คู่มือการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ
กรมสนับสนุนบริการสุขภาพ
ปีงบประมาณ 2558-2560

โดย

กลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ

สารบัญ

หน้า

๑. แผนภาพกระบวนการให้บริการและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ๑

๒. ภาคที่ ๑ การตรวจสอบตามมาตรฐานความมั่นคงปลอดภัย(ISO ๒๗๐๐๑)

หมวดที่ ๑ นโยบายความมั่นคงปลอดภัยในองค์กร (Policies for information security) ๒

หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัย (Organization of Information Security) ๑๐

หมวดที่ ๓ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security) ๒๑

หมวดที่ ๔ การจัดหมวดหมู่ และการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กร (Asset Management) ๒๙

หมวดที่ ๕ การควบคุมการเข้าถึง (Access Control) ๔๒

หมวดที่ ๖ การเข้ารหัสข้อมูล (Cryptographic controls) ๖๙

หมวดที่ ๗ ความมั่นคงปลอดภัยทางด้านกายภาพ และสิ่งแวดล้อม(Physical and Environmental security) ๗๒

หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security) ๘๕

หมวดที่ ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security) ๑๐๑

หมวดที่ ๑๐ ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and support processes) ๑๐๘

หมวดที่ ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) ๑๑๘

หมวดที่ ๑๒ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security incident Management) ๑๒๑

หมวดที่ ๑๓ การบริหารความต่อเนื่องของการดำเนินงานในองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity) ๑๒๗

หมวดที่ ๑๔ การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศในองค์กร(Compliance) ๑๓๙

๓. ภาคที่ ๒ การตรวจสอบตามมาตรฐานคุณภาพการให้บริการไอที(ITIL V.๓)

หมวดที่ ๑ กลยุทธ์ในการให้บริการระบบเทคโนโลยีสารสนเทศ(Strategy Generation) ๑๕๐

หมวดที่ ๒ Financial Management ๑๕๑

หมวดที่ ๓ Service Portfolio Management ๑๕๒

หมวดที่ ๔ Demand Management ๑๕๓

หมวดที่ ๕ Service Catalogue Management ๑๕๓

หมวดที่ ๖ Service Level Agreement ๑๕๔

หมวดที่ ๗ Capacity Management ๑๕๕

หมวดที่ ๘ Availability Management ๑๕๗

หมวดที่ ๙ IT Service Continuity Management ๑๕๘

หมวดที่ ๑๐ Information Security Management ๑๕๙

หมวดที่ ๑๑ Supplier Management ๑๕๙

หมวดที่ ๑๒ Transition Planning and Support ๑๖๐

สารบัญ

หน้า

หมวดที่ ๑๓ Service Asset and Configuration Management ๑๖๑
หมวดที่ ๑๔ Change Management ๑๖๒
หมวดที่ ๑๕ Release and Deployment Management ๑๖๓
หมวดที่ ๑๖ Service Validation and Testing Evaluation ๑๖๕
หมวดที่ ๑๗ Knowledge Management ๑๖๕
หมวดที่ ๑๘ Service Operation ๑๖๖

๔. คณะผู้จัดทำ ๑๖๘

คำนำ

ในปัจจุบันเทคโนโลยีเข้ามามีบทบาทในการดำเนินงานแทบทุกองค์กร เสมือนเส้นเลือดหล่อเลี้ยงองค์กร ซึ่งข้อมูลสารสนเทศและระบบเทคโนโลยี จึงมีความจำเป็นอย่างมากที่ทุกองค์กรใช้เป็นเครื่องมือในการเพิ่มประสิทธิภาพการดำเนินงานให้บรรลุเป้าหมาย แต่การตรวจสอบการดำเนินงานด้านงานเทคโนโลยีสารสนเทศจำเป็นต้องใช้ผู้มีความรู้ และทักษะ ความเชี่ยวชาญ ชำนาญเกี่ยวกับการปฏิบัติงานและการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยเฉพาะ มาดำเนินการตรวจสอบ จึงสามารถตรวจสอบงานเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ประสิทธิผล

ดังนั้น กลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ โดยชุมชนนักปฏิบัติมดงาน ตสน. ซึ่งประกอบด้วย ผู้ตรวจสอบภายในของกลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ ได้ระดมสมอง และพบปัญหาจากการตรวจสอบที่ผ่านมา การตรวจสอบงานเทคโนโลยีสารสนเทศ เป็นการตรวจสอบที่สำคัญและไม่มีแนวทางการตรวจสอบที่ชัดเจน ทำให้ผู้ตรวจสอบภายในปฏิบัติงานได้ไม่เป็นแนวทางเดียวกัน และยุ่งยากในการประเมินความเสี่ยงและระบบควบคุมภายใน เพื่อเพิ่มมูลค่าต่อการพัฒนางานเทคโนโลยีสารสนเทศของกรม และยกระดับคุณภาพการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ทั้งนี้ กลุ่มตรวจสอบภายใน ได้ตั้งหัวปลา เพื่อแก้ไขปัญหาว่า “การตรวจสอบงานเทคโนโลยีสารสนเทศให้เป็นไปตามมาตรฐานที่กรมกำหนด” ซึ่งต้องมีการพัฒนาแนวทางการตรวจสอบภายใน งานเทคโนโลยีสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ เพื่อใช้ในการตรวจสอบภายใน งานเทคโนโลยีสารสนเทศของหน่วยงานภายในสังกัดกรมสนับสนุนบริการสุขภาพ ที่สอดคล้องกับ กฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้อง และตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ ปี 2557 ซึ่งประกาศใช้ตามแนวทาง ISO 27001 และ ITIL V.3

กลุ่มตรวจสอบภายใน คาดหวังเป็นอย่างยิ่งว่าหนังสือเล่มนี้จะเป็นประโยชน์แก่ผู้ที่กำลังปฏิบัติงานผู้ตรวจสอบภายในงานเทคโนโลยีสารสนเทศ ที่ใช้แนวทาง ISO 27001 และ ITIL V.3 และผู้ที่สนใจในการใช้เป็นตำราในการศึกษา และค้นค้าทำความเข้าใจในการปฏิบัติงาน การตรวจสอบภายใน ด้านงานเทคโนโลยีสารสนเทศต่อไป

กลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ
สิงหาคม 2558

สารบัญ

หน้า

1. แผนภาพกระบวนการให้บริการและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 1

2. ภาคที่ 1 การตรวจสอบตามมาตรฐานความมั่นคงปลอดภัย(ISO 27001)

หมวดที่ 1 นโยบายความมั่นคงปลอดภัยในองค์กร (Policies for information security) 2
หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัย (Organization of Information Security) 10
หมวดที่ 3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security) 21
หมวดที่ 4 การจัดหมวดหมู่ และการควบคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กร (Asset Management) 29
หมวดที่ 5 การควบคุมการเข้าถึง (Access Control) 41
หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptographic controls) 67
หมวดที่ 7 ความมั่นคงปลอดภัยทางด้านกายภาพ และสิ่งแวดล้อม(Physical and Environmental security) 70
หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security) 83
หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security) 99
หมวดที่ 10 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and support processes) 107
หมวดที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) 117
หมวดที่ 12 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security incident Management) 121
หมวดที่ 13 การบริหารความต่อเนื่องของการดำเนินงานในองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity) 127
หมวดที่ 14 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศในองค์กร(Compliance) 138

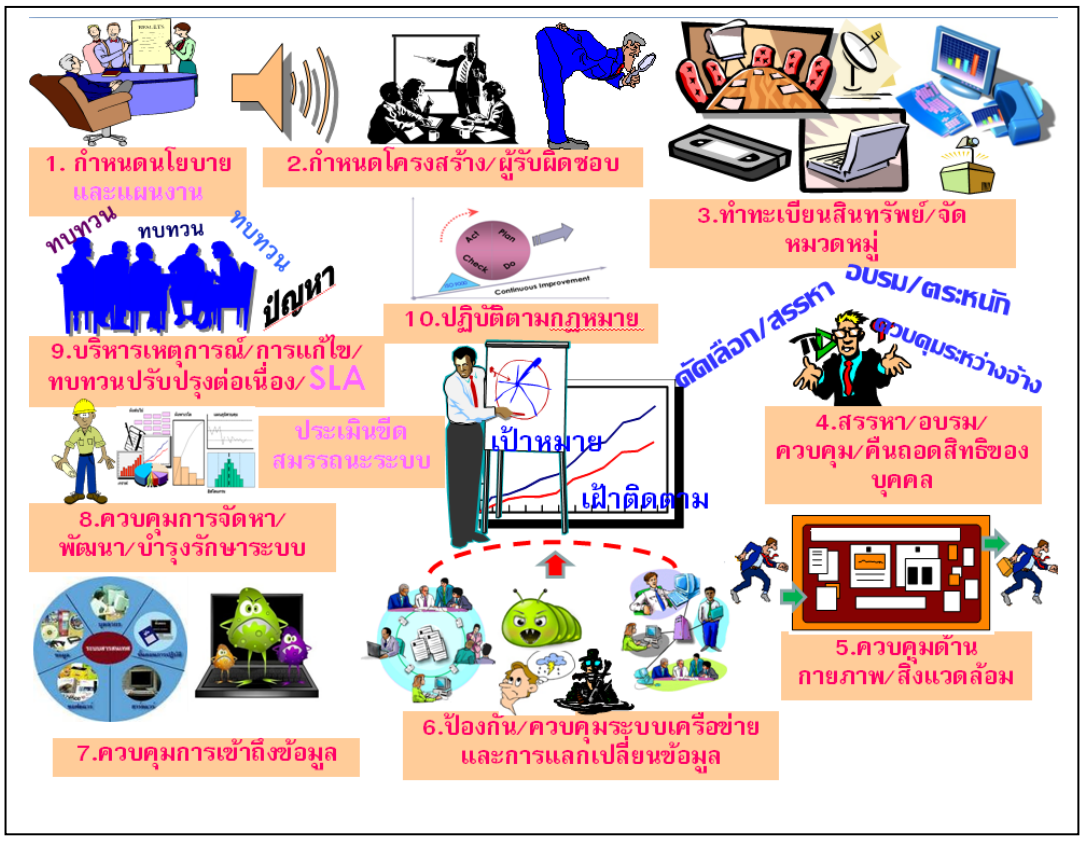
3. ภาคที่ 2 การตรวจสอบตามมาตรฐานคุณภาพการให้บริการไอที(ITIL V.3)

หมวดที่ 1 กลยุทธ์ในการให้บริการระบบเทคโนโลยีสารสนเทศ(Strategy Generation) 148
หมวดที่ 2 Financial Management 149
หมวดที่ 3 Service Portfolio Management 150
หมวดที่ 4 Demand Management 151
หมวดที่ 5 Service Catalogue Management 152
หมวดที่ 6 Service Level Agreement 153
หมวดที่ 7 Capacity Management 154
หมวดที่ 8 Availability Management 156
หมวดที่ 9 IT Service Continuity Management 157
หมวดที่ 10 Information Security Management 158
หมวดที่ 11 Supplier Management 159
หมวดที่ 12 Transition Planning and Support 160

สารบัญ

			หน้า
หมวดที่	13	Service Asset and Configuration Management	161
หมวดที่	14	Change Management	162
หมวดที่	15	Release and Deployment Management	163
หมวดที่	16	Service Validation and Testing Evaluation	165
หมวดที่	17	Knowledge Management	165
หมวดที่	18	Service Operation	166
4. คณะผู้จัดทำ			168
5. ภาคผนวก			169

แผนภาพกระบวนงานการให้บริการและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ



วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 1 นโยบายความมั่นคงปลอดภัยในองค์กร (Policies for information security)
หมายเลขเอกสาร WI0101

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 1 นโยบายความมั่นคงปลอดภัยในองค์กรซึ่งเกี่ยวกับการสอบทานกระบวนการขับเคลื่อนการนำนโยบายสู่การปฏิบัติที่เกิดประสิทธิภาพ ประสิทธิผล เป็นไปตามเจตนารมณ์ ของนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ที่กรมสนับสนุนบริการสุขภาพกำหนดไว้ เพื่อสร้างความเชื่อมั่นว่าทุกหน่วยงาน จัดให้มีการจัดกิจกรรม/กระบวนการขับเคลื่อน นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยมีวัตถุประสงค์ เพื่อให้บุคลากรหรือผู้ปฏิบัติงาน หรือผู้ใช้งานและบุคคลที่เกี่ยวข้อง ได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่ และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางปฏิบัติในการขับเคลื่อนนโยบาย รายละเอียดและการปฏิบัติตามนโยบาย

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

(1) การกำหนดขอบเขตการรักษาความมั่นคงปลอดภัย ครอบคลุมทั้ง 3 ระดับ ได้แก่ ผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ปฏิบัติงานทั่วไปในองค์กร

(2) การให้ความสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยของผู้บริหาร

(3) การกำหนดหลักการ วัตถุประสงค์ และเป้าหมายในการรักษาความปลอดภัยอย่างชัดเจนของหน่วยงาน

(4) การให้คำนิยามคำว่า “การรักษาความมั่นคงปลอดภัยสารสนเทศ”และความรับรู้ ความเข้าใจของคนในองค์กร

(5) การกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัย

(6) การทบทวนแนวทางปฏิบัติ/มาตรการที่รองรับนโยบาย ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อกรม เพื่อให้นโยบายมีความเหมาะสม เพียงพอ และได้ผล

ทั้งนี้ การสอบทาน ต้องคำนึงถึงปัจจัยที่ส่งผลกระทบต่อการนำนโยบายสู่การปฏิบัติ ดังนี้

(1) **ด้านนโยบาย** ซึ่งประกอบด้วยความชัดเจนในวัตถุประสงค์และเป้าหมายของนโยบาย รวมทั้งความชัดเจนของตัวชี้วัด มีการมอบหมายงานและมาตรการการให้คุณให้โทษ ความสามารถในการแก้ไขปัญหาของนโยบาย ความสามารถของนโยบายในการกำหนดโครงสร้างการปฏิบัติงานที่เหมาะสม และการสื่อสารนโยบายที่ชัดเจน

(2) **ด้านการกำหนดภารกิจและการมอบหมายงาน** ประกอบด้วย ขั้นตอนการปฏิบัติงานที่ชัดเจนเพื่อลดการใช้ดุลยพินิจในการปฏิบัติ ความสอดคล้องของโครงการ/แนวทางการปฏิบัติกับเป้าหมายของนโยบาย ความง่ายของวิธีการปฏิบัติงาน การกำหนดกฎระเบียบในการปฏิบัติงาน การกำหนดบทลงโทษและการให้รางวัล และการจัดสรรอำนาจหน้าที่ที่เหมาะสม การสื่อสารและกิจกรรมส่งเสริมในการนำนโยบายไปปฏิบัติ เช่น การสื่อสารที่ชัดเจน ความสม่ำเสมอ มาตรการกระตุ้นโดยใช้อำนาจ

(3) **ด้านทรัพยากร** ประกอบด้วย ความเพียงพอและความเหมาะสมในการจัดสรรทรัพยากรและการสนับสนุนอื่นๆ

(4) **ด้านลักษณะขององค์กรที่นำนโยบายไปปฏิบัติ** เช่น โครงสร้าง ระดับความซับซ้อนและกฎระเบียบที่ใช้ในการตัดสินใจ ความสามารถของบุคลากร ความพร้อมด้านสถานที่และอุปกรณ์จำนวนบุคลากร สมรรถนะในการนำนโยบายไปปฏิบัติในอดีต การปฏิสัมพันธ์และการสื่อสารประสานงานกันภายในองค์กร ลักษณะการเรียนรู้ขององค์กร การกำหนดมาตรฐานของการปฏิบัติงาน เป็นต้น

(5) **ด้านผู้บริหาร** ประกอบด้วย ความสามารถในการจูงใจของผู้นำ ภาวะผู้นำ การมีส่วนร่วมของผู้นำ ความผูกพันและการยอมรับในตัวผู้นำ ทักษะความเข้าใจด้านการบริหารงาน อำนาจหน้าที่ของผู้บริหาร การสร้างให้เกิดความผูกพันต่อบุคลากรในองค์กร ความสามารถในการแก้ไขปัญหาของผู้นำ

(6) **ด้านบุคลากรผู้ปฏิบัติงาน** ประกอบด้วย การคัดสรรบุคลากรที่เหมาะสม บุคลิกภาพของบุคลากร ทัศนคติต่อนโยบายและการรับรู้ ความเข้าใจ ยอมรับในนโยบาย ความร่วมมือและการตอบสนองของผู้ปฏิบัติ ความสามารถในการทำงานเป็นทีม ความจงรักภักดีต่อองค์กร ความสามารถในการปรับตัวกับนโยบาย ความสามารถในการเรียนรู้ และความสามารถในการเจรจาต่อรอง

(7) **ด้านสภาพแวดล้อม** ประกอบด้วย ผลกระทบจากสภาพเศรษฐกิจ สังคม การเมืองและเทคโนโลยี ผลกระทบจากการต่อต้านและคัดค้านนโยบายจากฝ่ายต่างๆและการสนับสนุนกลุ่มอิทธิพล กลุ่มผลประโยชน์ และการมีส่วนร่วมของบุคลากรภายนอกอย่างเป็นทางการ การสนับสนุนจากประชาชน

(8) **ด้านกลุ่มเป้าหมาย** ประกอบด้วย ความหลากหลายของพฤติกรรมกลุ่มเป้าหมายที่มีทัศนคติต่อนโยบาย ความเข้าใจในประโยชน์ที่ได้รับและผลเสียที่อาจเกิดขึ้น

(9) **ปัจจัยด้านการวางแผนและควบคุม** ประกอบด้วยประสิทธิภาพของการวางแผนและการควบคุม ระบบการติดตาม ควบคุมและประเมินผล ความเป็นธรรมของมาตรการการให้คุณให้โทษและการประเมินผลนโยบายและการปฏิบัติงานหรือโครงการ

(10) **ด้านการประสานงานและความร่วมมือ** ประกอบด้วย ความสามารถในการประสานงานระหว่างฝ่ายต่างๆ อย่างสม่ำเสมอ และวิเคราะห์ความซับซ้อนในการประสานงานกับจำนวนหน่วยงานที่เกี่ยวข้องยิ่งจำนวนหน่วยมากความซับซ้อนยิ่งเพิ่มมากขึ้น รวมทั้งการได้รับความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง

(11) ด้านการประชาสัมพันธ์ ประกอบด้วย ความสามารถการวิเคราะห์รูปแบบและวิธีการสื่อสาร รวมทั้งช่องทางการประชาสัมพันธ์ ความถี่และระยะเวลาในการประชาสัมพันธ์ที่ถูกต้องสอดคล้องตรงตามความต้องการของกลุ่มเป้าหมายและไม่ส่งผลกระทบกับการปฏิบัติงาน

(12) ด้านมาตรการในการติดตามประเมินผล ซึ่งประกอบด้วย มีการติดตามอย่างสม่ำเสมอและผลการประเมินที่สะท้อนกลับอย่างตรงกับความเป็นจริง เพื่อการนำไปสู่การปรับปรุงแก้ไขนโยบายที่ถูกต้องและจำเป็นต้องมีอย่างสม่ำเสมอ เพื่อประเมินแนวโน้มของความสำเร็จและสามารถแก้ไขปรับปรุงได้ทันท่วงที

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1. ความชัดเจนในนโยบาย		
เพื่อป้องกันความเข้าใจในนโยบายที่คลาดเคลื่อนไม่ตรงกันของทุกคนในองค์กร	1.1 การสื่อสารในหลายช่องทางอาจมีการประชุมชี้แจงทำความเข้าใจในนโยบายโดยกล่าวถึงวัตถุประสงค์และเป้าหมายของนโยบาย และผลผลิต ผลลัพธ์ที่นโยบายต้องการ	-สอบทานวิธีการสื่อสารทำความเข้าใจในนโยบาย -เอกสารที่เกี่ยวกับวิธีการสื่อสารทำความเข้าใจในนโยบาย เช่น รายงานการประชุม ,บทความ/การประชาสัมพันธ์เว็บไซด์,บอร์ดการประชาสัมพันธ์ ฯลฯ
	1.2 มีวิธีการประเมินผลการสื่อสาร/ประชาสัมพันธ์ เพื่อวัดทัศนคติต่อนโยบายและการรับรู้ ความเข้าใจ ยอมรับในนโยบาย ความร่วมมือและการตอบสนองของผู้ปฏิบัติ	-สอบทานกระบวนการประเมินผลการสื่อสารประชาสัมพันธ์ -เอกสารการประเมินผลการสื่อสารประชาสัมพันธ์ เช่น รายงานการประชุม, รานงานผลการประเมินการสื่อสารประชาสัมพันธ์
2. ความชัดเจนในแนวทางการปฏิบัติงาน		
เพื่อลดการใช้ดุลยพินิจในการปฏิบัติงานให้สอดคล้องกับเป้าหมายของนโยบาย และง่ายต่อ การปฏิบัติงาน รวมทั้งลดความเสี่ยงต่อการปฏิบัติงานไม่ตรงกันหรือไม่บรรลุเป้าหมาย	2.1 มีขั้นตอนการปฏิบัติงานที่สอดคล้องกับเป้าหมายของนโยบาย โดยอาจมีการประชุมระดมสมองในการวิเคราะห์นโยบายเกี่ยวกับวัตถุประสงค์นโยบายแต่ละข้อและกำหนดกลวิธีการดำเนินงาน/แผนงานให้เป็นไปตามเป้าหมาย	-ตรวจสอบความเหมาะสมของขั้นตอนการปฏิบัติงานที่หน่วยงานกำหนดไว้ ถึงกลวิธีดำเนินงาน/แผนงานสอดคล้องกับเป้าหมายของนโยบาย -สัมภาษณ์/สอบถาม/สังเกตการณ์ การนำขั้นตอนไปปฏิบัติเกิดผลตามที่คาดหวังเพียงใด
	2.2 มีการกำหนดผู้รับผิดชอบในแต่ละกลวิธีดำเนินงานหรือแผนงานไว้อย่างชัดเจน และมีการแต่งตั้งผู้รับผิดชอบการขับเคลื่อนนโยบาย	-ตรวจสอบคำสั่งแต่งตั้ง/การมอบหมายหน้าที่ผู้รับผิดชอบในแต่ละแผนงานเพื่อให้เกิดการขับเคลื่อนนโยบาย โดยพิจารณาอำนาจหน้าที่ที่เหมาะสม

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
3.การมอบหมายอำนาจหน้าที่อย่างเหมาะสมในการขับเคลื่อนนโยบาย		
เพื่อให้มีการแบ่งแยกความรับผิดชอบและไม่ให้เกิดการก้าวก่ายงานกัน รวมทั้งการละการไม่ปฏิบัติในส่วนงานที่สำคัญต่อการขับเคลื่อนนโยบาย	3.1 มีการกำหนดขอบเขตการรักษาความมั่นคงปลอดภัย ครอบคลุมทั้ง 3 ระดับ ได้แก่ ผู้บริหาร ผู้ปฏิบัติงาน ด้านเทคโนโลยีสารสนเทศ และผู้ปฏิบัติงานทั่วไปในองค์กร	-ตรวจสอบคำสั่งแต่งตั้ง/การมอบหมายหน้าที่ขอบเขตการรักษาความมั่นคงปลอดภัย ครอบคลุมทั้ง 3 ระดับ ได้แก่ ผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ปฏิบัติงานทั่วไปในองค์กร โดยพิจารณาอำนาจหน้าที่ที่เหมาะสม
	3.2 มีการกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัย	-ตรวจสอบคำสั่งแต่งตั้ง/การมอบหมายหน้าที่ผู้ที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัย โดยพิจารณาอำนาจหน้าที่ที่เหมาะสม
4. การให้ความสำคัญของผู้บริหารองค์กรและความสามารถในการบริหาร		
เพื่อลดความเสี่ยงต่อการไม่สามารถขับเคลื่อนนโยบายสู่การปฏิบัติให้เกิดผลสัมฤทธิ์ อันเนื่องจากไม่มีการสนับสนุนจากผู้บริหาร	4.1 การจัดกิจกรรมที่แสดงให้เห็นว่าผู้บริหารของหน่วยงานให้ความสำคัญในการขับเคลื่อนนโยบาย	-ตรวจสอบเอกสารแสดงให้เห็นว่าผู้บริหารให้ความสำคัญและสนับสนุนส่งเสริมและติดตามผลการดำเนินงานและเผยแพร่ด้านการรักษาความมั่นคงปลอดภัย -สัมภาษณ์ผู้บริหาร โดยผู้บริหารสามารถตอบกรอบทิศทางของนโยบายและประโยชน์แห่งนโยบายได้อย่างถูกต้อง รวมทั้งการวางวิสัยทัศน์ในการขับเคลื่อนนโยบายและแนวทางการยกระดับคุณภาพการปฏิบัติงานของหน่วยงานได้อย่างถูกต้อง

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
5. ความชัดเจนในการจัดระบบการควบคุม-กำกับ ติดตาม ประเมินผลการนำนโยบายสู่การปฏิบัติและการทบทวนแนวทางปฏิบัติ/นโยบาย		
เพื่อประเมินผลสัมฤทธิ์การนำนโยบายสู่การปฏิบัติที่ชัดเจน และทราบปัญหา/อุปสรรคในการดำเนินงาน เพื่อควบคุมการดำเนินการให้บรรลุเป้าหมายของนโยบาย	5.1 มีการติดตามอย่างสม่ำเสมอและผลการประเมินที่สะท้อนกลับอย่างตรงกับความเป็นจริง เพื่อการนำไปสู่การปรับปรุงแก้ไขนโยบายที่ถูกต้องและจำเป็นต้องมีอย่างสม่ำเสมอ เพื่อประเมินแนวโน้มของความสำเร็จและสามารถแก้ไขปรับปรุงได้ทันท่วงที	-ตรวจสอบเอกสารหลักฐานการติดตามประเมินผลการนำนโยบายสู่การปฏิบัติหรือผลการดำเนินงานตามแนวทางปฏิบัติรองรับนโยบายที่หน่วยงานกำหนดและปัญหา-อุปสรรคในการดำเนินงาน รวมทั้งการรายงานผลการดำเนินงานดังกล่าว -สอบทานและสัมภาษณ์เกี่ยวกับกระบวนการติดตามประเมินผลการนำนโยบายสู่การปฏิบัติหรือผลการดำเนินงานตามแนวทางปฏิบัติรองรับนโยบายที่หน่วยงานกำหนดและปัญหา-อุปสรรคในการดำเนินงาน รวมทั้งการรายงานผลการดำเนินงานดังกล่าว -ประเมินความเพียงพอและความเหมาะสมในการจัดสรรทรัพยากรและการสนับสนุนอื่นๆในกระบวนการนำนโยบายสู่การปฏิบัติ -สอบทานกระบวนการทบทวนแนวทางปฏิบัติตามนโยบาย -ตรวจสอบเอกสารการทบทวนแนวทางปฏิบัติตามนโยบาย

เกณฑ์การประเมินความเสี่ยง

(1) ความชัดเจนในนโยบาย โดยการให้คำนิยามคำว่า “การรักษาความมั่นคงปลอดภัยสารสนเทศ”และความรับรู้ ความเข้าใจของคนในองค์กร

ระดับ Level 1

-มีกระบวนการสื่อสารประชาสัมพันธ์นโยบาย

-จำนวนผู้ปฏิบัติงานที่รับผิดชอบงานเทคโนโลยีสารสนเทศ อย่างน้อย 1 คน สามารถบอกคำนิยามคำว่าการรักษาความมั่นคงปลอดภัยสารสนเทศได้อย่างถูกต้อง

ระดับ Level 2

-จำนวนผู้ปฏิบัติงานที่รับผิดชอบงานเทคโนโลยีสารสนเทศ อย่างน้อย 1 คน และหัวหน้างานหรือผู้บริหารหรือคณะกรรมการ ICT ของหน่วยงานจำนวน อย่างน้อย 2 คนขึ้นไป สามารถบอกคำนิยามคำว่าการรักษาความมั่นคงปลอดภัยสารสนเทศได้อย่างถูกต้อง

ระดับ Level 3

-มีการประเมินผลการสื่อสารประชาสัมพันธ์อย่างชัดเจนเป็นรูปธรรม

-จำนวนผู้ปฏิบัติงานที่รับผิดชอบงานเทคโนโลยีสารสนเทศ ทุกคนและหัวหน้างานหรือผู้บริหารหรือคณะกรรมการ ICT ของหน่วยงานจำนวน อย่างน้อย 2 คนขึ้นไป สามารถบอกคำนิยามคำว่าการรักษาความมั่นคงปลอดภัยสารสนเทศได้อย่างถูกต้อง

(2) ความชัดเจนในแนวทางการปฏิบัติงาน โดยการกำหนดหลักการ วัตถุประสงค์ และเป้าหมายในการรักษาความปลอดภัยอย่างชัดเจนของหน่วยงาน

ระดับ Level 1

-มีการกำหนดกระบวนการ/แนวทางปฏิบัติในการรักษาความปลอดภัยของหน่วยงานที่ชัดเจนรองรับ 14 ข้อกำหนดของนโยบายกรมฯ อย่างน้อย 1-5 กระบวนการ

ระดับ Level 2

-มีการกำหนดกระบวนการ/แนวทางปฏิบัติในการรักษาความปลอดภัยของหน่วยงานที่ชัดเจนรองรับ 14 ข้อกำหนดของนโยบายกรมฯ อย่างน้อย 6-13 กระบวนการ

ระดับ Level 3

-มีการกำหนดกระบวนการ/แนวทางปฏิบัติในการรักษาความปลอดภัยของหน่วยงานที่ชัดเจนรองรับ 14 ข้อกำหนดของนโยบายกรมฯ ครบถ้วนทั้ง 14 กระบวนการ

(3.)การมอบหมายอำนาจหน้าที่อย่างเหมาะสมในการขับเคลื่อนนโยบาย

(3.1) การกำหนดขอบเขตการรักษาความมั่นคงปลอดภัย ครอบคลุมทั้ง 3 ระดับ ได้แก่ ผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ปฏิบัติงานทั่วไปในองค์กร

ระดับ Level 1

-มีการกำหนดขอบเขต/บทบาทหน้าที่ในการรักษาความมั่นคงปลอดภัยครบถ้วนทั้ง 3 ระดับ ได้แก่ ผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ปฏิบัติงานทั่วไปในองค์กร

ระดับ Level 2

-มีการกำหนดขอบเขต/บทบาทหน้าที่ในการรักษาความมั่นคงปลอดภัยครบถ้วนทั้ง 3 ระดับ ได้แก่ ผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ปฏิบัติงานทั่วไปในองค์กรอย่างเหมาะสม

ระดับ Level 3

-มีการปฏิบัติในแต่ละระดับ ถูกต้องตามขอบเขตอำนาจหน้าที่ที่กำหนดไว้
-ไม่พบปัญหาการก้าวก่ายงานกันหรือการละไม่ปฏิบัติในกระบวนการสำคัญในการนำนโยบายสู่การปฏิบัติ

(3.2) การกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัย

ระดับ Level 1

-มีการกำหนดความรับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยที่ชัดเจน อย่างน้อยมีการกำหนดให้กับผู้ปฏิบัติงานที่รับผิดชอบงาน IT ทุกคน

ระดับ Level 2

-การกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้อง/ผู้ปฏิบัติงานในการบริหารจัดการความมั่นคงปลอดภัยที่ชัดเจนอย่างครบถ้วน
-ปัญหาจากการที่ผู้เกี่ยวข้องและผู้ปฏิบัติงานมีการทำงานที่ก้าวก่ายงานกันหรือละเว้นการไม่ปฏิบัติงานใดงานหนึ่งที่เป็นองค์ประกอบสำคัญของการบริหารจัดการความมั่นคงปลอดภัยไม่เกิน 2-3 ครั้ง

ระดับ Level 3

-การกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้อง/ผู้ปฏิบัติงานในการบริหารจัดการความมั่นคงปลอดภัยที่ชัดเจนอย่างครบถ้วน

-ไม่พบปัญหาจากการที่ผู้เกี่ยวข้องและผู้ปฏิบัติงานมีการทำงานที่ก้าวก่ายงานกันหรือละเว้นการไม่ปฏิบัติงานใดงานหนึ่งที่เป็นองค์ประกอบสำคัญของการบริหารจัดการความมั่นคงปลอดภัย

(4) การให้ความสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยของผู้บริหาร ต้องมีการกำหนดดังนี้

(4.1) หน่วยงานต้องแสดงให้เห็นว่าผู้บริหารให้ความสำคัญการดำเนินงานด้านการรักษาความมั่นคงปลอดภัย เช่น

- ลงนามคำสั่งการแต่งตั้งคณะกรรมการ CSO/ICT ของหน่วยงาน เพื่อสร้างกลไกการขับเคลื่อนกระบวนการรักษาความมั่นคงปลอดภัย
- อนุมัติให้มีการประกาศใช้แนวทางปฏิบัติหรือมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของหน่วยงาน
- อนุมัติให้จัดทำระบบรักษาความมั่นคงปลอดภัยของหน่วยงานหรือแผนงานโครงการที่สนับสนุนส่งเสริมหรือสร้าง/พัฒนาระบบความมั่นคงปลอดภัยให้เกิดขึ้นกับหน่วยงาน

(4.2) หน่วยงานต้องแสดงให้เห็นถึงการสนับสนุนส่งเสริมให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยเป็นไปอย่างมีประสิทธิภาพ เช่น

- กำหนดนโยบายในการควบคุม-กำกับ ติดตาม และประเมินผลการปฏิบัติตามนโยบายของกรมฯหรือแนวทาง/มาตรการที่หน่วยงานกำหนด

(4.3) การติดตามผลทุกไตรมาส หรือตามความเหมาะสม

- หน่วยงานแสดงให้เห็นถึง กำหนดนโยบายในการควบคุม-กำกับ ติดตาม และประเมินผลการปฏิบัติตามนโยบายของกรมฯหรือแนวทาง/มาตรการที่หน่วยงานกำหนด
- หน่วยงานแสดงให้เห็นถึงการติดตามผลของผู้บริหารในทุกไตรมาส หรือตามความเหมาะสม

(4.4) หน่วยงานแสดงให้เห็นว่าผู้บริหารมีการสนับสนุนหรือเผยแพร่และสื่อสารให้เจ้าหน้าที่ถือปฏิบัติ

-ผู้บริหารชี้แจงนโยบายหรือมาตรการหรือแนวคิดในการพัฒนาระบบการรักษาความมั่นคงปลอดภัยในที่ประชุมประจำเดือนของหน่วยงานหรือที่ประชุมคณะกรรมการ CSO/ICT ของหน่วยงาน โดยมีหลักฐานจากรายงานการประชุมประกอบ

-ผู้บริหารลงนามในบันทึกแจ้งเวียนเกี่ยวกับนโยบายหรือมาตรการ/แนวทางที่ให้เจ้าหน้าที่ในสังกัดถือปฏิบัติ

-ผู้บริหารมีการสื่อสารในช่องทางประชาสัมพันธ์ต่างๆ

ระดับ Level 1

-มีการแสดงหลักฐานในข้อใดข้อหนึ่ง ในข้อ 1-4

-สัมภาษณ์ผู้บริหารแล้วผู้บริหารสามารถตอบกรอบทิศทางของนโยบายและประโยชน์แห่งนโยบายได้อย่างถูกต้อง รวมทั้งการวางวิสัยทัศน์ในการขับเคลื่อน

ระดับ Level 2

-มีการแสดงหลักฐานได้ 2-3 ข้อ

-สัมภาษณ์ผู้บริหารแล้วผู้บริหารสามารถตอบกรอบทิศทางของนโยบายและประโยชน์แห่งนโยบายได้อย่างถูกต้อง รวมทั้งการวางวิสัยทัศน์ในการขับเคลื่อนนโยบายและแนวทางการยกระดับคุณภาพการปฏิบัติงานของหน่วยงานได้อย่างถูกต้อง

ระดับ Level 3

-มีการแสดงหลักฐานได้ทุกข้อตั้งแต่ 1-4 ข้อ อย่างครบถ้วน

-สัมภาษณ์ผู้บริหารแล้วผู้บริหารสามารถตอบกรอบทิศทางของนโยบายและประโยชน์แห่งนโยบายได้อย่างถูกต้อง รวมทั้งการวางวิสัยทัศน์ในการขับเคลื่อนนโยบายและแนวทางการยกระดับคุณภาพการปฏิบัติงานของหน่วยงานได้อย่างถูกต้อง

(5) การทบทวนแนวทางปฏิบัติ/มาตรการที่รองรับนโยบาย ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อกรม เพื่อให้นโยบายมีความเหมาะสม เพียงพอ และได้ผล

ระดับ Level 1

-มีการทบทวนนโยบาย/แนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนด อย่างน้อย 1 ครั้งต่อปี หรือตามรอบระยะเวลาที่หน่วยงานกำหนด หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญส่งผลกระทบต่อกรมหรือหน่วยงาน

ระดับ Level 2

-การทบทวนดังกล่าว ระบุถึงผลการดำเนินงานตามแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนด และผลสัมฤทธิ์ต่อวัตถุประสงค์ของนโยบาย และการประเมินความเพียงพอและความเหมาะสมในการจัดสรรทรัพยากรและการสนับสนุนอื่นๆในกระบวนการนำนโยบายสู่การปฏิบัติ รวมทั้งปัญหา/อุปสรรค

-มีการรายงานผลการปฏิบัติงานสู่คณะกรรมการ CSO ระดับหน่วยงานและระดับกรม

ระดับ Level 3

-มีการนำข้อมูลผลการดำเนินงานสู่การทบทวนนโยบาย/แนวทางปฏิบัติ/มาตรการที่หน่วยงานต้องปรับปรุงแก้ไข เพื่อให้เกิดประสิทธิภาพ ประสิทธิผลของการนำนโยบายสู่การปฏิบัติได้ตามความคาดหวังของนโยบายกรมฯ

-ไม่พบปัญหาที่พบด้านการรักษาความมั่นคงปลอดภัย เมื่อมีการทบทวนนโยบาย/แนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดแล้ว

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ
(Organization of Information Security)
หมายเลขเอกสาร WI0201

