบับนี้ประกอบด้วย

หมวด ๑ นโยบายความมั่นคงปลอดภัยในองค์กร
หมวด ๒ โครงสร้างทางด้านความมั่นคงปลอดภัย
หมวด ๓ ความมั่นคงปลอดภัยของบุคลากร
หมวด ๔ การบริหารทรัพย์สินและการจัดระดับชั้นความลับของข้อมูล
หมวด ๕ การควบคุมการเข้าถึงระบบ
หมวด ๗ การควบคุมทางกายภาพ
หมวด ๘ การป้องกันไวรัสและโปรแกรมอรรถประโยชน์
หมวด ๑๒ การบริหารปัญหาการแก้ไขปัญหาเหตุการณ์ความไม่มั่นคงปลอดภัย
ระบบความรับผิดทางละเมิดและแพ่ง
ฐานข้อมูล/ระบบสารสนเทศ

สารบัญ

แนวทางปฏิบัติ		**หน้า**
หมวด ๑	นโยบายความมั่นคงปลอดภัยในองค์กร	๑
หมวด ๒	โครงสร้างทางด้านความมั่นคงปลอดภัย	๒
หมวด ๓	ความมั่นคงปลอดภัยของบุคลากร	๓
หมวด ๔	การบริหารทรัพย์สินและการจัดระดับชั้นความลับของข้อมูล	๔
หมวด ๕	การควบคุมการเข้าถึงระบบ	๕
หมวด ๗	การควบคุมทางกายภาพ	๘
หมวด ๘	การป้องกันไวรัสและโปรแกรมอรรถประโยชน์	๑๐
หมวด ๑๒	การบริหารปัญหาการแก้ไขปัญหาเหตุการณ์ความไม่มั่นคงปลอดภัย	๑๑
ระบบความรับผิดทางละเมิดและแพ่ง		๑๓
ฐานข้อมูล/ระบบสารสนเทศ		๑๔

หมวด ๑ นโยบายความมั่นคงปลอดภัยในองค์กร

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

แนวทางปฏิบัติ

๑. การจัดทำนโยบาย

๑.๑. ต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษรและผู้บริหารผู้รับผิดชอบ และผู้ใช้งานของแต่ละกลุ่ม/ฝ่าย/งานต้องมีส่วนร่วมในการจัดทำนโยบาย และอย่างน้อยต้องได้รับอนุมัติจากคณะกรรมการรักษาความมั่นคงปลอดภัยของกองกฎหมาย

๑.๒. ต้องทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ โดยต้องมีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง ซึ่งต้องมีการระบุความเสี่ยงที่เกี่ยวข้อง จัดลำดับความสำคัญของข้อมูลและระบบคอมพิวเตอร์ กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง

๑.๓. ต้องจัดเก็บนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้อง สามารถเข้าถึงได้โดยง่าย

๒. รายละเอียดของนโยบาย

๒.๑. ต้องระบุวัตถุประสงค์และขอบเขตอย่างชัดเจน และมีเนื้อหาครอบคลุมในเรื่องต่อไปนี้

- การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
- การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
- การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
- การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
- การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
- การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

๓. การปฏิบัติตามนโยบาย

๓.๑. ต้องประกาศใช้และสื่อสารนโยบายให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้สามารถปฏิบัติตามได้ เช่น ประกาศแจ้งเวียน หรือ จัดการฝึกอบรม เป็นต้น

๓.๒. ต้องมีระบบติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัด

๓.๓. ต้องมีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยหน่วยงานที่กรมสนับสนุนบริการสุขภาพกำหนด อย่างน้อยปีละครั้ง

๓.๔. ต้องแจ้งกลุ่มเทคโนโลยีสารสนเทศและการสื่อสาร กรมสนับสนุนบริการสุขภาพโดยเร็ว เมื่อมีกรณีที่ส่งผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

๓.๕. ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน เช่น หน้าที่ของผู้ใช้งาน หน้าที่และความรับผิดชอบของเจ้าหน้าที่รักษาความปลอดภัยระบบเครือข่าย เป็นต้น

หมวด ๒ โครงสร้างทางด้านความมั่นคงปลอดภัย

วัตถุประสงค์

เพื่อกำหนดให้มีโครงสร้างองค์กรด้านการรักษาความมั่นคงปลอดภัย การแบ่งแยกอำนาจหน้าที่และให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่าย/งานด้านสารสนเทศและคอมพิวเตอร์ซึ่งเป็นการลดความเสี่ยงด้าน infrastructure risk

กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานที่เกี่ยวข้องกับนโยบายด้านความมั่นคงปลอดภัยอย่างชัดเจนและให้มีการกำหนดข้อตกลงระหว่างผู้ปฏิบัติกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร รวมทั้งมีกระบวนการให้หน่วยงานต่างๆที่เกี่ยวข้องมีส่วนร่วมและประสานให้เกิดความมั่นคงความปลอดภัยอย่างมีประสิทธิภาพ