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ **หมวดที่ 2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ** ซึ่งดำเนินการตรวจสอบกลไก/โครงสร้างการบริหารจัดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของทุกหน่วยงาน และสอบทานถึงประสิทธิภาพ ประสิทธิผลการขับเคลื่อนของกลไก/โครงสร้างที่เหมาะสมต่อการปฏิบัติให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศกรมสนับสนุนบริการสุขภาพที่กำหนด

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกลไก/โครงสร้างการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน ดังนี้

(1) การแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ(CSO) ขึ้นในหน่วยงาน

(2) การกำหนดบทบาทหน้าที่ของคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) หน่วยงาน ครอบคลุม 4 กระบวนการ ได้แก่ การวางแผนและการกำหนดแนวปฏิบัติ/มาตรการ, การสื่อสารประชาสัมพันธ์ , การควบคุม-กำกับติดตาม ,การประเมินผลการนำนโยบาย/แนวปฏิบัติ/มาตรการสู่การปฏิบัติ

(3) กระบวนการขับเคลื่อนระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงาน โดยมีการประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) ของหน่วยงานอย่างน้อย 2 ครั้งต่อปี ครั้งที่ 1 เป็นการสื่อสารนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดขึ้นและประกาศใช้ ครั้งที่ 2 เป็นการติดตามประเมินผลการปฏิบัติตามนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดขึ้นและประเมินการสื่อสารนโยบาย/แนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดไว้

(4) การทบทวนหรือแก้ไขและเพิ่มเติมคณะกรรมการได้ทุกปี เพื่อให้คณะกรรมการทันสมัยและเหมาะสม/สอดคล้องกับวัฒนธรรมของหน่วยงาน อันเป็นกลไกการขับเคลื่อนที่แท้จริงในการปฏิบัติงาน

(5) การกำหนดบทบาทหน้าที่ของหัวหน้างาน IT และผู้ปฏิบัติงาน IT

(6) การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

(7) การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.การแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ(CSO) ขึ้นในหน่วยงาน		
เพื่อให้มีกลไก/โครงสร้างการบริหารในรูปคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เหมาะสมต่อการปฏิบัติให้เกิดการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพ	1.1การแต่งตั้งคณะกรรมการ CSO อย่างน้อย 3 ท่าน	-ตรวจสอบคำสั่งแต่งตั้งคณะกรรมการ CSO อย่างน้อย 3 ท่าน -ตรวจสอบความเหมาะสมของโครงสร้างคณะกรรมการ CSO ที่เหมาะสมในการสื่อสาร/ดำเนินงาน/ควบคุม-กำกับ ประเมินผลการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
-เพื่อประเมินความเพียงพอเหมาะสมของอำนาจหน้าที่ของคณะกรรมการ CSO ต่อการปฏิบัติ/ขับเคลื่อนการบริหารจัดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน	1.2 มีการมอบหมายอำนาจหน้าที่ของคณะกรรมการ CSO ที่ครอบคลุม 4 กระบวนการ ได้แก่ การกำหนดแนวปฏิบัติ/มาตรการ การสื่อสาร การติดตามควบคุม-กำกับการนำนโยบาย/แนวปฏิบัติ/มาตรการสู่การปฏิบัติงาน การประเมินการนำนโยบาย/แนวปฏิบัติ/มาตรการสู่การปฏิบัติ	-ตรวจสอบคำสั่งแต่งตั้งคณะกรรมการ CSO ในส่วนการมอบหมายอำนาจหน้าที่ของคณะกรรมการ -สอบทานการปฏิบัติหน้าที่ของคณะกรรมการ CSO หน่วยงานว่าได้ ปฏิบัติตามบทบาทหน้าที่ที่กำหนดไว้อย่างครบถ้วน เช่น จากรายงานการประชุมคณะกรรมการ CSO หน่วยงาน
2.กระบวนการขับเคลื่อนระบบการรักษาความมั่นคงปลอดภัยสารสนเทศโดยคณะกรรมการ CSO		
เพื่อสร้างความมั่นใจว่าหน่วยงานมีการขับเคลื่อนการบริหารจัดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานในรูปคณะกรรมการ CSO	2.1 มีการประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) ของหน่วยงานอย่างน้อย 2 ครั้งต่อปี **ครั้งที่ 1** เป็นการสื่อสารนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดขึ้นและประกาศใช้ **ครั้งที่ 2** เป็นการติดตามประเมินผลการปฏิบัติตามนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดขึ้นและประเมินการสื่อสารนโยบาย/แนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดไว้	-สอบทาน/สัมภาษณ์/สอบถามกระบวนการขับเคลื่อนการบริหารจัดการรักษาความมั่นคงปลอดภัยในรูปคณะกรรมการ CSO -ตรวจสอบเอกสารหลักฐานกระบวนการขับเคลื่อนการบริหารจัดการรักษาความมั่นคงปลอดภัยในรูปคณะกรรมการ CSO เช่น รายงานการประชุมคณะกรรมการ CSO -ประเมินความเพียงพอในการขับเคลื่อนการบริหารจัดการรักษาความมั่นคงปลอดภัยในรูปคณะกรรมการ CSO

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
3.การทบทวนหรือแก้ไขเพิ่มเติมคณะกรรมการ		
เพื่อให้การปฏิบัติงานของคณะกรรมการทันสมัยและเหมาะสม/สอดคล้องกับวัฒนธรรมของหน่วยงาน เพื่อให้การดำเนินงานบรรลุเป้าหมายของนโยบาย	3.1 มีการทบทวนหรือแก้ไขเพิ่มเติมคณะกรรมการอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงอันส่งผลกระทบต่อนโยบายหรือการปฏิบัติงาน	-ตรวจสอบการทบทวนหรือแก้ไขเพิ่มเติมคณะกรรมการ เช่น คำสั่งทบทวน/แต่งตั้งคณะกรรมการCSO หรือรายงานการประชุมที่เกี่ยวกับการทบทวนคณะกรรมการ CSO ทั้งรายชื่อคณะกรรมการและบทบาทอำนาจหน้าที่ที่เหมาะสมต่อการดำเนินงานในปัจจุบัน
4.การกำหนดบทบาทหน้าที่ของหัวหน้างาน IT และผู้ปฏิบัติงาน IT		
เพื่อให้การปฏิบัติงานของหัวหน้างาน IT และผู้ปฏิบัติงานที่รับผิดชอบงาน IT มีประสิทธิภาพ ประสิทธิผล และชัดเจน ไม่ก้าวก่ายงานหรือละการไม่ปฏิบัติงานในกระบวนการสำคัญในการบริหารจัดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงาน	4.1มีการกำหนดบทบาทหน้าที่(Job Description) ของหัวหน้างาน ITไว้อย่างชัดเจน 4.2 มีการกำหนดบทบาทหน้าที่(Job Description) ของผู้ปฏิบัติงาน ITไว้อย่างชัดเจน 4.3 มีแผนผังโครงสร้างการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานที่ชัดเจน	-ตรวจสอบบทบาทหน้าที่(Job Description) ของหัวหน้างาน IT -ตรวจสอบบทบาทหน้าที่(Job Description) ของผู้ปฏิบัติงาน IT -ตรวจสอบแผนผังโครงสร้างการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน -สอบทาน/สัมภาษณ์/สอบทานและสังเกตการณ์การปฏิบัติงานของผู้ปฏิบัติงานITและหัวหน้างาน IT ว่ามีการปฏิบัติตามโครงสร้างที่กำหนดหรือไม่ -ตรวจสอบการบันทึกปัญหาที่เกิดขึ้นในการปฏิบัติงานและการรายงานผลการปฏิบัติงานและรายงานผลเหตุการณ์ที่ไม่คาดคิด
5.การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)		
-เพื่อให้มีผู้ปฏิบัติงานในการบริหารจัดการระบบการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ ประสิทธิผลและต่อเนื่อง -เพื่อให้การดำเนินงานการบริหารจัดการระบบการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ ประสิทธิผลและต่อเนื่อง	5.1 มีการจัดทำบัญชีหรือทะเบียนรายชื่อผู้ประสานงานที่เกี่ยวข้องในการช่วยเหลือ/แก้ไขปัญหา หรือผู้มีอำนาจในการอนุมัติจัดการกับปัญหาและเหตุการณ์ที่อาจทำให้เกิดความไม่มั่นคงปลอดภัยของระบบเทคโนโลยีของหน่วยงาน โดยมีรายละเอียดอย่างน้อยคือ ชื่อ-ที่อยู่-หมายเลขโทรศัพท์-อีเมล์ของผู้ที่จะติดต่อ/ผู้มีอำนาจอยู่อย่างครบถ้วนและทันสมัยอยู่เสมอ และการแจ้งเวียนข้อมูลการติดต่อ/ผู้มีอำนาจ แก่ผู้เกี่ยวข้องให้แก้ไขปรับปรุงข้อมูลเป็นระยะตามความเหมาะสมและส่งแจ้งเวียนให้ทุกหน่วยงานทราบถือปฏิบัติ	-ตรวจสอบทะเบียนรายชื่อผู้ประสานงานในการช่วยเหลือแก้ไขและผู้มีอำนาจในการอนุมัติจัดการกับปัญหาและเหตุการณ์ที่อาจทำให้ไม่มั่นคงปลอดภัยของระบบสารสนเทศหน่วยงาน

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	5.2 มีขั้นตอนการติดต่อรายชื่อผู้ประสานงานดังกล่าว ตามกลุ่มเหตุการณ์ที่อาจเกิดขึ้นที่เหมาะสม โดยบุคคลหรือทีมงาน IT ที่สร้างรายชื่อการติดต่อดังกล่าว ควรต้องระบุสถานที่และเหตุการณ์ที่เกิดขึ้นยกเป็นตัวอย่างให้ผู้ใช้ทราบว่าเมื่อเกิดเหตุการณ์ดังนี้ สามารถติดต่อใครได้บ้าง	-ตรวจสอบขั้นตอนการติดต่อรายชื่อผู้ประสานงานตามกลุ่มเหตุการณ์ที่อาจเกิดขึ้นที่เหมาะสมและผู้มีอำนาจในการอนุมัติจัดการกับปัญหาและเหตุการณ์ที่อาจทำให้ไม่มั่นคงปลอดภัยของระบบสารสนเทศหน่วยงาน
	5.3 คณะกรรมการ CSO ระดับหน่วยงาน ต้องมีการแต่งตั้ง/การมอบหมายผู้ที่ประสานงานรายชื่อ/ผู้มีอำนาจดังกล่าวไว้ รวมทั้งควรกำหนดมอบหมายให้มีผู้แทนสำรองกรณีที่ผู้ประสานงานไม่สามารถปฏิบัติงานได้	-ตรวจสอบการแต่งตั้ง/มอบหมายผู้ที่ประสานงานและผู้มีอำนาจในการอนุมัติจัดการกับปัญหาและเหตุการณ์ที่อาจทำให้ไม่มั่นคงปลอดภัยของระบบสารสนเทศหน่วยงาน -ตรวจสอบการแต่งตั้งผู้ปฏิบัติการแทนกรณีที่ผู้ที่ประสานงานและผู้มีอำนาจในการอนุมัติจัดการกับปัญหาและเหตุการณ์ไม่สามารถปฏิบัติหน้าที่ได้
6.การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)		
-เพื่อให้หน่วยงานมีการเฝ้าระวังและรับรู้ข้อมูลข่าวสารภัยคุกคามต่อระบบสารสนเทศและป้องกันได้ทันท่วงที	6.1 ผู้อำนวยการสำนักบริหาร ต้องจัดทำรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ สนง.ตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ กสท. โทรคมนาคม ทศท คอร์ปอเรชั่น ThaiCERT เป็นต้น	-ตรวจสอบรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ สนง.ตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ กสท. โทรคมนาคม ทศท คอร์ปอเรชั่น ThaiCERT เป็นต้นที่มีอยู่ในหน่วยรับตรวจ -สำหรับสำนักบริหารตรวจสอบเพิ่มเติมในส่วนกระบวนการจัดทำรายชื่อและการปรับปรุงข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ
	6.2 ผู้อำนวยการสำนักบริหาร ต้องแจ้งเวียนให้ทุกหน่วยงานในสังกัดกรมฯ ทราบปัญหาและภัยคุกคามใหม่ๆที่เกิดขึ้น เพื่อเป็นการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงที ที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย รวมทั้งแนวทางปฏิบัติที่เหมาะสมและมีประสิทธิภาพ	-ตรวจสอบการแจ้งเวียนปัญหาและภัยคุกคามใหม่ๆที่เกิดขึ้น เพื่อเป็นการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงที ที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย รวมทั้งแนวทางปฏิบัติที่เหมาะสมและมีประสิทธิภาพที่มีอยู่ในหน่วยรับตรวจ -สำหรับสำนักบริหาร ตรวจสอบเพิ่มเติมเกี่ยวกับกระบวนการแจ้งเวียนปัญหา/ภัยคุกคามที่แจ้งเตือนทุกหน่วยงาน

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	6.3 คณะกรรมการ CSO ระดับกรมมีอำนาจในการอนุมัติการตัดสินใจในการอนุญาตให้มีการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน	-ตรวจสอบอำนาจหน้าที่ในการอนุมัติการตัดสินใจในการอนุญาตให้มีการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันของคณะกรรมการ CSO ระดับกรม
	6.4 คณะกรรมการ CSO ระดับกรมต้องจัดระบบที่ทำให้เกิดการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน เพื่อให้เกิดการพัฒนาความรู้เกี่ยวกับข้อมูลและการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัย	-ตรวจสอบจัดระบบการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน
	6.5 คณะกรรมการ CSO ระดับหน่วยงาน ต้องประเมินผลการปฏิบัติในของหน่วยงานว่าเป็นไปตามแนวทางการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงทีที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย รวมทั้งแนวทางปฏิบัติที่เหมาะสมและมีประสิทธิภาพ รวมทั้งประเมินผลการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานกับหน่วยงานอื่นๆ	-ตรวจสอบผลการประเมินการปฏิบัติงานของหน่วยงานว่าเป็นไปตามการแจ้งเตือนให้ระวังในการปฏิบัติงาน -สอบทาน/สัมภาษณ์กระบวนการประเมินผลการปฏิบัติงานของหน่วยงานของคณะกรรมการ CSO

เกณฑ์การประเมินความเสี่ยง

(1.) การแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) ขึ้นในหน่วยงาน

ระดับ Level 1

-มีการแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ(CSO) ขึ้นในหน่วยงาน อย่างน้อย 1 ชุด อันประกอบด้วยอย่างน้อย คือ ประธาน, คณะกรรมการอย่างน้อย 1 ท่าน และเลขานุการ (ผู้รับผิดชอบด้าน IT ของหน่วย)

ระดับ Level 2

-การแต่งตั้งคณะกรรมการ CSO ของหน่วยงานมีความเหมาะสมในการปฏิบัติงานที่ไม่ทำให้เกิดปัญหาอุปสรรคในการสื่อสารประชาสัมพันธ์และการวางแผน ควบคุม-กำกับติดตามประเมินผลการนำนโยบายสู่การปฏิบัติ

ระดับ Level 3

-ไม่พบปัญหาความเสี่ยงจากการกำหนดโครงสร้างหรือกลไกการบริหารจัดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศหน่วยงาน

(2.) การขับเคลื่อนระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ(CSO)ของหน่วยงาน

ระดับ Level 1

-หน่วยงานจัดให้มีการขับเคลื่อนระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงาน โดยมีการประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) ของหน่วยงานอย่างน้อย 2 ครั้งต่อปี ครั้งที่ 1 เป็นการสื่อสารนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดขึ้นและประกาศใช้ ครั้งที่ 2 เป็นการติดตามประเมินผลการปฏิบัติตามนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดขึ้นและประเมินการสื่อสารนโยบาย/แนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดไว้

ระดับ Level 2

-หน่วยงานจัดให้มีการขับเคลื่อนระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงาน โดยมีการประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ(CSO)ของหน่วยงานอย่างน้อย 3 ครั้งต่อปีขึ้นไป ครั้งที่ 1 เป็นการสื่อสารนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดขึ้นและประกาศใช้ ครั้งที่ 2 เป็นการติดตามควบคุม-กำกับการปฏิบัติตามนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนด ครั้งที่ 3 เป็นการประเมินผลการปฏิบัติตามนโยบายกรมฯและแนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดขึ้นและประเมินการสื่อสารนโยบาย/แนวทางปฏิบัติ/มาตรการที่หน่วยงานกำหนดไว้

ระดับ Level 3

-มีการรวบรวมข้อมูลและวิเคราะห์สรุปผลการดำเนินการขับเคลื่อนให้ผู้บริหารหน่วยงานและคณะกรรมการ CSO ระดับกรมฯ รับทราบ อย่างน้อย 1 ครั้งต่อปี

-ไม่พบปัญหาความเสี่ยงในกระบวนการขับเคลื่อนนโยบายและการบริหารจัดการรักษาความมั่นคงปลอดภัยของหน่วยงานในรูปคณะกรรมการ

(3.) การกำหนดบทบาทหน้าที่ของคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) หน่วยงาน

ระดับ Level 1

-มีการกำหนดบทบาทหน้าที่ของคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) หน่วยงานไว้

ระดับ Level 2

-การกำหนดบทบาทหน้าที่ของคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) หน่วยงาน ครอบคลุมทั้งมิติการกำหนดนโยบายและวางแผนงานการดำเนินงานรองรับนโยบาย รวมทั้งขับเคลื่อนนโยบายและแผนงาน/มาตรการ ติดตามควบคุม-กำกับและประเมินผลการนำนโยบายสู่การปฏิบัติ

ระดับ Level 3

-การปฏิบัติของคณะกรรมการ CSO หน่วยงาน ปฏิบัติตามบทบาทหน้าที่ที่กำหนดไว้อย่างครบถ้วน

-ผู้อำนวยการระดับหน่วยงาน/ผู้ปฏิบัติงาน/ผู้เกี่ยวข้องรับทราบขอบเขตอำนาจคณะกรรมการ CSO หน่วยงาน อย่างน้อย 2 คน

(4.)การทบทวนหรือแก้ไขแลเพิ่มเติมคณะกรรมการ

ระดับ Level 1

-มีการทบทวนคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) หน่วยงาน 1 ครั้งต่อปี

ระดับ Level 2

- มีการทบทวนคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (CSO) หน่วยงาน 1 ครั้งต่อปีและเมื่อมีการเปลี่ยนแปลงของหน่วยงานที่กระทบต่อการปฏิบัติงานของคณะกรรมการ CSO หน่วยงาน ที่อาจทำให้การปฏิบัติงานของคณะกรรมการ CSO หน่วยงานไม่บรรลุตามเจตนาของนโยบาย

ระดับ Level 3

- ผู้อำนวยการระดับหน่วยงาน/ผู้ปฏิบัติงาน/ผู้เกี่ยวข้องรับทราบการทบทวนคณะกรรมการ CSO หน่วยงาน อย่างน้อย 2 คน
- ไม่พบปัญหาความเสี่ยงในการปฏิบัติหน้าที่ของคณะกรรมการ CSO ที่มาจากการทบทวนคณะกรรมการ

(5.) การกำหนดบทบาทหน้าที่ของหัวหน้างาน IT และผู้ปฏิบัติงาน IT

ระดับ Level 1

- มีการกำหนดขอบเขตอำนาจหน้าที่หัวหน้างาน IT ระดับหน่วยงาน
- มีการกำหนดขอบเขตอำนาจหน้าที่ผู้รับผิดชอบงาน IT

ระดับ Level 2

- มีการปฏิบัติตามอำนาจหน้าที่ของหัวหน้างาน IT ระดับหน่วยงานและผู้รับผิดชอบงาน IT อย่างครบถ้วนตามที่กำหนด

ระดับ Level 3

- ผู้อำนวยการระดับหน่วยงาน/ผู้ปฏิบัติงาน/ผู้เกี่ยวข้องรับทราบขอบเขตอำนาจของหัวหน้างาน ITและผู้รับผิดชอบงาน IT อย่างน้อย 2 คน

(6.)การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

1. รายชื่อเหล่านี้ควรจะทันสมัยมีการ Updateหรือปรับปรุงเมื่อมีการเปลี่ยนแปลงข้อมูลผู้ที่จะติดต่อหรือผู้มีอำนาจและแจ้งเวียนให้ผู้เกี่ยวข้องรับทราบ
2. หัวหน้าหน่วยควรมีการมอบหมายผู้ที่ประสานงานรายชื่อ/ผู้มีอำนาจดังกล่าวไว้ รวมทั้งควรกำหนดมอบหมายให้มีผู้แทนสำรองกรณีที่ผู้ประสานงานไม่สามารถปฏิบัติงานได้
3. หัวหน้าหน่วยควรมีการแจ้งเวียนข้อมูลการติดต่อ/ผู้มีอำนาจให้แก้ไขปรับปรุงข้อมูลเป็นระยะตามความเหมาะสม
4. กรณีเกิดเหตุฉุกเฉินผู้ใช้งานทุกคนสามารถติดตามตามรายชื่อข้อมูลการติดต่อ เพื่อแจ้งเหตุฉุกเฉินในเหตุการณ์ที่อาจก่อให้เกิดความไม่มั่นคงปลอดภัยได้ตลอดเวลา
5. บุคคลหรือทีมงาน IT ที่สร้างรายชื่อการติดต่อดังกล่าว ควรต้องระบุสถานที่และเหตุการณ์ที่เกิดขึ้นยกเป็นตัวอย่างให้ผู้ใช้งานทราบว่าเมื่อเกิดเหตุการณ์ดังนี้ สามารถติดต่อใครได้บ้าง

ระดับ Level 1

- ระดับกรมฯ ผู้อำนวยการสำนักบริหาร มีการกำหนดบัญชี/ทะเบียนรายชื่อผู้ติดต่อประสานงาน กรณีเกิดเหตุการณ์อันอาจเกิดความไม่มั่นคงปลอดภัยของระบบสารสนเทศ และมีรายละเอียดที่ครบถ้วน รวมทั้งมีรายชื่อที่ครอบคลุมผู้ที่ควรติดต่อประสานงานได้
- ระดับกรมฯ ผู้อำนวยการสำนักบริหาร บัญชี/ทะเบียนรายชื่อผู้ติดต่อประสานงานดังกล่าว มีการปรับปรุงข้อมูลให้ทันสมัยอยู่เสมอและแจ้งเวียนให้ทุกหน่วยงานในสังกัดกรมทราบและถือปฏิบัติ
- ระดับหน่วยงาน คณะกรรมการ CSO ระดับหน่วยงาน มีการมอบหมายหรือแต่งตั้งผู้ประสานงานในรายชื่อดังกล่าว
- ระดับหน่วยงาน คณะกรรมการ CSO ระดับหน่วยงาน มีการสื่อสารและกำหนดให้บุคลากรที่เกี่ยวข้องทุกคนถือปฏิบัติ

ระดับ Level 2

- ระดับกรมฯ ผู้อำนวยการสำนักบริหาร มีการกำหนดบัญชี/ทะเบียนรายชื่อผู้ติดต่อประสานงาน กรณีเกิดเหตุการณ์อันอาจเกิดความไม่มั่นคงปลอดภัยของระบบสารสนเทศ และมีรายละเอียดที่ครบถ้วน รวมทั้งมีรายชื่อที่ครอบคลุมผู้ที่ควรติดต่อประสานงานได้

- ระดับกรมฯ ผู้อำนวยการสำนักบริหาร บัญชี/ทะเบียนรายชื่อผู้ติดต่อประสานงานดังกล่าว มีการปรับปรุงข้อมูลให้ทันสมัยอยู่เสมอและแจ้งเวียนให้ทุกหน่วยงานในสังกัดกรมทราบและถือปฏิบัติ
- ระดับกรมฯ ผู้อำนวยการสำนักบริหาร มีการแจ้งเวียนรายชื่อผู้ประสานงานให้มีการปรับปรุงแก้ไขในระยะเวลาที่กำหนด
- ระดับหน่วยงาน คณะกรรมการ CSO ระดับหน่วยงาน มีการมอบหมายหรือแต่งตั้งผู้ประสานงานในรายชื่อดังกล่าว พร้อมทั้งผู้ประสานงานสำรองไว้ในกรณีที่ผู้ประสานงานคนแรกไม่สามารถปฏิบัติหน้าที่ได้
- ระดับหน่วยงาน คณะกรรมการ CSO ระดับหน่วยงาน มีการสื่อสารและกำหนดให้บุคลากรที่เกี่ยวข้องทุกคนถือปฏิบัติทั่วทั้งองค์กร อย่างน้อยร้อยละ 40 ของบุคลากรที่สุ่มตรวจ
- ระดับหน่วยงาน ผลการดำเนินการตามขั้นตอน ร้อยละของการติดต่อประสานงานปัญหาสามารถแก้ไขได้อย่างรวดเร็วมีประสิทธิภาพ ได้อย่างน้อยร้อยละ 60 ของจำนวนครั้งที่มีการติดต่อประสานงาน

ระดับ Level 3

- ระดับกรมฯ ผู้อำนวยการสำนักบริหาร มีการกำหนดบัญชี/ทะเบียนรายชื่อผู้ติดต่อประสานงาน กรณีเกิดเหตุการณ์อันอาจเกิดความไม่มั่นคงปลอดภัยของระบบสารสนเทศ และมีรายละเอียดที่ครบถ้วน รวมทั้งมีรายชื่อที่ครอบคลุมผู้ที่ควรติดต่อประสานงานได้
- ระดับกรมฯ ผู้อำนวยการสำนักบริหาร บัญชี/ทะเบียนรายชื่อผู้ติดต่อประสานงานดังกล่าว มีการปรับปรุงข้อมูลให้ทันสมัยอยู่เสมอและแจ้งเวียนให้ทุกหน่วยงานในสังกัดกรมทราบและถือปฏิบัติ
- ระดับกรมฯ ผู้อำนวยการสำนักบริหาร มีการแจ้งเวียนรายชื่อผู้ประสานงานให้มีการปรับปรุงแก้ไขในระยะเวลาที่กำหนด
- ระดับหน่วยงาน คณะกรรมการ CSO ระดับหน่วยงาน มีการมอบหมายหรือแต่งตั้งผู้ประสานงานในรายชื่อดังกล่าว พร้อมทั้งผู้ประสานงานสำรองไว้ในกรณีที่ผู้ประสานงานคนแรกไม่สามารถปฏิบัติหน้าที่ได้
- ระดับหน่วยงาน คณะกรรมการ CSO ระดับหน่วยงาน มีการสื่อสารและกำหนดให้บุคลากรที่เกี่ยวข้องทุกคนถือปฏิบัติทั่วทั้งองค์กร อย่างน้อยร้อยละ 80
- ระดับหน่วยงาน คณะกรรมการ CSO ระดับหน่วยงาน มีการติดตามประเมินผล การติดต่อประสานงานกับขั้นตอนและบัญชีรายชื่อที่กำหนดไว้ สามารถดำเนินการตามขั้นตอนและรายชื่อดังกล่าวได้อย่างถูกต้องและได้ประสิทธิภาพในการแก้ไขปัญหาได้ทันท่วงที
- ระดับหน่วยงาน ผลการดำเนินการตามขั้นตอน ทุกๆครั้งที่มีการติดต่อประสานงานปัญหาสามารถแก้ไขได้อย่างรวดเร็วมีประสิทธิภาพ

(7.)การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

ระดับ Level 1

1. ผู้อำนวยการสำนักบริหาร มีการจัดทำรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ

2. ผู้อำนวยการสำนักบริหาร มีการแจ้งเวียนให้ทุกหน่วยงานในสังกัดกรมฯ ทราบปัญหาและภัยคุกคามใหม่ๆที่เกิดขึ้น เพื่อเป็นการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงที ที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย รวมทั้งแนวทางปฏิบัติที่เหมาะสมและมีประสิทธิภาพ

3. คณะกรรมการ CSO ระดับกรม มีปฏิบัติหน้าที่ตามอำนาจในการอนุมัติการตัดสินใจในการอนุญาตให้มีการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันหรือไม่และในขอบเขตอำนาจ

4. คณะกรรมการ CSO ระดับกรม มีการจัดระบบที่ทำให้เกิดการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานเพื่อให้เกิดการพัฒนาความรู้เกี่ยวกับข้อมูลและการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัย

5. คณะกรรมการ CSO ระดับหน่วยงาน มีการประเมินผลการปฏิบัติในของหน่วยงานว่าเป็นไปตามแนวทางการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงที ที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย และมีประเมินผลการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานกับหน่วยงานอื่นๆ

6. ร้อยละของปัญหาด้านการรักษาความมั่นคงปลอดภัย ของแต่ละหน่วยงานสามารถแก้ไขและเตรียมความพร้อมในการเผชิญปัญหาภัยคุกคามใหม่ได้อย่างมีประสิทธิภาพ ร้อยละ 40

7. จำนวนครั้งบุคลากรที่ปฏิบัติงานด้าน IT เกิดการแลกเปลี่ยนเรียนรู้ เกี่ยวกับข้อมูลและการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัย ไม่น้อยกว่า 10 ครั้ง/ปี

ระดับ Level 2

1. ผู้อำนวยการสำนักบริหาร มีการจัดทำรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ

2. ผู้อำนวยการสำนักบริหาร มีการแจ้งเวียนให้ทุกหน่วยงานในสังกัดกรมฯ ทราบปัญหาและภัยคุกคามใหม่ๆที่เกิดขึ้น เพื่อเป็นการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงที ที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย รวมทั้งแนวทางปฏิบัติที่เหมาะสมและมีประสิทธิภาพ

3. คณะกรรมการ CSO ระดับกรม มีปฏิบัติหน้าที่ตามอำนาจในการอนุมัติการตัดสินใจในการอนุญาตให้มีการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันหรือไม่และในขอบเขตอำนาจ

4. คณะกรรมการ CSO ระดับกรม มีการจัดระบบที่ทำให้เกิดการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน เพื่อให้เกิดการพัฒนาความรู้เกี่ยวกับข้อมูลและการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัย

5. คณะกรรมการ CSO ระดับหน่วยงาน มีการประเมินผลการปฏิบัติในของหน่วยงานว่าเป็นไปตามแนวทางการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงที ที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย และมีประเมินผลการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานกับหน่วยงานอื่นๆ

6. ร้อยละของปัญหาด้านการรักษาความมั่นคงปลอดภัย ของแต่ละหน่วยงานสามารถแก้ไขและเตรียมความพร้อมในการเผชิญปัญหาภัยคุกคามใหม่ได้อย่างมีประสิทธิภาพ ร้อยละ 60

7. จำนวนครั้งบุคลากรที่ปฏิบัติงานด้าน IT เกิดการแลกเปลี่ยนเรียนรู้ เกี่ยวกับข้อมูลและการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัย ไม่น้อยกว่า 20 ครั้ง/ปี

ระดับ Level 3

1. ผู้อำนวยการสำนักบริหาร มีการจัดทำรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ

2. ผู้อำนวยการสำนักบริหาร มีการแจ้งเวียนให้ทุกหน่วยงานในสังกัดกรมฯ ทราบปัญหาและภัยคุกคามใหม่ๆที่เกิดขึ้น เพื่อเป็นการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงที ที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย รวมทั้งแนวทางปฏิบัติที่เหมาะสมและมีประสิทธิภาพ

3. คณะกรรมการ CSO ระดับกรม มีปฏิบัติหน้าที่ตามอำนาจในการอนุมัติการตัดสินใจในการอนุญาตให้มีการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันหรือไม่และในขอบเขตอำนาจ

4. คณะกรรมการ CSO ระดับกรม มีการจัดระบบที่ทำให้เกิดการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน เพื่อให้เกิดการพัฒนาความรู้เกี่ยวกับข้อมูลและการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัย

5. คณะกรรมการ CSO ระดับหน่วยงาน มีการประเมินผลการปฏิบัติในของหน่วยงานว่าเป็นไปตามแนวทางการแจ้งเตือนให้ระวังในการปฏิบัติงานได้อย่างทันท่วงที ที่อาจเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัย และมีประเมินผลการแลกเปลี่ยนเรียนรู้ด้านภัยคุกคามหรือช่องโหว่ที่อาจเกิดความไม่มั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานกับหน่วยงานอื่นๆ

6. ร้อยละของปัญหาด้านการรักษาความมั่นคงปลอดภัย ของแต่ละหน่วยงานสามารถแก้ไขและเตรียมความพร้อมในการเผชิญปัญหาภัยคุกคามใหม่ได้อย่างมีประสิทธิภาพ ร้อยละ 80

7. จำนวนครั้งบุคลากรที่ปฏิบัติงานด้าน IT เกิดการแลกเปลี่ยนเรียนรู้ เกี่ยวกับข้อมูลและการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัย ไม่น้อยกว่า 30 ครั้ง/ปี

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)
หมายเลขเอกสาร WI0301

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร ซึ่งดำเนินการตรวจสอบเกี่ยวกับความเสี่ยงอันเกิดจากการกระทำของบุคลากร จากการขโมย การฉ้อโกงและการใช้อุปกรณ์ผิดวัตถุประสงค์ และการตรวจสอบกระบวนการสร้างความตระหนักถึงความเข้าใจเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยของบุคลากรในองค์กร เพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติงาน รวมทั้งให้บุคลากรหรือพนักงานผู้รับจ้างทราบการปฏิบัติในระหว่างปฏิบัติงานและเมื่อสิ้นสุดการปฏิบัติงาน/โยกย้ายหรือสิ้นสุดหน้าที่ หรือสิ้นสุดการจ้าง

2.0 ขอบข่าย

วิธีการปฏิบัติงานนี้ ครอบคลุมการสอบทาน ดังนี้

1.กระบวนการสรรหาบุคลากร/คนเข้าทำงาน **(Prior to employment)** โดยมีวัตถุประสงค์: เพื่อให้มั่นใจได้ว่า บุคลากร (Employees) และผู้รับจ้างเหมา (Contractors) และผู้รับจ้างเหมาต่อช่วง รวมทั้งบุคลากรภายนอก เหล่านั้น เข้าใจหน้าที่และความรับผิดชอบของตน รวมถึงการสรรหาคนทำงานที่มีความเหมาะสมกับบทบาทที่ได้รับมอบหมาย หน่วยงานต้องกำหนดมาตรการ/สัญญาจ้างที่ครอบคลุมประเด็น ดังนี้ไว้

1.1 การกำหนดบทบาทหน้าที่ความรับผิดชอบ (Roles and responsibilities) ของบุคลากร (Employees) และผู้รับจ้างเหมา (Contractors) และผู้รับจ้างเหมาต่อช่วง รวมทั้งบุคลากรภายนอก เหล่านั้น สอดคล้องและปฏิบัติตามกฎ ระเบียบเกี่ยวกับความมั่นคงปลอดภัยขององค์กร

1.2 การคัดกรองประวัติ(Screening) หรือการตรวจสอบประวัติบุคคล (Background Verification Checking) เน้นการคัดกรองคนที่ไม่มีประวัติเสื่อมเสีย หรือ พัวพันกับอาชญากรรม และมีความรู้ ความสามารถเหมาะกับการปฏิบัติงานในหน้าที่ความรับผิดชอบที่กำหนดไว้

1.3 การกำหนดเงื่อนไขการจ้างงาน(Terms and conditions of employment) การจัดทำสัญญาจ้างที่ครอบคลุมเพียงพอและสอดคล้องกับการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร

2. ระหว่างที่ยังเป็นพนักงาน (during employment) โดยมีวัตถุประสงค์: เพื่อให้มั่นใจว่าบุคลากรทุกคน และบุคลากรที่ติดต่อหรือควบคุมกำกับงานผู้รับจ้างเหมา/ผู้รับเหมาต่อช่วง มีความตระหนักในข้อมูลภัยคุกคามความปลอดภัย และรับทราบบทบาทหน้าที่ ความรับผิดชอบ รวมทั้งมีความพร้อมในการสนับสนุนนโยบายความปลอดภัยขององค์กรในระหว่างการทำงาน เพื่อลดความเสี่ยงจากการผิดพลาดของมนุษย์

2.1 การฝึกอบรม (Information security awareness, education and training) เพื่อให้เกิดความตระหนักในข้อมูลภัยคุกคามความปลอดภัย และรับทราบบทบาทหน้าที่ ความรับผิดชอบ รวมทั้งมีความพร้อมในการสนับสนุนนโยบายความปลอดภัยขององค์กรในระหว่างการทำงานในองค์กร

2.2 การกำหนดบทลงโทษ (Disciplinary process) เมื่อมีการละเมิดมาตรการที่กำหนดนี้

3. เมื่อสิ้นสุดการจ้างหรือลาออกหรือโอนย้าย (Termination and change of employment) โดยมีวัตถุประสงค์: เพื่อให้แน่ใจว่าบุคลากรขององค์กร หรือผู้รับจ้างเหมา และผู้รับจ้างเหมาต่อช่วง หรือบุคลากรภายนอกองค์กร มีการสิ้นสุดการจ้างหรือลาออก/โอนย้ายออกจากองค์กรหรือการเปลี่ยนแปลงการจ้างงาน โดยหน่วยงานต้องกำหนดมาตรการ/สัญญาจ้างที่ครอบคลุมประเด็น ดังนี้ไว้

3.1 บทบาทหน้าที่ความรับผิดชอบ (Termination responsibilities) หน่วยงานต้องกำหนดขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

3.2 การกลับมาของสินทรัพย์ขององค์กร (Return of assets) บุคลากรทุกคน หรือผู้รับจ้างเหมาและผู้รับจ้างเหมาต่อช่วย รวมทั้งบุคลากรภายนอกที่เข้ามาปฏิบัติงานในองค์กร เมื่อมีการเลิกจ้างงานของพวกเขาสัญญาหรือข้อตกลง หน่วยงานต้องกำหนดว่าต้องคืนสินทรัพย์ขององค์กรทั้งหมดที่อยู่ในครอบครองใดบ้าง

3.3 การถอนถอดสิทธิในการเข้าถึงข้อมูลขององค์กร (Removal of access rights) เมื่อมีการสิ้นสุดการจ้างงาน หรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.กระบวนการสรรหาบุคลากร/คนเข้าทำงาน		
เพื่อป้องกันความเสี่ยงในการสรรหาบุคลากรเข้าทำงานที่อาจก่อให้เกิดความไม่ปลอดภัยต่อระบบสารสนเทศของหน่วยงาน	1.1ต้องมีการกำหนดบทบาทหน้าที่ความรับผิดชอบ (Roles and responsibilities) ของบุคลากร (Employees) และผู้รับจ้างเหมา (Contractors) และผู้รับจ้างเหมาต่อช่วง รวมทั้งบุคลากรภายนอกเหล่านั้น ให้สอดคล้องและปฏิบัติตามกฎ ระเบียบเกี่ยวกับความมั่นคงปลอดภัยขององค์กร	-ตรวจสอบเอกสารการสรรหาบุคลากร/คนเข้าทำงานว่ามีการกำหนดบทบาทและหน้าที่ความรับผิดชอบที่ชัดเจนและสอดคล้องและปฏิบัติตามกฎ ระเบียบเกี่ยวกับความมั่นคงปลอดภัยขององค์กร -สอบทาน/สัมภาษณ์/สอบถามกระบวนการสรรหาบุคลากร/คนเข้าทำงาน -ประเมินความเสี่ยงในการสรรหาบุคลากร/คนเข้าทำงาน
	1.2 การคัดกรองประวัติ (Screening) หรือการตรวจสอบประวัติบุคคล (Background Verification Checking) เน้นการคัดกรองคนที่ไม่มีประวัติเสื่อมเสีย หรือ พัวพันกับอาชญากรรม และมีความรู้ ความสามารถเหมาะกับการปฏิบัติงานในหน้าที่ความรับผิดชอบที่กำหนดไว้	-ตรวจสอบเอกสารการคัดกรอง/สรรหาบุคลากร/คนเข้าทำงาน เกี่ยวกับประวัติเสื่อมเสีย หรือ พัวพันกับอาชญากรรม และมีความรู้ ความสามารถเหมาะกับการปฏิบัติงานในหน้าที่ความรับผิดชอบที่กำหนดไว้ -สอบทานกระบวนการคัดกรองประวัติบุคลากรและความรู้ความสามารถในการปฏิบัติงาน
	1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment) การจัดทำสัญญาจ้างที่ครอบคลุมเพียงพอและสอดคล้องกับการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร	-ตรวจสอบการกำหนดเงื่อนไขการจ้างงานว่าครอบคลุมเพียงพอและสอดคล้องกับการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
2.ระหว่างการปฏิบัติงานในองค์กร		
เพื่อให้เกิดความตระหนักในข้อมูลภัยคุกคามความปลอดภัย และรับทราบบทบาทหน้าที่ ความรับผิดชอบ รวมทั้งมีความพร้อมในการสนับสนุนนโยบายความปลอดภัยขององค์กรในระหว่างการทำงานในองค์กร	2.1 มีการฝึกอบรม โดยจัดหลักสูตรการอบรม และประเมินผลการอบรมอย่างชัดเจน อย่างน้อยปีละครั้ง 2.2 มีการชี้แจงหรือแลกเปลี่ยนความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านระบบสารสนเทศเป็นระยะอย่างเหมาะสม	-ตรวจสอบเอกสารการจัดการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศหน่วยงานและการประเมินผล -สอบทาน/สัมภาษณ์กระบวนการจัดอบรมดังกล่าว -ตรวจสอบหลักฐานการชี้แจงหรือแลกเปลี่ยนความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านระบบสารสนเทศตามระยะเวลาที่เหมาะสม -สอบทาน/สัมภาษณ์กระบวนการชี้แจงหรือแลกเปลี่ยนความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านระบบสารสนเทศ
	2.3 มีการกำหนดบทลงโทษในการละเมิดแนวทางปฏิบัติ/มาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่หน่วยงานกำหนด	-ตรวจสอบการกำหนดบทลงโทษในการละเมิดแนวทางปฏิบัติ/มาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ -สอบทาน/สัมภาษณ์กระบวนการลงโทษการละเมิดแนวทางปฏิบัติ/มาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
3.เมื่อสิ้นสุดการจ้างหรือย้ายหรือลาออก		
เพื่อให้แน่ใจว่าบุคลากรขององค์กรหรือผู้รับจ้างเหมา และผู้รับจ้างเหมาต่อช่วง หรือบุคลากรภายนอกองค์กรมีการสิ้นสุดการจ้างหรือลาออก/โอนย้ายออกจากองค์กรหรือการเปลี่ยนแปลงการจ้างงาน	3.1 บทบาทหน้าที่ความรับผิดชอบหน่วยงานต้องกำหนดขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน	-ตรวจสอบการกำหนดขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน -สัมภาษณ์การกำหนดขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน
	3.2 การกลับมาของสินทรัพย์ขององค์กร บุคลากรทุกคน หรือผู้รับจ้างเหมาและผู้รับจ้างเหมาต่อช่วง รวมทั้งบุคลากรภายนอกที่เข้ามาปฏิบัติงานในองค์กร เมื่อมีการเลิกจ้างงานของพวกเขาสัญญาหรือข้อตกลง หน่วยงานต้องกำหนดว่าต้องคืนสินทรัพย์ขององค์กรทั้งหมดที่อยู่ในครอบครองใดบ้าง	-สอบทานกระบวนการคืนทรัพย์สินขององค์กร เมื่อบุคลากรทุกคน หรือผู้รับจ้างเหมาและผู้รับจ้างเหมาต่อช่วย รวมทั้งบุคลากรภายนอกที่เข้ามาปฏิบัติงานในองค์กร เมื่อมีการเลิกจ้างงานของพวกเขาสัญญาหรือข้อตกลง -ตรวจสอบมาตรการคืนทรัพย์สินขององค์กรเมื่อสิ้นสุดการจ้างหรือมีการพ้นจากตำแหน่งหน้าที่หรือการโอนย้ายหรือลาออก

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	3.3 การถอนถอดสิทธิในการเข้าถึงข้อมูลขององค์กร เมื่อมีการสิ้นสุดการจ้างงาน หรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน	-สอบทานกระบวนการถอนถอดสิทธิในการเข้าถึงข้อมูลขององค์กร เมื่อมีการสิ้นสุดการจ้างงาน หรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน **โดยสุ่มตรวจการเข้าถึงระบบข้อมูลขององค์กรด้วยสิทธิของบุคลากรที่สิ้นสุดการจ้างงาน** หรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน -ตรวจสอบมาตรการ/แนวทางปฏิบัติในการถอดถอนสิทธิของบุคลากรที่สิ้นสุดการจ้าง/โอนย้ายหรือลาออก

เกณฑ์การประเมินความเสี่ยง

(1.) ก่อนการจ้างหรือสรรหาบุคลากร/คนเข้าทำงาน

1.1 การกำหนดบทบาทหน้าที่ความรับผิดชอบ ให้สอดคล้องกับการปฏิบัติตามนโยบาย/แนวทางปฏิบัติ/มาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน

ระดับ Level 1

-มีการกำหนดแนวทางปฏิบัติ/มาตรการ/ขั้นตอนการปฏิบัติ การกำหนดบทบาทหน้าที่ความรับผิดชอบ แต่ยังไม่ครอบคลุมความเสี่ยงในการเข้ามาปฏิบัติงานโดยไม่สอดคล้องกับการปฏิบัติตามนโยบาย/แนวทางปฏิบัติ/มาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน

ระดับ Level 2

-มีการปฏิบัติตามแนวทางปฏิบัติ/มาตรการการกำหนดบทบาทหน้าที่ความรับผิดชอบให้ครอบคลุมความเสี่ยงในการเข้ามาปฏิบัติงานที่สอดคล้องกับการปฏิบัติตามนโยบาย/แนวทางปฏิบัติ/มาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงที่พบ จากสาเหตุบุคลากรที่เข้ามาปฏิบัติงานในองค์กร

1.2 การคัดกรองประวัติบุคลากร

ระดับ Level 1

-มีการกำหนดแนวทางปฏิบัติ/มาตรการ/ขั้นตอนการปฏิบัติ ในการคัดกรองประวัติหรือการตรวจสอบประวัติบุคคล (Background Verification Checking) เน้นการคัดกรองคนที่ไม่มีประวัติเสื่อมเสีย หรือ พัวพันกับอาชญากรรม และมีความรู้ ความสามารถเหมาะกับการปฏิบัติงานในหน้าที่ความรับผิดชอบที่กำหนดไว้

ระดับ Level 2

-มีปฏิบัติตามแนวทางปฏิบัติ/มาตรการ/ขั้นตอนการปฏิบัติ ในการคัดกรองประวัติหรือการตรวจสอบประวัติบุคคล (Background Verification Checking) เน้นการคัดกรองคนที่ไม่มีประวัติเสื่อมเสีย หรือ พัวพันกับอาชญากรรม และมีความรู้ ความสามารถเหมาะกับการปฏิบัติงานในหน้าที่ความรับผิดชอบที่กำหนดไว้อย่างครบถ้วน

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงที่พบ จากสาเหตุบุคลากรที่เข้ามาปฏิบัติงานในองค์กร

1.3 การกำหนดเงื่อนไขในการจ้างงาน

ระดับ Level 1

-มีการกำหนดแนวปฏิบัติ/มาตรการเกี่ยวกับการกำหนดเงื่อนไขในการจ้างที่ครอบคลุมความเสี่ยงในการจ้างงานเข้ามาปฏิบัติในองค์กร

ระดับ Level 2

-มีการปฏิบัติตามแนวปฏิบัติ/มาตรการเกี่ยวกับการกำหนดเงื่อนไขในการจ้างที่ครอบคลุมความเสี่ยงในการจ้างงานเข้ามาปฏิบัติในองค์กรอย่างครบถ้วน

ระดับ Level 3

-ไม่มีปัญหาหรือความเสี่ยงที่เกิดจากการกำหนดเงื่อนไขการจ้างงาน

(2.) ระหว่างการปฏิบัติงาน

2.1 การฝึกอบรม

ระดับ Level 1

-มีการกำหนดแนวปฏิบัติ/มาตรการเกี่ยวกับการฝึกอบรมเพื่อให้เกิดความตระหนักในข้อมูลภัยคุกคามความปลอดภัย และรับทราบบทบาทหน้าที่ ความรับผิดชอบ รวมทั้งมีความพร้อมในการสนับสนุนนโยบายความปลอดภัยขององค์กรในระหว่างการทำงานในองค์กร

ระดับ Level 2

-มีการปฏิบัติตามแนวปฏิบัติ/มาตรการเกี่ยวกับการฝึกอบรม โดยมีการจัดหลักสูตรและดำเนินการฝึกอบรมให้ได้ประสิทธิภาพ ประสิทธิผลและการรายงานการประเมินผลการฝึกอบรม เพื่อนำข้อมูลสู่การพัฒนาปรับปรุงต่อไป

ระดับ Level 3

-มีการชี้แจงหรือแลกเปลี่ยนความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านระบบสารสนเทศเป็นระยะอย่างเหมาะสม

-ไม่พบปัญหาหรือความเสี่ยงจากการปฏิบัติงานของผู้ปฏิบัติงานทั่วไปในองค์กรและผู้ดูแลระบบต่อความไม่มั่นคงปลอดภัยของระบบสารสนเทศหน่วยงาน

2.2 บทลงโทษ

ระดับ Level 1

-มีการกำหนดแนวปฏิบัติ/มาตรการเกี่ยวกับการกำหนดบทลงโทษเมื่อมีผู้ละเมิด

ระดับ Level 2

-มีการปฏิบัติตามแนวปฏิบัติ/มาตรการเกี่ยวกับการกำหนดบทลงโทษเมื่อมีผู้ละเมิด

ระดับ Level 3

-ไม่พบปัญหาหรือความเสี่ยงในการละเมิดแนวปฏิบัติ/มาตรการที่กำหนดไว้

(3.)เมื่อสิ้นสุดการจ้างหรือโอนย้าย/ลาออก

3.1 บทบาทหน้าที่ความรับผิดชอบ หน่วยงานต้องกำหนดขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

ระดับ Level 1

-มีการกำหนดแนวปฏิบัติ/มาตรการเกี่ยวกับกำหนดขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

ระดับ Level 2

-มีการปฏิบัติให้เป็นไปตามแนวปฏิบัติ/มาตรการเกี่ยวกับกำหนดขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

ระดับ Level 3

-ไม่พบปัญหาหรือความเสี่ยงเกี่ยวกับการไม่ปฏิบัติตามขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

3.2 การกลับมาของสินทรัพย์ขององค์กร

ระดับ Level 1

-มีการกำหนดแนวปฏิบัติ/มาตรการเกี่ยวกับการกลับมาของสินทรัพย์ขององค์กรสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

ระดับ Level 2

-มีการปฏิบัติให้เป็นไปตามแนวปฏิบัติ/มาตรการเกี่ยวกับการกลับมาของสินทรัพย์ขององค์กรสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

ระดับ Level 3

-ไม่พบปัญหาหรือความเสี่ยงเกี่ยวกับการไม่ปฏิบัติตามแนวปฏิบัติ/มาตรการเกี่ยวกับการกลับมาของสินทรัพย์ขององค์กรสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

-ไม่มีการฝ่าฝืนแนวปฏิบัติ/มาตรการเกี่ยวกับการกลับมาของสินทรัพย์ขององค์กรสำหรับการดำเนินการเลิกจ้างงานหรือการเปลี่ยนแปลงของการจ้างงาน

3.3 การถอนถอดสิทธิในการเข้าถึงข้อมูลขององค์กร เมื่อมีการสิ้นสุดการจ้างงาน หรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน

ระดับ Level 1

-มีการกำหนดแนวปฏิบัติ/มาตรการเกี่ยวกับการถอนถอดสิทธิในการเข้าถึงข้อมูลขององค์กร เมื่อมีการสิ้นสุดการจ้างงาน หรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน

ระดับ Level 2

-มีการปฏิบัติให้เป็นไปตามแนวปฏิบัติ/มาตรการเกี่ยวกับการถอนถอดสิทธิในการเข้าถึงข้อมูลขององค์กร เมื่อมีการสิ้นสุดการจ้างงาน หรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน

ระดับ Level 3

-ไม่พบปัญหาหรือความเสี่ยงเกี่ยวกับการปฏิบัติตามการถอนถอดสิทธิในการเข้าถึงข้อมูลขององค์กร เมื่อมีการสิ้นสุดการจ้างงาน หรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน

-ไม่มีการไม่ถอนถอดสิทธิในการเข้าถึงข้อมูลองค์กรของบุคลากรที่การสิ้นสุดการจ้างงานหรือการโยกย้าย/โอนหรือการพ้นจากตำแหน่งที่ปฏิบัติงาน

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset Management)
หมายเลขเอกสาร WI0401

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset Management) ซึ่งเป็นการสอบทานกระบวนการบริหารทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดการใช้งานอย่างคุ้มค่า ได้ประสิทธิภาพและประสิทธิผล และควบคุมการสูญหายของทรัพย์สินด้านเทคโนโลยีสารสนเทศ

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

(1) การบริหารจัดการบัญชีทรัพย์สิน (Inventory of assets)
1.1. หน่วยงานจัดทำทะเบียนบัญชีทรัพย์สิน (อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software) ประกอบด้วย ชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ
1.2.หน่วยงานขึ้นทะเบียนทรัพย์สินที่ได้รับจัดสรรใหม่ทุกครั้ง
1.3.มีการตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง

(2) ผู้ถือครองทรัพย์สิน (ownership of assets)
2.1 หน่วยงานต้องระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software
2.2 มีการปรับปรุงรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์เครือข่ายและ Software ทุกครั้งเมื่อมีการเปลี่ยนแปลง / ทำหนังสือขอใช้ ระบุระยะเวลาในการใช้

(3) การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)
3.1 การจัดทำกฎ ระเบียบ หลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับ
3.2 ภารกิจและบุคลากรและ มีการทบทวนปีละ 1 ครั้ง
3.3 การจัดทำคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์-เครือข่ายและ software รวมทั้งกำหนดขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์
3.4 การประกาศใช้ กฎ ระเบียบ หลักเกณฑ์ และคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์เครือข่าย และ Software ให้ผู้ใช้

3.5 การจัดให้มีการตรวจสอบ บำรุงรักษา อุปกรณ์คอมพิวเตอร์ เครือข่ายและsoftware ให้มีความพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง

(4) การคืนทรัพย์สิน (Return of assets)

4.1 มีการกำหนดนโยบายให้ผู้ใช้ต้องคืนทรัพย์สินของกรมทั้งหมดที่กรมถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา สิ้นสุดข้อตกลงการจ้าง หรือทุกครั้งที่มีการเปลี่ยนแปลงกรม

(5) การจัดชั้นความลับของสารสนเทศ (Information classification)

5.1 มีการการจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)

5.2 หน่วยงานกำหนดชั้นความลับสารสนเทศ

5.3 มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

(6) การกำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการ เช่น กำหนดให้มีการใส่รหัสผ่านก่อนการใช้อุปกรณ์ อุปกรณ์เหล่านั้นต้องลงทะเบียนก่อนเข้าสู่ระบบ

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.การบริหารจัดการบัญชีทรัพย์สิน (Inventory of assets)		
-เพื่อให้ระบบบริหารจัดการงานด้านทรัพย์สินเทคโนโลยีสารสนเทศของหน่วยงานมีประสิทธิภาพ -เพื่อให้มั่นใจได้ว่าทะเบียนสินทรัพย์ด้านเทคโนโลยีสารสนเทศมีความครบถ้วน ถูกต้อง และปลอดภัย	1.1 จัดทำทะเบียนบัญชีทรัพย์สิน (อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software) ประกอบด้วย ชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ	-ตรวจสอบและพิสูจน์**ความครบถ้วนและถูกต้องของทะเบียน**หรือบัญชีทรัพย์สิน ซึ่งอย่างน้อยต้องประกอบด้วยชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ
เพื่อให้สินทรัพย์ด้านเทคโนโลยีสารสนเทศของหน่วยงานที่มีการจัดสรรเพิ่มใหม่มีการถูกบันทึกลงทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศของหน่วยงานเพื่อให้ทะเบียนดังกล่าวมีความเป็นปัจจุบัน	1.2 ขึ้นทะเบียนทรัพย์สินที่ได้รับจัดสรรใหม่ทุกครั้ง	-ตรวจสอบและพิสูจน์ทรัพย์สินที่ได้รับจัดสรรใหม่ในปีนั้นๆ ว่ามีอยู่ในทะเบียนหรือไม่
เพื่อให้สินทรัพย์ด้านเทคโนโลยีสารสนเทศของหน่วยงานมีการตรวจสอบ ปรับปรุง ทบทวน ความครบถ้วน ใช้งานได้ และมีอยู่จริงของทรัพย์สินด้านเทคโนโลยีสารสนเทศของหน่วยงาน	1.3 การตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ 1 ครั้ง	-ตรวจนับความมีอยู่จริงของทรัพย์สินถูกต้องตรงกับทะเบียน กำหนดให้เป็นการสุ่มตรวจนับแบบเป็นระบบ(Systematic Sampling) โดยมีขั้นตอนดัง WK1_PD04 -ตรวจความถูกต้องคุณลักษณะของทรัพย์สินที่ตรงกับทะเบียนทรัพย์สิน โดยการสุ่มตรวจสอบคุณลักษณะตามขั้นตอนการสุ่มตรวจแบบเป็นระบบ(WK1_PD04) และตรวจสอบคุณลักษณะของทรัพย์สินที่ถูกต้องตรงกับทะเบียน ตามขั้นตอนการตรวจคุณลักษณะของทรัพย์สิน WK2_PD04

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
2.ผู้ถือครองทรัพย์สิน (ownership of assets)		
เพื่อให้ทรัพย์สินด้านเทคโนโลยีสารสนเทศของหน่วยงานสามารถทราบได้ถึงผู้ถือครอง คนปัจจุบันได้	2.1 ระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software	-ตรวจสอบรายชื่อผู้ถือครองในทะเบียนทรัพย์สินว่ามีการระบุหรือไม่ -ตรวจสอบ/ซักถามรายชื่อผู้ถือครองในทะเบียนทรัพย์สินให้ตรงกับผู้ถือครองตัวจริง โดยวิธีการสุ่มตรวจแบบเป็นระบบ (Systematic Sampling) ดัง WK1_PD04
	2.2 มีการปรับปรุงรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์เครือข่ายและ Software ทุกครั้งเมื่อมีการเปลี่ยนแปลง / ทำหนังสือขอใช้ ระบุระยะเวลาในการใช้	-ตรวจสอบรายชื่อบุคลากรใหม่หรือบุคลากรที่มีการโอน/ย้าย/ลาออก/สิ้นสุดการปฏิบัติงานในหน่วยงานแล้ว ว่าตรงกับทะเบียนทรัพย์สินที่ระบุผู้ถือครองหรือไม่
3.การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)		
เพื่อให้หน่วยงานมีกฎ ระเบียบ หรือหลักเกณฑ์ในการจัดสรรอุปกรณ์คอมพิวเตอร์อย่างเหมาะสม	3.1 การจัดทำกฎ ระเบียบ หลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับภารกิจและบุคลากรและ มีการทบทวนปีละ 1 ครั้ง	-ตรวจสอบเอกสารที่แสดงให้เห็นถึงกฎระเบียบ หลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับภารกิจและบุคลากร -สอบทานวิธีการทบทวนกฎ ระเบียบหลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์
เพื่อให้หน่วยงานมีแนวทางในการปฏิบัติเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์-เครือข่ายและ software รวมทั้งกำหนดขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์	3.2 การจัดทำคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์-เครือข่ายและ software รวมทั้งกำหนดขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์	-ตรวจสอบคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์-เครือข่ายและ software รวมทั้งกำหนดขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์ โดยใช้วิธีการสุ่มตรวจตามประเภทของอุปกรณ์ -ตรวจสอบคุณภาพของคู่มือการใช้งาน โดยให้ผู้ปฏิบัติงาน ดำเนินการดูแลรักษาตามคู่มือ อย่างน้อย 2 คน
เพื่อให้หน่วยงานมีการสื่อสารให้บุคลากร เจ้าหน้าที่ภายในหน่วยงานทราบถึง กฎ ระเบียบ หลักเกณฑ์และ คู่มือการใช้งานอุปกรณ์คอมพิวเตอร์เครือข่าย และ Software ให้ผู้ใช้	3.3 การประกาศใช้ กฎ ระเบียบ หลักเกณฑ์ และคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ เครือข่าย และ software ให้ผู้ใช้	-สอบทาน/สัมภาษณ์วิธีการสื่อสารกฎระเบียบ หลักเกณฑ์ และคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ เครือข่าย และ software ให้ผู้ใช้
เพื่อให้หน่วยงานมีกระบวนการในการตรวจสอบ บำรุงรักษา อุปกรณ์คอมพิวเตอร์ เครือข่ายและ software ให้มีความพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง	3.4 การจัดให้มีการตรวจสอบบำรุงรักษา อุปกรณ์คอมพิวเตอร์ เครือข่ายและsoftware ให้มีความพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง	-ตรวจสอบแผนการบำรุงรักษาอุปกรณ์ -ตรวจสอบผลการดำเนินการบำรุงรักษาอุปกรณ์ เช่น รายงานผลการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
4.การคืนทรัพย์สิน (Return of assets)		
เพื่อให้หน่วยงานมีแนวทางมาตรการในการปฏิบัติเกี่ยวกับการคืนทรัพย์สินของบุคลากรที่สิ้นสุดการทำงานและลดความเสี่ยงในการสูญหายในทรัพย์สินของหน่วยงาน	4.1 มีการกำหนดนโยบายให้ผู้ใช้ต้องคืนทรัพย์สินของกรมทั้งหมดที่กรมถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา สิ้นสุดข้อตกลงการจ้าง หรือทุกครั้งที่มีการเปลี่ยนแปลงกรม	-ตรวจสอบนโยบาย/มาตรการการคืนทรัพย์สินของหน่วยงาน เมื่อสิ้นสุดการจ้างงาน หมดสัญญา สิ้นสุดข้อตกลงการจ้าง หรือทุกครั้งที่มีการเปลี่ยนแปลงกรม -ตรวจสอบผลการปฏิบัติตามนโยบาย/มาตรการการคืนทรัพย์สินของหน่วยงาน เช่น จากรายงานผลการคืนทรัพย์สิน
5. การจัดชั้นความลับของสารสนเทศ (Information classification)		
เพื่อให้ข้อมูลสารสนเทศของหน่วยงานที่มีความลับ	5.1 มีการการจัดหมวดหมู่ทรัพย์สินสารสนเทศ แบ่งเป็น ฮาร์ดแวร์ ซอฟแวร์ ข้อมูล ผู้ใช้	-ตรวจสอบทะเบียน/บัญชีของทรัพย์สินสารสนเทศว่ามีการจัดหมวดหมู่หรือไม่
	5.2 หน่วยงานกำหนดชั้นความลับสารสนเทศ แบ่งเป็น ปกติ ลับ ลับมาก ลับที่สุด	-สัมภาษณ์กระบวนการกำหนดชั้นความลับสารสนเทศ -ตรวจสอบเอกสารการกำหนดชั้นความลับสารสนเทศ เช่น รายงานการประชุม ประกาศแจ้งเวียน
เพื่อให้ข้อมูลสารสนเทศของหน่วยงานที่มีความลับ/ความสำคัญต่อหน่วยงานและองค์กร ถูกจัดเก็บตามนโยบายของกรมสนับสนุนบริการสุขภาพ	5.3มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ -ไม่ลับ คือ สามารถเผยแพร่ได้ -ลับ คือ เข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องกับงาน -ลับมาก คือ เข้าถึงได้เฉพาะหัวหน้างาน/หัวหน้ากลุ่ม -ลับที่สุด คือ เข้าถึงได้เฉพาะผู้บริหารหน่วยงานเท่านั้น	-สัมภาษณ์การกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับ -ตรวจสอบว่าหน่วยงานได้ปฏิบัติตามการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับ ได้แก่ โปรแกรม Smart ระบบสารสนเทศของหน่วยงาน
6.การกำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการ		
เพื่อป้องกันการเข้าถึงอุปกรณ์และข้อมูลสารสนเทศขององค์กร โดยไม่ได้รับอนุญาต	6.1 การกำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการ เช่น กำหนดให้มีการใส่รหัสผ่านก่อนการใช้อุปกรณ์ อุปกรณ์เหล่านั้นต้องลงทะเบียนก่อนเข้าสู่ระบบ	-ตรวจสอบแนวทางปฏิบัติ/มาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการว่าได้มีการกำหนดไว้หรือไม่ -ตรวจสอบการเข้าใช้อุปกรณ์คอมพิวเตอร์ว่ามีการล็อกหน้าจอและให้เข้าด้วยรหัสผ่านหรือไม่ -ตรวจสอบการเข้าใช้งานในระบบสารสนเทศของหน่วยงานมีการล็อกและให้ลงทะเบียนก่อนเข้าสู่ระบบหรือไม่

เกณฑ์การประเมินความเสี่ยง

(1) การบริหารจัดการบัญชีทรัพย์สิน (Inventory of assets)

1.1 หน่วยงานจัดทำทะเบียนบัญชีทรัพย์สิน (อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software) ประกอบด้วย ชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ

ระดับ Level 1

หน่วยงาน มีการจัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ แต่รายละเอียดของข้อมูลในการจัดเก็บไม่ครบถ้วน

ระดับ Level 2

มีการจัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีรายละเอียดครบถ้วนตามนโยบายกรมสนับสนุนบริการสุขภาพ

ระดับ Level 3

มีการจัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ ครบถ้วนตามนโยบายกรมสนับสนุนบริการสุขภาพ และรายละเอียดของข้อมูลในการจัดเก็บครบถ้วน ถูกต้อง

1.2 หน่วยงานขึ้นทะเบียนทรัพย์สินที่ได้รับจัดสรรใหม่ทุกครั้ง

ระดับ Level 1

มีการเพิ่มทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ได้รับจัดสรรเพิ่มขึ้นมาใหม่

ระดับ Level 2

มีการเพิ่มทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ได้รับจัดสรรเพิ่มขึ้นมาใหม่ และมีวิธีการ/แนวทางในการปฏิบัติในกรณีที่มีทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศเพิ่มมาใหม่หรือได้รับจัดสรร

ระดับ Level 3

-มีการเพิ่มทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ได้รับจัดสรรเพิ่มขึ้นมาใหม่ และมีวิธีการแนวทางในการปฏิบัติในกรณีที่มีทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศเพิ่มมาใหม่หรือได้รับจัดสรร

-แสดงให้เห็นถึงขั้นตอนและผู้รับผิดชอบในการเพิ่มทรัพย์สินด้านเทคโนโลยีสารสนเทศของหน่วยงาน

1.3 มีการตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ 1 ครั้ง

ระดับ Level 1

มีการทบทวน ตรวจสอบ ปรับปรุง ทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง แต่ไม่สามารถแสดงให้เห็นถึงกระบวนการ ทบทวน ตรวจสอบ ปรับปรุงได้

ระดับ Level 2

-มีการทบทวน ตรวจสอบ ปรับปรุง ทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศมากกว่า 1 ครั้ง/ปี

-มีกระบวนการแสดงให้เห็นถึงการทบทวน ตรวจสอบ ปรับปรุง เป็นลายลักษณ์ อักษร

ระดับ Level 3

-หน่วยงาน มีการทบทวน ตรวจสอบ ปรับปรุง ทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ มากกว่า 1 ครั้ง/ปี

-มีกระบวนการแสดงให้เห็นถึงการทบทวน ตรวจสอบ ปรับปรุง เป็นลายลักษณ์ อักษร

(2) ผู้ถือครองทรัพย์สิน (ownership of assets)

2.1 หน่วยงานต้องระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software

2.2 มีการปรับปรุงรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์เครือข่ายและ Software ทุกครั้งเมื่อมีการเปลี่ยนแปลง / ทำหนังสือขอใช้ ระบุระยะเวลาในการใช้

ระดับ Level 1

-มีการระบุชื่อผู้ถือครองทรัพย์สินด้านเทคโนโลยีสารสนเทศ

ระดับ Level 2

-มีการปรับปรุงรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์เครือข่ายและ Software ทุกครั้งเมื่อมีการเปลี่ยนแปลง / ทำหนังสือขอใช้ ระบุระยะเวลาในการใช้

ระดับ Level 3

-มีกระบวนการ วิธีการ มาตรการในการเปลี่ยนแปลง ข้อมูลผู้ถือครอง

(3) การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

3.1 การจัดทำกฎ ระเบียบ หลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับภารกิจและบุคลากรและ มีการทบทวนปีละ 1 ครั้ง

ระดับ Level 1

-มีนโยบาย กฎ ระเบียบ หลักเกณฑ์ในการจัดสรรอุปกรณ์คอมพิวเตอร์ให้กับบุคลากร

ระดับ Level 2

-มีการกำหนดนโยบาย กฎ ระเบียบ หลักเกณฑ์ในการจัดสรรอุปกรณ์คอมพิวเตอร์ให้กับบุคลากรอย่างเหมาะสมและเป็นไปในรูปคณะกรรมการ

-มีการนำนโยบาย กฎ ระเบียบ หลักเกณฑ์ในการจัดสรรอุปกรณ์คอมพิวเตอร์ให้กับบุคลากรมาทบทวนอย่างน้อยปีละ 1 ครั้ง

ระดับ Level 3

-บุคลากรภายในหน่วยงานได้รับการจัดสรรอุปกรณ์คอมพิวเตอร์ตรงต่อ นโยบายของหน่วยงานที่ได้ตั้งไว้

3.2 การจัดทำคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์-เครือข่ายและ software รวมทั้งกำหนดขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์

ระดับ Level 1

-มีแนวทางในการปฏิบัติเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์-เครือข่ายและ software รวมทั้งกำหนดขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์

ระดับ Level 2

-มีกระบวนการนำแนวทาง คู่มือดังกล่าว อธิบาย/สื่อสารให้ผู้ใช้งานเข้าใจ

ระดับ Level 3

-มีการประเมินผลแนวทาง คู่มือดังกล่าวอย่างน้อยปีละ 1 ครั้ง

3.3 การประกาศใช้ กฎ ระเบียบ หลักเกณฑ์ และคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ เครือข่าย และ software ให้ผู้ใช้

ระดับ Level 1

-มีกระบวนการในการตรวจสอบ บำรุงรักษา อุปกรณ์คอมพิวเตอร์ เครือข่ายและ software ให้มีความพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง

ระดับ Level 2

-มีกระบวนการดังกล่าว และมีการนำผลการตรวจสอบ ไปสู่การพัฒนาในปีถัดไป

ระดับ Level 3

-มีการจัดทำแนวทาง คู่มือ วิธีการปฏิบัติกระบวนการในการตรวจสอบ บำรุงรักษา อุปกรณ์คอมพิวเตอร์ เครือข่ายและSoftware

3.4 การจัดให้มีการตรวจสอบ บำรุงรักษา อุปกรณ์คอมพิวเตอร์ เครือข่ายและsoftware ให้มีความพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง

ระดับ Level 1

-มีสื่อสารให้บุคลากร เจ้าหน้าที่ภายในหน่วยงานทราบถึง กฎ ระเบียบ หลักเกณฑ์ และคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ เครือข่าย และ Software ให้ผู้ใช้

ระดับ Level 2

-มีการประเมินผลการรับทราบ เข้าใจเกี่ยวกับ กฎ ระเบียบ หรือคู่มือดังกล่าวของบุคลากรภายในหน่วยงาน

ระดับ Level 3

-มีการนำผลการประเมินดังกล่าวไปสู่การพัฒนาในปีถัดไป

(4) การคืนทรัพย์สิน (Return of assets)

4.1 มีการกำหนดนโยบายให้ผู้ใช้ต้องคืนทรัพย์สินของกรมทั้งหมดที่กรมถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา สิ้นสุดข้อตกลงการจ้าง หรือทุกครั้งที่มีการเปลี่ยนแปลงกรม

ระดับ Level 1

-มีการกำหนดนโยบายให้ผู้ใช้ต้องคืนทรัพย์สินของกรมทั้งหมดที่กรมถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา สิ้นสุดข้อตกลงการจ้าง หรือทุกครั้งที่มีการเปลี่ยนแปลงกรม

ระดับ Level 2

-มีการแจ้งเวียน อธิบาย ทำความเข้าใจเกี่ยวกับนโยบายดังกล่าวให้บุคลากรภายในหน่วยงานทราบ และเข้าใจถึงเหตุผลความจำเป็น

ระดับ Level 3

-มีการตรวจเช็คทุกครั้งเมื่อมีบุคลากรภายในหน่วยงานลาออกจากการทำงาน

(5) การจัดชั้นความลับของสารสนเทศ (Information classification)

5.1 มีการการจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)

5.2 หน่วยงานกำหนดชั้นความลับสารสนเทศ

5.3 มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

ระดับ Level 1

1.มีการการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

2.หน่วยงาน ไม่มีการจัดลำดับความสำคัญและกำหนดชั้นความลับของข้อมูลสารสนเทศของหน่วยงาน

3.หน่วยงานไม่มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

ระดับ Level 2

1.มีการการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

2.หน่วยงาน มีการจัดลำดับความสำคัญและกำหนดชั้นความลับของข้อมูลสารสนเทศของหน่วยงาน

3.หน่วยงานไม่มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

ระดับ Level 3

1. มีการการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

2. หน่วยงาน มีการจัดลำดับความสำคัญและกำหนดชั้นความลับของข้อมูลสารสนเทศของหน่วยงาน

3. หน่วยงานมีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

(6) การกำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการ เช่น กำหนดให้มีการใส่รหัสผ่านก่อนการใช้อุปกรณ์ อุปกรณ์เหล่านั้นต้องลงทะเบียนก่อนเข้าสู่ระบบ

ระดับ Level 1

-หน่วยงาน ไม่มีการกำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการ เช่น กำหนดให้มีการใส่รหัสผ่านก่อนการใช้อุปกรณ์ อุปกรณ์เหล่านั้นต้องลงทะเบียนก่อนเข้าสู่ระบบ

ระดับ Level 2

-มีการกระบวนการตรวจเช็คอุปกรณ์ที่มีการยืม ข้อมูลต่าง ๆ ภายในเครื่องทุกครั้ง ก่อน-หลัง

ระดับ Level 3

-มีการประเมินผลมาตรการดังกล่าวอย่างน้อยปีละ 1 ครั้ง และนำไปสู่การพัฒนา

วิธีปฏิบัติงาน Work Instruction

เรื่อง ขั้นตอนการตรวจสอบคุณลักษณะทรัพย์สินเทคโนโลยีสารสนเทศที่ถูกต้องตรงกับทะเบียน

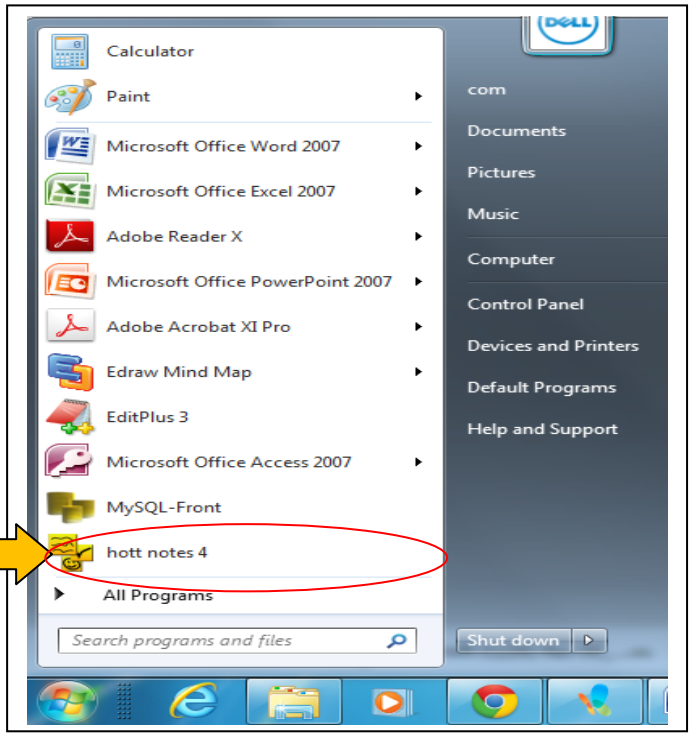
❒ เอกสารควบคุม ❒ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