แนวทางปฏิบัติ

๑. ผู้บริหารและหัวหน้างาน/หัวหน้าโครงการ ต้องกำหนดและส่งเสริมสนับสนุนให้เกิดโครงสร้างแผนผังสายการบังคับบัญชา และมี job description ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งานและการมอบหมายงานรวมทั้งความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่าย/งาน สารสนเทศและคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร

๒. จัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น เช่น ผู้บริหารระบบ (system administrator) เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (computer operator) เป็นต้น

๓. จัดให้มีการกำหนดข้อตกลงระหว่างผู้ปฏิบัติกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร

๔. ต้องมีกระบวนการให้หน่วยงานต่างๆที่เกี่ยวข้องมีส่วนร่วมและประสานให้เกิดความมั่นคงความปลอดภัยอย่างมีประสิทธิภาพ

หมวด ๓ ความมั่นคงปลอดภัยของบุคลากร

วัตถุประสงค์

เพื่อให้บุคลากรภายในและผู้ที่รับจ้างองค์กรเข้าใจถึงบทบาท หน้าที่ความรับผิดชอบของตน เพื่อลดความเสี่ยงจากการขโมย การฉ้อโกงและการใช้อุปกรณ์ผิดวัตถุประสงค์และการตระหนักถึงรวมถึงความเข้าใจเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัย และลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติงาน รวมทั้งให้บุคลากรหรือพนักงานผู้รับจ้างทราบการปฏิบัติในระหว่างปฏิบัติงานและเมื่อสิ้นสุดการปฏิบัติงาน/โยกย้ายหรือสิ้นสุดหน้าที่ หรือสิ้นสุดการจ้าง

แนวทางปฏิบัติ

๑. ต้องจัดระบบการสรรหาบุคลากรที่จะปฏิบัติงานและระบบควบคุมกำกับระหว่างการจ้าง/การปฏิบัติงาน รวมทั้งเมื่อสิ้นสุดการจ้าง/การพ้นจากตำแหน่งหน้าที่ โดยคำนึงถึงความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

๒. ก่อนการจ้างงาน

๒.๑ ต้องกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคลากรหรือพนักงานที่องค์กรว่าจ้าง และหรือหน่วยงานภายนอกที่องค์กรต้องการว่าจ้างให้มาปฏิบัติงานในองค์กรและจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

๒.๒ ต้องตรวจสอบคุณสมบัติของผู้สมัครและเงื่อนไขการจ้างงาน ทั้งกรณีจ้างงานเป็นพนักงาน การว่าจ้างลักษณะสัญญาจ้างและการว่าจ้างจากหน่วยงานภายนอก โดยละเอียด

๓ ระหว่างการจ้างงาน

๓.๑ กำหนดให้พนักงานหรือบุคลากรที่ได้รับการว่าจ้างให้มาปฏิบัติหน้าที่ภายในองค์กร ปฏิบัติตามมาตรการรักษาความปลอดภัยขององค์กร

๓.๒ ต้องอบรมให้ความรู้ และสร้างความตระหนัก รวมทั้งเสริมความรู้เกี่ยวกับการความมั่นคงปลอดภัยอย่างสม่ำเสมอ และการอบรมต้องครอบคลุมถึงนโยบายและขั้นตอนการปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่บุคลากรหรือพนักงานรับผิดชอบ

๓.๓ ต้องกำหนดให้มีกระบวนการทางวินัย เพื่อลงโทษพนักงานหรือบุคลากร ผู้ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านการรักษาความมั่นคงปลอดภัยขององค์กร

๔ เมื่อสิ้นสุดการจ้างงานหรือสิ้นสุดการปฏิบัติหน้าที่

๔.๑ ต้องกำหนดแนวทางการปฏิบัติเมื่อสิ้นสุดการจ้างหรือการพ้นจากหน้าที่ ต้องคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน และถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศ

หมวด ๔ การบริหารทรัพย์สินและการจัดระดับชั้นความลับของข้อมูล

วัตถุประสงค์

เพื่อบริหารจัดการทรัพย์สินและควบคุมการสูญหายของทรัพย์สิน ตลอดจนการควบคุมการเข้าถึงข้อมูล ที่มีระดับชั้นความลับแตกต่างกัน เพื่อความปลอดภัยในข้อมูลและทรัพย์สินขององค์กร

แนวทางปฏิบัติ

๑. จัดทำทะเบียนสินทรัพย์ด้านเทคโนโลยีสารสนเทศ และกำหนดผู้รับผิดชอบต่ออุปกรณ์ รวมทั้งจัดระบบบริหารจัดการทรัพย์สารสนเทศอย่างเป็นระบบ

๒. ทบทวนทะเบียนสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้มีความครบถ้วนถูกต้องเป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้งจัดทำ