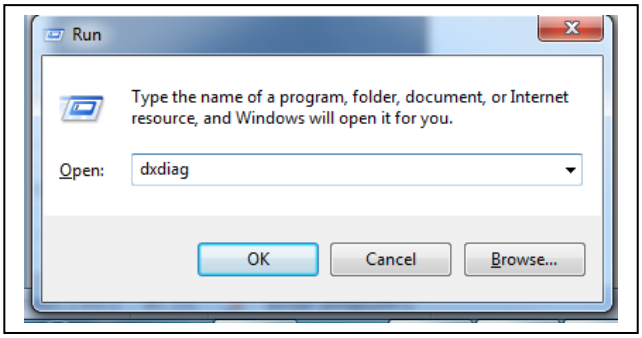
1.ประเภทเครื่องคอมพิวเตอร์

1.1 วิธีที่ 1 เข้าไปดูสเปคโดยใช้คำสั่ง DOS ดังขั้นตอนนี้

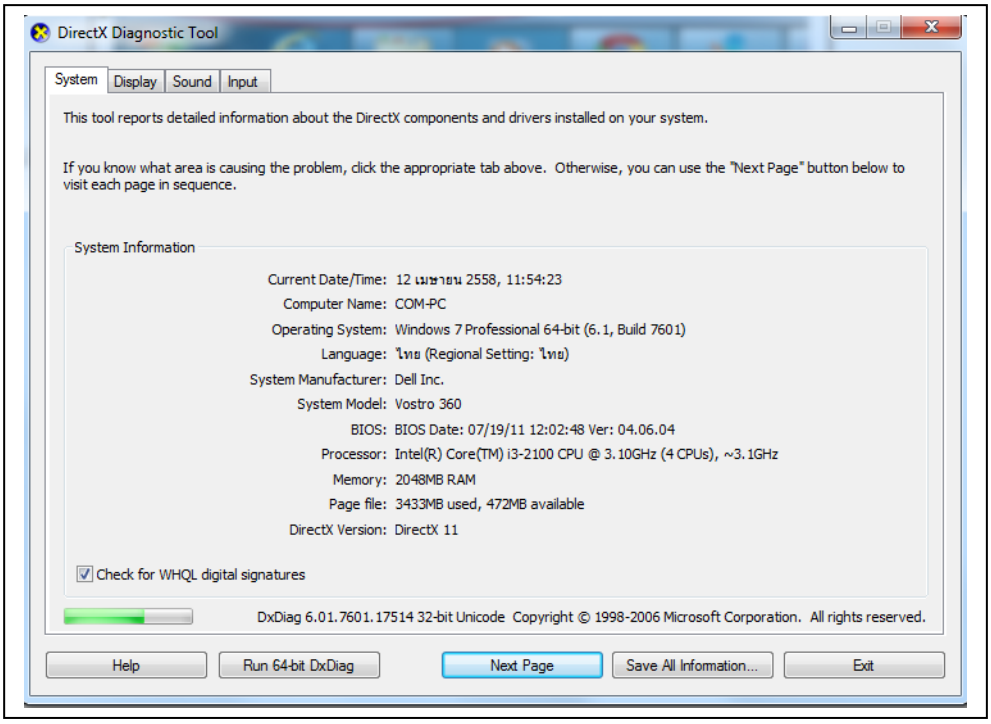
ขั้นตอนที่ 1 ไปที่ Start พิมพ์คำว่า run ในช่องว่างแล้ว Enter



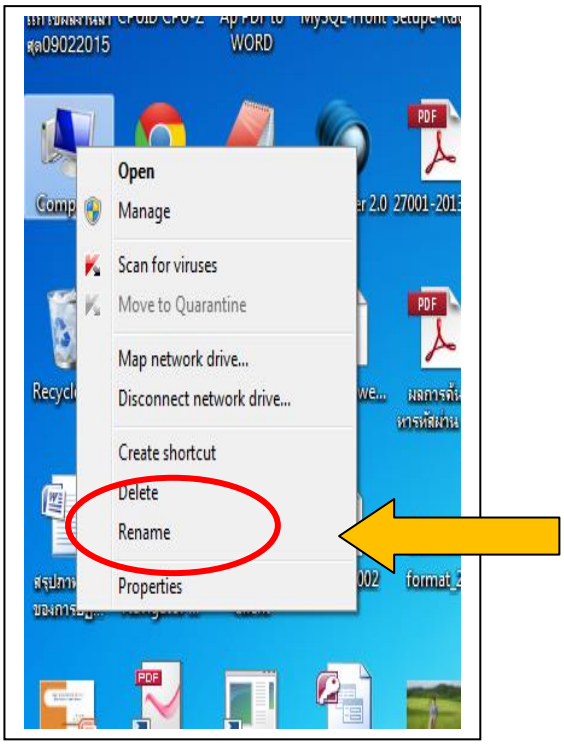
ขั้นตอนที่ 2 จะพบหน้าต่าง run พิมพ์คำว่า dxdiag ลงในช่อง open แล้วกดปุ่ม OK



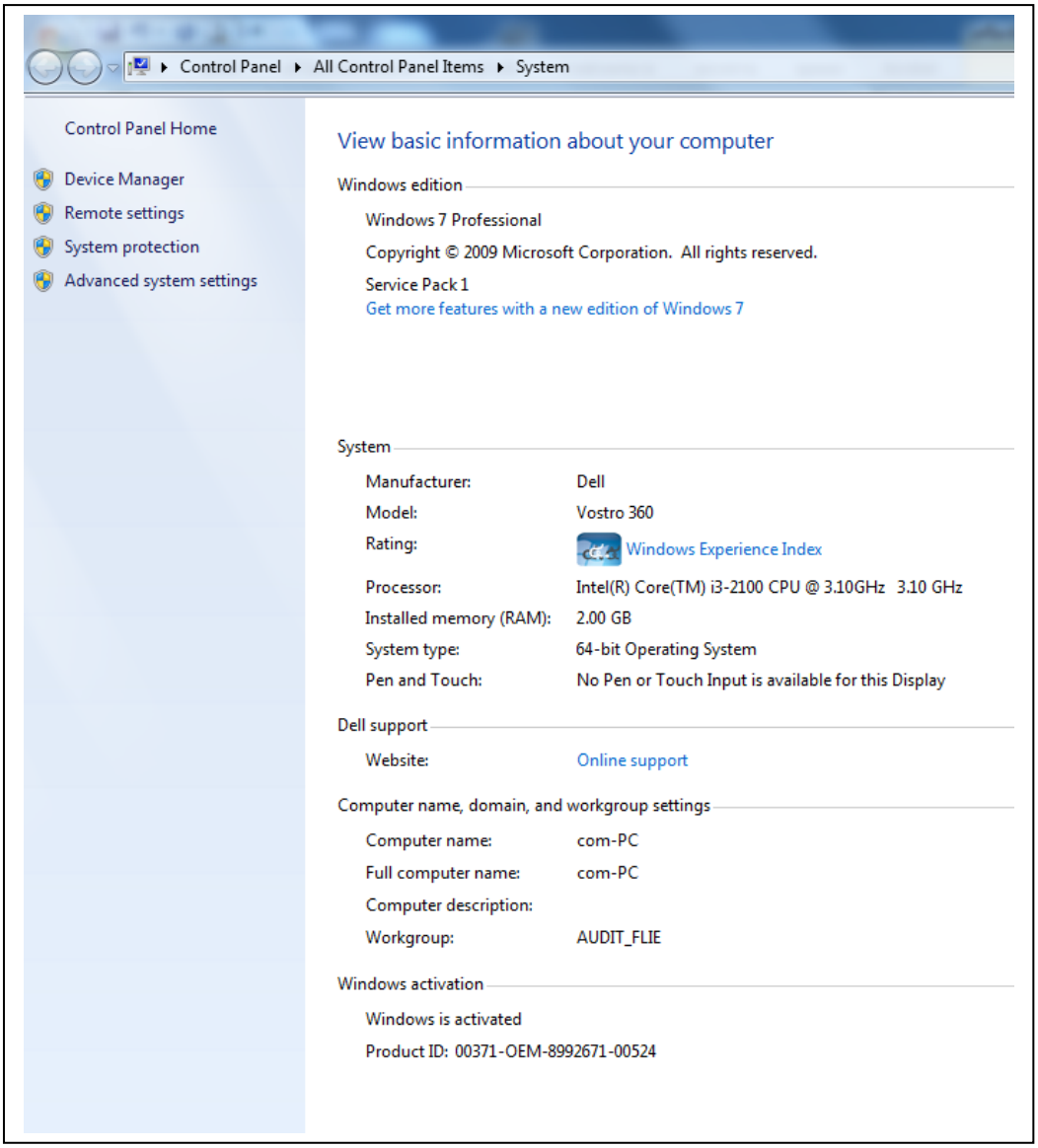
ขั้นตอนที่ 3 จะพบหน้าต่าง สามารถดูค่า CPU RAM ระบบปฏิบัติการ และกดปุ่ม Exit เพื่อออกจากโปรแกรม



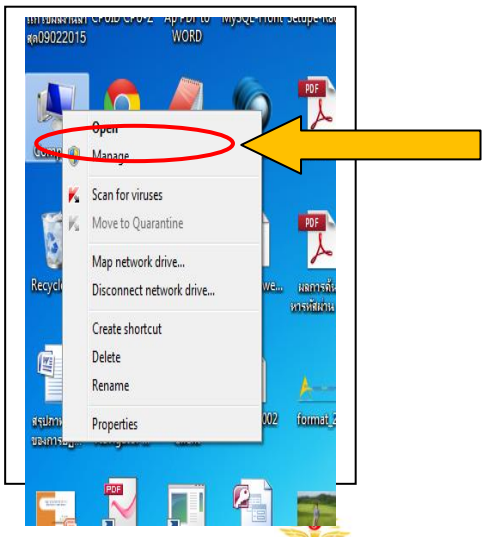
1.2 วิธีที่ 2 เอาเมาส์คลิกขวาที่ไอคอน My computer ที่อยู่หน้าจอภาพ หรือเลือก Computer แล้วเลือก Properties



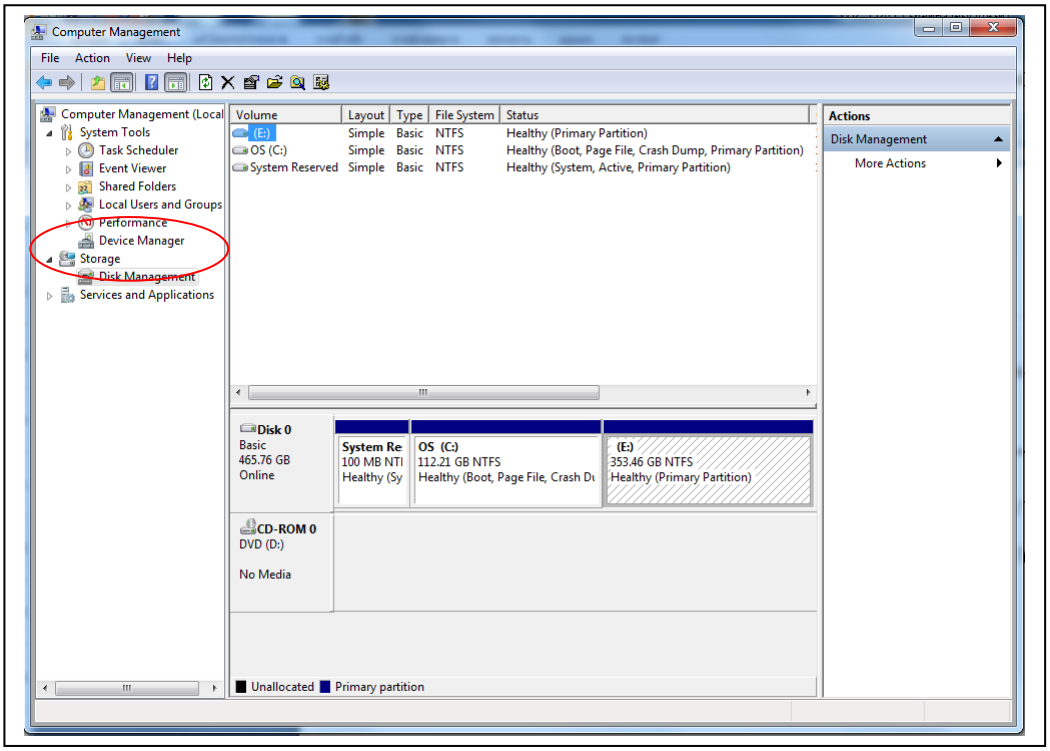
วิธีนี้จะเห็นสเปค เกี่ยวกับ CPU RAM ระบบปฏิบัติการ ชื่อ Work Group



1.3 วิธีที่ 3 ต้องการดูขนาดฮาร์ดิส เอาเมาส์คลิกขวาที่ไอคอน My computer ที่อยู่หน้าจอภาพ หรือเลือก Computer แล้วเลือก Manage แล้วเลือก Disk management



จะเห็นขนาดฮาร์ดิกส์ แบ่งเป็นกี่ไดร์ฟ



วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 5 การควบคุมการเข้าถึง (Access Control)
หมายเลขเอกสาร WI0501

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 5 การควบคุมการเข้าถึง (Access Control) เพื่อประเมินความเสี่ยงในการควบคุมการเข้าถึงระบบสารสนเทศ/ข้อมูลและอุปกรณ์ที่สำคัญขององค์กร รวมทั้งประเมินการปฏิบัติของหน่วยงานให้เป็นไปตามนโยบายที่กรมฯกำหนดไว้

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

1. นโยบายควบคุมการเข้าถึง (Access Control Policy)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
   2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)
   2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)
   2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)
   2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users) การจัดการกับรหัสผ่าน
   2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)
   การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal of adjustment of access rights)
3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)
   3.1 มีการสร้างจิตสำนึกความรับผิดชอบในการเข้าใช้งานระบบข้อมูลสารสนเทศและอุปกรณ์เครื่องมือ
   3.2 มีการกำหนดให้เจ้าหน้าที่ ที่มีอุปกรณ์คอมพิวเตอร์กำหนดรหัสผ่านในการเข้าใช้งานอุปกรณ์นั้นๆ
4. ระบบบริหารจัดการรหัสผ่าน (Password management system)
5. การควบคุมการเข้าถึงระบบ (System and application access control)

5.1 มีการออกมาตรการการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส

5.2 มีการสร้างระบบจัดเก็บ log ไฟล์ในการเข้าถึงเครือข่ายของกรม

5.3 มีการพิจารณาการเปิดเข้าใช้งาน port ของผู้ร้องขอใช้งานโดยกำหนดระยะเวลาในการใช้งานตามที่ผู้ดูแลระบบจะอนุญาต

5.4 มีการกำหนด vlan ในการเข้าใช้งานระบบเครือข่ายของกรมนั้นๆ

5.5 ถ้าไม่มีการใช้งานในระยะเวลาหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเตอร์เน็ต (session timeout) เพื่อนำสัญญาณไปให้ผู้ที่ร้องขอคนอื่นต่อไป

5.6 มีการจัดทำคู่มือขั้นตอนการใช้งาน

5.7 มีการกำหนดรหัสผ่านโดยผู้ดูแลระบบและจัดเก็บไว้ที่ผู้ดูแลระบบในรูปแบบแฟ้มเอกสารที่มีการปิดผนึกที่มิดชิด

5.8 มีการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่าง เช่น ผู้บริหาร, ผู้ปฏิบัติงาน ฯลฯ

5.9 มีการกำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น

5.10 ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

6. อุปกรณ์คอมพิวเตอร์แบบพกพา Digital device

7. การปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

8. การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

9. การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to program source code)

10. ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.นโยบายควบคุมการเข้าถึง (Access Control Policy)		
เพื่อควบคุมการเข้าถึงสินทรัพย์ข้อมูลควรได้รับการบันทึกไว้อย่างชัดเจนในนโยบายการควบคุมการเข้าถึงและวิธีการ การเข้าถึงเครือข่ายและการเชื่อมต่อควรจะจำกัด	1.1 มีการกำหนดนโยบาย/แนวทางปฏิบัติ/มาตรการ การควบคุมการเข้าถึงระบบขององค์กรที่เป็นลายลักษณ์อักษร	-ตรวจสอบนโยบาย/แนวทางปฏิบัติ/มาตรการ การควบคุมการเข้าถึงระบบขององค์กรที่เป็นลายลักษณ์อักษร
	1.2 มีการทบทวนนโยบาย/แนวทางปฏิบัติ/มาตรการ การควบคุมการเข้าถึงระบบขององค์กรอย่างน้อยปีละครั้ง	-ตรวจสอบการทบทวนนโยบาย/แนวทางปฏิบัติ/มาตรการ การควบคุมการเข้าถึงระบบขององค์กร -สัมภาษณ์เกี่ยวกับกระบวนการทบทวนนโยบาย/แนวทางปฏิบัติ/มาตรการ การควบคุมการเข้าถึงระบบขององค์กร
2.การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)		
1.เพื่อให้มั่นใจว่าผู้ใช้งานมีการเข้าถึงข้อมูลโดยได้รับการอนุญาตแล้ว 2.เพื่อให้มีการกำหนดขั้นตอน/แนวทางปฏิบัติในการลงทะเบียน/ถอนถอดสิทธิของผู้ใช้งานในระบบเครือข่าย	2.1การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน	-ทดสอบการลงทะเบียนและการถอดถอนสิทธิผู้ใช้งานในระบบสารสนเทศของหน่วยงาน ว่าระบบสามารถให้มีการลงทะเบียนและถอนถอดสิทธิผู้ใช้งานได้หรือไม่
1. เพื่อให้มั่นใจว่าสิทธิในการใช้งานของผู้ใช้งานถูกต้องและเหมาะสมในควบคุมสิทธิ 2. เพื่อให้มีการกำหนดให้มีการประชุมพิจารณาสิทธิในการเข้าถึงข้อมูลของเจ้าหน้าที่ใหม่ และมีการทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เดิม	2.2การจัดการสิทธิการเข้าถึงของผู้ใช้งาน -มีการกำหนดให้มีการพิจารณาสิทธิในการเข้าถึงข้อมูลของผู้ใช้โดยกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ -มีการทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เดิม	-ตรวจสอบการกำหนดสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศหน่วยงานและการเข้าถึงอุปกรณ์ที่ใช้งานหรือระบบเครือข่าย 1.ว่าการกำหนดสิทธิ์เหล่านั้นมีการให้สิทธิอย่างถูกต้องเหมาะสมหรือไม่ 2.และเป็นไปตามระดับชั้นความลับสารสนเทศที่หน่วยงานกำหนดหรือไม่ -สัมภาษณ์ถึงกระบวนการทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เดิม -ทดสอบสิทธิ์ของเจ้าหน้าที่เดิมว่าได้มีการปฏิบัติการให้สิทธิที่ทบทวนไว้หรือไม่
1. เพื่อให้หน่วยงานมีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ 2. เพื่อให้หน่วยงานมีการกำหนดระดับสิทธิของการเข้าใช้งานด้านระบบคอมพิวเตอร์, ระบบเครือข่ายให้เหมาะสมกับผู้ใช้งานและผู้ดูแลระบบให้เหมาะสมตามการกำหนดระดับชั้นความลับสารสนเทศ	2.3การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ -มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ -มีการกำหนดระดับสิทธิของการเข้าใช้งานด้านระบบคอมพิวเตอร์, ระบบเครือข่ายให้เหมาะสมกับผู้ใช้งานและผู้ดูแลระบบ	-ตรวจสอบการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศโดยตรวจสอบจากบัญชีสิทธิรหัสผ่านว่าอนุญาตให้ผู้ใช้งานแต่ละระดับเข้าถึงข้อมูลตามระดับชั้นความลับหรือไม่

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1. การมอบรหัสผ่านของผู้ใช้งานผ่านกระบวนการที่มีการควบคุมข้อมูลอันเป็นความลับที่เหมาะสม 2. ไม่มีปัญหาหรือความเสี่ยงในการมอบรหัสผ่านของผู้ใช้อันเป็นข้อมูลที่เป็นความลับ	2.4การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน -มีการมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ โดยมีการควบคุมผ่านกระบวนการบริหารจัดการที่เป็นทางการ	-สัมภาษณ์กระบวนการมอบข้อมูลรหัสผ่านของผู้ใช้งานและผู้ดูแลระบบ -ตรวจสอบขั้นตอนการบริหารจัดการข้อมูลรหัสผ่านของผู้ใช้งาน -ทดสอบการออกรหัสผ่านของผู้ใช้งานจากระบบว่ามีขั้นตอนเป็นไปตามที่กำหนดไว้หรือไม่
1. เพื่อให้มีการกำหนดขั้นตอนการปฏิบัติในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้งอย่างเป็นลายลักษณ์อักษร 2. เพื่อให้มีการปฏิบัติตามขั้นตอนการปฏิบัติในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง	2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน -มีการกำหนดให้เจ้าของทรัพย์สินต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง	-ตรวจสอบบัญชีสิทธิ/รหัสผ่านผู้ใช้งาน โดยการทดสอบ สุ่มตรวจรหัสผ่านผู้ใช้งานในการเข้าใช้ระบบ และใช้การสุ่มตรวจแบบเป็นระบบ(Systematic Sampling) ดังเอกสาร WI0502 -ตรวจสอบขั้นตอนการปฏิบัติในการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน
1. เพื่อให้มีการกำหนดขั้นตอนการปฏิบัติในการถอนถอดหรือปรับปรุงสิทธิในการเข้าถึงอย่างเป็นลายลักษณ์อักษร 2. เพื่อให้มีการปฏิบัติตามขั้นตอนการปฏิบัติในการถอนถอดหรือปรับปรุงสิทธิในการเข้าถึงอย่างน้อยปีละ 1 ครั้ง	2.6การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง -มีการถอดถอนสิทธิการเข้าถึงของพนักงานและลูกจ้างเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนแปลงการจ้างงาน	-ตรวจสอบขั้นตอนการปฏิบัติในการถอนถอดหรือปรับปรุงสิทธิในการเข้าถึงที่เป็นลายลักษณ์อักษร -สุ่มตรวจการถอดถอนหรือปรับปรุงสิทธิการเข้าถึงของพนักงานและลูกจ้างเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนแปลงการจ้างงาน ใช้การสุ่มตรวจแบบเป็นระบบ(Systematic Sampling) ดังเอกสาร WI0502
3.หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)		
1.สร้างจิตสำนึกให้เกิดความตระหนักในระดับความลับของข้อมูล	3.1 มีการสร้างจิตสำนึกความรับผิดชอบในการเข้าใช้งานระบบข้อมูลสารสนเทศและอุปกรณ์เครื่องมือ	-ตรวจสอบการฝึกอบรมหรือชี้แจงประชุมเพื่อสร้างจิตสำนึกความรับผิดชอบในการเข้าใช้งานระบบข้อมูลสารสนเทศและอุปกรณ์เครื่องมือ -สัมภาษณ์กระบวนการอบรม
1.เพื่อให้มีการกำหนดขั้นตอนการปฏิบัติงานในการกำหนดรหัสผ่านในการเข้าใช้งานทุกอุปกรณ์ 2.เพื่อให้เกิดการปฏิบัติตามขั้นตอนดังกล่าวที่กำหนดไว้	3.2 มีการกำหนดให้เจ้าหน้าที่ ที่มีอุปกรณ์คอมพิวเตอร์กำหนดรหัสผ่านในการเข้าใช้งานอุปกรณ์นั้นๆ	-ตรวจสอบการกำหนดขั้นตอนการปฏิบัติงานในการกำหนดรหัสผ่านในการเข้าใช้งานทุกอุปกรณ์ -ทดสอบการเข้าใช้งานคอมพิวเตอร์และอุปกรณ์ โดยใช้การสุ่มตรวจแบบเป็นระบบ (Systematic Sampling) ดังเอกสาร WI0502

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
4.ระบบบริหารจัดการรหัสผ่าน (Password management system)		
1. เพื่อให้หน่วยงาน ต้องจัดทำระบบบริหารจัดการรหัสผ่านที่มีปฏิสัมพันธ์กับผู้ใช้งานเพื่อให้มีการรหัสผ่านที่คุณภาพยากต่อการคาดเดา 2.เพื่อป้องกันการเข้าใช้งานในระบบโดยผู้ที่ไม่ได้รับการอนุญาต 3.เพื่อป้องกันการสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลจากผู้ที่ไม่ได้รับอนุญาต	4.1 มีระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มีคุณภาพ เช่น รหัสผ่านมีความซับซ้อน คาดเดาได้ยาก เข้ารหัสในการจัดเก็บ	-ตรวจสอบระบบบริหารจัดการรหัสผ่านที่มีปฏิสัมพันธ์กับผู้ใช้งาน โดยการบังคับให้มีการตั้งรหัสผ่านที่มีคุณภาพ เช่น รหัสผ่านมีความซับซ้อน คาดเดาได้ยาก
5.การควบคุมการเข้าถึงระบบ (System and application access control)		
1.เพื่อให้มีการกำหนดมาตรการและขั้นตอนการปฏิบัติในการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส 2.เพื่อให้เกิดการปฏิบัติตามขั้นตอนดังกล่าวที่กำหนดไว้	5.1 มีการออกมาตรการการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส	-ตรวจสอบมาตรการและขั้นตอนการปฏิบัติในการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรสว่าหน่วยงานระบุไว้อย่างไร -ทดสอบการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส ให้ผู้ตรวจสอบภายในปฏิบัติตามขั้นตอนใน WI0503
1.เพื่อให้มีการกำหนดขั้นตอนวิธีการสร้าง/ดูแลบำรุงรักษาระบบการจัดเก็บ Log ไฟล์ในการเข้าถึงเครือข่ายองค์กรอย่างเป็นลายลักษณ์อักษร 2.เพื่อให้เกิดการปฏิบัติตามขั้นตอนดังกล่าวที่กำหนดไว้	5.2 มีการสร้างระบบจัดเก็บ log ไฟล์ในการเข้าถึงเครือข่ายของกรม	-ตรวจสอบขั้นตอนวิธีการสร้าง/ดูแลบำรุงรักษาระบบการจัดเก็บ Log ไฟล์ในการเข้าถึงเครือข่ายองค์กรที่เป็นลายลักษณ์อักษร -ทดสอบการบริหารจัดการระบบจัดเก็บ log ไฟล์ในการเข้าถึงเครือข่ายของกรมและหน่วยงาน โดยให้ผู้ปฏิบัติงานแสดงวิธีการเรียกดู log ที่จัดเก็บไว้ และแสดงให้ดูถึงวันที่ของแพ็คเกทข้อมูลที่จัดเก็บใน log เพื่อตรวจสอบว่าจัดเก็บ log ไว้ 90 วันตาม พรบ. -สัมภาษณ์ผู้ดูแลระบบ/ผู้ปฏิบัติงาน IT ที่รับผิดชอบดูแลบริหารจัดการ log ให้อธิบายการบริหารจัดการและการลบ log ว่ามีหลักการอย่างไร

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.เพื่อให้มีการกำหนดหลักเกณฑ์การพิจารณาการเปิดเข้าใช้งาน Port ของผู้ร้องขอใช้งาน โดยกำหนดระยะเวลาในการใช้งานตามที่ผู้ดูแลระบบอนุญาต 2.กำหนดให้มีขั้นตอนการปฏิบัติในการเปิดเข้าใช้งาน Port เพื่อเป็นมาตรฐานแนวทางปฏิบัติประกอบการปฏิบัติที่ถูกต้อง	5.3 มีการพิจารณาการเปิดเข้าใช้งาน port ของผู้ร้องขอใช้งานโดยกำหนดระยะเวลาในการใช้งานตามที่ผู้ดูแลระบบจะอนุญาต	-ตรวจสอบหลักเกณฑ์การพิจารณาการเปิดเข้าใช้งาน Port ของผู้ร้องขอใช้งาน โดยกำหนดระยะเวลาในการใช้งานตามที่ผู้ดูแลระบบอนุญาต -ตรวจสอบขั้นตอนการปฏิบัติในการเปิดเข้าใช้งาน Port ของหน่วยงาน -กรณีที่หน่วยงานมีเครื่องแม่ข่าย ผู้ตรวจสอบสัมภาษณ์และให้ผู้ดูแลระบบแสดงให้ดูถึงการเปิด port ในปัจจุบันว่าเปิด port ใดบ้างและทำไมต้องเปิด port นั้นไว้ อาจใช้วิธีการตามขั้นตอนการตรวจสอบ port ตามเอกสาร WI0504
เพื่อป้องกันการสูญหาย/เสียหาย/การดักเปลี่ยนแปลงข้อมูลที่อยู่ระหว่างการรับ-ส่ง/โอนย้ายข้อมูลผ่านระบบเครือข่าย	5.4 มีการกำหนด vlan ในการเข้าใช้งานระบบเครือข่ายของกรมนั้นๆ	-ตรวจสอบการกำหนด Vlan โดยผู้ตรวจสอบภายในใช้การตรวจสอบตามขั้นตอนในเอกสาร WI0505
เพื่อป้องกันการสูญหาย/เสียหาย/การดักเปลี่ยนแปลงข้อมูลที่อยู่ระหว่างการรับ-ส่ง/โอนย้ายข้อมูลผ่านระบบเครือข่าย	5.5 ถ้าไม่มีการใช้งานในระยะเวลาหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเตอร์เน็ต (session timeout) เพื่อนำสัญญาณไปให้ผู้ที่ร้องขอคนอื่นต่อไป	-ทดสอบการเข้าอินเทอร์เน็ตและอยู่เฉยๆไม่ต้องขยับเมาส์ แล้วจับเวลาว่าจะตัดสัญญาณอินเตอร์เน็ตใช้เวลาเท่าไร (ค่ามาตรฐานอยู่ระหว่าง 15 นาที)
เพื่อป้องกันการสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลผ่านระบบเครือข่าย	5.6 มีการจัดทำคู่มือขั้นตอนการใช้งาน	-ตรวจสอบคู่มือการใช้งานเครือข่าย
	5.7 มีการกำหนดรหัสผ่านโดยผู้ดูแลระบบและจัดเก็บไว้ที่ผู้ดูแลระบบในรูปแบบแฟ้มเอกสารที่มีการปิดผนึกที่มิดชิด	-ตรวจสอบการจัดเก็บรหัสผ่านและสถานที่จัดเก็บรหัสผ่าน
1.เพื่อป้องกันการเข้าใช้งานในระบบที่ไม่ถูกต้อง เหมาะสม ตามประเภทการใช้งาน 2.เพื่อป้องกันการสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลจากผู้ใช้งานที่ไม่ได้รับอนุญาต	5.8 มีการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่าง เช่น ผู้บริหาร, ผู้ปฏิบัติงาน ฯลฯ	-ตรวจสอบรหัสผ่านว่ามีการแยกประเภทผู้ใช้งานและกำหนดระดับการเข้าถึงข้อมูลหรือไม่

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.เพื่อป้องกันการเข้าใช้งานในระบบโดยผู้ที่ไม่ได้รับการอนุญาต 2.เพื่อป้องกันการสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลจากผู้ที่ไม่ได้รับอนุญาต	5.9 มีการกำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น	-ผู้ตรวจสอบภายใน ทำการทดสอบขอใช้รหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบและสังเกตการณ์การปฏิบัติงานว่าดำเนินตามขั้นตอนการกำหนดรหัสผ่านตามที่หน่วยงานกำหนดหรือไม่
1. เพื่อให้หน่วยงานมีการกำหนดคู่มือ/ขั้นตอนการล็อกอินเข้าใช้งานในระบบอย่างถูกต้องที่มีความมั่นคงปลอดภัย 2.เพื่อป้องกันการเข้าใช้งานในระบบโดยผู้ที่ไม่ได้รับการอนุญาต	5.10 ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	-ตรวจสอบขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าใช้งานระบบ -ทดสอบการเข้าล็อกอินเข้าใช้งานระบบ
6.อุปกรณ์คอมพิวเตอร์แบบพกพา Digital device		
1. เพื่อป้องกันความเสี่ยงในการสูญหาย/เสียหายต่ออุปกรณ์คอมพิวเตอร์แบบพกพา 2. เพื่อป้องกันความเสี่ยงในการสูญหายหรือเสียหายหรือโจรกรรมข้อมูลสารสนเทศในอุปกรณ์คอมพิวเตอร์แบบพกพา	6.1 หน่วยงานต้องกำหนดนโยบาย/แนวทางปฏิบัติ/มาตรการ/ขั้นตอน ให้มีการบันทึกข้อมูลเกี่ยวกับคอมพิวเตอร์พกพา เพื่อข้อมูลที่บันทึกเป็นการพิสูจน์เครื่องที่ใช้งานจริง ในการเข้ามาใช้งานยังระบบได้	-ตรวจสอบนโยบาย/แนวทางปฏิบัติ/มาตรการ/ขั้นตอน ให้มีการบันทึกข้อมูลเกี่ยวกับคอมพิวเตอร์พกพา เพื่อข้อมูลที่บันทึกเป็นการพิสูจน์เครื่องที่ใช้งานจริง ในการเข้ามาใช้งานยังระบบได้ว่าเป็นลายลักษณ์อักษรหรือไม่
	6.2 หน่วยงานต้องกำหนด/แต่งตั้งผู้มีหน้าที่รับผิดชอบในดูแลและการอนุญาตสิทธิในการใช้อุปกรณ์คอมพิวเตอร์แบบพกพา และ Digital Device ของหน่วยงาน	-ตรวจสอบคำสั่งแต่งตั้งหรือมอบหมายผู้มีหน้าที่รับผิดชอบในดูแลและการอนุญาตสิทธิในการใช้อุปกรณ์คอมพิวเตอร์แบบพกพา และ Digital Device ของหน่วยงาน
	6.3 หน่วยงานต้องกำหนด/แต่งตั้งผู้มีหน้าที่รับผิดชอบในการกำหนดสิทธิการเข้าถึงของ IMEI (Internal Mobile Equipment Identity) หรือ MAC Address สำหรับอุปกรณ์เครือข่ายคอมพิวเตอร์แบบพกพาและ Digital Device ที่ได้รับอนุญาต	-ตรวจสอบคำสั่งแต่งตั้งหรือมอบหมายผู้มีหน้าที่รับผิดชอบในการกำหนดสิทธิการเข้าถึงของ IMEI (Internal Mobile Equipment Identity) หรือ MAC Address สำหรับอุปกรณ์เครือข่ายคอมพิวเตอร์แบบพกพาและ Digital Device ที่ได้รับอนุญาต

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	6.4 กำหนดขั้นตอนการปฏิบัติในการกำหนดสิทธิการเข้าถึงของ IMEI (Internal Mobile Equipment Identity) หรือ MAC Address สำหรับอุปกรณ์เครือข่ายคอมพิวเตอร์แบบพกพาและ Digital Device ที่ได้รับอนุญาต	-ตรวจสอบขั้นตอนการปฏิบัติในการกำหนดสิทธิการเข้าถึงของ IMEI (Internal Mobile Equipment Identity) หรือ MAC Address สำหรับอุปกรณ์เครือข่ายคอมพิวเตอร์แบบพกพาและ Digital Device ที่ได้รับอนุญาต -ให้ผู้ปฏิบัติทดสอบการปฏิบัติตามขั้นตอนการปฏิบัติในการกำหนดสิทธิการเข้าถึงของ IMEI (Internal Mobile Equipment Identity) หรือ MAC Address สำหรับอุปกรณ์เครือข่ายคอมพิวเตอร์แบบพกพาและ Digital Device ที่ได้รับอนุญาต
	6.5 หน่วยงานต้องมีการจำกัดช่องทางการเข้าออกของระบบ เมื่อมีการใช้งานระบบเครือข่ายไร้สาย (Wireless Security) และมีการเชื่อมต่อจากภายนอก (Tunnel Routing Policy) ตามนโยบายของระบบเครือข่ายและสารสนเทศ	-สัมภาษณ์การจำกัดช่องทางการเข้าออกระบบเครือข่าย ว่าเป็นไปตามนโยบายของระบบเครือข่ายและสารสนเทศ
7.การปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)		
1. เพื่อให้แน่ใจว่าการรักษาความปลอดภัยของข้อมูลที่ระบบการเข้าถึงผ่าน Teleworking 2. ผู้ปฏิบัติงานมีความรู้ว่าขั้นตอนการรักษาความปลอดภัยของข้อมูลที่ระบบการเข้าถึงผ่าน Teleworking เพื่อป้องกันข้อมูลที่ผ่านเข้า-ออกในระบบ Teleworking	7.1 มีการกำหนดขั้นตอนการส่งข้อมูลเข้า-ออกผ่านระบบ Teleworking ที่ปลอดภัย และกำหนดนโยบายการเชื่อมต่อ Inbound และ Outbound ให้รัดกุม โดยเรียงจาก Source Address, Destination Address, Service, Scheduled และ Security Feature รวมทั้งผู้มีอำนาจในการอนุญาติในการเข้าใช้งานระบบปฏิบัติการผ่านทางไกล	-ตรวจสอบขั้นตอนการส่งข้อมูลเข้า-ออกผ่านระบบ Teleworking ที่ปลอดภัย และกำหนดนโยบายการเชื่อมต่อ Inbound และ Outbound ให้รัดกุม โดยเรียงจาก Source Address, Destination Address, Service, Scheduled และ Security Feature รวมทั้งผู้มีอำนาจในการอนุญาติในการเข้าใช้งานระบบปฏิบัติการผ่านทางไกล
	7.2 มีการกำหนดผู้รับผิดชอบต่อกระบวนการส่งข้อมูลเข้า-ออกผ่านระบบ Teleworking ที่ปลอดภัย หรือกำหนดระยะเวลาในการเข้าใช้งาน	-ตรวจสอบคำสั่งแต่งตั้งหรือมอบหมายผู้รับผิดชอบต่อกระบวนการส่งข้อมูลเข้า-ออกผ่านระบบ Teleworking ที่ปลอดภัย หรือกำหนดระยะเวลาในการเข้าใช้งาน