๓. ระบุความเป็นเจ้าของของทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

๔. ต้องจัดทำกฎ ระเบียบหรือหลักเกณฑ์ในการนำทรัพย์สินไปใช้อย่างเป็นลายลักษณ์อักษร เช่น บันทึกการยืม-คืน ทรัพย์สิน

๕. ต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว

๖. ต้องจัดระดับชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บและเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ

๗. ต้องกำหนดวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๘. ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (storage) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (distributed database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

หมวด ๕ การควบคุมการเข้าถึงระบบ

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบเครือข่าย ระบบปฏิบัติการ แอพพลิเคชั่นและสารสนเทศที่สำคัญของหน่วยงาน ผ่านข้อกำหนดต่างๆเพื่อสร้างความปลอดภัยในการเข้าถึงสารสนเทศของหน่วยงาน

ระเบียบปฏิบัติ

๑. ต้องมีการกำหนดนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร โดยพิจารณาจากความต้องการขององค์กรและความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

๒. ต้องกำหนดให้มีขั้นตอนการปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนการบริหารจัดการการเข้าถึงของผู้ใช้งานระบบ เพื่อให้มีสิทธิต่างๆในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนการปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน

๓. ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

๔. ต้องจัดให้มีกระบวนการบริหารจัดการรหัสส่งผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านแก่ผู้ใช้งาน

๕. ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

๖. ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

๗. ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มบริการสารสนเทศที่ใช้งาน กลุ่มผู้ใช้ และกลุ่มระบบสารสนเทศ

๘. ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กรต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอปพลิเคชั่นที่ใช้ในขององค์

๙. ต้องจัดให้มีระบบการบริหารจัดการรหัสผ่านที่มีการควบคุมรหัสผ่านอย่างมีคุณภาพ

๑๐. ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้ เมื่อผู้ใช้ไม่ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

๑๑. ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

๑๒. ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชั่นต่างๆของแอฟพลิเคชั่นตามนโยบายการควบคุมการเข้าถึงสารสนเทศที่กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทผู้ใช้งาน

๑๓. ต้องมีนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านั้น

การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (user privilege)

๑. ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิ

๒. การใช้งานอินเทอร์เนต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่

๓. ควรมีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

๔. ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (log out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

๕. ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ share files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว

๖. ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติและต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง และระงับการใช้งานทันทีเมื่อพ้นระยะเวลา ดังกล่าว

การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่าน (password)

๑. ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (identification and authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี user account เป็นของตนเอง ทั้ งนี้การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและมีความรัดกุมหรือไม่นั้น จะใช้ปัจจัยดังต่อไปนี้

๑.๑ ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ ๖ ตัวอักษร

๑.๑ ควรใช้อักขระพิเศษประกอบ เช่น : ; <>เป็นต้น

๑.๒ สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๖ เดือน ส่วนผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริหารระบบ (system administrator) และผู้ใช้งานที่ติดมากับระบบ (default user) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๓ เดือน

๑.๓ ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

๑.๔ ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕๖” เป็นต้น

๑.๕ ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น

๑.๖ ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งโดยทั่วไปไม่ควรเกิน ๕ ครั้ง

๑.๗ ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย

๑.๘ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

๑.๙ ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

๑.๑๐ ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของพนักงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (default user) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่นdisable ลบออกจากระบบ หรือ เปลี่ยน password เป็นต้น

๒. ต้องมีการการบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง และต้องจัดทำแผนผังระบบเครือข่าย (network diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

หมวด ๗ การควบคุมทางกายภาพ

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงทางกายภาพ โดยมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องหรือไม่ได้รับอนุญาตก่อให้เกิดความเสียหาย หรือการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร หรือล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk)

แนวทางปฏิบัติ

๑. การควบคุมหน่วยงาน

๑.๑. การจัดการบริเวณโดยรอบหน่วยงาน เช่น ต้องจัดสรรพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบเพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของหน่วยงาน

๑.๒. การควบคุมการเข้า-ออก ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องรักษาความปลอดภัยและอนุญาตให้ผ่านเข้าออกเฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

๑.๓. การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อห้องทำงานและทรัพย์สินอื่นๆ ดังนี้

๑.๓.๑. ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องคอมพิวเตอร์ PC หรือ Notebook และอุปกรณ์ต่อพ่วง รวมทั้งอุปกรณ์ระบบเครือข่ายและทรัพย์สินด้านเทคโนโลยีสารสนเทศต่างๆ เป็นต้น ไว้ในตู้เก็บอุปกรณ์ของหน่วยงาน

๑.๓.๒. ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงาน เพื่อลดความเสี่ยงจากภัยคุกคามด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

๒. ความมั่นคงปลอดภัยของอุปกรณ์

๒.๑. การจัดวางและป้องกันอุปกรณ์ ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงาน เพื่อลดความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่รับอนุญาต