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
เพื่อให้การส่งข้อมูลเข้า-ออกผ่านระบบ Teleworking มีความปลอดภัย ไม่มีความเสี่ยงต่อการสูญหาย/เสียหาย/โจรกรรม	7.3 มีการแต่งตั้งผู้สามารถตรวจสอบผู้ใช้งานพร้อมระบุตัวตนของผู้ใช้งาน รวมทั้งตรวจสอบสถานะและรายการเชื่อมต่อระบบได้ เมื่อมีการเชื่อมต่อการปฏิบัติงานระยะไกล	-ตรวจสอบคำสั่งแต่งตั้งผู้สามารถตรวจสอบผู้ใช้งานพร้อมระบุตัวตนของผู้ใช้งาน รวมทั้งตรวจสอบสถานะและรายการเชื่อมต่อระบบได้ เมื่อมีการเชื่อมต่อการปฏิบัติงานระยะไกล
	7.4 เมื่อมีการเชื่อมต่อการปฏิบัติงานระยะไกล สามารถตรวจสอบผู้ใช้งานพร้อมระบุตัวตนของผู้ใช้งาน รวมทั้งตรวจสอบสถานะและรายการเชื่อมต่อระบบได้	-ผู้ตรวจสอบภายใน ให้ผู้ปฏิบัติงาน It ดำเนินการเชื่อมต่อการปฏิบัติงานระยะไกลและสังเกตการณ์ปฏิบัติงานว่ามีการเข้าใช้งานอย่างถูกต้องหรือไม่และสัมภาษณ์การกำหนด/จำกัด/ให้สิทธิ์การใช้งานระยะไกลอย่างไรบ้าง
	7.5 ในกรณีที่มีความจำเป็นขั้นสูงสุด ผู้รับผิดชอบสามารถอนุญาตให้ใช้งานได้ตามความเหมาะสม	-สัมภาษณ์ผู้ปฏิบัติงาน IT ในกรณีที่มีเหตุฉุกเฉินจะปฏิบัติอย่างไรในการควบคุมการใช้งานระยะไกล
8.การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)		
1. เพื่อให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ในหน่วยงานอย่างสม่ำเสมอและมีมาตรการกำหนดห้ามผู้ใช้งานโปรแกรมอรรถประโยชน์ที่ไม่มีลิขสิทธิ์ถูกต้อง 2.เพื่อป้องกันความเสี่ยงต่อภัยคุมคามการโจรกรรมข้อมูลหรือการสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลจากผู้ที่ไม่ได้รับอนุญาต	8.1 มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ในหน่วยงาน ผู้ใช้งานห้ามลงโปรแกรมอรรถประโยชน์ที่ไม่มีลิขสิทธิ์ถูกต้อง	-สัมภาษณ์หลักเกณฑ์การใช้งานโปรแกรมอรรถประโยชน์ หน่วยงานปฏิบัติ/ควบคุมอย่างไร -สุ่มตรวจเครื่องคอมพิวเตอร์ของหน่วยงานว่ามีการติดตั้งโปรแกรมอรรถประโยชน์หรือไม่
9.การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to program source code)		
1. เพื่อให้มีการกำหนดระดับความปลอดภัยของเข้าใช้ซอร์สโค๊ดของโปรแกรมเป็นลำดับขั้นความปลอดภัย 2. เพื่อป้องกันเกี่ยวกับข้อมลสูญหายหรือ มีซอร์สโค๊ดที่ไม่ได้รับการอัพเดตรายการแก้ไขเข้าไปอย่างถูกต้อง	9.1มีการกำหนดระดับความปลอดภัยของเข้าใช้ซอร์สโค๊ดของโปรแกรมเป็นลำดับขั้นความปลอดภัย เพื่อป้องกันเกี่ยวกับข้อมลสูญหายหรือ มีซอร์สโค๊ดที่ไม่ได้รับการอัพเดตรายการแก้ไขเข้าไปอย่างถูกต้อง	-ตรวจสอบนโยบาย/แนวทางปฏิบัติในการควบคุมระดับความปลอดภัยของเข้าใช้ซอร์สโค๊ดของโปรแกรม -ผู้ตรวจสอบภายใน ให้ผู้ปฏิบัติงาน IT อธิบายและปฏิบัติแสดงถึงกระบวนการควบคุมระดับความปลอดภัยของเข้าใช้ซอร์สโค๊ดของโปรแกรม

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
10.ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)		
เพื่อให้มีความปลอดภัยในข้อมูลกระบวนการบริหารโครงการ IT ของหน่วยงาน	1.มีการกำหนดนโยบายให้มีการตรวจสอบการบริหารจัดการและการดำเนินงานที่เกี่ยวข้องกับข้อมูลที่ใช้ในการบริหารโครงการด้านเทคโนโลยีสารสนเทศ	-ตรวจสอบนโยบายให้มีการตรวจสอบการบริหารจัดการและการดำเนินงานที่เกี่ยวข้องกับข้อมูลที่ใช้ในการบริหารโครงการด้านเทคโนโลยีสารสนเทศ
	2.มีระบบหรือขั้นตอนการกลั่นกรองความมั่นคงปลอดภัยของข้อมูลที่ใช้ในการบริหารโครงการ	-สัมภาษณ์ขั้นตอนการกลั่นกรองความมั่นคงปลอดภัยของข้อมูลที่ใช้ในการบริหารโครงการ
	3.ผู้อำนวยการระดับหน่วยงาน/คณะกรรม CSO ระดับหน่วย ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศที่ใช้ในการบริหารโครงการด้านเทคโนโลยีสารสนเทศ	-ตรวจสอบผลการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศที่ใช้ในการบริหารโครงการด้านเทคโนโลยีสารสนเทศของคณะกรรมการ CSO ระดับหน่วยงาน

เกณฑ์การประเมินความเสี่ยง

(1) นโยบายควบคุมการเข้าถึง (Access Control Policy)

ระดับ Level 1

-มีการกำหนดนโยบาย/แนวทางปฏิบัติ/มาตรการที่เป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการกำหนดนโยบาย/แนวทางปฏิบัติ/มาตรการที่เป็นลายลักษณ์อักษร โดยมีการทบทวนกระบวนการดำเนินงานองค์กร ให้สอดคล้องตามความต้องการในควบคุมการเข้าถึงข้อมูลของหน่วยงาน/องค์กร

-จำนวนปัญหาหรือความเสี่ยงต่อการเข้าถึงข้อมูลหน่วยงาน ไม่เกิน 5 ครั้ง/ปี

ระดับ Level 3

-มีการกำหนดนโยบาย/แนวทางปฏิบัติ/มาตรการที่เป็นลายลักษณ์อักษร โดยมีการทบทวนกระบวนการดำเนินงานองค์กร ให้สอดคล้องตามความต้องการในควบคุมการเข้าถึงข้อมูลของหน่วยงาน/องค์กร

-ไม่พบปัญหาหรือความเสี่ยงต่อการเข้าถึงข้อมูลหน่วยงาน

(2) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)

ระดับ Level 1

-มีการกำหนดขั้นตอน/แนวทางปฏิบัติในการลงทะเบียน/ถอนถอดสิทธิของผู้ใช้งานในระบบเครือข่ายอย่างเป็นลายลักษณ์อักษรและสื่อสารอย่างน้อย 2 ช่องทาง

ระดับ Level 2

-มีการกำหนดขั้นตอน/แนวทางปฏิบัติในการลงทะเบียน/ถอนถอดสิทธิของผู้ใช้งานในระบบเครือข่ายอย่างเป็นลายลักษณ์อักษรและสื่อสารอย่างน้อย 2 ช่องทาง และบุคลากรร้อยละ 80 รับทราบ

-มีการลงทะเบียนสำหรับพนักงานใหม่และมีการปรับปรุงระบบข้อมูลพนักงานเก่าที่โอนย้าย อย่างครบถ้วน (จากการสุ่มตรวจ)

-จำนวนปัญหาในการเข้าใช้งานในระบบเครือข่ายโดยไม่ได้รับอนุญาต ไม่เกิน 3 ครั้ง/ปี

ระดับ Level 3

-ไม่พบปัญหาในการเข้าใช้งานในระบบเครือข่ายโดยไม่ได้รับอนุญาต

2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)

ระดับ Level 1

-มีการกำหนดขั้นตอน/แนวทางปฏิบัติให้มีการประชุมพิจารณาสิทธิในการเข้าถึงข้อมูลของเจ้าหน้าที่ใหม่ และมีการทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เดิมไว้เป็นลายลักษณ์อักษร

ระดับ Level 2

-ร้อยละการเข้าใช้งานในระบบเครือข่ายเป็นไปอย่างถูกต้องตามสิทธิ์ที่กำหนดไว้ 80% ของจำนวนสิทธิผู้ใช้งานที่สุ่มตรวจ

-จำนวนปัญหาการเข้าใช้งานในระบบเครือข่ายที่ไม่ถูกต้องตามสิทธิ์ที่กำหนดไว้และเกิดความเสี่ยง/เสียหายต่อองค์กร ไม่เกิน 3 ครั้ง/ปี

ระดับ Level 3

-ร้อยละการเข้าใช้งานในระบบเครือข่ายเป็นไปอย่างถูกต้องตามสิทธิ์ที่กำหนดไว้ 100% ของจำนวนสิทธิผู้ใช้งานที่สุ่มตรวจ

-ไม่พบปัญหาการเข้าใช้งานในระบบเครือข่ายที่ไม่ถูกต้องตามสิทธิ์ที่กำหนดไว้และเกิดความเสี่ยง/เสียหายต่อองค์กร

2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

ระดับ Level 1

-มีการกำหนดขั้นตอน/แนวทางปฏิบัติในการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ อย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-การบริหารจัดการสิทธิ์สอดคล้องกับระดับชั้นความลับสารสนเทศที่กำหนด

-ร้อยละการเข้าใช้งานในระบบเครือข่ายเป็นไปอย่างถูกต้องตามสิทธิ์ที่กำหนดไว้และสอดคล้องกับระดับชั้นความลับสารสนเทศ 80% ของจำนวนสิทธิผู้ใช้งานที่สุ่มตรวจ

ระดับ Level 3

-ร้อยละการเข้าใช้งานในระบบเครือข่ายเป็นไปอย่างถูกต้องตามสิทธิ์ที่กำหนดไว้ 100% ของจำนวนสิทธิผู้ใช้งานที่สุ่มตรวจ

-ไม่พบปัญหาการเข้าใช้งานในระบบเครือข่ายที่ไม่ถูกต้องตามสิทธิ์ที่กำหนดไว้และเกิดความเสี่ยง/เสียหายต่อองค์กร

2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users) การจัดการกับรหัสผ่าน

ระดับ Level 1

-มีการกำหนดขั้นตอน/แนวทางปฏิบัติ ในการมอบรหัสผ่านของผู้ใช้งานผ่านกระบวนการที่มีการควบคุมข้อมูลอันเป็นความลับที่เหมาะสม อย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-ร้อยละของการปฏิบัติตามขั้นตอน/แนวทางปฏิบัติ ในการมอบรหัสผ่านของผู้ใช้งานตามที่กำหนดไว้ได้ 80% ของจำนวนสิทธิผู้ใช้งานที่สุ่มตรวจ

ระดับ Level 3

-ร้อยละของการปฏิบัติตามขั้นตอน/แนวทางปฏิบัติ ในการมอบรหัสผ่านของผู้ใช้งานตามที่กำหนดไว้ได้ 100% ของจำนวนสิทธิผู้ใช้งานที่สุ่มตรวจ

-ไม่พบปัญหาหรือความเสี่ยงในการรั่วไหลข้อมูลอันเป็นความลับในระหว่างการส่งมอบรหัสผ่านของผู้ใช้งาน

2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้งอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-จำนวนการปฏิบัติตามขั้นตอนการปฏิบัติในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

-จำนวนปัญหาหรือความเสี่ยงเกี่ยวกับสิทธิในการเข้าใช้งานที่ไม่เป็นปัจจุบัน ไม่เกิน 3 ครั้ง/ปี

ระดับ Level 3

-ไม่พบปัญหาหรือความเสี่ยงเกี่ยวกับสิทธิในการเข้าใช้งานที่ไม่เป็นปัจจุบัน ไม่เกิน 3 ครั้ง/ปี

2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal of adjustment of access rights)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการถอนถอดหรือปรับปรุงสิทธิในการเข้าถึงอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-จำนวนมีการปฏิบัติตามขั้นตอนการปฏิบัติในการถอนถอดหรือปรับปรุงสิทธิในการเข้าถึงอย่างน้อยปีละ 1 ครั้ง

ระดับ Level 3

-ไม่พบปัญหาหรือความเสี่ยงเกี่ยวกับสิทธิในการเข้าใช้งานที่ไม่เป็นปัจจุบัน ไม่เกิน 3 ครั้ง/ปี

(3) **หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)**

3.1 มีการสร้างจิตสำนึกความรับผิดชอบในการเข้าใช้งานระบบข้อมูลสารสนเทศและอุปกรณ์เครื่องมือ

ระดับ Level 1

-มีการกำหนดขั้นตอนในการฝึกอบรม/รณรงค์ให้เกิดความตระหนักถึงความมั่นคงปลอดภัยและใช้งานในระบบอย่างถูกต้องอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-จำนวนครั้งของการฝึกอบรม/รณรงค์ให้เกิดความตระหนักถึงความมั่นคงปลอดภัยและใช้งานในระบบอย่างถูกต้อง อย่างน้อย 1 ครั้ง/ปี

-ร้อยละบุคลากรที่ผ่านการอบรมให้เกิดความตระหนักถึงความมั่นคงปลอดภัยและใช้งานในระบบอย่างถูกต้อง ค่าเป้าหมาย 80%

ระดับ Level 3

-มีการประเมินผลการฝึกอบรม/รณรงค์ให้เกิดความตระหนักถึงความมั่นคงปลอดภัยและใช้งานในระบบอย่างถูกต้อง

-ไม่พบปัญหาหรือความเสี่ยงเกี่ยวกับการใช้งานของผู้ใช้งานที่ไม่มีความตระหนักถึงความมั่นคงปลอดภัยและใช้งานในระบบ

3.2 มีการกำหนดให้เจ้าหน้าที่ ที่มีอุปกรณ์คอมพิวเตอร์กำหนดรหัสผ่านในการเข้าใช้งานอุปกรณ์นั้นๆ

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติงานในการกำหนดรหัสผ่านในการเข้าใช้งานทุกอุปกรณ์อย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-ร้อยละของอุปกรณ์ที่มีการกำหนดรหัสผ่านในการเข้าใช้งาน ค่าเป้าหมาย 60%

-จำนวนปัญหา/ความเสี่ยงที่เกิดจากการไม่กำหนดรหัสผ่านในการเข้าใช้งานอุปกรณ์ต่างๆ ไม่เกิน 3 ครั้ง/ปี

ระดับ Level 3

-ร้อยละของอุปกรณ์ที่มีการกำหนดรหัสผ่านในการเข้าใช้งาน ค่าเป้าหมาย 100%

-ไม่พบปัญหา/ความเสี่ยงที่เกิดจากการไม่กำหนดรหัสผ่านในการเข้าใช้งานอุปกรณ์ต่างๆ

(4) **ระบบบริหารจัดการรหัสผ่าน (Password management system)**

ระดับ Level 1

- มีระบบบริหารจัดการรหัสผ่านที่มีปฏิสัมพันธ์กับผู้ใช้งานเพื่อให้มีการรหัสผ่านที่คุณภาพยากต่อการคาดเดา

ระดับ Level 2

-ยังพบรหัสผ่านที่ไม่มีคุณภาพ ซึ่งง่ายต่อการคาดเดา อย่างน้อย 1 รหัส

ระดับ Level 3

-ไม่พบปัญหาหรือความเสี่ยงต่อจากระบบบริหารจัดการรหัสผ่าน

(5) การควบคุมการเข้าถึงระบบ (System and application access control)

1.1 มีการออกมาตรการการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส

ระดับ Level 1

-มีการกำหนดมาตรการและขั้นตอนการปฏิบัติในการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรสอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-ร้อยละการปฏิบัติตามมาตรการและขั้นตอนการปฏิบัติในการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส ค่าเป้าหมาย 60%

ระดับ Level 3

-ร้อยละการปฏิบัติตามมาตรการและขั้นตอนการปฏิบัติในการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส ค่าเป้าหมาย 100%

-ไม่พบปัญหา/ความเสี่ยงที่เกิดจากการไม่กำหนดการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส

1.2 มีการสร้างระบบจัดเก็บ log ไฟล์ในการเข้าถึงเครือข่ายของกรม

ระดับ Level 1

-มีการกำหนดขั้นตอนวิธีการสร้าง/ดูแลบำรุงรักษาระบบการจัดเก็บ Log ไฟล์ในการเข้าถึงเครือข่ายองค์กรอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-ร้อยละการปฏิบัติตามการสร้างและการวางแผนในการดูแลบำรุงรักษาระบบการจัดเก็บ Log ไฟล์ในการเข้าถึงเครือข่ายองค์กร ค่าเป้าหมาย 60%

ระดับ Level 3

-ร้อยละการปฏิบัติตามการสร้างและการวางแผนในการดูแลบำรุงรักษาระบบการจัดเก็บ Log ไฟล์ในการเข้าถึงเครือข่ายองค์กร ค่าเป้าหมาย 100%

-ไม่พบปัญหา/ความเสี่ยงที่เกิดจากระบบการจัดเก็บ Log ไฟล์ในการเข้าถึงเครือข่ายองค์กรตามที่กฎหมายกำหนด

1.3 มีการพิจารณาการเปิดเข้าใช้งาน port ของผู้ร้องขอใช้งานโดยกำหนดระยะเวลาในการใช้งานตามที่ผู้ดูแลระบบจะอนุญาต

ระดับ Level 1

-มีกำหนดหลักเกณฑ์การพิจารณาการเปิดเข้าใช้งาน Port และขั้นตอนการปฏิบัติในการเปิดเข้าใช้งาน Portอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-ร้อยละการปฏิบัติตามหลักเกณฑ์การพิจารณาและขั้นตอนการปฏิบัติการเปิดเข้าใช้งาน Port ค่าเป้าหมาย 60%

-มีการเฝ้าระวังตรวจสอบความไม่ปลอดภัย ตามตรงแผนการตรวจสอบ 60%

ระดับ Level 3

-มีการปฏิบัติตามหลักเกณฑ์การพิจารณาและขั้นตอนการปฏิบัติการเปิดเข้าใช้งาน Port ค่าเป้าหมาย 100%

-มีการเฝ้าระวังตรวจสอบความไม่ปลอดภัย ตามตรงแผนการตรวจสอบ 100%

-ไม่พบปัญหา/ความเสี่ยงที่เกิดจากการเปิดใช้งาน Port

1.4 มีการกำหนด vlan ในการเข้าใช้งานระบบเครือข่ายของกรมนั้นๆ

ระดับ Level 1

-มีการกำหนดมาตรการการใช้ Vlan ในการรับ-ส่งข้อมูลผ่านระบบเครือข่ายลายลักษณ์อักษร

ระดับ Level 2

-ร้อยละการปฏิบัติตามมาตรการการใช้ Vlan ค่าเป้าหมาย 60%

-ร้อยละการปฏิบัติการเฝ้าระวังตรวจสอบความไม่ปลอดภัยตรงตามแผนการเฝ้าระวังตรวจสอบความไม่ปลอดภัย ค่าเป้าหมาย 60%

-จำนวนปัญหา/ความเสี่ยงการสูญหาย/เสียหาย/การดักเปลี่ยนแปลงข้อมูลที่อยู่ระหว่างการรับ-ส่ง/โอนย้ายข้อมูลผ่านระบบเครือข่าย ไม่เกิน 3 ครั้ง/ปี

ระดับ Level 3

-ร้อยละการปฏิบัติตามมาตรการการใช้ Vlan ค่าเป้าหมาย 100%

-ร้อยละการปฏิบัติการเฝ้าระวังตรวจสอบความไม่ปลอดภัยตรงตามแผนการเฝ้าระวังตรวจสอบความไม่ปลอดภัย ค่าเป้าหมาย 100%

-ไม่พบปัญหา/ความเสี่ยงการสูญหาย/เสียหาย/การดักเปลี่ยนแปลงข้อมูลที่อยู่ระหว่างการรับ-ส่ง/โอนย้ายข้อมูลผ่านระบบเครือข่าย

1.5 ถ้าไม่มีการใช้งานในระยะเวลาหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเตอร์เน็ต (session timeout) เพื่อนำสัญญาณไปให้ผู้ที่ร้องขอคนอื่นต่อไป

ระดับ Level 1

-มีการกำหนดนโยบายหรือแนวทางปฏิบัติให้มีการตัดสัญญาณอินเตอร์เน็ต เมื่อไม่มีการใช้งานในระยะเวลาหนึ่ง เพื่อนำสัญญาณไปให้ผู้ที่ร้องขอคนอื่น

ระดับ Level 2

-มีการประกาศให้ผู้ปฏิบัติงานทราบเกี่ยวกับปฏิบัติตามนโยบายหรือแนวทางปฏิบัติให้มีการตัดสัญญาณอินเตอร์เน็ต

-ผู้ปฏิบัติงาน/ผู้ใช้งานระบบ ทราบเกี่ยวกับปฏิบัติตามนโยบายหรือแนวทางปฏิบัติให้มีการตัดสัญญาณอินเตอร์เน็ต อย่างน้อย 80%ของผู้ปฏิบัติงาน/ผู้ใช้งานระบบที่สุ่มตรวจ

ระดับ Level 3

-ผู้ปฏิบัติงาน/ผู้ใช้งานระบบ ทราบเกี่ยวกับปฏิบัติตามนโยบายหรือแนวทางปฏิบัติให้มีการตัดสัญญาณอินเตอร์เน็ต อย่างน้อย 100%ของผู้ปฏิบัติงาน/ผู้ใช้งานระบบที่สุ่มตรวจ

-มีการปฏิบัติตามนโยบายหรือแนวทางปฏิบัติให้มีการตัดสัญญาณอินเตอร์เน็ต

1.6 มีการจัดทำคู่มือขั้นตอนการใช้งาน

ระดับ Level 1

-มีการกำหนดคู่มือและขั้นตอนการใช้งานในการปฏิบัติทั้งผู้ดูแลระบบและผู้ใช้งานผ่านระบบเครือข่ายลายลักษณ์อักษร

ระดับ Level 2

-ร้อยละบุคลากรที่สุ่มตรวจ สามารถการปฏิบัติตามคู่มือและขั้นตอนการใช้งานในการปฏิบัติทั้งผู้ดูแลระบบและผู้ใช้งานผ่านระบบเครือข่าย ได้อย่างถูกต้อง อย่างน้อย 1 คน

-จำนวนปัญหาหรือความเสี่ยง การสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลผ่านระบบเครือข่าย ไม่เกิน 3 ครั้ง/ปี

ระดับ Level 3

-ร้อยละบุคลากรที่สุ่มตรวจ สามารถการปฏิบัติตามคู่มือและขั้นตอนการใช้งานในการปฏิบัติทั้งผู้ดูแลระบบและผู้ใช้งานผ่านระบบเครือข่าย ได้อย่างถูกต้อง อย่างน้อย 3 คน

-ไม่พบปัญหาหรือความเสี่ยง การสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลผ่านระบบเครือข่าย

1.7 มีการกำหนดรหัสผ่านโดยผู้ดูแลระบบและจัดเก็บไว้ที่ผู้ดูแลระบบในรูปแบบแฟ้มเอกสารที่มีการปิดผนึกที่มิดชิด

ระดับ Level 1

-มีการกำหนดคู่มือและขั้นตอนการกำหนดรหัสผ่านที่ดำเนินการโดยผู้ดูแลระบบลายลักษณ์อักษร

ระดับ Level 2

-แสดงให้เห็นว่าเอกสารรหัสผ่านเหล่านั้น ถูกจัดเก็บในรูปแบบแฟ้มเอกสารที่ปิดผนึกมิดชิดและสถานที่จัดเก็บมีความปลอดภัย

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการจัดเก็บเอกสารที่ไม่ปลอดภัย

1.8 มีการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่าง เช่น ผู้บริหาร, ผู้ปฏิบัติงาน ฯลฯ

ระดับ Level 1

-มีการกำหนดคู่มือ/ขั้นตอนการกำหนดสิทธิการเข้าใช้งานในระบบที่เหมาะสมเป็นลายลักษณ์อักษร

ระดับ Level 2

-ผู้ปฏิบัติงานมีความเข้าใจและสามารถปฏิบัติได้ตามคู่มืออย่างถูกต้อง อย่างน้อย 1 คน

-มีการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่างๆไว้อย่างเหมาะสม

ระดับ Level 3

-ผู้ปฏิบัติงานมีความเข้าใจและสามารถปฏิบัติได้ตามคู่มืออย่างถูกต้อง อย่างน้อย 3 คน

-มีการปฏิบัติตามการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่างๆ

-ไม่พบปัญหาการสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลจากผู้ใช้งานที่ไม่ได้รับอนุญาต

1.9 มีการกำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น

ระดับ Level 1

-มีการกำหนดคู่มือ/ขั้นตอนการกำหนดให้ผู้เข้ามาใช้งาน ต้องขอรหัสผ่าน เพื่อเข้าใช้งานในระบบจากผู้ดูแลระบบ และรหัสผ่านเหล่านั้นสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้อย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีหลักฐาน/แบบฟอร์มการขอรหัสผ่าน ตามคู่มือ/ขั้นตอนที่กำหนดไว้

-ผู้ปฏิบัติงานมีความเข้าใจและสามารถปฏิบัติได้ตามคู่มืออย่างถูกต้อง อย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติงานมีความเข้าใจและสามารถปฏิบัติได้ตามคู่มืออย่างถูกต้อง อย่างน้อย 3 คน

-ไม่พบปัญหาการสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

1.10 ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

ระดับ Level 1

- มีการกำหนดกำหนดนโยบายการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัย อย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีคู่มือ/ขั้นตอนการการล็อกอินเข้าใช้งานในระบบที่มีความมั่นคงปลอดภัย อย่างเป็นลายลักษณ์อักษร

-ผู้ปฏิบัติงานมีความเข้าใจและสามารถปฏิบัติได้ตามคู่มืออย่างถูกต้อง อย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติงานมีความเข้าใจและสามารถปฏิบัติได้ตามคู่มืออย่างถูกต้อง อย่างน้อย 3 คน

-ไม่พบปัญหาการสูญหาย/เสียหาย/การเปลี่ยนแปลงแก้ไขข้อมูล/การรั่วไหลของข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

(6) อุปกรณ์คอมพิวเตอร์แบบพกพา Digital device

ระดับ Level 1

-มีการกำหนดนโยบาย/แนวทางปฏิบัติ/มาตรการ/ขั้นตอน ให้มีการบันทึกข้อมูลเกี่ยวกับคอมพิวเตอร์พกพา เพื่อข้อมูลที่บันทึกเป็นการพิสูจน์เครื่องที่ใช้งานจริง ในการเข้ามาใช้งานยังระบบได้ จำนวน 1 ชุด

ระดับ Level 2

-มีการกำหนด/แต่งตั้งผู้มีหน้าที่รับผิดชอบในดูแลและการอนุญาตสิทธิในการใช้อุปกรณ์คอมพิวเตอร์แบบพกพา และ Digital Device ของหน่วยงาน

-มีการกำหนด/แต่งตั้งผู้มีหน้าที่รับผิดชอบในการกำหนดสิทธิการเข้าถึงของ IMEI (Internal Mobile Equipment Identity) หรือ MAC Address สำหรับอุปกรณ์เครือข่ายคอมพิวเตอร์แบบพกพาและ Digital Device ที่ได้รับอนุญาต และมีการกำหนดขั้นตอนการปฏิบัติในการกำหนดสิทธิการเข้าถึงดังกล่าว

ระดับ Level 3

-มีการจำกัดช่องทางการเข้าออกของระบบ เมื่อมีการใช้งานระบบเครือข่ายไร้สาย (Wireless Security) และมีการเชื่อมต่อจากภายนอก (Tunnel Routing Policy) ตามนโยบายของระบบเครือข่ายและสารสนเทศ

-ไม่พบปัญหาของอุปกรณ์คอมพิวเตอร์แบบพกพาและข้อมูลสารสนเทศในอุปกรณ์คอมพิวเตอร์แบบพกพาของหน่วยงานมีการสูญหาย/เสียหายหรือถูกโจรกรรม

(7) การปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

ระดับ Level 1

-มีการกำหนดขั้นตอนการส่งข้อมูลเข้า-ออกผ่านระบบ Teleworking ที่ปลอดภัย และกำหนดนโยบายการเชื่อมต่อ Inbound และ Outbound ให้รัดกุม โดยเรียงจาก Source Address, Destination Address, Service, Scheduled และ Security Feature รวมทั้งมีการกำหนดผู้มีอำนาจในการอนุญาติในการเข้าใช้งานระบบปฏิบัติการผ่านทางไกล

ระดับ Level 2

-มีการกำหนดผู้รับผิดชอบต่อกระบวนการส่งข้อมูลเข้า-ออกผ่านระบบ Teleworking ที่ปลอดภัย หรือการกำหนดระยะเวลาในการเข้าใช้งาน

ระดับ Level 3

-มีการแต่งตั้งผู้สามารถตรวจสอบผู้ใช้งานพร้อมระบุตัวตนของผู้ใช้งาน รวมทั้งมีการตรวจสอบสถานะและรายการเชื่อมต่อระบบได้ เมื่อมีการเชื่อมต่อการปฏิบัติงานระยะไกล

-ไม่พบปัญหาหรือความเสี่ยงที่พบ การส่งข้อมูลเข้า-ออกผ่านระบบ Teleworking ไม่มีความปลอดภัยต่อการสูญหาย/เสียหาย/โจรกรรม

(8) การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

ระดับ Level 1

-มีการกำหนดมาตรการห้ามผู้ใช้งานโปรแกรมอรรถประโยชน์ที่ไม่มีลิขสิทธิ์ถูกต้องเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีแผนการตรวจสอบควบคุมการใช้โปรแกรมอรรถประโยชน์ในหน่วยงานอย่างสม่ำเสมอ

ระดับ Level 3

-มีผลการรายงานการตรวจสอบควบคุมการใช้โปรแกรมอรรถประโยชน์ในหน่วยงานครบถ้วนตามแผนที่กำหนด

-มีการสรุปวิเคราะห์การปฏิบัติตามมาตรการกำหนดห้ามผู้ใช้งานโปรแกรมอรรถประโยชน์ที่ไม่มีลิขสิทธิ์ถูกต้อง ระบุถึงการประเมินผลและปัญหา/อุปสรรค นำเสนอต่อคณะกรรมการ CSO หน่วยงาน จำนวน 1 ครั้ง/ปี

(9) **การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to program source code)**

ระดับ Level 1

-มีการกำหนดระดับความปลอดภัยของเข้าใช้ซอร์สโค๊ดของโปรแกรมเป็นลำดับขั้นความปลอดภัยอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีขั้นตอนการปฏิบัติการเข้าใช้ซอร์สโค๊ดของโปรแกรมเป็นลำดับขั้นความปลอดภัยอย่างเป็นลายลักษณ์อักษร

ระดับ Level 3

-มีการปฏิบัติตามการควบคุมการเข้าถึงซอร์สโค๊ดของโปรแกรมตามที่กำหนดไว้

-ไม่พบปัญหาเกี่ยวกับข้อมลสูญหายหรือ มีซอร์สโค๊ดที่ไม่ได้รับการอัพเดตรายการแก้ไขเข้าไปอย่างถูกต้อง

(10)**ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)**

ระดับ Level 1

-คณะกรรมการ CSO ระดับหน่วยงาน มีการกำหนดแนวทางปฏิบัติให้มีการตรวจสอบการบริหารจัดการและการดำเนินงานที่เกี่ยวข้องกับข้อมูลข้อมูลที่ใช้ในการบริหารโครงการด้านเทคโนโลยีสารสนเทศ

ระดับ Level 2

-คณะกรรมการ CSO ระดับหน่วยงาน มีระบบหรือขั้นตอนการกลั่นกรองความมั่นคงปลอดภัยของข้อมูลที่ใช้ในการบริหารโครงการ

-ผู้อำนวยการหรือคณะกรรมการ CSO ระดับหน่วยงาน มีการกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ

ระดับ Level 3

-ผู้บริหารและผู้ปฏิบัติงานด้านการบริหารจัดการโครงการ IT ของหน่วยงานทุกคน รับททราบหรือมีความรู้ ความเข้าใจในการมีระบบหรือขั้นตอนการกลั่นกรองความมั่นคงปลอดภัยของข้อมูลที่ใช้ในการบริหารโครงการ รวมทั้งวัตถุประสงค์/ความต้องการของนโยบายในการสร้างความมั่นคงปลอดภัยของสารสนเทศการบริหารโครงการ

-มีการรายงานผลการตรวจสอบการบริหารจัดการโครงการที่เสี่ยงต่อความไม่มั่นคงปลอดภัยในข้อมูลสารสนเทศของการบริหารโครงการ อย่างเป็นลายลักษณ์อักษร

วิธีปฏิบัติงาน Work Instruction

เรื่อง ขั้นตอนการสุ่มตรวจความมีอยู่จริงของทรัพย์สินด้านเทคโนโลยีสารสนเทศ

การสุ่มตัวอย่างแบบเป็นระบบ(Systematic Sampling)

❒ เอกสารควบคุม ❒ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

การสุ่มตัวอย่างแบบเป็นระบบ(Systematic Sampling) เป็นการสุ่มตรวจจากประชากรที่ทราบจำนวนทั้งหมดที่แน่นอนและเป็นการสุ่มตัวอย่างที่ต้องกำหนดหมายเลขลงบนสมาชิกทุกหน่วยประชากร และเป็นการสุ่มตัวอย่างที่มีระยะห่างเท่ากัน แบ่งเป็น 2 กรณี คือ

1.กรณีที่ 1 ผลหารของ N/n เป็นเลขจำนวนเต็ม มีขั้นตอนดังนี้

ขั้นตอนที่ 1 กำหนดหมายเลขประชากรตั้งแต่หมายเลข 1 ถึงหมายเลข N

ขั้นตอนที่ 2 หาช่วงการสุ่มตรวจ k=N/n (ซึ่ง N = ขนาดประชากร n=ขนาดของกลุ่มตัวอย่าง) สุ่มตัวอย่างจากหมายเลข 1 ถึง k โดยวิธีการสุ่มตรวจอย่างแบบสุ่มเชิงเดียว เช่น การจับสลาก

ขั้นตอนที่ 3 หาหน่วยตัวอย่างที่ 2 ซึ่งเกิดจากหมายเลขของหน่วยตัวอย่างแรกบวกด้วย k หน่วยตัวอย่างที่ 3 เกิดจากหมายเลขของหน่วยตัวอย่างที่ 2 บวกด้วย k เป็นเช่นนี้เรื่อยๆไปจนถึงหน่วยตัวอย่างที่ N เกิดจากหมายเลขของหน่วยตัวอย่างที่ n-1 บวกด้วย k

ตัวอย่างเช่น กลุ่มตรวจสอบภายในต้องการสุ่มตรวจความมีอยู่จริงของเครื่องคอมพิวเตอร์ของสำนักงานฯเขต 1 ที่มีเครื่องทั้งหมดจำนวน 50 เครื่อง ต้องการสุ่มตัวอย่าง 10 เครื่อง ด้วยวิธีการสุ่มตัวอย่างแบบเป็นระบบ(Systematic Sampling) ซึ่งมีขั้นตอนดังนี้

ขั้นตอนที่ 1 กำหนดหมายเลขประชากรตั้งแต่หมายเลข 1 ถึงหมายเลข 30

ขั้นตอนที่ 2 หาช่วงการสุ่มตรวจ k=N/n ในที่นี้ N=50 และn=10 ดังนั้น k= 50/10 = 5 และสุ่มหาตัวอย่างแรกแบบสุ่มเชิงเดียว เช่น การจับสลากจากหมายเลข 1-5 สมมุติสุ่มได้หมายเลข 1

ขั้นตอนที่ 3 หาหน่วยตัวอย่างที่ 2 ถึงหน่วยตัวอย่างที่ 10 ได้ดังนี้

หน่วยตัวอย่างที่ 1 คือ หมายเลข 1
หน่วยตัวอย่างที่ 2 คือ หมายเลข 1+5 = 6
หน่วยตัวอย่างที่ 3 คือ หมายเลข 6+5 = 11
หน่วยตัวอย่างที่ 4 คือ หมายเลข 11+5 = 16
หน่วยตัวอย่างที่ 5 คือ หมายเลข 16+5 = 21
หน่วยตัวอย่างที่ 6 คือ หมายเลข 21+5 = 26
หน่วยตัวอย่างที่ 7 คือ หมายเลข 26+5 = 31
หน่วยตัวอย่างที่ 8 คือ หมายเลข 31+5 = 36
หน่วยตัวอย่างที่ 9 คือ หมายเลข 36+5 = 41
หน่วยตัวอย่างที่ 10 คือ หมายเลข 41+5 = 46

2.กรณีที่ 2 ผลหารของ N/n ไม่ใช่เลขจำนวนเต็ม มีขั้นตอนดังนี้

ตัวอย่างเช่น กลุ่มตรวจสอบภายในต้องการสุ่มตรวจความมีอยู่จริงของเครื่องคอมพิวเตอร์ของสำนักงานฯเขต 1 ที่มีเครื่องทั้งหมดจำนวน 50 เครื่อง ต้องการสุ่มตัวอย่าง 8 เครื่อง ด้วยวิธีการสุ่มตัวอย่างแบบเป็นระบบ(Systematic Sampling) ซึ่งมีขั้นตอนดังนี้

ขั้นตอนที่ 1 กำหนดหมายเลขประชากรตั้งแต่หมายเลข 1 ถึงหมายเลข 50

ขั้นตอนที่ 2 หาช่วงการสุ่มตรวจ k=N/n ในที่นี้ N=50 และn=8 ดังนั้น k= 50/8 = 6.27 และสุ่มหาตัวอย่างแรกแบบสุ่มเชิงเดียว เช่น การจับสลากจากหมายเลข 1-7 สมมุติสุ่มได้หมายเลข 5