๒.๒. ระบบสนับสนุนการทำงาน ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบการระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง ระบบสายสื่อสำรอง เป็นต้น

๒.๓. ต้องกำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น การป้องกันให้พิจารณาความเสี่ยงต่ออุปกรณ์เหล่านั้น

๒.๔. ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูล เพื่อดูว่าข้อมูลสำคัญและซอฟแวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนจะทิ้งอุปกรณ์ดังกล่าว ทั้งนี้เพื่อป้องกันข้อมูลดังกล่าวหากนำอุปกรณ์กลับมาใช้อีกครั้ง

๒.๕. ต้องกำหนดระเบียบ ขั้นตอนปฏิบัติในการนำทรัพย์สินขององค์กรที่สำคัญออกนอกสำนักงาน เพื่อป้องกันการนำทรัพย์สินขององค์กรไปใช้นอกสำนักงาน โดยไม่ได้รับอนุญาต

๓. **การป้องกันความเสียหาย**จากภัยคุกคามต่างๆ เช่นไฟไหม้ น้ำท่วม แผ่นดินไหว หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

๓.๑. ระบบป้องกันไฟไหม้

๓.๑.๑. ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

๓.๑.๒. ต้องมีระบบดับเพลิง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

๓.๒. ระบบป้องกันไฟฟ้าขัดข้อง

๓.๒.๑. ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟอย่างน้อยเครื่องสำรองไฟ (UPS)

๓.๒.๒. กรณีมีระบบสารสนเทศที่สำคัญของหน่วยงาน ไปฝากให้บริการหน่วยงานอื่นดูแลบำรุงรักษา ต้องมีหลักฐานยืนยันจากหน่วยงานที่รับฝากให้บริการนั้น ว่ามีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ

๓.๒.๓. ต้องกำหนดให้เดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันการเข้าถึงโดยไม่ได้รับการอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายเหล่านั้นเสียหาย

๓.๒.๔. ต้องทำให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

๓.๓. ระบบควบคุมอุณหภูมิและความชื้น

๒.๓.๑ ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

๒.๓.๒ ต้องมีการวางแผนและคู่มือบำรุงรักษาระบบเครื่องปรับอากาศ และมีการตรวจสอบดำเนินการตามแผนงานที่กำหนดอย่างต่อเนื่อง

หมวด ๘ การป้องกันไวรัสและโปรแกรมอรรถประโยชน์

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงทางกายภาพ โดยมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องหรือไม่ได้รับอนุญาตก่อให้เกิดความเสียหาย หรือการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร หรือล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk)

แนวทางปฏิบัติ

๑. การป้องกันไวรัส

๑.๑ ต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่องเช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น

๑.๒ ควรให้ความรู้แก่ผู้ใช้งานในการป้องกันไวรัสให้แก่ผู้ใช้งานเพื่อใช้เป็นแนวทางปฏิบัติ อย่างสม่ำเสมอ

๑.๓ หากเครื่องคอมพิวเตอร์ของผู้ใช้งานท่านใดตรวจพบว่ามีไวรัส ให้ดำเนินการแจ้งเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศโดยทันที

๒. การกำหนดโปรแกรมอรรถประโยชน์

๒.๑ คณะกรรมการรักษาความมั่นคงปลอดภัยระดับหน่วยงาน ได้มีการกำหนดโปรแกรมอรรถประโยชน์ที่จะใช้ในหน่วยงาน

๒.๒. ผู้ใช้งานควรตรวจสอบโปรแกรมใช้งานในเครื่องคอมพิวเตอร์ของตนเอง หากพบว่ามีโปรแกรมอรรถประโยชน์อื่นใดที่ไม่ถูกกำหนดไว้ตามความเห็นของคณะกรรมการรักษาความมั่นคงปลอดภัยระดับหน่วยงาน ให้ดำเนินการแจ้งผู้ดูแลระบบของหน่วยงาน

๓.๓ หากผู้ใช้งานต้องการเพิ่มเติมโปรแกรมอรรถประโยชน์อื่นใดที่ไม่ถูกกำหนดไว้ตามความเห็นของคณะกรรมการรักษาความมั่นคงปลอดภัยระดับหน่วยงาน ให้แจ้งต่อคณะกรรมการเพื่อนำเข้าที่ประชุมเพื่อพิจารณา

หมวด ๑๒ การบริหารปัญหาการแก้ไขปัญหาเหตุการณ์ความไม่มั่นคงปลอดภัย

วัตถุประสงค์

เพื่อให้สามารถแก้ไขปัญหากับเหตุการณ์ที่เกิดขึ้น ที่เกี่ยวกับความมั่นคงปลอดภัยจัดทำระเบียบวิธีการปฏิบัติต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ที่กำลังจะเกิดขึ้น/ที่เกิดขึ้น ณ ขณะนั้น/หลังเกิดเหตุการณ์ขึ้นแล้ว และป้องกันการติดขัดหรือหยุดชะงักของการปฏิบัติงานในองค์กร และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