ขั้นตอนที่ 3 หาหน่วยตัวอย่างที่ 2 ถึงหน่วยตัวอย่างที่ 8 ได้ดังนี้

หน่วยตัวอย่างที่ 1 คือ หมายเลข 5

หน่วยตัวอย่างที่ 2 คือ หมายเลข 5+7 = 12

หน่วยตัวอย่างที่ 3 คือ หมายเลข 12+7 = 19

หน่วยตัวอย่างที่ 4 คือ หมายเลข 19+7 = 26

หน่วยตัวอย่างที่ 5 คือ หมายเลข 26+7 = 33

หน่วยตัวอย่างที่ 6 คือ หมายเลข 33+7 = 40

หน่วยตัวอย่างที่ 7 คือ หมายเลข 40+7 = 47

หน่วยตัวอย่างที่ 8 คือ หมายเลข 47+7 = 54 หมายถึง หมายเลข 4

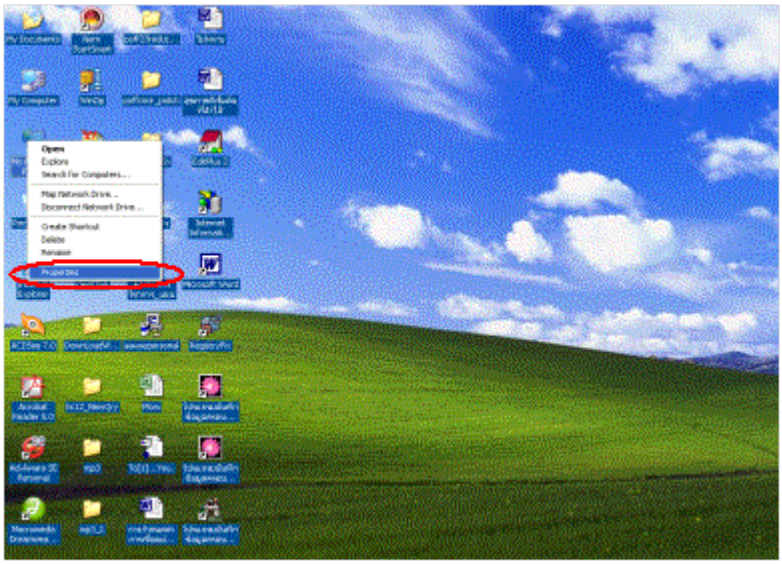
วิธีปฏิบัติงาน Work Instruction
เรื่อง ขั้นตอนการทดสอบการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส

❒ เอกสารควบคุม ❒ เอกสารไม่ควบคุม

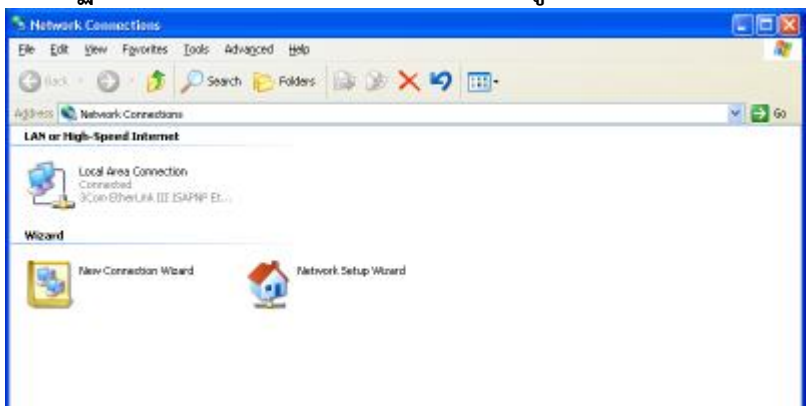
ขั้นตอนการทำงาน

1.ตรวจสอบการกำหนดค่า IP Address ของเครื่องที่จะใช้ทดสอบ

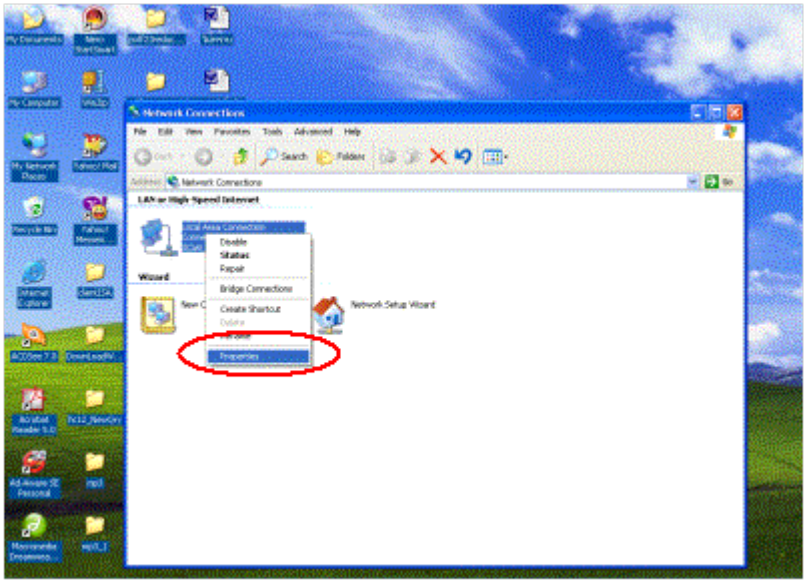
1.1 คลิกขวาที่ ไอคอน My Network Places บน Desktop แล้วเลือก Properties



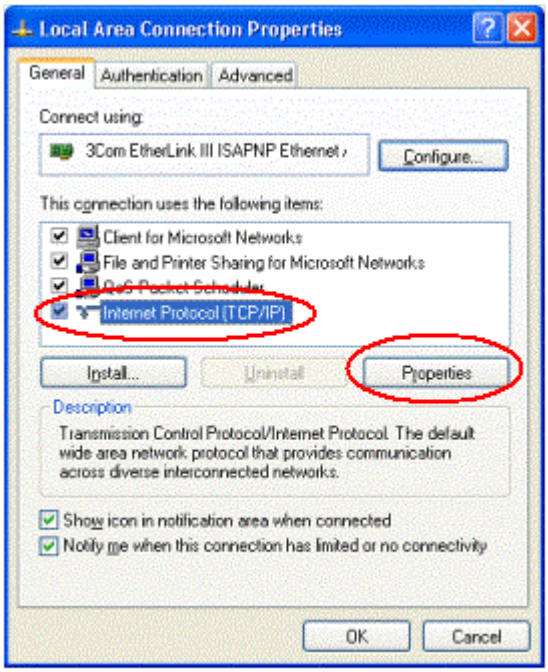
1.2 จะปรากฏหน้าต่าง Network Connections ดังรูป



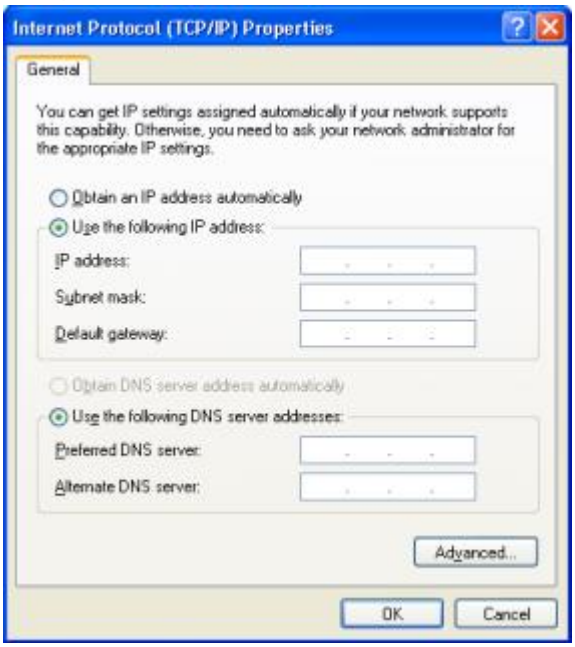
1.3 คลิกขวาที่ Local Area Connection แล้วเลือก Properties



1.4 จะปรากฏหน้าต่าง Local Area Connection Properties ดังรูป
จากนั้นคลิกที่ Internet Protocol (TCP/IP) แล้วคลิกที่ Properties



1.5 จะปรากฏหน้าต่าง Internet Protocol (TCP/IP) Properties ดังรูป



1.6 จากนั้นกำหนดค่าต่างๆ ซึ่งมีรูปแบบดังนี้

ค่า IP Address และ Subnet Mask มีรูปแบบการตั้งค่าดังนี้

IP Address = 192.168.1.XXX

โดยค่า XXX หมายถึง เลขใดก็ได้ที่อยู่ระหว่าง 2 ถึง 253 โดยแต่ละเครื่องที่อยู่ในเครือข่ายเดียวกันจะต้องมีเลข XXX ไม่ซ้ำกัน

ตัวอย่างเช่น เครื่องแม่ข่ายเป็น 192.168.1.201 เครื่องลูกข่ายเป็น 192.168.1.202 หรือ 192.168.1.203

Subnet Mask = 255.255.255.0

Default gateway = 192.168.1.1

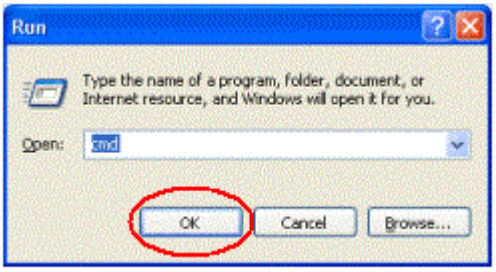
Preferred DNS Server = 192.168.1.1

แล้วคลิกปุ่ม **OK**

2.ทดสอบการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส

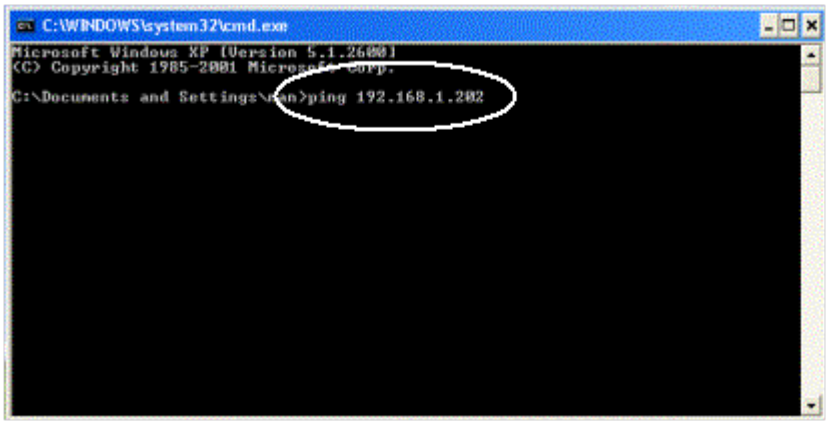
2.1 คลิกที่ปุ่ม Start แล้วเลือก Run... ดังรูป

2.2 จะปรากฏหน้าต่าง Run จากนั้นพิมพ์คำสั่ง cmd ในช่อง Open แล้วคลิกปุ่ม OK ดังรูป

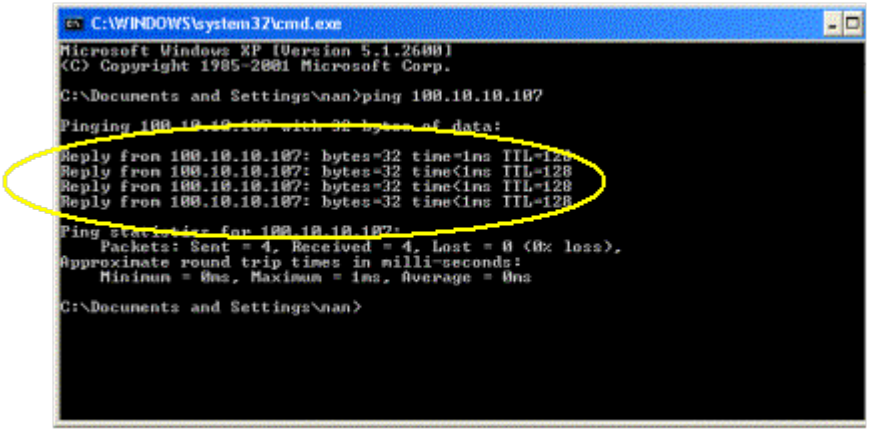


2.3 จะปรากฏหน้าต่าง C:\WINDOWS\System32\cmd.exeจากนั้นพิมพ์คำสั่ง ping ตามด้วยเลข IP ของเครื่องคอมพิวเตอร์ที่ต้องการติดต่อด้วย แล้ว enter (สามารถ ping จากเครื่องคอมพิวเตอร์เครื่องอื่นไปหาเครื่องคอมพิวเตอร์เป้าหมายได้ เพื่อตรวจสอบว่ามีการกำหนด IP ไว้)

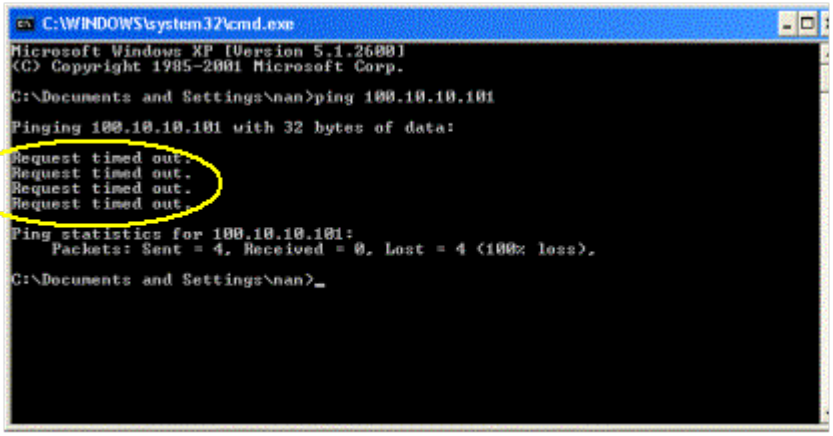
ตัวอย่างเช่น ping 192.168.1.202 ดังรูป



หากเครื่องสามารถเข้าถึงเครื่องคอมพิวเตอร์ที่ต้องการติดต่อได้ จะขึ้น Reply ให้ 4 บรรทัด ดังรูป



หากไม่สามารถเข้าถึงเครื่องคอมพิวเตอร์ที่ต้องการติดต่อได้ จะปรากฏ Request timed out ดังรูป



วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)
หมายเลขเอกสาร WI0601

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography) โดยดำเนินการตรวจสอบการเข้ารหัสข้อมูลที่สำคัญขององค์กร เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหรือรั่วไหลของข้อมูลองค์กร

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

(1) นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

(2) การบริหารจัดการกุญแจ (Key Management)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)		
เพื่อให้มีการปฏิบัติในการป้องกันข้อมูล โดยการเข้ารหัสข้อมูล	1.1 มีการประกาศนโยบายในการใช้มาตรการเข้ารหัสข้อมูลอย่างเป็นลายลักษณ์อักษร	-ตรวจสอบนโยบายการใช้มาตรการการเข้ารหัสข้อมูลที่เป็นลายลักษณ์อักษร
	1.2 ผู้ปฏิบัติงาน IT มีความเข้าใจในนโยบายการเข้ารหัสข้อมูลอย่างถูกต้อง	-สัมภาษณ์ความเข้าใจในนโยบายการเข้ารหัสข้อมูลที่องค์กรกำหนดไว้
	1.3 ผู้ปฏิบัติงาน IT มีการปฏิบัติในการเข้ารหัสข้อมูลตามที่หน่วยงานกำหนดไว้	-ให้ผู้ปฏิบัติงานแสดงถึงการปฏิบัติในการเข้ารหัสข้อมูลตามที่หน่วยงานกำหนดไว้
2.การบริหารจัดการกุญแจ (Key Management)		
เพื่อให้ข้อมูลสำคัญขององค์กรมีความปลอดภัยและมีผู้รับผิดชอบชัดเจน	2.1 มีการจัดเก็บกุญแจไว้ในที่ปลอดภัย	-สัมภาษณ์เกี่ยวกับสถานที่ในการจัดเก็บรักษากุญแจไว้ในที่ปลอดภัย
	2.2 มีการเปลี่ยนแปลงหรือปรับปรุงกุญแจได้อย่างเหมาะสม	-สัมภาษณ์กระบวนการในการเปลี่ยนแปลงหรือปรับปรุงกุญแจที่เหมาะสม
	2.3 มีการกำหนดผู้รับผิดชอบในการบริหารจัดการกุญแจ	-ตรวจสอบคำสั่งหรือการมอบหมายหน้าที่ผู้ดูแลบริหารจัดการกุญแจ

เกณฑ์การประเมินความเสี่ยง

(1) นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

ระดับ Level 1

-มีการกำหนดนโยบายการใช้มาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีขั้นตอนมาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศเป็นลายลักษณ์อักษร แต่จัดเก็บไว้ในที่ไม่ปลอดภัย

ระดับ Level 3

-มีการปฏิบัติตามนโยบาย/มาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศที่กำหนดไว้อย่างครอบคลุมครบถ้วน

- ไม่พบปัญหาจากการสูญหาย/เสียหาย/ถูกเปลี่ยนแปลงแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

(2) การบริหารจัดการกุญแจ (Key Management)

ระดับ Level 1

-มีนโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการกำหนดระบบการบริหารจัดการวงจรชีวิตของกุญแจหรือเปลี่ยนแปลงแก้ไขหรือปรับปรุงกุญแจได้อย่างเหมาะสม

ระดับ Level 3

-มีการกำหนดผู้รับผิดชอบในการบริหารจัดการกุญแจเป็นลายลักษณ์อักษร

-มีการจัดเก็บกุญแจไว้ในที่ปลอดภัย

- ไม่พบปัญหาจากการสูญหาย/เสียหาย/ถูกเปลี่ยนแปลงแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(Physical and environmental security)
หมายเลขเอกสาร WI0701

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากความไม่ปลอดภัยทางกายภาพต่อระบบสารสนเทศ ขององค์กร

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

1. พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

(1) ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

(2) การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

(3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและอุปกรณ์ (Securing office, room and facilities)

(4) การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environment threats)

(5) การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working is secure areas)

(6) พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

2. อุปกรณ์ (Equipment)

(1) การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)

(2) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(3) ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

(4) การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

(5) การนำทรัพย์สินของกรมออกนอกสำนักงาน (Removal of assets)

(6) ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off-premises)

(7) ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

7.1 มีการตรวจสอบการลบข้อมูลและทำลายสื่อบันทึกข้อมูลก่อนทิ้งอุปกรณ์

(8) อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended use equipment)

(9) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)		
เพื่อป้องกันความปลอดภัยทางกายภาพ	1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter) หน่วยงานต้องกำหนดขอบเขตหรือบริเวณพื้นในการรักษาความมั่นคงปลอดภัย โดยการประเมินความเสี่ยง เพื่อนำไปจัดลำดับความเสี่ยงในการเข้า-ออกทางกายภาพ ดังนี้ (1) ความเสี่ยงสูง เช่น ห้อง Datacenter, ระบบฐานข้อมูล (2) ความเสี่ยงปานกลาง ระบบเครือข่าย เช่น Wall Mount Rack และตู้ network ห้อง Datacenter (3) ความเสี่ยงต่ำ ห้องปฏิบัติงาน, เครื่อง Client ณ จุดปฏิบัติงาน	-ตรวจสอบการกำหนดขอบเขตหรือบริเวณพื้นในการรักษาความมั่นคงปลอดภัยโดยการประเมินความเสี่ยง เพื่อนำไปจัดลำดับความเสี่ยงในการเข้า-ออกทางกายภาพอย่างเหมาะสมหรือไม่

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
เพื่อให้พื้นที่ที่ต้องการรักษาความปลอดภัยต้องมีการป้องกันโดยมีการควบคุมการเข้าออกอย่างเหมาะสม	1.2 การควบคุมการเข้าออกทางกายภาพ (Physical entry controls) (1) ระดับความเสี่ยงสูง - กั้นห้องให้เป็นสัดส่วนมั่นคงแข็งแรง - มีระบบการรักษาความปลอดภัยในการเข้าออก สแกนนิ้วมือ หรือสแกนม่านตา - กล้องวงจรปิดครอบคลุมพื้นที่ 100 % - กำหนดผู้รับผิดชอบและผู้ดูแลอุปกรณ์ทุกอย่าง - มีระเบียบ มาตรการในการปฏิบัติการเข้าออกทางกายภาพ โดยเฉพาะการดำเนินการด้วยบุคคลภายนอกต้องมีเจ้าหน้าที่ติดตามตลอดเวลา - มีเจ้าหน้าที่รักษาความปลอดภัย (2) ระดับความเสี่ยงปานกลาง - กั้นห้องให้เป็นสัดส่วน- กล้องวงจรปิดเฉพาะบางส่วนที่สำคัญ- กำหนดผู้รับผิดชอบ- เจ้าหน้าที่รักษาความปลอดภัย- คีย์การ์ด- ตำแหน่งการติดตั้งที่เหมาะสมของระบบ Network (2.3) ระดับความเสี่ยงต่ำ - เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) - กำหนดผู้รับผิดชอบ - กล้องวงจรปิด พื้นที่โดยรวม - ตำแหน่งที่เหมาะสมสำหรับการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย	-ตรวจสอบ/เยี่ยมชมสถานที่ที่เป็นพื้นที่ที่กำหนดไว้รักษาความปลอดภัยและระบบการควบคุม-เข้าออกสถานที่ว่าเป็นไปตามที่นโยบายกำหนดหรือไม่
1.เพื่อให้มีการจัดระบบการรักษาความปลอดภัยทางกายภาพที่เหมาะสม สำหรับสำนักงาน ห้องทำงานและอุปกรณ์ 2.เพื่อป้องกันความเสี่ยงอันเกิดจากทางกายภาพ สำหรับสำนักงาน ห้องทำงานและอุปกรณ์	1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและอุปกรณ์ (Securing office, room and facilities) - มีเจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ควบคุมการเข้าออกบริเวณ - อุปกรณ์ต่างๆที่เกี่ยวข้องกับงานระบบ ต้องติดตั้งในตู้เพื่อป้องกัน การทำลาย การปิดระบบ - มีการกำหนดพื้นที่ในการปฏิบัติงานตามตำแหน่งหน้าที่ของผู้ดูแลระบบ -กำหนดผู้รับผิดชอบและดูแลอุปกรณ์ห้องแม่ข่าย -มีระบบป้องกันความปลอดภัย เช่น Firewall antivirus การกำหนดสิทธิ์ใช้งาน	-ตรวจสอบ/เยี่ยมชมพื้นที่สำนักงานและการรักษาความมั่นคงปลอดภัย

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
เพื่อให้หน่วยงานมีการจัดระบบการป้องกันทางกายภาพ รองรับความเสี่ยง/ความเสียหายจากไฟไหม้น้ำท่วมแผ่นดินไหวระเบิดความไม่สงบและรูปแบบอื่น ๆ ภัยพิบัติของธรรมชาติ หรือที่มนุษย์สร้างขึ้น	1.4 การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environment threats) - มีระบบเตือนภัยฉุกเฉิน กรณีไฟไหม น้ำท่วม - มีอุปกรณ์ดับเพลิงตามมาตรฐาน - มีระบบปรับอากาศและความคุมความชื้น - แผน คู่มือ การซักซ้อม และการสรุปผล การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม - กรมมีแผนการใช้งานด้าน Disaster Recovery Site หรือระบบคอมพิวเตอร์สำรองเมื่อมีเหตุการณ์ด้านภัยพิบัติของสภาพแวดล้อมขึ้น -มีระบบปรับอุณหภูมิภายในห้องให้เหมาะสมกับความชื้น -มีระบบสำรองไฟ รองรับอุปกรณ์ให้เพียงพอ เครื่องปั่นไฟฟ้า 1.5 การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working is secure areas) -มีระบบเตือนภัยฉุกเฉิน กรณีไฟไหม้ น้ำท่วม แผ่นดินไหว - มีระบบเตือนภัยฉุกเฉิน กรณีไฟไหม น้ำท่วม - มีอุปกรณ์ดับเพลิงตามมาตรฐาน - มีระบบปรับอากาศและความคุมความชื้น - แผน คู่มือ การซักซ้อม และการสรุปผล การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม - กรมมีแผนการใช้งานด้าน Disaster Recovery Site หรือระบบคอมพิวเตอร์สำรองเมื่อมีเหตุการณ์ด้านภัยพิบัติของสภาพแวดล้อมขึ้น -มีระบบปรับอุณหภูมิภายในห้องให้เหมาะสมกับความชื้น -มีอุปกรณ์ดับเพลิงตามมาตรฐาน -มีระบบสำรองไฟ รองรับอุปกรณ์ให้เพียงพอ เครื่องปั่นไฟฟ้า	-ตรวจสอบ/เยี่ยมชมพื้นที่และระบบป้องกันภัยคุกตามจากภายนอกและสภาพแวดล้อมว่าเป็นไปตามที่กำหนดหรือไม่ -ตรวจสอบ/เยี่ยมชมพื้นที่และระบบป้องกันภัยคุกตามจากภายนอกและสภาพแวดล้อมว่าเป็นไปตามที่กำหนดหรือไม่

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.เพื่อให้มีการกำหนดจุดหรือบริเวณที่สามารถเข้าถึงพื้นที่ที่ถูกกำหนดเป็นขอบเขตที่ต้องรักษาความปลอดภัย 2.เพื่อป้องกันความเสี่ยงต่อการเข้าถึงพื้นที่ที่ถูกกำหนดเป็นขอบเขตที่ต้องรักษาความปลอดภัยโดยไม่ได้รับอนุญาต	1.6 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas) -จุดหรือบริเวณที่สามารถเข้าถึงกรม เช่น พื้นที่สำหรับรับสิ่งของบริเวณอื่น ๆ ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่ของกรมได้ต้องมีการควบคุม และหากเป็นไปได้ จุดหรือบริเวณดังกล่าวควรแยกออกมาจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต	-ตรวจสอบ/เยี่ยมชมสถานที่พื้นที่สำหรับรับ-ส่งของ
2. อุปกรณ์ (Equipment)		
อุปกรณ์จะได้รับการจัดวางหรือการป้องกันเพื่อลดความเสี่ยงจากภัยคุกคามด้านสิ่งแวดล้อมและอันตรายและโอกาสสำหรับการเข้าถึงไม่ได้รับอนุญาต	2.1 การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection) -มีการกำหนดพื้นที่ที่ใช้ในการติดตั้งอุปกรณ์ที่มีความสำคัญให้เข้าถึงยาก -มีการจัดวางอุปกรณ์ที่มีความสำคัญ ไม่ให้เสี่ยงต่อภัยคุกคามด้านสิ่งแวดล้อมและอันตรายและโอกาสสำหรับการเข้าถึงไม่ได้รับอนุญาต	-ตรวจสอบ/เยี่ยมชมสถานที่
1.อุปกรณ์ที่สำคัญต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่น ๆ 2.เพื่อไม่ให้เกิดปัญหา/ความเสี่ยงอันสาเหตุมาจากการล้มเหลวของระบบอุปกรณ์สนับสนุนการทำงานต่างๆ	2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) อุปกรณ์ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ โดยมีการวิเคราะห์และจัดลำดับความเสี่ยงเพื่อจัดระบบป้องกันอุปกรณ์ที่เหมาะสม (1) ความเสี่ยงสูง ต้องมีระบบสำรองไฟฟ้าทั้ง UPS และเครื่องกำเนิดไฟฟ้า (2) ความเสี่ยงปานกลาง ต้องมีระบบสำรองไฟฟ้าUPS (3) ความเสี่ยงต่ำมีระบบสำรองไฟฟ้าหรือไม่ก็ได้	-ตรวจสอบ/เยี่ยมชมสถานที่

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.เพื่อให้หน่วยงานมีการจัดการป้องกันการเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งส่งข้อมูลหรือสนับสนุนบริการสารสนเทศจากการขัดขวางการทำงานการแทรกแซงสัญญาณ หรือการทำให้เสียหาย 2.เพื่อป้องกัน/ลดความเสี่ยงจากการขัดขวางการทำงานการแทรกแซงสัญญาณ หรือการทำให้เสียหายต่อการเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งใช้ในการรับ-ส่งข้อมูลหรือสนับสนุนบริการสารสนเทศ	2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)การเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งส่งข้อมูลหรือสนับสนุนบริการสารสนเทศ ต้องมีการป้องกันจากการขัดขวางการทำงานการแทรกแซงสัญญาณ หรือการทำให้เสียหาย หรือ การขโมย ไฟไหม้ วัตถุระเบิด ควัน น้ำ หรือความล้มเหลวของน้ำประปา ฝุ่น สารเคมี การรบกวนแหล่งจ่ายไฟฟ้า การรบกวนการสื่อสาร รังสีแม่เหล็กไฟฟ้า ป่าเถื่อน การกิน/ดื่ม/สูญบุหรี่ที่ใกล้กับพื้นที่ที่รักษาความปลอดภัย (1) ความเสี่ยงสูง การเดินสายต้องใช้สายป้องกันการรบกวนสัญญาณและการเข้าถึงสายสัญญาณ (2) ความเสี่ยงปานกลาง การเดินสายต้องป้องกันการเข้าถึงสายสัญญาณ (3) ความเสี่ยงต่ำใช้สายสัญญาณธรรมดา (4) ต้องมีแผนการตรวจสอบระบบการเดินสายไฟ สายเคเบิ้ล สายสื่อสาร	-ตรวจสอบ/เยี่ยมชมสถานที่การเดินสายสัญญาณและสายสื่อสาร
1. เพื่อให้หน่วยงานจัดระบบการบำรุงรักษาอุปกรณ์อย่างถูกต้อง 2. เพื่อให้มีสภาพการใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง	2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้องเพื่อให้มีสภาพการใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง (1) ระบบที่มีความเสี่ยงสูงต้องบำรุงรักษาทุก 1 เดือน (2) ระบบที่มีความเสี่ยงปานกลางต้องบำรุงรักษาทุก 3 เดือน (3) ระบบที่มีความเสี่ยงต่ำต้องบำรุงรักษาทุก 12 เดือน	-ตรวจสอบ/เยี่ยมชมสถานที่ -สัมภาษณ์การบำรุงรักษาอุปกรณ์ -สอบทานแผนการบำรุงรักษาและการปฏิบัติในการบำรุงรักษา

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.เพื่อให้หน่วยงานมีการจัดระบบการป้องกันทรัพย์สินของกรมออกนอกสำนักงานที่เหมาะสมและเป็นไปตามที่กรมกำหนด โดยมีการขออนุญาตอย่างถูกต้อง 2.เพื่อป้องกัน/ลดความเสี่ยงในการสูญหาย/เสียหายของทรัพย์สินของกรม	2.5 การนำทรัพย์สินของกรมออกนอกสำนักงาน (Removal of assets) อุปกรณ์ สารสนเทศหรือซอฟแวร์ต้องไม่มีการนำออกนอกสำนักงาน โดยปราศจากการขออนุญาต (1) ทรัพย์สินที่มีความเสี่ยงสูงไม่ให้ออกนอกสถานที่ (2) ทรัพย์สินที่มีความเสี่ยงปานกลางและต่ำ มีระบบการควบคุมดูแลทรัพย์สิน การลงทะเบียนทรัพย์สิน /ครุภัณฑ์ แบบฟอร์มการยืม – คืนทรัพย์สิน	-สัมภาษณ์กระบวนการนำทรัพย์สินของกรมออกนอกสำนักงาน -ตรวจสอบแบบฟอร์มการนำทรัพย์สินของกรมออกนอกสำนักงาน
1.เพื่อให้หน่วยงานจัดระบบการป้องกัน/รักษาความปลอดภัยต่อทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน โดยการประเมินความเสี่ยงของการปฏิบัติงานภายนอกสำนักงาน 2.ไม่พบปัญหา/ความเสี่ยงในการใช้งานทรัพย์สินที่อยู่ภายนอกสำนักงาน	2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off-premises) (1) กำหนดรหัสการเข้าถึงการใช้งานอุปกรณ์คอมพิวเตอร์ (2) กำหนดผู้รับผิดชอบและดูแลอุปกรณ์ (3) กำหนดผู้รับผิดชอบและดูแลอุปกรณ์ห้องแม่ข่าย (4) มีระบบป้องกันความปลอดภัย เช่น Antivirus การกำหนดสิทธิ์ใช้งาน	-สัมภาษณ์การจัดการรักษาความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานว่าดำเนินการอย่างไรบ้าง
1.เพื่อให้หน่วยงานมีการกำหนดขั้นตอน/มาตรการการลบและทำลายสื่อบันทึกข้อมูลก่อนทิ้งอุปกรณ์ 2.เพื่อให้มีการปฏิบัติตามขั้นตอน/มาตรการการลบและทำลายสื่อบันทึกข้อมูลก่อนทิ้งอุปกรณ์ 3.เพื่อมั่นใจว่าข้อมูลสำคัญและซอฟแวร์ที่มีใบอนุญาตมีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์หรือก่อนนำอุปกรณ์ไปใช้งานสถานที่อื่น	2.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่นอุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องมีการตรวจสอบ เพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟแวร์ที่มีใบอนุญาตมีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์หรือก่อนนำอุปกรณ์ไปใช้งานสถานที่อื่น โดยมีการตรวจสอบการลบข้อมูลและทำลายสื่อบันทึกข้อมูลก่อนทิ้งอุปกรณ์	-สัมภาษณ์การทำลายอุปกรณ์/สื่อการจัดเก็บข้อมูลที่ไม่ใช้แล้วหน่วยงานมีการดำเนินการอย่างไร

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.เพื่อให้หน่วยงานกำหนดมาตรการการป้องกันอุปกรณ์หรือทรัพย์สินขององค์กรที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล 2.เพื่อให้มีการปฏิบัติตามมาตรการการป้องกันอุปกรณ์หรือทรัพย์สินขององค์กรที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล	2.8 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended use equipment) ผู้ใช้งานต้องมีการป้องกันอย่างเหมาะสม ซึ่งเป็นอุปกรณ์ที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล	-สัมภาษณ์ในกรณีที่ไม่มีผู้ดูแลหน่วยงานทำการป้องกันอุปกรณ์ข้อมูลอย่างไร
1.เพื่อป้องกันเอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ 2.เพื่อป้องกันสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการนำมาใช้งาน (เพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร)	2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy) -เอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ และป้องกันสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ เมื่อมีการนำมาใช้งาน ต้องทำเรื่องขออนุญาตการนำไปใช้งานงานและกำหนดระยะเวลาเริ่มใช้งาน ระบุระยะเวลาในการนำส่งคืน ระบุถึงการจัดเก็บในระยะเวลาการใช้งาน	-สัมภาษณ์และเยี่ยมชมสถานที่ว่าเป็นไปตามนโยบายโต๊ะทำงานปลอดเอกสารหรือไม่และหน้าจอคอมพิวเตอร์มีการล็อกหน้าจอไว้หรือไม่

เกณฑ์การประเมินความเสี่ยง

(1.)พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

(1.1) ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

ระดับ Level 1

-มีการกำหนดขอบเขตหรือบริเวณพื้นในการรักษาความมั่นคงปลอดภัย

ระดับ Level 2

-มีหลักเกณฑ์ในการกำหนดขอบเขตหรือบริเวณพื้นในการรักษาความมั่นคงปลอดภัยที่ถูกต้อง โดยการประเมินความเสี่ยง

-มีการสื่อสารให้กับบุคลากรในองค์กรทราบอย่างชัดเจนและถือปฏิบัติ

ระดับ Level 3

-บุคลากรภายในองค์กรอย่างน้อย 3 คนทราบพื้นที่ที่ต้องรักษาความปลอดภัย

-ไม่พบความเสี่ยงในการเข้า-ออกทางกายภาพ

(1.2) การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

ระดับ Level 1

-มีการจัดระบบควบคุมการเข้า-ออกทางกายภาพ แต่มิได้ประเมินความเสี่ยงและจัดระบบตามระดับความเสี่ยงที่กรมกำหนด

ระดับ Level 2

-มีการจัดระบบควบคุมการเข้า-ออกทางกายภาพ โดยการประเมินความเสี่ยงและจัดระบบการควบคุมตามระดับความเสี่ยงตามที่กรมกำหนด

ระดับ Level 3

-ระบบการควบคุมการเข้าออกทางกายภาพ มีการจัดเก็บข้อมูลการเข้า-ออก เพื่อการพิสูจน์/ค้นหาผู้บุกรุกได้

-ไม่พบปัญหา/ความเสี่ยงในการเข้า-ออกทางกายภาพ

(1.3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและอุปกรณ์ (Securing office, room and facilities)

ระดับ Level 1

-มีการจัดระบบควบคุมทางกายภาพ สำหรับสำนักงาน ห้องทำงานและอุปกรณ์ มีอย่างน้อยตามที่กรมกำหนด

ระดับ Level 2

-มีการจัดระบบควบคุมทางกายภาพ สำหรับสำนักงาน ห้องทำงานและอุปกรณ์ มีอย่างน้อยตามที่กรมกำหนดและตามมาตรฐานกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงอันเกิดจากทางกายภาพ สำหรับสำนักงาน ห้องทำงานและอุปกรณ์

(1.4) การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environment threats)

ระดับ Level 1

-มีการจัดระบบการป้องกันทางกายภาพ โดยมีอย่างน้อยที่กรมกำหนดไว้ ดังระบุข้างต้น

ระดับ Level 2

-มีการจัดระบบการป้องกันทางกายภาพ เพื่อรองรับความเสี่ยง/ความเสียหายจากไฟไหม้ น้ำท่วมแผ่นดินไหวระเบิดความไม่สงบและรูปแบบอื่น ๆ ภัยพิบัติของธรรมชาติ หรือที่มนุษย์สร้างขึ้น

ระดับ Level 3

-ไม่พบความเสี่ยง/ความเสียหายจากไฟไหม้น้ำท่วมแผ่นดินไหวระเบิดความไม่สงบและรูปแบบอื่น ๆ ภัยพิบัติของธรรมชาติ หรือที่มนุษย์สร้างขึ้น

(1.5) การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working is secure areas)

ระดับ Level 1

-มีการจัดระบบการป้องกันทางกายภาพ โดยมีอย่างน้อยที่กรมกำหนดไว้ ดังระบุข้างต้น

ระดับ Level 2

-มีการจัดระบบการป้องกันทางกายภาพ เพื่อรองรับความเสี่ยง/ความเสียหายจากไฟไหม้ น้ำท่วมแผ่นดินไหวระเบิดความไม่สงบและรูปแบบอื่น ๆ ภัยพิบัติของธรรมชาติ หรือที่มนุษย์สร้างขึ้น