แนวทางปฏิบัติ

๑. การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย

๑.๑ ต้องกำหนดระเบียบวิธีปฏิบัติในการรายงานเมื่อพบเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอด เพื่อให้ผู้ที่รับผิดชอบสามารถทำการแก้ไขได้ทันท่วงที

๑.๒ ต้องกำหนดระเบียบวิธีปฏิบัติในการรายงานเมื่อพบจุดอ่อนที่เกี่ยวกับความมั่นคงปลอดภัย เพื่อให้ผู้ที่รับผิดชอบสามารถทำการแก้ไขหรือหาแนวทางการป้องกันได้ทันท่วงที

๒. การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

๒.๑ ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนในการปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ได้อย่างรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

๒.๒ ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยต้องแบ่งประเภทของเหตุการณ์ ปริมาณที่เกิดและค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย เพื่อเป็นการเรียนรู้จากเหตุการณ์ที่เกิดขึ้น และเตรียมการป้องกันไว้ล่วงหน้าได้

๒.๓ ต้องกำหนดการเก็บรวบรวมหลักฐานที่เกี่ยวกับความมั่นคงปลอดภัยและพบว่าเหตุการณ์ที่เกิดขึ้นมีการดำเนินการทางกฎหมายแพ่งหรืออาญา

๓. การสำรองข้อมูลและระบบสารสนเทศ

๓.๑ ต้องกำหนดมาตรการในการสร้างความต่อเนื่องให้กับองค์กรให้สามารถดำเนินต่อไปได้ในช่วงเวลาที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงักหรือล้มเหลว

๓.๒ ต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลให้เหมาะสมกับองค์กร

๓.๓ ต้องมีการบันทึกทุกครั้งเมื่อทำการสำรองข้อมูล เพื่อความถูกต้องครบถ้วน และควรตรวจสอบบันทึกอย่างสม่ำเสมอ

๔. การเก็บรักษาข้อมูลสำรองและสื่อบันทึก

๔.๑ ต้องมีการจัดเก็บสื่อบันทึกข้อมูลสำรองพร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ โดยมีระบบควบคุมการเข้าออก และระบบควบคุมสภาพแวดล้อมอย่างเหมาะสม

๔.๒ ต้องกำหนดวิธีการนำข้อมูลกลับมาใช้ ในอนาคตเมื่อต้องมีการเก็บข้อมูลเป็นระยะเวลานานเพื่อป้องกันการเข้ากันไม่ได้ของสื่อบันทึกข้อมูลกับอุปกรณ์ที่ใช้ในการดึงข้อมูล

๔.๓ ต้องมีการติดฉลากรายละเอียดให้กับสื่อบันทึกข้อมูล เพื่อให้สามารถทำการค้นหาได้อย่างสะดวกและไม่ผิดพลาด

๔.๔ ต้องมีทะเบียนควบคุมการขอใช้สื่อบันทึกข้อมูล อย่างเป็นลายลักษณ์อักษร

๔.๕ ต้องระเบียบวิธีปฏิบัติในการทำลายข้อมูลในสื่อบันทึกข้อมูลที่ไม่ได้ใช้งานแล้ว

๕. การเตรียมพร้อมกรณีฉุกเฉิน

๕.๑ ต้องมีการจัดทำแผนหรือระเบียบวิธีปฏิบัติในกรณีฉุกเฉิน เพื่อให้สามารถกู้ระบบกลับมาใช้งานได้รวดเร็วที่สุด และให้เกิดผลกระทบน้อยที่สุด

๕.๒ ต้องมีการทดสอบแผนฉุกเฉินอย่างน้อยปีละ ๒ ครั้ง โดยจำลองจากสถานการณ์จริง

๕.๓ ต้องมีการประชาสัมพันธ์แผนฉุกเฉินให้ผู้ที่เกี่ยวข้องและไม่เกี่ยวข้องทราบ เฉพาะเท่าที่จำเป็น

๕.๔ ต้องมีการจดทำบันทึกรายละเอียดของเหตุการณ์ฉุกเฉินที่เกิดขึ้น โดยต้องมีสาเหตุและวิธีแก้ไขปัญหาไว้ด้วย

๕.๕ ต้องกำหนดให้มีการคอยกำกับ ดูแล และควบคุมการปฏิบัติงานจากผู้บริหาร ให้เป็นไปตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ได้รับผิดชอบของตนเอง และต้องมีการทบทวนมาตรการด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ เพื่อให้มาตรการด้านความมั่นคงปลอดภัยมีความทันสมัยและได้ผลเป็นอย่างดี

ระบบความรับผิดทางละเมิดและแพ่ง

<u>วัตถุประสงค์</u>

กำหนดให้มีการคอยกำกับ ดูแล และควบคุมการปฏิบัติงานจากผู้บริหาร ให้เป็นไปตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ได้รับผิดชอบของตนเอง เพื่อป้องกันการละเมิดข้อกำหนดด้านความมั่นคงปลอดภัยขององค์กร