ระดับ Level 3

-ไม่พบความเสี่ยง/ความเสียหายจากไฟไหม้น้ำท่วมแผ่นดินไหวระเบิดความไม่สงบและรูปแบบอื่น ๆ ภัยพิบัติของธรรมชาติ หรือที่มนุษย์สร้างขึ้น

(1.6) พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

ระดับ Level 1

-มีการกำหนดจุดหรือบริเวณที่สามารถเข้าถึงพื้นที่ที่ถูกกำหนดเป็นขอบเขตที่ต้องรักษาความปลอดภัยอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการจัดระบบการควบคุมป้องกันการเข้าถึงพื้นที่ที่ถูกกำหนดเป็นขอบเขตที่ต้องรักษาความปลอดภัย โดยไม่ได้รับอนุญาตที่เหมาะสม

ระดับ Level 3

-ปัญหา/ความเสี่ยงต่อการเข้าถึงพื้นที่ที่ถูกกำหนดเป็นขอบเขตที่ต้องรักษาความปลอดภัยโดยไม่ได้รับอนุญาต

(2.) อุปกรณ์ (Equipment)

(2.1) การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)

ระดับ Level 1

-มีการกำหนดพื้นที่ที่ใช้ในการติดตั้งอุปกรณ์ที่มีความสำคัญให้เข้าถึงยาก

-มีการกำหนดว่าอุปกรณ์ใดบ้างที่มีความสำคัญ

ระดับ Level 2

-มีการจัดวางอุปกรณ์ที่มีความสำคัญ ไม่ให้เสี่ยงต่อภัยคุกคามด้านสิ่งแวดล้อมและอันตรายและโอกาสสำหรับการเข้าถึงไม่ได้รับอนุญาต

-มีการติดตั้งอุปกรณ์ต้องติดตั้งในตู้เก็บอุปกรณ์ให้มิดชิดและมีระบบเตือนภัยฉุกเฉิน

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงจากภัยคุกคามด้านสิ่งแวดล้อมและอันตรายและโอกาสสำหรับการเข้าถึงไม่ได้รับอนุญาต

(2.2) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

ระดับ Level 1

-มีการกำหนดอุปกรณ์ที่สำคัญที่ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่น ๆ โดยมีการวิเคราะห์และจัดลำดับความเสี่ยง เพื่อจัดระบบป้องกันอุปกรณ์ที่เหมาะสมตามที่กรมฯกำหนด

-มีการจัดระบบป้องกันอุปกรณ์ที่สำคัญตามที่กรมฯกำหนด แต่ยังไม่ครอบคลุมครบถ้วน

ระดับ Level 2

-มีการจัดระบบป้องกันอุปกรณ์ที่สำคัญตามที่กรมฯกำหนดอย่างครอบคลุมครบถ้วน

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงอันสาเหตุมาจากการล้มเหลวของระบบอุปกรณ์สนับสนุนการทำงานต่างๆ

(2.3) ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

ระดับ Level 1

-มีการจัดการป้องกันการเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งใช้ในการรับ-ส่งข้อมูลหรือสนับสนุนบริการสารสนเทศไม่ครอบคลุม และไม่เป็นไปตามที่กรมกำหนด

-มีแผนการตรวจสอบระบบการเดินสายไฟ สายเคเบิ้ล สายสื่อสาร

ระดับ Level 2

-มีการจัดการป้องกันการเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งใช้ในการรับ-ส่งข้อมูลหรือสนับสนุนบริการสารสนเทศครอบคลุม และเป็นไปตามที่กรมกำหนด

-มีการดำเนินการตรวจสอบระบบการเดินสายไฟ สายเคเบิ้ล สายสื่อสาร แต่ไม่สม่ำเสมอ

ระดับ Level 3

-มีการดำเนินการตรวจสอบระบบการเดินสายไฟ สายเคเบิ้ล สายสื่อสาร แต่สม่ำเสมอและมีการรายงานผลการตรวจสอบที่เหมาะสม

-ไม่พบปัญหา/ความเสี่ยงจากการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหายต่อการเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งใช้ในการรับ-ส่งข้อมูลหรือสนับสนุนบริการสารสนเทศ

(2.4) การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

ระดับ Level 1

-มีการจัดระบบการบำรุงรักษาอุปกรณ์ อย่างน้อยมีการวางแผน-ดำเนินการตามแผน-ตรวจสอบการบำรุงรักษาอุปกรณ์-นำผลการตรวจสอบการบำรุงรักษาอุปกรณ์มาวิเคราะห์หาสาเหตุและปรับปรุงแก้ไข

-มีการกำหนดความถี่ในการบำรุงรักษาแต่ละอุปกรณ์ตามความเสี่ยง

ระดับ Level 2

-อุปกรณ์มีความพร้อมใช้งาน สภาพใช้งานอยู่ระดับปานกลาง-ดีขึ้นไปไม่ต่ำกว่าร้อยละ 80 ของอุปกรณ์ทั้งหมด

-อุปกรณ์ทั้งหมดในหน่วยงานมีการหยุดชะงักการใช้งาน ไม่เกิน 3 ครั้งต่อปี

ระดับ Level 3

-ไม่พบอุปกรณ์ทั้งหมดในหน่วยงานมีการหยุดชะงักการใช้งาน

(2.5) การนำทรัพย์สินของกรมออกนอกสำนักงาน (Removal of assets)

ระดับ Level 1

-มีการจัดระบบการป้องกันทรัพย์สินของกรมออกนอกสำนักงาน ตามที่กรมกำหนด

ระดับ Level 2

-มีการจัดระบบการป้องกันทรัพย์สินของกรมออกนอกสำนักงาน ตามที่กรมกำหนดและเหมาะสม

-พบปัญหา/ความเสี่ยงจากการนำทรัพย์สินของกรมออกนอกสำนักงาน ไม่เกิน 3 ครั้ง/ปี

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงจากการนำทรัพย์สินของกรมออกนอกสำนักงาน

(2.6) ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off-premises)

ระดับ Level 1

-มีจัดระบบการป้องกัน/รักษาความปลอดภัยต่อทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานตามที่กรมกำหนด

ระดับ Level 2

-มีจัดระบบการป้องกัน/รักษาความปลอดภัยต่อทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานโดยการประเมินความเสี่ยงของการปฏิบัติงานภายนอกสำนักงานและตามที่กรมกำหนด

ระดับ Level 3

ไม่พบปัญหา/ความเสี่ยงในการใช้งานทรัพย์สินที่อยู่ภายนอกสำนักงาน

(2.7) ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

2.7.1 มีการตรวจสอบการลบข้อมูลและทำลายสื่อบันทึกข้อมูลก่อนทิ้งอุปกรณ์

ระดับ Level 1

-มีการกำหนดขั้นตอน/มาตรการการลบและทำลายสื่อบันทึกข้อมูลก่อนทิ้งอุปกรณ์ เป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอน/มาตรการการลบและทำลายสื่อบันทึกข้อมูลก่อนทิ้งอุปกรณ์

ระดับ Level 3

ไม่พบปัญหา/ความเสี่ยงข้อมูลสำคัญและซอฟแวร์ที่มีใบอนุญาตที่มีอยู่ในสื่อบันทึกข้อมูลกรณีที่ต้องกำจัดอุปกรณ์ หรือนำอุปกรณ์ไปใช้งานสถานที่อื่น

(2.8) อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended use equipment)

ระดับ Level 1

-มีการกำหนดมาตรการการป้องกันอุปกรณ์หรือทรัพย์สินขององค์กรที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล เป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามมาตรการการป้องกันอุปกรณ์หรือทรัพย์สินขององค์กรที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล แต่ยังไม่ครอบคลุมทุกอุปกรณ์

ระดับ Level 3

-มีการปฏิบัติตามมาตรการการป้องกันอุปกรณ์หรือทรัพย์สินขององค์กรที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแลครอบคลุมทุกอุปกรณ์

-ไม่พบปัญหา/ความเสี่ยงของอุปกรณ์หรือทรัพย์สินขององค์กรที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล

(2.9) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

ระดับ Level 1

-มีการกำหนดมาตรการ/ขั้นตอนป้องกันเอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้และสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการนำมาใช้งาน (เพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร) เป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามมาตรการ/ขั้นตอนป้องกันเอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้และสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการนำมาใช้งาน (เพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร) ค่าเป้าหมาย 100%

ระดับ Level 3

ไม่พบปัญหา/ความเสี่ยงในการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)
หมายเลขเอกสาร WI0801

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security) เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน มีความมั่นคงปลอดภัย

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

1. ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)
2. การบริหารจัดการเปลี่ยนแปลง (Change management)
3. การบริหารจัดการขีดความสามารถของระบบ (Capacity management)
4. การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)
5. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)
   (5.1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)
6. การสำรองข้อมูล (Information Backup)
   (6.1) มีการสำรองข้อมูลและระบบสารสนเทศ
   (6.2) การทดสอบข้อมูลสำรอง(กู้ระบบคืน)
   (6.3) การเก็บรักษาข้อมูลสำรองและสื่อบันทึก
7. การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)
   (7.1) การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)
   (7.2) การป้องกันข้อมูลล็อก (Protection of log information)
   (7.3) ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)
   (7.4) การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

8. การควบคุมการติดตั้งซอร์ฟแวร์บนระบบให้บริการ (Control of operation software)

(8.1) การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operation systems)

(8.2) การบริการจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

(8.2.1) การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

(8.2.2) การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)

9. สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

(9.1) มาตรการการตรวจประเมินระบบ (Information systems audit controls)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1. ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)		
1.เพื่อให้มีการจัดทำคู่มือ/ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษรและมีการทบทวนปรับปรุงให้ทันสมัยอยู่เสมอ 2.ผู้ที่จำเป็นต้องใช้งานสามารถเข้าถึงคู่มือ/ขั้นตอนการปฏิบัติงานได้ เพื่อปฏิบัติงานได้อย่างถูกต้อง	1.มีการจัดทำคู่มือ/ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษรและมีการทบทวนปรับปรุงให้ทันสมัยอยู่เสมอ 2.มีการจัดเก็บคู่มือ/ขั้นตอนการปฏิบัติงานไว้ในสถานที่ที่ผู้จำเป็นต้องใช้งานสามารถเข้าถึงได้	-ตรวจสอบคู่มือ/ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษรและการทบทวนคู่มือให้เป็นปัจจุบัน -สุ่มตรวจให้ผู้ปฏิบัติงานหยิบคู่มือการปฏิบัติงานที่จัดเก็บไว้ ได้อย่างรวดเร็วและสามารถเข้าถึงได้สำหรับผู้มีความจำเป็น
3.เพื่อให้มีระบบการควบคุมกำกับติดตามประเมินผลการปฏิบัติงานให้เป็นไปตามคู่มือ/ขั้นตอนการปฏิบัติงาน 4.ไม่พบปัญหา/ความเสี่ยงในการปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศ	3.มีระบบการควบคุมกำกับ ติดตามประเมินผลการปฏิบัติงานให้เป็นไปตามคู่มือ/ขั้นตอนการปฏิบัติงาน 4.มีการปฏิบัติตามคู่มือ/ขั้นตอนการปฏิบัติงานได้อย่างถูกต้อง	-สัมภาษณ์กระบวนการควบคุมกำกับติดตามประเมินผลการปฏิบัติงานให้เป็นไปตามคู่มือ/ขั้นตอนการปฏิบัติงาน -ตรวจสอบรายงานผลการดำเนินงานและการติดตามประเมินผลการปฏิบัติงานให้เป็นไปตามคู่มือ/ขั้นตอนการปฏิบัติงาน

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
2.การบริหารจัดการเปลี่ยนแปลง (Change management)		
1.เมื่อมีการเปลี่ยนแปลงขององค์กรที่สำคัญอันส่งผลกระทบต่อความมั่นคงปลอดภัยของการดำเนินงาน อุปกรณ์ ประมวลผลสารสนเทศและระบบ ต้องมีระบบในการควบคุมเพื่อไม่ให้เกิดความเสี่ยงหรือความเสียหายต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศขององค์กร 2.เพื่อให้มีการกำหนดขั้นตอนการปฏิบัติในการควบคุมการดำเนินงานเมื่อมีการขององค์กรที่สำคัญอันส่งผลกระทบต่อความมั่นคงปลอดภัยของการดำเนินงาน อุปกรณ์ ประมวลผลสารสนเทศและระบบ	1.มีระบบการควบคุมการดำเนินงาน อุปกรณ์ประมวลผลสารสนเทศและระบบเมื่อมีการเปลี่ยนแปลงขององค์กร 2.มีการกำหนดขั้นตอนการปฏิบัติในการควบคุมการดำเนินงาน เมื่อมีการขององค์กรที่สำคัญอันส่งผลกระทบต่อความมั่นคงปลอดภัยของการดำเนินงาน อุปกรณ์ ประมวลผลสารสนเทศและระบบ 3.มีการกำหนดระดับชั้นของผู้ให้ข่าวสาร	-ตรวจสอบกระบวนงานควบคุมการดำเนินงาน อุปกรณ์ประมวลผลสารสนเทศและระบบ เมื่อมีการเปลี่ยนแปลงขององค์กร และขั้นตอนการปฏิบัติงาน รวมทั้ง Work Flow และการจัดระดับชั้นของผู้ให้ข้อมูลข่าวสาร -สัมภาษณ์การปฏิบัติงานในการควบคุมการดำเนินงาน อุปกรณ์ประมวลผลสารสนเทศและระบบ เมื่อมีการเปลี่ยนแปลงขององค์กร และขั้นตอนการปฏิบัติงาน รวมทั้ง Work Flow และการจัดระดับชั้นของผู้ให้ข้อมูลข่าวสาร
3. การบริหารจัดการขีดความสามารถของระบบ (Capacity management)		
1.เพื่อให้มีการใช้ทรัพยากรของระบบต้องมีการติดตาม ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ 2.เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความพร้อมใช้งานตลอดเวลา	การใช้ทรัพยากรของระบบต้องมีการติดตาม ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ (1) มีการกำหนดหน้าที่ความรับผิดชอบของผู้ดูแลข้อมูล (2) มีการวางแผนการตรวจสอบประเมินขีดความสามารถของระบบและกำหนดค่าสูงสุดที่ยอมรับได้ของขีดความสามารถของระบบ	-สำหรับหน่วยงานที่มีเครื่องแม่ข่าย ผู้ตรวจสอบภายใน ต้องเรียกดูข้อมูลดังนี้ 1.คำสั่งหรือการมอบหมายหน้าที่ของผู้ดูแลระบบ 2.แผนการตรวจสอบประเมินสมรรถนะระบบและการกำหนดค่าสูงสุดที่ยอมรับได้ของขีดความสามารถของระบบ อย่างน้อยได้แก่ CPU RAM HD Bandwidth

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.เพื่อให้มีการใช้ทรัพยากรของระบบต้องมีการติดตาม ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ 2.เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความพร้อมใช้งานตลอดเวลา	ทั้งทางด้านอุปกรณ์ระบบคอมพิวเตอร์ และระบบเครือข่าย อย่างน้อยการประเมินค่า CPU, RAM, Storage, Network Utilization (3) ดำเนินการตรวจสอบประเมินขีดความสามารถของระบบดังระบุข้างต้น (4) ดำเนินการวิเคราะห์ ประมวลผลขีดสมรรถนะของระบบเพื่อค้นหาสาเหตุและปัญหารวมทั้งแนวทางการแก้ไขอย่างเป็นระบบ รวมทั้ง ติดตามปรับปรุง และคาดการความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพ (5) สรุปผลการบริหารจัดการขีดสมรรถนะของระบบ	3.ผลการตรวจสอบประเมินขีดสมรรถนะของระบบที่ผ่านมาอย่างน้อย 6 เดือน ได้แก่ ค่า CPU RAM HD Bandwidth 4.ผลการวิเคราะห์ ประมวลผลขีดสมรรถนะของระบบ โดยระบุปัญหาและสาเหตุและแนวทางการแก้ไข และการติดตามปรับปรุง รวมทั้งการวางแผนในอนาคต 5.สรุปผลการบริหารจัดการขีดสมรรถนะของระบบ -สัมภาษณ์กระบวนการตรวจประเมินขีดสมรรถนะของระบบ -สำหรับหน่วยงานที่ไม่มีเครื่องแม่ข่าย ของเรียกดูผลรายงานการเฝ้าระวังความพร้อมใช้งานของเครือข่ายในหน่วยงาน เช่น การตรวจสอบการเข้าใช้งานเครือข่าย ความเร็วในการเข้าใช้งานเครือข่าย และสมรรถนะในการใช้งานของระบบ และสุ่มตรวจคอมพิวเตอร์สมรรถนะของเครื่องในหน่วยงาน -สัมภาษณ์การดูแลเฝ้าระวังการใช้งานคอมพิวเตอร์และเครือข่ายของหน่วยงานด้านความพร้อมใช้งาน และความรวดเร็วในการใช้งาน
4.การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)		
1.การพัฒนา การทดสอบ และการให้บริการของหน่วยงาน ต้องมีการจัดทำแยกกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับการอนุญาต	4.1มีการกำหนดมาตรการ/ขั้นตอนการพัฒนา การทดสอบ และการให้บริการของหน่วยงาน โดยให้มีการปฏิบัติตามที่หน่วยงานกำหนด (1) มีการสำรองข้อมูลก่อนการปรับปรุงแก้ไข เพื่อการพัฒนาการทดสอบและการให้บริการออกจากกัน	-สำหรับหน่วยงานที่มีการพัฒนาระบบสารสนเทศหรือโปรแกรม/ซอฟแวร์ ให้ผู้ตรวจสอบภายในดำเนินการตรวจดังนี้ 1.ตรวจสอบแนวทาง/มาตรการในการพัฒนา การทดสอบและการให้บริการสารสนเทศของหน่วยงานที่เป็นลายลักษณ์อักษรโดยระบุเกี่ยวกับการสำรองข้อมูลก่อนการปรับปรุงแก้ไข เพื่อการพัฒนาการทดสอบและการให้บริการออกจากกัน

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
2.เพื่อให้หน่วยงานมีการกำหนดมาตรการ/ขั้นตอนการพัฒนา การทดสอบ และการให้บริการของหน่วยงาน โดยให้มีการปฏิบัติตามที่หน่วยงานกำหนด 3.เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับการอนุญาต	(2) ต้องจัดทำการแยกระบบในการพัฒนาและระบบการตรวจสอบและระบบการให้บริการออกจากกันเพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสำหรับการให้บริการโดยไม่ได้รับอนุญาต	2.ให้ผู้ดูและระบบ แสดงให้เห็นว่าหน่วยงานมีการแยกระบบในการพัฒนาและระบบการทดสอบ รวมทั้งระบบที่ใช้ในการตรวจสอบ และระบบการให้บริการจริงออกจากกัน
5. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)		
1.เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี 2.เพื่อให้หน่วยงานมีการกำหนดขั้นตอนการปฏิบัติในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมไม่ประสงค์ดีตามที่กรมฯกำหนด	1.มีการกำหนดขั้นตอนการปฏิบัติในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมไม่ประสงค์ดี ให้เป็นไปตามที่กรมฯกำหนดอย่างน้อย ดังนี้ (1) มีระบบการตรวจจับการป้องกันการกู้คืนข้อมูลจากผู้ที่ไม่ประสงค์ดี (2) มีการจัดอบรมเจ้าหน้าที่ให้ทราบถึงพฤติกรรมที่พึงประสงค์ต่อการใช้งานที่ถูกต้อง ปลอดภัย และไม่มีความเสี่ยง (3) มีการติดตั้งระบบป้องกันโปรแกรมที่ไม่ประสงค์ดีรวมทั้งตรวจสอบประสิทธิภาพให้สามารถป้องกันได้อย่างมีประสิทธิภาพ (4) ต้องมีการตรวจสอบประเมินผลมาตรการที่กำหนดไว้อย่างสม่ำเสมอเพื่อนำมาสู่การปรับปรุงความมั่นคงปลอดภัย 2.มีการปฏิบัติที่เป็นไปตามขั้นตอนการปฏิบัติในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมไม่ประสงค์ดีตามที่กรมฯกำหนด	-ตรวจสอบขั้นตอนการปฏิบัติในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมไม่ประสงค์ดี ต้องมีอย่างน้อยที่กรมฯกำหนด 4 ข้อ -สอบทานการปฏิบัติที่เป็นไปตามขั้นตอนการปฏิบัติในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมไม่ประสงค์ดีตามที่กรมฯกำหนด 1.ให้ผู้ดูแลระบบแสดงระบบการตรวจจับการป้องกัน การกู้คืนข้อมูลจากผู้ที่ไม่ประสงค์ดี 2.แสดงเอกสารการจัดอบรมและผลการจัดอบรมเจ้าหน้าที่ให้ทราบถึงพฤติกรรมที่พึงประสงค์ต่อการใช้งานที่ถูกต้องปลอดภัย 3.สุ่มตรวจสอบว่าการติดตั้งระบบป้องกันโปรแกรมที่ไม่ประสงค์ดีไว้ที่เครื่องของหน่วยงานหรือไม่ และมีการรายงานผลการประเมินประสิทธิภาพของโปรแกรมและสุ่มตรวจวันเวลาในการ Update ฐานข้อมูลของโปรแกรมทันสมัยหรือไม่ 4.ตรวจสอบรายงานผลการประเมินและปัญหาการป้องกันโปรแกรมที่ไม่ประสงค์ดี

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
6. การสำรองข้อมูล (Information Backup)		
1.เพื่อให้มีการกำหนดขั้นตอนการสำรองและกู้คืนระบบตามที่กรมกำหนด 2.เพื่อให้มีการปฏิบัติตามขั้นตอนที่กรมกำหนดไว้ 3.เพื่อป้องกันข้อมูลสูญหาย	(6.1) มีการสำรองข้อมูลและระบบสารสนเทศ (1) ต้องสำรองข้อมูลสำคัญของกระบวนงานหลัก หรือข้อมูลที่สำคัญต่อการดำเนินงานของหน่วยงานทุกระดับ รวมถึงโปรแกรมระบบปฏิบัติการ (operating system) โปรแกรมระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง	-สัมภาษณ์การกำหนดรายงานข้อมูลที่สำคัญและกระบวนการคัดเลือกและการกำหนดความถี่ในการสำรองข้อมูลว่าทำอย่างไร ใช้หลักเกณฑ์ในการกำหนดอย่างไร เหมาะสมกับทรัพยากรหรือไม่ -ตรวจสอบการกำหนดนโยบาย/แนวทางปฏิบัติในการสำรองข้อมูลที่สำคัญของหน่วยงาน -สัมภาษณ์วิธีการสำรองข้อมูล
1.เพื่อให้มีการกำหนดขั้นตอนการสำรองและกู้คืนระบบตามที่กรมกำหนด 2.เพื่อให้มีการปฏิบัติตามขั้นตอนที่กรมกำหนดไว้ 3.เพื่อป้องกันข้อมูลสูญหาย	(2) ต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียดดังนี้(ตามแบบฟอร์ม 1) -ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง -ประเภทสื่อบันทึก (media) -จำนวนที่ต้องสำรอง (copy) -รอบระยะเวลาการสำรอง (cycle) (3) ขั้นตอนและวิธีการสำรองโดยละเอียด รวมถึงผู้ที่มีหน้าที่และความรับผิดชอบในการสำรองข้อมูล (4) สถานที่สำรองข้อมูล ต้องมีระยะห่างในการจัดเก็บไม่น้อยกว่า 20 กม. (ศูนย์ วศ. / ศูนย์ สช.) ที่อยู่ตามเขตปริมณฑล หรือในเขตพื้นที่กำหนด (5) วิธีการเก็บรักษาสื่อบันทึก เช่น สำรอง Online /Hard copy (6) ต้องมีการบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ(ตามแบบฟอร์ม 2)	-ตรวจสอบขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลของหน่วยงานว่าอย่างน้อยต้องระบุตามที่กำหนดไว้ได้แก่ 1.ข้อมูลที่สำรอง 2.ความถี่ในการสำรอง 3.ประเภทสื่อที่บันทึก 4.จำนวนที่ต้องสำรอง 5.รอบระยะเวลาการสำรอง 6.ขั้นตอนและวิธีการสำรอง 7.ผู้รับผิดชอบในการสำรองข้อมูล 8.สถานที่สำรองข้อมูล 9.วิธีการเก็บรักษาสื่อบันทึกข้อมูลที่สำรอง 10.ผู้บันทึกกิจกรรมและผู้สุ่มตรวจสอบ -ตรวจสอบแผนการสำรองข้อมูล -ตรวจสอบรายงานผลการสำรองข้อมูลตามแผนและการสุ่มตรวจ -สัมภาษณ์กระบวนการวางแผนและปฏิบัติงานตามแผน รวมถึงการรายงานผลการสำรองข้อมูล

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	(6.2) การทดสอบข้อมูลสำรอง(กู้ระบบคืน) (1) ต้องทดสอบข้อมูลสำรองอย่างน้อยทุก 4 เดือน เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้ (2) ต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูล/กู้ระบบคืนสำรองจากสื่อบันทึกมาใช้งาน (ตามแบบฟอร์ม 3)	-ตรวจสอบการกำหนดขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูล/กู้ระบบคืนสำรองจากสื่อบันทึกมาใช้งาน -สัมภาษณ์การปฏิบัตินาการทดสอบและการนำข้อมูล/กู้ระบบคืนสำรองจากสื่อบันทึกมาใช้งาน -ตรวจสอบผลการปฏิบัติในการทดสอบ อย่างน้อยทุก 4 เดือนและการนำข้อมูล/กู้ระบบคืนสำรองจากสื่อบันทึกมาใช้งาน
	(6.3) การเก็บรักษาข้อมูลสำรองและสื่อบันทึก (1) ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่โดยมีระยะห่างในการจัดเก็บไม่น้อยกว่า 20 กม. (ศูนย์ วศ. / ศูนย์ สช.) ที่อยู่ตามเขตปริมณฑลหรือในเขตพื้นที่กำหนด เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออก และระบบควบคุมสภาพแวดล้อมอย่างเหมาะสมด้วย (2) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน (3) ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด (4) การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจ และควรจัดทำทะเบียนควบคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา(ตามแบบฟอร์ม 4)	-ตรวจสอบการสถานที่และการจัดเก็บสื่อบันทึกข้อมูลที่สำรอง โดยสถานที่ต้องมีการควบคุมการเข้าออกอย่างเหมาะสม -กรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องตรวจสอบวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ตรวจสอบการจัดเก็บสื่อบันทึกข้อมูลเป็นประเภทใดและจัดเก็บไว้อย่างไร กรณีต้องนำมาใช้ต้องทำอย่างไร -ตรวจสอบฉลาดที่ติดบนสื่อบันทึกข้อมูลที่สำรอง ว่ามีระบบการบริหารจัดการอย่างไรให้เกิดความรวดเร็วและป้องกันการใช้งานที่ผิดพลาด -ตรวจสอบข้อกำหนดในการขอใช้งานสื่อบันทึกข้อมูลที่สำรอง เพื่อตรวจดูขั้นตอนและการอำนาจในการควบคุมที่เหมาะสม และสัมภาษณ์ผู้ปฏิบัติงานให้อธิบายกรณีที่มีผู้ขอใช้งานสื่อบันทึกที่สำรองข้อมูลไว้ต้องปฏิบัติอย่างไร

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	(5) ต้องกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์(ตามแบบฟอร์ม 5)	-ตรวจสอบนโยบาย/แนวทางปฏิบัติเกี่ยวกับขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์ -สุ่มสัมภาษณ์ผู้ปฏิบัติงานเกี่ยวกับการปฏิบัติในการทำลายข้อมูลในสื่อที่ไม่ได้ใช้งาน
7. การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)		
1.เพื่อให้หน่วยงานมีการกำหนดคู่มือ/ขั้นตอนการบริหารจัดการการบันทึกข้อมูลล็อกที่ถูกต้องทั้งวิธีการและระยะเวลาในการจัดเก็บที่สอดคล้องกับ พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ปี 50 รวมทั้งการบันทึกเหตุการณ์ความมั่นคงปลอดภัย จัดเก็บและทบทวนอย่างสม่ำเสมอ 2.ไม่พบปัญหา/ความเสี่ยงจากไม่บันทึกหรือบริหารจัดการการจัดเก็บข้อมูลล็อกที่ไม่ถูกต้อง	(7.1) การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging) ข้อมูลล็อกแสดงเหตุการณ์ซึ่งบันทึกกิจกรรมผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บและทบทวนอย่างสม่ำเสมอ -มีการบันทึกการทำงานของระบบที่ไม่เป็นไปตามปกติ ความผิดพลาดในการทำงานของระบบ -เหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บและทบทวนอย่างสม่ำเสมอ -กำหนดวิธีการและระยะเวลาในการจัดเก็บให้สอดคล้องกับ พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ปี 50	-ตรวจสอบแนวทางการปฏิบัติในการบันทึกข้อมูลล็อกแสดงเหตุการณ์ -สัมภาษณ์ผู้ดูแลระบบถึงการบริหารจัดการบันทึกข้อมูลล็อกแสดงเหตุการณ์และวิธีการลบข้อมูลล็อก -ให้ผู้ดูแลระบบแสดง log ที่จัดเก็บไว้ เพื่อแสดงให้เห็นว่ามีการจัดเก็บเป็นไปตามพรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ปี 2550
	(7.2) การป้องกันข้อมูลล็อก (Protection of log information) อุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต -อุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต -ต้องมีการตรวจสอบติดตามประเมินผลระบบการป้องกันข้อมูลล็อกที่มีประสิทธิภาพ	-สัมภาษณ์ผู้ดูแลระบบถึงการป้องกันข้อมูลล็อก จากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาตและกระบวนการติดตามระบบการป้องกันข้อมูลล็อกที่มีประสิทธิภาพ -ตรวจสอบโดยให้ผู้ปฏิบัติงานแสดงให้เห็นถึงการป้องกันข้อมูล

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	(7.3) ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs) -กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อก ข้อมูลดังกล่าวต้องมีการป้องกันและทบทวนอย่างสม่ำเสมอ 1.มีการกำหนดขั้นตอนการปฏิบัติของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการในการบันทึกข้อมูลล็อกอย่างเป็นลายลักษณ์อักษรและมีการทบทวนอย่างสม่ำเสมอ	ล็อก จากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาตและกระบวนการติดตาม -ตรวจสอบการทบทวนขั้นตอนการปฏิบัติงานในการบันทึกข้อมูลล็อก
1.เพื่อการสืบค้นข้อมูลที่ถูกต้องตรงกัน 2.เพื่อให้หน่วยงานมีการบริหารจัดการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และ Note book/server/Firewall ให้ถูกต้องตรงกัน(จัดทำแผนการตั้งเวลาของนาฬิกาให้ถูกต้องตรงกัน-ดำเนินตั้งเวลา-ตรวจสอบ-สรุปผลการดำเนินการ)	(7.4) การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization) 1.มีการกำหนดขั้นตอนการปฏิบัติในการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และ Note book/server/Firewallของหน่วยงานให้ถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้ อย่างเป็นลายลักษณ์อักษร 2.มีระบบการตรวจสอบ ควบคุม-กำกับเวลานาฬิกาของเครื่องคอมพิวเตอร์และ Note book/server/Firewallของหน่วยงาน อย่างเป็นระบบและต่อเนื่อง 3.ทุกอุปกรณ์ภายในหน่วยงานมีการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และ Note book/server/Firewallของหน่วยงานให้ถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้	-สุ่มตรวจการตั้งนาฬิกาถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้ -ตรวจสอบการกำหนดขั้นตอนการปฏิบัติในการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และNote book/server/Firewallของหน่วยงานให้ถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้ อย่างเป็นลายลักษณ์อักษร

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
8. การควบคุมการติดตั้งซอร์ฟแวร์บนระบบให้บริการ (Control of operation software)		
1.มีการปฏิบัติในการติดตั้งและควบคุมการติดตั้งซอฟแวร์บนระบบการให้บริการที่ถูกต้อง 2.เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง	(8.1) การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operation systems) ให้มีการกำหนดขั้นตอนปฏิบัติสำหรับการควบคุมติดตั้งซอฟแวร์บนระบบการให้บริการต้องมีการปฏิบัติให้สอดคล้อง ดังนี้	-ตรวจสอบการกำหนดขั้นตอนปฏิบัติสำหรับการควบคุมติดตั้งซอฟแวร์บนระบบการให้บริการตามที่กรมกำหนดไว้
	-วิเคราะห์วางแผนการติดตั้งซอฟต์แวร์บนระบบการให้บริการเพื่อป้องกันความเสี่ยงต่อผลกระทบในการติดตั้งซอฟต์แวร์ระบบให้บริการที่อาจเกิดความล้มเหลว -มีขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องมีการปฏิบัติตามให้สอดคล้อง -สรุปวิเคราะห์ประเมินผล การติดตั้งซอฟต์แวร์เพื่อนำไปสู่การปรับปรุงวางแผนการติดตั้งซอฟต์แวร์	
1.เพื่อให้มีการกำหนดขั้นตอนการบริหารจัดการช่องโหว่ทางเทคนิคของระบบที่ใช้งานที่เหมาะสม 2.เพื่อให้ระบบการให้บริการไม่มีภัยคุกคามอันสาเหตุมาจากความเสี่ยงในการบริหารจัดการช่องโหว่ทางเทคนิค	(8.2.1) การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities) มีการกำหนดขั้นตอน/มาตรการบริหารจัดการช่องโหว่ทางเทคนิคของระบบที่ใช้งานที่เหมาะสม	-ตรวจสอบการกำหนดขั้นตอน/มาตรการบริหารจัดการช่องโหว่ทางเทคนิคของระบบที่ใช้งานที่เหมาะสม -สัมภาษณ์กระบวนการบริหารจัดการช่องโหว่ทางเทคนิคของระบบ
1.เพื่อให้มีการกำหนดกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์ของหน่วยงาน 2.เพื่อให้หน่วยงานไม่พบปัญหา/ความเสี่ยงจากการติดตั้งซอฟแวร์อันเป็นช่องโหวนำภัยคุกคามมาสู่ระบบ/องค์กร	(8.2.2) การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation) กฎเกณฑ์ควบคุมการติดตั้งซอฟแวร์โดยผู้ใช้งานต้องมีการกำหนดและปฏิบัติตาม -มีกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งานต้องมีการกำหนดและปฏิบัติตาม -มีการตรวจสอบช่องโหวทางเทคนิคอย่างสม่ำเสมอ รวมทั้งมีการวิเคราะห์สรุปประเมินผลเพื่อนำไปสู่การปรับปรุงอย่างเป็นระบบและต่อเนื่อง	-ตรวจสอบกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์ -ตรวจสอบรายงานผลการตรวจสอบช่องโหวทางเทคนิคว่าได้ดำเนินการอย่างสม่ำเสมอและมีการสรุปวิเคราะห์ประเมินผลอันนำไปสู่การปรับปรุง -สัมภาษณ์การตรวจสอบการควบคุมการติดตั้งซอฟต์แวร์

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
9.สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)		
เพื่อให้หน่วยงานมีการวางแผนและตกลงร่วมกันอย่างระมัดระวังในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบการให้บริการเพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ	9.1 มาตรการการตรวจประเมินระบบ (Information systems audit controls) -มีการขั้นตอนการปฏิบัติในการวางแผนและตกลงร่วมกันอย่างระมัดระวังในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบการให้บริการอย่างน้อยตามที่กรมกำหนดและตามมาตรการดังนี้ (1) มีการกำหนดผู้ดูแลระบบเครือข่าย (2) มีการกำหนดสิทธิ์และการให้สิทธิ์แก่ผู้ใช้งานในระบบเครือข่าย (3) มีการวางแผนความต้องการใช้ทรัพยากรสารสนเทศที่มีประสิทธิภาพ (4) มีหลักเกณฑ์ในการตรวจรับระบบสารสนเทศที่พัฒนาแล้ว	-ตรวจสอบมาตรการการตรวจประเมินระบบเป็นไปตามที่หน่วยงานกำหนดหรือไม่ -สัมภาษณ์การดำเนินการตามมาตรการการตรวจประเมินระบบ

เกณฑ์การประเมินความเสี่ยง

(1.) ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

ระดับ Level 1

-มีการจัดทำคู่มือ/ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร

ระดับ Level 2

-ผู้ปฏิบัติงานสามารถปฏิบัติงานตามคู่มือ/ขั้นตอนการปฏิบัติงานได้อย่างถูกต้อง จำนวน 1-2 คน

-มีระบบการควบคุมกำกับ ติดตามประเมินผลการปฏิบัติงานให้เป็นไปตามคู่มือ/ขั้นตอนการปฏิบัติงาน

ระดับ Level 3

-ผู้ปฏิบัติงานสามารถปฏิบัติงานตามคู่มือ/ขั้นตอนการปฏิบัติงานได้อย่างถูกต้อง จำนวน 3 คน

-มีการทบทวนปรับปรุงคู่มือ/ขั้นตอนการปฏิบัติงานให้ทันสมัยอยู่เสมอ

-ไม่พบปัญหา/ความเสี่ยงในการปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศ

(2.) การบริหารจัดการเปลี่ยนแปลง (Change management)

ระดับ Level 1

-การกำหนดขั้นตอนการปฏิบัติในการควบคุมการดำเนินงาน เมื่อมีการเปลี่ยนแปลงขององค์กรที่สำคัญอันส่งผลกระทบต่อความมั่นคงปลอดภัยของการดำเนินงาน อุปกรณ์ประมวลผลสารสนเทศและระบบที่เป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนการปฏิบัติในการควบคุมการดำเนินงาน เมื่อมีการเปลี่ยนแปลงขององค์กรที่สำคัญอันส่งผลกระทบต่อความมั่นคงปลอดภัยของการดำเนินงาน อุปกรณ์ประมวลผลสารสนเทศและระบบ