<u>ระเบียบปฏิบัติ</u>

๑. การปฏิบัติตามข้อกำหนดทางกฎหมาย

๑.๑ ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ตามข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง

๑.๒ ต้องป้องกันไม่ให้ผู้ใช้งานอุปกรณ์ประมวลผลสารสนเทศนำไปใช้งานผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต

๒. การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค

๒.๑ ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรการด้านความมั่นคงปลอดภัย

๒.๒ ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยขององค์กร

๓. การตรวจประเมินสารสนเทศ

๓.๑ ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อการปฏิบัติงาน เช่น การหยุดชะงักของระบบในระหว่างการตรวจประเมิน

๓.๒ ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศเพื่อป้องกันการใช้งานผิดวัตถุประสงค์

ฐานข้อมูล/ระบบสารสนเทศ

วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง และเพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก และการดำเนินงานที่เกี่ยวกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

แนวทางปฏิบัติ

๑. การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติ

๑.๑ ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน และปรับปรุงตามระยะเวลาอันสมควรและแจกจ่ายผู้เกี่ยวข้อง

๑.๒ ต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง และปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

๑.๓ ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบ เพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไข โดยไม่ได้รับอนุญาต หรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินขององค์กร

๑.๔ ต้องจัดให้มีการแยกระบบสำหรับการพัฒนา ทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

๒. บันทึกเพื่อการตรวจสอบ (audit logs)

๒.๑ หากระบบบริการสารสนเทศของหน่วยงาน ฝากไว้ให้หน่วยงานอื่นดูแลหน่วยงานต้องทำข้อตกลงให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (login-logout logs) บันทึกการพยายามเข้าสู่ระบบ (login attempts) บันทึกการใช้ command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๒.๒ หน่วยงาน ควรมีการตรวจสอบ โดยร้องขอรายงานการบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอจากหน่วยงานที่ให้บริการดูแลระบบสารสนเทศด้านเทคนิค

๒.๓ สำนักฯต้องทำข้อตกลงกับหน่วยให้บริการดูแบระบบสารสนเทศของสำนักฯ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๓. การเฝ้าระวังทางด้านความมั่นคงปลอดภัย

๓.๑ ต้องกำหนดให้มีการบันทึกกิจกรรมการใช้งานของผู้ใช้งาน รวมทั้งการปฏิเสธการใช้บริการระบบและเหตุการณ์ต่างๆที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

๓.๒ ต้องกำหนดให้มีขั้นตอนการปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอเพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

๓.๓ ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

๓.๔ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ

๓.๕ ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

๓.๖ต้องจัดทำเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่/เทคโนโลยีใหม่ หรือที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบ/อุปกรณ์ นั้นมาใช้งาน

๓.๗ ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืน เพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดีและควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องกับผู้ใช้งานด้วย

๓.๘ ต้องกำหนดกำหนดระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้อยู่ และต้องกำหนดไว้ในข้อตกลงการให้บริการเครือข่าย

๓.๙ ต้องกำหนดขั้นตอนการปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

๓.๑๐ ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๑๑ ต้องกำหนดนโยบายขั้นตอนปฏิบัติการส่งสื่อบันทึกข้อมูลออกนอกองค์กรโดยไม่ได้รับอนุญาตหรือใช้งานผิดวัตถุประสงค์ หรือเกิดความเสียหายของข้อมูลระหว่างการส่ง

๓.๑๒ ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

๓.๑๓ ต้องกำหนดนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรที่เชื่อมโยงกัน

๓.๑๔ ต้องกำหนดมาตรการป้องกันสารสนเทศระบบธุรกรรมออนไลน์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๓.๑๕ ต้องกำหนดมาตรการการป้องกันสารสนเทศที่มีการรับ-ส่งทางระบบเครือข่ายสาธารณะเพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง หรือสารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย หรืออาจเกิดการเปลี่ยนแปลงของสารสนเทศโดยไม่ได้รับอนุญาตหรือถูกเปิดเผยหรือทำสำเนาโดยไม่ได้รับอนุญาต

๓.๑๖ ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่สู่สาธารณะ

๔. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

การสำรองข้อมูล

๔.๑ ต้องสำรองข้อมูลสำคัญของหน่วยงาน

๔.๒ ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้

- ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
- ประเภทสื่อบันทึก (media)
- สถานที่และวิธีการเก็บรักษาสื่อบันทึก

ลงชื่อ.....

(นางจันฑนา จินดาถาวรกิจ)

ผู้อำนวยการกองกฎหมาย

ภาคผนวก

การวิเคราะห์ข้อมูลของหน่วยงาน

แบบฟอร์มการวิเคราะห์ข้อมูล ของหน่วยงาน กองกฎหมาย

กลุ่มงาน	ข้อมูล	ระดับความสำคัญ			ชั้นความลับ				การเข้าถึง				สามารถนำเข้าระบบ internet ได้	การจัดเก็บ
		สูง	ปานกลาง	น้อย	ลับที่สุด	ลับมาก	ลับ	ทั่วไป	ผู้บริหาร (ผอ.)	ผู้ดูแลระบบ (หน.กลุ่ม)	จนท.ในกลุ่มงานที่เกี่ยวข้อง	ผู้ใช้งานทั่วไป		
ก.พัฒนากฎหมายและนิติกรรมสัญญา	๑. ข้อมูลความคืบหน้าการพัฒนากฎหมาย	/						/	/	/	ทุกคน	/	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๒. ข้อมูลความเห็นผู้เกี่ยวข้องในการจัดทำประชาพิจารณ์	/					/		/	/	ทุกคน	-	-	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๓. ข้อมูล กฎหมาย กฎระเบียบที่ได้รับการประกาศใช้ (มีระบบฐานข้อมูล)	/						/	/	/	ทุกคน	/	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๔. ข้อมูลแนวทางการพัฒนาปรับปรุง แก้ไขกฎหมาย	/					/	/	/	/	ทุกคน	/	/	ใส่แฟ้มเอกสารวางในชั้นวาง
ก.กฎหมายและคดี	๑. ข้อมูลสถานพยาบาล/เสริมความงาม ที่ถูกดำเนินคดี	/				/			/	/	ทุกคน	-	เฉพาะคดีที่ยุติแล้ว	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๒. ข้อมูลสถานพยาบาล/เสริมความงามที่ได้รับการตรวจเฝ้าระวัง	/					/		/	/	ทุกคน	-	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๓.ข้อมูลผู้เข้าอบรมด้านการบังคับใช้กฎหมาย		/					/	/	/	ทุกคน	/	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๔. ข้อมูลแนวทางการดำเนินคดีตามกำหมายที่เกี่ยวข้อง	/						/	/	/	ทุกคน	/	/	ใส่แฟ้มเอกสารวางในชั้นวาง

กลุ่มงาน	ข้อมูล	ระดับความสำคัญ			ชั้นความลับ				การเข้าถึง				สามารถนำเข้าระบบ internet ได้	การจัดเก็บ
		สูง	ปานกลาง	น้อย	ลับที่สุด	ลับมาก	ลับ	ทั่วไป	ผู้บริหาร (ผอ.)	ผู้ดูแลระบบ (หน.กลุ่ม)	จนท.ในกลุ่มงานที่เกี่ยวข้อง	ผู้ใช้งานทั่วไป		
ก. เสริมสร้างวินัยและพิทักษ์ระบบคุณธรรม	๑. ข้อมูลการตรวจร่างนิติกรรมสัญญา		/					/	/	/	ทุกคน	/	-	ใส่ตู้เก็บเอกสาร
	๒. ข้อมูลผู้ถูกดำเนินการด้านละเมิด	/				/			/	/	-	-	-	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๓. ข้อมูลแนวทางการดำเนินงานด้านตรวจร่างนิติกรรมสัญญาและการดำเนินการด้านละเมิด		/					/	/	/	ทุกคน	/	/	ใส่ตู้เก็บเอกสาร
	๔. ข้อมูลความผิดของบุคลากรที่ถูกดำเนินคดีด้านวินัย (มีฐานข้อมูล)	/					/		/	/	เฉพาะผู้รับผิดชอบคดี	-	-	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๕. ข้อมูลความรู้ เรื่องวินัยอุทธรณ์ร้องทุกร์	/					/		/	/	ทุกคน	-	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๖. ข้อมูลรายชื่อผู้เข้าอบรมความรู้เรื่องวินัย อุทธรณ์ ร้องทุกข์		/					/	/	/	ทุกคน	/	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๗ .ข้อมูลแนวทางการดำเนินงานด้านวินัย	/						/	/	/	/	/	/	

กลุ่มงาน	ข้อมูล	ระดับความสำคัญ			ชั้นความลับ				การเข้าถึง				สามารถนำเข้าระบบ internet ได้	การจัดเก็บ
		สูง	ปานกลาง	น้อย	ลับที่สุด	ลับมาก	ลับ	ทั่วไป	ผู้บริหาร (ผอ.)	ผู้ดูแลระบบ (หน.กลุ่ม)	จนท.ในกลุ่มงานที่เกี่ยวข้อง	ผู้ใช้งานทั่วไป		
ก.คุ้มครองและพิทักษ์สิทธิ	๑. ข้อมูลเรื่องร้องเรียนสถานพยาบาลเอกชน (มีระบบฐานข้อมูล)	/				/			/	/	ทุกคน	/	เฉพาะสรุปรายงานภาพรวม	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๒. ข้อมูลสถานพยาบาลเอกชนที่ถูกดำเนินการตามกฎหมาย	/				/			/	/	ทุกคน	-	-	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๓. ข้อมูลผู้เข้าอบรมด้านการรับรู้สิทธิ	/						/	/	/	ทุกคน	/-	/	ใส่แฟ้มเอกสารวางในชั้น
	๔. ข้อมูลสิทธิในการคุ้มครองผู้บริโภคตามกฎหมาย (สิทธิผู้บริโภค ขั้นตอนการรับเรื่องร้องเรียน)	/						/	/	/	ทุกคน	/	-	ใส่แฟ้มเอกสารวางในชั้น
ก.การโฆษณาและพิจารณาเปรียบเทียบคดี	๑. ข้อมูลโฆษณาผิดกฎหมายที่ได้รับการจัดการ		/				/		/	/	ทุกคน		เฉพาะสรุปรายงานภาพรวม	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๒. ข้อมูลแนวทางการดำเนินงานเรื่องร้องเรียนการดำเนินงานด้านพิจารณาและจัดการโฆษณา	/						/	/	/	ทุกคน	/	/	ใส่แฟ้มเอกสารวางในชั้น

กลุ่มงาน	ข้อมูล	ระดับความสำคัญ			ชั้นความลับ				การเข้าถึง				สามารถนำเข้าระบบ internet ได้	การจัดเก็บ
		สูง	ปานกลาง	น้อย	ลับที่สุด	ลับมาก	ลับ	ทั่วไป	ผู้บริหาร (ผอ.)	ผู้ดูแลระบบ (หน.กลุ่ม)	จนท.ในกลุ่มงานที่เกี่ยวข้อง	ผู้ใช้งานทั่วไป		
ก. บริหารงานทั่วไป	๑. ข้อมูลบุคลากรของหน่วยงาน	/					/		/	/	-	-	-	ใส่แฟ้มในตู้เก็บเอกสาร
	๒.ข้อมูลวัสดุครุภันฑ์ของหน่วยงาน	/					/		/	/	วราพร ,สุภามาส	-	-	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๓. ข้อมูลเอกสารตามระเบียบพัสดุ		/				/		/	/	วราพร ,สุภามาส	-	-	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๔. ข้อมูลคำสั่ง/ระเบียบ การเงิน การคลัง พัสดุ	/						/	/	/	ทุกคน	/	-	ใส่แฟ้มเอกสารวางในชั้น
	๕.ข้อมูลรายจ่ายประจำของหน่วยงาน(ค่าสาธารณูปโภค ,น้ำ,ไฟ)	/						/	/	/	ทุกคน	/	-	ใส่แฟ้มเอกสารวางในชั้น
	๖.ข้อมูลการเลื่อนขั้นเงินเดือน ข้าตอบแทนพิเศษ ข้าราชการ/พนักงานราชการ	/				/			/	/	-	/	-	ใส่แฟ้มเอกสารวางในชั้น

กลุ่มงาน	ข้อมูล	ระดับความสำคัญ			ชั้นความลับ				การเข้าถึง				สามารถนำเข้าระบบ internet ได้	การจัดเก็บ
		สูง	ปานกลาง	น้อย	ลับที่สุด	ลับมาก	ลับ	ทั่วไป	ผู้บริหาร (ผอ.)	ผู้ดูแลระบบ (หน.กลุ่ม)	จนท.ในกลุ่มงานที่เกี่ยวข้อง	ผู้ใช้งานทั่วไป		
ก. บริหารงานทั่วไป	๗. ข้อมูลผลการดำเนินงานของหน่วยงาน		/			/		/	/	/	ทุกคน	/	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๘. ข้อมูลแผนปฏิบัติการ/โครงการของหน่วยงาน		/			/		/	/	/	ทุกคน	/	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๙.ข้อมูลแผนยุทธศาสตร์ของหน่วยงาน		/			/		/	/	/	ทุกคน	/	/	ใส่ตู้เก็บเอกสารล็อคกุญแจ
	๑๐. ข้อมูลคำของบประมาณของหน่วยงาน		/			/		/	/	/	ทุกคน	/	/	ใส่แฟ้มเอกสารวางในชั้น

คณะผู้จัดทำ

ชื่อหนังสือ : แนวทางการปฏิบัติด้านความมั่นคงปลอดภัย กองกฎหมาย
กรมสนับสนุนบริการสุขภาพ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

ที่ปรึกษา : นางจันฑนา จินดาถาวรกิจ ผู้อำนวยการกองกฎหมาย

ผู้จัดทำ : นางสาวศิริรัตน์ ประเสริฐวสุ นักวิเคราะห์นโยบายและแผนชำนาญการ
นางสาวดวงกมล สุขนิมิตร์ นักวิเคราะห์นโยบายและแผน

พิมพ์ที่ : กองกฎหมาย กรมสนับสนุนบริการสุขภาพ

ปีที่พิมพ์ : ธันวาคม ๒๕๖๔