-มีการกำหนดระดับชั้นของผู้ให้ข่าวสาร

ระดับ Level 3

-มีปฏิบัติตามข้อกำหนดระดับชั้นของผู้ให้ข่าวสาร

-ไม่พบปัญหา/ความเสี่ยงหรือความเสียหายอันเกิดจากการเปลี่ยนแปลงขององค์กรที่ส่งผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศขององค์กร

(3.) การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติงานตามที่กรมกำหนดใน 5 ประเด็นดังระบุข้างต้น

ระดับ Level 2

-มีการจัดระบบตามขั้นตอนการปฏิบัติงานที่กรมกำหนดอย่างครบถ้วนทั้ง 5 ประเด็น

ระดับ Level 3

-ระบบเทคโนโลยีสารสนเทศมีความพร้อมใช้งาน อย่างน้อย 99%

(4.) การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

ระดับ Level 1

-มีการกำหนดมาตรการ/ขั้นตอนการพัฒนา การทดสอบ และการให้บริการของหน่วยงาน โดยให้มีการปฏิบัติตามที่หน่วยงานกำหนด

ระดับ Level 2

-มีการปฏิบัติตามมาตรการ/ขั้นตอนการพัฒนา การทดสอบ และการให้บริการของหน่วยงาน สำหรับการพัฒนา การทดสอบ และการให้บริการ

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยง ในการเข้าถึงหรือการเปลี่ยนแปลงสำหรับการให้บริการโดยไม่ได้รับอนุญาต สำหรับการพัฒนา การทดสอบ และการให้บริการ

(5.) การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

(5.1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมไม่ประสงค์ดี ให้เป็นไปตามที่กรมฯกำหนดเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติที่เป็นไปตามขั้นตอนการปฏิบัติในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมไม่ประสงค์ดีตามที่กรมฯกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมไม่ประสงค์ดี

(6.) การสำรองข้อมูล (Information Backup)

(6.1) มีการสำรองข้อมูลและระบบสารสนเทศ

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการสำรองข้อมูลตามที่กรมกำหนดเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติที่เป็นไปตามขั้นตอนการปฏิบัติในการสำรองข้อมูลตามที่กรมกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการสูญหาย/เสียหาย ของข้อมูล

(6.2) การทดสอบข้อมูลสำรอง(กู้ระบบคืน)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการทดสอบข้อมูลสำรอง/กู้คืนระบบตามที่กรมกำหนดเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติที่เป็นไปตามขั้นตอนการปฏิบัติในการทดสอบข้อมูลสำรอง/กู้คืนระบบตามที่กรมกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการสูญหาย/เสียหาย ของข้อมูล

(6.3) การเก็บรักษาข้อมูลสำรองและสื่อบันทึก

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการเก็บรักษาข้อมูลสำรองตามที่กรมกำหนด

ระดับ Level 2

-มีการปฏิบัติที่เป็นไปตามขั้นตอนการปฏิบัติในการเก็บรักษาข้อมูลสำรองและกู้คืนระบบตามที่กรมกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการสูญหาย/เสียหาย ของข้อมูล

(7.) การบันทึกข้อมูลล๊อกและการเฝ้าระวัง (Logging and Monitoring)

(7.1) การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)

ระดับ Level 1

-มีการกำหนดคู่มือ/ขั้นตอนการบริหารจัดการการบันทึกข้อมูลล็อกที่ถูกต้องทั้งวิธีการและระยะเวลาในการจัดเก็บที่สอดคล้องกับ พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ปี 50 รวมทั้งการบันทึกเหตุการณ์ความมั่นคงปลอดภัย จัดเก็บและทบทวนอย่างสม่ำเสมอ

ระดับ Level 2

-มีการปฏิบัติตามคู่มือ/ขั้นตอนการบริหารจัดการการบันทึกข้อมูลล็อกที่กำหนดไว้

-ผู้ปฏิบัติงานสามารถปฏิบัติตามคู่มือ/ขั้นตอนการบริหารจัดการการบันทึกข้อมูลล็อกที่กำหนดไว้ อย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติงานสามารถปฏิบัติตามคู่มือ/ขั้นตอนการบริหารจัดการการบันทึกข้อมูลล็อกที่กำหนดไว้ อย่างน้อย 3 คน

-ไม่พบปัญหา/ความเสี่ยงจากไม่บันทึกหรือบริหารจัดการการจัดเก็บข้อมูลล็อกที่ไม่ถูกต้อง

(7.2) การป้องกันข้อมูลล็อก (Protection of log information)

ระดับ Level 1

-มีอุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต

ระดับ Level 2

-มีการตรวจสอบติดตามประเมินผลระบบการป้องกันข้อมูลล็อกที่มีประสิทธิภาพ

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการเปลี่ยนแปลงแก้ไขและการเข้าถึงอุปกรณ์บันทึกข้อมูลล็อกโดยไม่ได้รับอนุญาต

(7.3) ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการในการบันทึกข้อมูลล็อกอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-ผู้ปฏิบัติงานสามารถปฏิบัติตามขั้นตอนที่กำหนดไว้ อย่างน้อย 1 คน

-มีการทบทวนขั้นตอนการปฏิบัติของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการในการบันทึกข้อมูลล็อกอย่างสม่ำเสมอ

ระดับ Level 3

-ผู้ปฏิบัติงานสามารถปฏิบัติตามขั้นตอนที่กำหนดไว้ อย่างน้อย 3 คน

-ไม่พบปัญหา/ความเสี่ยงในการปฏิบัติของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการในการบันทึกข้อมูลล็อก

(7.4) การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และNote book/server/Firewallของหน่วยงานให้ถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้ อย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีระบบการตรวจสอบ ควบคุม-กำกับเวลานาฬิกาของเครื่องคอมพิวเตอร์และNote book/server/Firewallของหน่วยงาน อย่างเป็นระบบและต่อเนื่อง

-มีแผนการตรวจสอบการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และNote book/server/Firewallของหน่วยงานให้ถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้ อย่างเป็นลายลักษณ์อักษร

-มีการดำเนินการตรวจสอบการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และNote book/server/Firewallของหน่วยงานให้ถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้ อย่างเป็นลายลักษณ์อักษร

-มีการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และNote book/server/Firewallของหน่วยงานให้ถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้ แต่ไม่ครบถ้วนในอุปกรณ์ทุกชิ้น

ระดับ Level 3

-ทุกอุปกรณ์ภายในหน่วยงานมีการตั้งเวลานาฬิกาของเครื่องคอมพิวเตอร์และNote book/server/Firewallของหน่วยงานให้ถูกต้องตรงกันและเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้

-ไม่พบปัญหา/ความเสี่ยงจากการสืบค้นข้อมูลที่ไม่ถูกต้องตรงกันของเวลาในการสร้างและเปลี่ยนแปลงข้อมูล

(8.) การควบคุมการติดตั้งซอร์ฟแวร์บนระบบให้บริการ (Control of operation software)

(8.1) การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operation systems)

ระดับ Level 1

-มีขั้นตอนการปฏิบัติในการติดตั้งและควบคุมการติดตั้งซอฟแวร์บนระบบการให้บริการที่ถูกต้องเป็นรูปเล่มและเป็นลายลักษณ์อักษร

ระดับ Level 2

-ผู้ปฏิบัติงานสามารถปฏิบัติตามคู่มือ/ขั้นตอนที่กำหนดไว้อย่างถูกต้อง อย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติงานสามารถปฏิบัติตามคู่มือ/ขั้นตอนที่กำหนดไว้อย่างถูกต้อง อย่างน้อย 3 คน

-ไม่พบปัญหา/ความเสี่ยงในการทำงานของระบบการให้บริการ

(8.2) การบริการจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

(8.2.1) การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

ระดับ Level 1

-มีการกำหนดขั้นตอน/มาตรการการบริหารจัดการช่องโหว่ทางเทคนิคของระบบที่ใช้งานที่เหมาะสม และมีการทบทวนอย่างสม่ำเสมอ

ระดับ Level 2

-ผู้ปฏิบัติสามารถปฏิบัติตามขั้นตอน/มาตรการการบริหารจัดการช่องโหว่ทางเทคนิคของระบบที่ใช้งาน อย่างน้อย 1 คน

-มีการปฏิบัติตามขั้นตอน/มาตรการการบริหารจัดการช่องโหว่ทางเทคนิคของระบบที่ใช้งานที่หน่วยงานกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงของระบบการให้บริการไม่มีภัยคุกคามอันสาเหตุมาจากความเสี่ยงในการบริหารจัดการช่องโหว่ทางเทคนิค

(8.2.2) การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)

ระดับ Level 1

-มีการกำหนดกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์ของหน่วยงาน

-มีการปฏิบัติตามกฎเกณฑ์/มาตรการในการควบคุมการติดตั้งซอฟต์แวร์ของหน่วยงาน

ระดับ Level 2

-มีการตรวจสอบช่องโหวทางเทคนิคอย่างสม่ำเสมอ รวมทั้งมีการวิเคราะห์สรุปประเมินผลเพื่อนำไปสู่การปรับปรุงอย่างเป็นระบบและต่อเนื่อง

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงจากการติดตั้งซอฟแวร์อันเป็นช่องโหวนำภัยคุกคามมาสู่ระบบ/องค์กร

(9.) สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

(9.1) มาตรการการตรวจประเมินระบบ (Information systems audit controls)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติการตรวจประเมินระบบการให้บริการ โดยเน้นการวางแผนและตกลงร่วมกันระหว่างผู้ตรวจประเมินและผู้รับการตรวจประเมิน

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนการปฏิบัติการตรวจประเมินระบบการให้บริการที่กำหนดไว้

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการหยุดชะงักของระบบอันเนื่องมาจากการตรวจประเมินระบบการให้บริการ

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
หมายเลขเอกสาร WI0901

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security) ในการดำเนินการตรวจสอบการการโอนถ่ายข้อมูลและการสื่อสารรับ-ส่งข้อมูลผ่านระบบเครือข่าย เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหรือรั่วไหลของข้อมูลองค์กร

2.0 ขอบข่าย

วิธีการปฏิบัติงานฉบับนี้ ครอบคลุมการสอบทานกระบวนความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)สู่การปฏิบัติ ดังนี้

1.การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

1.1 มาตรการเครือข่าย (Network controls)

1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

1.3 การแบ่งแยกเครือข่าย (Segregation in networks)

2. การถ่ายโอนสารสนเทศ (Information transfer)

2.1 นโยบายและขั้นตอนปฏิบัติสำหกรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic massaging)

2.4 ข้อตกลงการรักษาความลับหรือไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)		
เพื่อป้องกันสารสนเทศในระบบต่างๆ	1.1มาตรการเครือข่าย (Network controls) หน่วยงานต้องมีการบริหารจัดการและควบคุม โดยมีการกำหนดขั้นตอน/มาตรการในการบริหารจัดการและควบคุมระบบเครือข่าย อย่างน้อยตามที่กรมกำหนดดังนี้ (1) ออกมาตรการการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส (2) สร้างระบบจัดเก็บ LOG ไฟล์ในการเข้าถึงเครือข่ายของกรม (3) พิจารณาการเปิดเข้าใช้งาน port ของผู้ร้องขอใช้งาน โดยกำหนดระยะเวลาในการเข้าใช้งานตามที่ผู้ดูแลระบบจะอนุญาต (4) มีการกำหนด Vlan ในการเข้าใช้งานระบบเครือข่ายของกรมนั้นๆ (5) ถ้าไม่มีการใช้งานในระยะเวลาหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเตอร์เน็ต(Session timeout) เพื่อนำสัญญาณไปให้ผู้ร้องขอคนอื่นต่อไป	-ตรวจสอบมาตรการเครือข่ายของหน่วยงานที่กำหนดเป็นลายลักษณ์อักษรว่าครอบคลุมทั้ง 5 ข้อตามที่นโยบายกำหนดหรือไม่ ยกเว้นหน่วยงานที่ไม่มีเครื่องแม่ข่ายไม่ต้องตรวจสอบข้อ 2 และข้อ 3 และ 4 เนื่องจากการจัดเก็บ Log ไฟล์และ Port รวมทั้ง VLAN จะดำเนินการโดย IT กรมฯ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services) 1.ต้องมีการกำหนดขั้นตอนการให้บริการเครือข่าย โดยอย่างน้อยตามที่กรมกำหนดดังนี้ (1) กำหนดขั้นตอนการใช้บริการข้อมูลของหน่วยงาน (2) การตรวจสอบการให้บริการ เพื่อวัดความพึงพอใจของผู้รับบริการ (3) มีการพัฒนาและปรับปรุงระบบสารสนเทศให้มีความทันสมัยและเป็นปัจจุบัน (4) มีการยืนยันตัวบุคคลที่แท้จริง (5) มีระบบตรวจสอบการเป็นบุคคลที่แท้จริง 2.มีข้อตกลงการให้บริการเครือข่ายที่ชัดเจนเป็นลายลักษณ์อักษร 3.มีการบริหารจัดการข้อตกลงการให้บริการเครือข่ายที่ชัดเจนและมีผลการดำเนินงานที่สอดคล้องข้อตกลงการให้บริการเครือข่าย	-ตรวจสอบการกำหนดความมั่นคงปลอดภัยสำหรับบริการเครือข่ายของหน่วยงานและข้อตกลงการให้บริการเครือข่ายที่เป็นลายลักษณ์อักษรและการบริหารจัดการข้อตกลง -ตรวจสอบผลการดำเนินงานที่สอดคล้องกับข้อตกลงการให้บริการเครือข่าย -สัมภาษณ์กระบวนการให้บริการหรือใช้บริการข้อมูลระบบเครือข่าย รวมถึงการวัดความพึงพอใจผู้ใช้บริการ และการพัฒนาปรับปรุงระบบสารสนเทศและการยืนยันตัวตน รวมถึงการบริหารจัดการเครือข่ายและข้อตกลงในการให้บริการเครือข่าย -สุ่มตรวจสอบระบบการยืนยันตัวตนในระบบเครือข่าย
เพื่อป้องกันข้อมูลสารสนเทศและระบบการให้บริการเครือข่ายจากภัยคุกคาม	**1.3 การแบ่งแยกเครือข่าย (Segregation in networks)** ต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด (1) กำหนดผู้ดูแลระบบเครือข่าย (2) กำหนดสิทธิและการให้สิทธิแก่ผู้ใช้งานในระบบเครือข่าย (3) มีการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่างๆ เช่น ผู้บริหาร, ผู้ปฏิบัติงานตามตำแหน่งแผนกหรือหน้าที่การงาน ฯลฯ	-ตรวจสอบ 1.ความเหมาะสมในแผนผังการแบ่งเครือข่ายกับการรักษาความมั่นคงปลอดภัยหรือไม่ 2.การกำหนดผู้ดูและระบบเครือข่าย 3.การกำหนดสิทธิและการให้สิทธิแก่ผู้ใช้งานระบบเครือข่ายเหมาะสมหรือไม่ 4.ความเหมาะสมในการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่างๆ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
2.การถ่ายโอนสารสนเทศ (Information transfer)		
เพื่อให้ข้อมูลสารสนเทศที่มีการถ่ายโอนได้รับการป้องกัน	2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures) 1.มีการกำหนดนโยบาย ขั้นตอนการปฏิบัติงาน และมาตรการสำหรับการถ่ายโอนอย่างเป็นทางการต้องมีการปฏิบัติเพื่อป้องกันสารสนเทศที่มีการถ่ายโอน โดยผ่านการใช้งานอุปกรณ์การสื่อสารทุกประเภทอย่างเป็นลายลักษณ์อักษร 2.มีการปฏิบัติตามขั้นตอน/มาตรการมาตรการสำหรับการถ่ายโอน	-ตรวจสอบนโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ -สัมภาษณ์กระบวนการกำหนดนโยบายและขั้นตอนปฏิบัติ รวมทั้งกระบวนการปฏิบัติงานจริงทำอย่างไร มีปัญหาอย่างไร -ตรวจสอบผลการดำเนินงานในการถ่ายโอนข้อมูลหรือการรายงานผลการถ่ายโอนข้อมูล
1.เพื่อให้หน่วยงานมีการกำหนดข้อตกลงสำหรับการถ่ายโอนสารสนเทศให้มีความมั่นคงปลอดภัยอย่างน้อยตามที่กรมกำหนด 2.เพื่อให้มีความเข้าใจตกลงในการสร้างความมั่นคงปลอดภัยของข้อมูลที่ถ่ายโอน 3.ไม่เกิดความเสี่ยงของข้อมูลที่ถ่ายโอน	2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer) โดยต้องมีข้อตกลงสำหรับการถ่ายโอนสารสนเทศให้มีความมั่นคงปลอดภัยต้องมีการระบุระหว่างองค์กรกับหน่วยงานภายนอก (1) กำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น (2) กำหนดข้อตกลง แนวทาง วิธีปฏิบัติ ระยะเวลา ของการถ่ายโอนสารสนเทศ (3) มีการบันทึก วันเวลาที่มีการถ่ายโอนสารสนเทศในระหว่างกรม (4) จำกัดการเข้าถึงสารสนเทศเมื่อมีการโอนย้ายเสร็จสิ้นแล้ว	-ตรวจสอบข้อตกลงสำหรับการถ่ายโอนสารสนเทศให้มีความมั่นคงปลอดภัย -สัมภาษณ์การจัดทำข้อตกลงสำหรับการถ่ายโอนสารสนเทศให้มีความมั่นคงปลอดภัยทำอย่างไร
1.เพื่อให้หน่วยงานกำหนดให้บุคลากรใช้เมล์อิเล็กทรอนิกส์ของกระทรวงไอซีที (mail.go.th) เฉพาะงานที่เกี่ยวข้องกับงานราชการ เพื่อป้องกันสารสนเทศ	2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic massaging) 1.มีการกำหนดให้บุคลากรใช้เมล์อิเล็กทรอนิกส์ของกระทรวงไอซีที (mail.go.th) เฉพาะงานที่เกี่ยวข้องกับงานราชการ เพื่อป้องกันสารสนเทศ	-สัมภาษณ์การใช้อีเมล์ของบุคลากรในหน่วยงานว่ามีการกำหนดนโยบายอย่างไร และขั้นตอนการใช้งานอีเมล์ -สุ่มสัมภาษณ์ผู้ปฏิบัติงานทั่วไปถึงอีเมล์ที่ใช้และให้เปิดอีเมล์ให้ผู้ตรวจสอบภายในดูว่าทำอย่างไร

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
2.เพื่อให้หน่วยงานมีการกำหนดขั้นตอนการใช้งานเมล์อิเล็กทรอนิกส์ของกระทรวงไอซีที(mail.go.th) เฉพาะงานที่เกี่ยวข้องกับงานราชการ เพื่อให้บุคลากรปฏิบัติตามได้อย่างถูกต้อง 3.ไม่พบความเสี่ยงจากสารสนเทศที่เกี่ยวกับการส่งข้อความทางอิเล็กทรอนิกส์รั่วไหล/สูญหาย/เสียหาย	2.มีการกำหนดขั้นตอนการใช้งานเมล์อิเล็กทรอนิกส์ของกระทรวงไอซีที (mail.go.th) เฉพาะงานที่เกี่ยวข้องกับงานราชการ เพื่อให้บุคลากรปฏิบัติตามได้อย่างถูกต้อง	
1.เพื่อให้หน่วยงานกำหนดขั้นตอนการปฏิบัติในการรักษาความลับหรือการไม่เปิดเผยความลับของหน่วยงานและมีการทบทวนแนวทางปฏิบัติอย่างสม่ำเสมอและอย่างน้อยครอบคลุมตามนโยบายกรม เป็นลายลักษณ์อักษร 2.ข้อมูลที่ถูกกำหนดว่าเป็นความลับได้รับการป้องกันและไม่มีการรั่วไหล/สูญหาย/เสียหาย	2.4 ข้อตกลงการรักษาความลับหรือไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements) มีการกำหนดขั้นตอนการปฏิบัติในการรักษาความลับหรือการไม่เปิดเผยความลับของหน่วยงานและมีการทบทวนแนวทางปฏิบัติอย่างสม่ำเสมอและอย่างน้อยครอบคลุมตามนโยบายกรม เป็นลายลักษณ์อักษร ดังนี้ (1) กำหนดผู้ดูแลหลักที่รับผิดชอบในข้อมูลที่สำคัญ (2) มีการกำหนดโทษในการรักษาความลับลากรไม่เปิดเผยความลับ	-ตรวจสอบข้อตกลงการรักษาความลับหรือไม่เปิดเผยความลับที่เป็นลายลักษณ์อักษร และการกำหนดผู้รับผิดชอบหลักในข้อมูลที่สำคัญ รวมถึงบทลงโทษที่หน่วยงานกำหนด -สัมภาษณ์ผู้ปฏิบัติงาน IT ถึงวัตถุประสงค์การจัดทำข้อตกลงการรักษาความลับหรือไม่เปิดเผยความลับและการกำหนดผู้รับผิดชอบหลักในข้อมูลที่สำคัญ รวมถึงบทลงโทษที่หน่วยงานกำหนด

เกณฑ์การประเมินความเสี่ยง

(1.) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

1.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

1.1.1 มาตรการเครือข่าย (Network controls)

ระดับ Level 1

-มีการกำหนดขั้นตอน/มาตรการในการบริหารจัดการและควบคุมระบบเครือข่าย อย่างน้อยตามที่กรมกำหนด

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอน/มาตรการในการบริหารจัดการและควบคุมระบบเครือข่ายอย่างน้อยตามที่กรมกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงจากภัยคุกคามในระบบเครือข่าย

1.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

ระดับ Level 1

-มีการกำหนดขั้นตอนการให้บริการเครือข่าย โดยอย่างน้อยตามที่กรมกำหนด

-มีข้อตกลงการให้บริการเครือข่ายที่ชัดเจนเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการบริหารจัดการข้อตกลงการให้บริการเครือข่ายที่ชัดเจนและมีผลการดำเนินงานที่สอดคล้องข้อตกลงการให้บริการเครือข่าย

ระดับ Level 3

-ข้อตกลงการให้บริการเครือข่ายด้านความมั่นคงปลอดภัยได้รับการตอบสนอง

1.1.3 การแบ่งแยกเครือข่าย (Segregation in networks)

ระดับ Level 1

-มีการจัดแบ่งเครือข่ายตามกลุ่มการใช้งานที่กำหนด แสดง Network Diagram ที่แสดงถึงการแบ่งเครือข่ายตามกลุ่มผู้ใช้งานที่เหมาะสม

ระดับ Level 2

-ผู้ปฏิบัติงานมีความเข้าใจถึงจุดประสงค์และการปฏิบัติในการจัดแบ่งเครือข่ายที่ถูกต้องอย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติงานมีความเข้าใจถึงจุดประสงค์และการปฏิบัติในการจัดแบ่งเครือข่ายที่ถูกต้องอย่างน้อย 3 คน

-ไม่พบปัญหา/ความเสี่ยงจากการใช้งานตามกลุ่มผู้ใช้งานที่ไม่มีความจำเป็นในการเข้าถึงระบบเครือข่ายที่ต้องรักษาความปลอดภัย

1.2 การถ่ายโอนสารสนเทศ (Information transfer)

1.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

ระดับ Level 1

-มีการกำหนดนโยบาย ขั้นตอนการปฏิบัติงาน และมาตรการสำหรับการถ่ายโอนอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-ผู้ปฏิบัติสามารถอธิบายปฏิบัติตามขั้นตอน/มาตรการมาตรการสำหรับการถ่ายโอนได้อย่างน้อย 1 คน

-มีการปฏิบัติตามขั้นตอน/มาตรการมาตรการสำหรับการถ่ายโอน

ระดับ Level 3

-ผู้ปฏิบัติสามารถอธิบายปฏิบัติตามขั้นตอน/มาตรการมาตรการสำหรับการถ่ายโอนได้อย่างน้อย 3 คน

-ไม่พบปัญหา/ความเสี่ยงของข้อมูลสารสนเทศที่มีการถ่ายโอน

1.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

ระดับ Level 1

-มีการกำหนดข้อตกลงสำหรับการถ่ายโอนสารสนเทศให้มีความมั่นคงปลอดภัย อย่างน้อยตามที่กรมกำหนด

ระดับ Level 2

-ผู้ปฏิบัติงานสามารถอธิบายวิธีการสร้างความมั่นคงปลอดภัยสำหรับข้อมูลที่ถ่ายโอนระหว่างหน่วยงานได้อย่างชัดเจน อย่างน้อย 1 คน

-มีการปฏิบัติตามข้อตกลงสำหรับการถ่ายโอนสารสนเทศให้มีความมั่นคงปลอดภัยอย่างน้อยตามที่กรมกำหนด

ระดับ Level 3

-ผู้ปฏิบัติงานสามารถอธิบายวิธีการสร้างความมั่นคงปลอดภัยสำหรับข้อมูลที่ถ่ายโอนระหว่างหน่วยงานได้อย่างชัดเจน อย่างน้อย 3 คน

-ไม่เกิดความเสี่ยงของข้อมูลที่ถ่ายโอน

1.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic massaging)

ระดับ Level 1

-มีการกำหนดให้บุคลากรใช้เมล์อิเล็กทรอนิกส์ของกระทรวงไอซีที(mail.go.th) เฉพาะงานที่เกี่ยวข้องกับงานราชการ เพื่อป้องกันสารสนเทศ

ระดับ Level 2

-มีการกำหนดขั้นตอนการใช้งานเมล์อิเล็กทรอนิกส์ของกระทรวงไอซีที(mail.go.th) เฉพาะงานที่เกี่ยวข้องกับงานราชการ เพื่อให้บุคลากรปฏิบัติตามได้อย่างถูกต้อง

ระดับ Level 3

-ไม่พบความเสี่ยงจากสารสนเทศที่เกี่ยวกับการส่งข้อความทางอิเล็กทรอนิกส์ของหน่วยงานเกิดการรั่วไหล/สูญหาย/เสียหาย

1.2.4 ข้อตกลงการรักษาความลับหรือไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการรักษาความลับหรือการไม่เปิดเผยความลับของหน่วยงานและมีการทบทวนแนวทางปฏิบัติอย่างสม่ำเสมอและอย่างน้อยครอบคลุมตามนโยบายกรม เป็นลายลักษณ์อักษร

ระดับ Level 2

-ผู้ปฏิบัติงานสามารถอธิบายวัตถุประสงค์และขั้นตอนการปฏิบัติในการรักษาความลับหรือการไม่เปิดเผยความลับของหน่วยงานอย่างถูกต้องและครอบคลุม อย่างน้อย 1 คน

-มีการปฏิบัติเพื่อแสดงให้เห็นว่าได้ปฏิบัติตามขั้นตอนการปฏิบัติในการรักษาความลับหรือการไม่เปิดเผยความลับของหน่วยงานอย่างถูกต้องและครอบคลุม

ระดับ Level 3

-ผู้ปฏิบัติงานสามารถอธิบายวัตถุประสงค์และขั้นตอนการปฏิบัติในการรักษาความลับหรือการไม่เปิดเผยความลับของหน่วยงานอย่างถูกต้องและครอบคลุม อย่างน้อย 3 คน

-ไม่พบข้อมูลที่ถูกกำหนดว่าเป็นความลับมีการรั่วไหล/สูญหาย/เสียหาย

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบ
(System acquisition, development and maintenance)
หมายเลขเอกสาร WI1001

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance) ซึ่งดำเนินการตรวจสอบ เพื่อควบคุม กำกับ ดูแลการพัฒนาระบบสารสนเทศให้เป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัย

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance) ดังนี้

1. ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)
    1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification)
    1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)
    1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)
2. ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)
    2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)
    2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)
    2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

2.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

3. ข้อมูลสำหรับการทดสอบ (Test data)

3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)		
1.เพื่อให้การพัฒนาระบบของหน่วยงาน ต้องสำรวจความต้องการ/คำนึงถึงความมั่นคงปลอดภัยในกระบวนการพัฒนา/ออกแบบระบบ 2.เพื่อให้ระบบสารสนเทศที่หน่วยงานพัฒนาไม่มีช่องโหว่ด้านความมั่นคงปลอดภัย	1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ 1.1.1การพัฒนาระบบต้องมีการสำรวจความต้องการหรือคำนึงถึงด้านความมั่นคงปลอดภัยของระบบด้วย และมีการดำเนินงานอย่างน้อยตามที่กรมกำหนด -ระบบสารสนเทศใหม่ ต้องมีการรักษาความปลอดภัย ที่สอดคล้องและสามารถเชื่อมโยงกับระบบเดิมได้ -ระบบสารสนเทศเก่า จะต้องมีการป้องกันการเข้าใช้ server โดยอนุญาตให้เฉพาะบุคคลที่มีหน้าที่การทำงานโดยใช้การ login ด้วย user name และ password ของบุคคลนั้น -การยืนยันการเข้าใช้ว่าเป็นบุคคลไม่ใช่ program การ update ต่างๆต้องเป็นแบบ manual เท่านั้น 2.การพัฒนาระบบต้องมีการออกแบบที่คำนึงถึงความมั่นคงปลอดภัยของระบบด้วย	-สัมภาษณ์กระบวนการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ -ตรวจสอบเอกสารประกอบการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศในการพัฒนาและออกแบบระบบสารสนเทศ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
เพื่อให้สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศของหน่วยงาน ซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกัน	1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะระบบที่พัฒนาหรือกำลังพัฒนาหรือจะพัฒนา โดยหน่วยงานต้องปฏิบัติตามขั้นตอนการปฏิบัติในการควบคุมสารสนเทศของหน่วยงานอย่างน้อยตามที่กรมกำหนด -จากการเปลี่ยนแปลงข้อมูลบนเครือข่ายสาธารณะโดยการกำหนด user name และ password ของผู้เข้าถึงข้อมูล -ข้อมูลต้องระบุได้ว่าบุคคลใดเป็นผู้สร้างข้อมูลและมีการสำเนา/สำรองข้อมูลทุกครั้งเพื่อสามารถย้อนดูข้อมูลเก่า ณ เวลานั้นได้ -การเปิดเผยข้อมูลบนเครือข่ายสาธารณะ ต้องได้รับการอนุญาตของผู้ดูแลระบบเท่านั้น -ไม่อนุญาตให้แก้ไขข้อมูลใดๆ ที่ถูกสร้างขึ้น	-สัมภาษณ์การปฏิบัติในการควบคุมสารสนเทศของหน่วยงาน -สุ่มตรวจสอบฐานข้อมูลว่ามีการจัดเก็บชื่อผู้สร้างข้อมูลและการสำรองข้อมูลเพื่อย่อยดูข้อมูลเก่าได้ -ตรวจสอบเอกสารพจนานุกรมฐานข้อมูลว่ามีการกำหนดโครงสร้างฐานข้อมูลในการจัดเก็บชื่อผู้สร้างข้อมูลหรือไม่
เพื่อให้สารสนเทศของบริการสารสนเทศ ได้รับการป้องกันจากการรับ-ส่งข้อมูลที่ไม่สมบูรณ์/การส่งข้อมูลผิดเส้นทาง/การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต/การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต/การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต	1.3 การป้องกันธุรกรรมของบริการสารสนเทศ 1.3.1 มีการกำหนดขั้นตอนปฏิบัติ/เงื่อนไขในการพัฒนาระบบสารสนเทศ ให้มีการป้องกันจากการรับ-ส่งข้อมูลที่ไม่สมบูรณ์/การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต/การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต/การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต	-สุ่มตรวจสอบการให้บริการสารสนเทศของหน่วยงาน ว่ามีการป้องกันจากการรับ-ส่งข้อมูลที่ไม่สมบูรณ์/การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต/การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต/การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต
2.ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)		
เพื่อให้การพัฒนาระบบสารสนเทศหรือซอฟแวร์ของหน่วยงานมีแนวทางปฏิบัติที่เกิดความมั่นคงปลอดภัย	2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย โดยหน่วยงานต้องกำหนดเกณฑ์สำหรับการพัฒนาซอฟแวร์และระบบต้องมีการกำหนดและปฏิบัติตามสำหรับการพัฒนาระบบขององค์กร โดยมีการแต่งตั้งผู้ดูแลควบคุมระบบซอฟต์แวร์ โดยให้กำหนดระยะเวลาอัพเดตซอฟต์แวร์ทุกๆ 6 เดือน	-ตรวจสอบนโยบายและแนวทางปฏิบัติในการพัฒนาระบบสารสนเทศหรือซอฟแวร์ของหน่วยงานให้มีความมั่นคงปลอดภัย -สัมภาษณ์เกี่ยวกับกระบวนการในการกำหนดนโยบายและแนวทางปฏิบัติในการพัฒนาระบบสารสนเทศหรือซอฟแวร์ของหน่วยงาน

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.เมื่อมีการเปลี่ยนแปลงระบบในช่วงวงจรการพัฒนาระบบ ต้องมีการควบคุมโดยปฏิบัติตามขั้นตอนปฏิบัติการเปลี่ยนแปลงระบบที่กำหนดไว้อย่างเป็นทางการ 2.ไม่พบปัญหา/ความเสี่ยง จากการเปลี่ยนแปลงระบบในช่วงวงจรการพัฒนาระบบ	2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ -มีการกำหนดขั้นตอนการปฏิบัติในการควบคุมการเปลี่ยนแปลงระบบอย่างเป็นลายลักษณ์อักษร -มีการแต่งตั้งคณะทำงานดูแลการเข้าใช้งานระบบและตั้งข้อปฏิบัติในการเข้าใช้งาน -มีการปฏิบัติตามขั้นตอนการปฏิบัติในการควบคุมการเปลี่ยนแปลงระบบ	-ตรวจสอบขั้นตอนการปฏิบัติในการควบคุมการเปลี่ยนแปลงระบบ -สัมภาษณ์การปฏิบัติตามขั้นตอนในการควบคุมการเปลี่ยนแปลงที่กำหนด
เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐาน ระบบสำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยขององค์กร	2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ -มีการกำหนดขั้นตอนการปฏิบัติให้ต้องมีการทบทวนและทดสอบระบบเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานระบบที่สำคัญ -มีการทบทวนและทดสอบระบบที่พัฒนาเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐาน เพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยขององค์กร	
1.เพื่อควบคุมการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูป 2.เพื่อให้มีการกำหนดขั้นตอนปฏิบัติในการควบคุมการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูป ตามที่กรมกำหนด 3.ไม่พบปัญหา/ความเสี่ยงในการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูป	2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป -มีการกำหนดขั้นตอนปฏิบัติในการควบคุมการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูป ตามที่กรมกำหนด -มีการปฏิบัติในการควบคุมการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูป	
เพื่อให้หน่วยงานมีการกำหนดขั้นตอนการวางแผนวิเคราะห์ออกแบบระบบตามหลักวิศวกรรมระบบที่คำนึงถึงด้านความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและมีการทบทวนปรับปรุงอย่างต่อเนื่อง อย่างน้อยตามที่กรมกำหนด	2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย โดยมีการกำหนดขั้นตอนการวางแผนวิเคราะห์ออกแบบระบบตามหลักวิศวกรรมระบบที่คำนึงถึงด้านความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและมีการทบทวนปรับปรุงอย่างต่อเนื่อง อย่างน้อยตามที่กรมกำหนดดังนี้ -มีคำสั่งจัดตั้งคณะกรรมการระบบด้านความมั่นคงปลอดภัย -จัดทำแบบแปลนโครงสร้างทางวิศวกรรมและสามารถรองรับการแก้ไขเพิ่มเติมในอนาคตได้ -ตรวจทาน ปรับปรุง แก้ไขและทดสอบระบบทุก ๆ จุดและกระจายการออกแบบไปยังส่วนกลาง	

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย -มีการกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย -มีการปฏิบัติตามขั้นตอนที่กำหนดไว้ อย่างน้อยที่กรมกำหนด	
เพื่อให้หน่วยงานมีการกำกับ ดูแล เฝ้าระวังและติดตามการพัฒนาระบบที่จ้างหน่วยงานภายนอกมาดำเนินการ	2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ -มีการกำหนดขั้นตอนปฏิบัติในการควบคุม-กำกับดูแล เฝ้าระวังและติดตามการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ -มีผลการปฏิบัติตามขั้นตอนปฏิบัติในการควบคุม-กำกับดูแล เฝ้าระวังและติดตามการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ	
เพื่อให้หน่วยงานมีการกำหนดขั้นตอนในการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่อยู่ในช่วงพัฒนาระบบ และต้องมีการกำหนดผลลัพธ์ที่ต้องการในการทดสอบด้านความมั่นคงปลอดภัย	2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ -มีการกำหนดขั้นตอนในการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่อยู่ในช่วงพัฒนาระบบ และต้องมีการกำหนดผลลัพธ์ที่ต้องการในการทดสอบด้านความมั่นคงปลอดภัย เป็นลายลักษณ์อักษร -มีการปฏิบัติตามขั้นตอนการปฏิบัติในการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบที่กำหนด	
เพื่อให้หน่วยงานมีการกำหนดแผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ สำหรับระบบใหม่ ระบบที่ปรับปรุงและระบบเวอร์ชั่นใหม่	2.9 การทดสอบเพื่อรับรองระบบ -มีการกำหนดแผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ สำหรับระบบใหม่ ระบบที่ปรับปรุงและระบบเวอร์ชั่นใหม่ -มีการปฏิบัติตามแผนการทดสอบระบบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ -จัดบุคลากรในการทดลองและประเมินผลการใช้งานของระบบ	
3.ข้อมูลสำหรับการทดสอบ (Test data)		
เพื่อให้มีการป้องกันข้อมูลที่นำไปใช้ในการทดสอบ	3.1การป้องกันข้อมูลสำหรับการทดสอบ -มีการกำหนดขั้นตอน/แนวทางปฏิบัติในการป้องกันข้อมูลที่นำไปใช้ในการทดสอบ โดยแยกระบบที่ทดสอบจากระบบที่ใช้งาน -มีการปฏิบัติตามขั้นตอน/แนวทางปฏิบัติในการป้องกันข้อมูลที่นำไปใช้ในการทดสอบที่กำหนดอย่างน้อยที่กรมกำหนด คือ แยกระบบที่ทดสอบจากระบบที่ใช้งาน	-สัมภาษณ์กระบวนการป้องกันข้อมูลสำหรับการทดสอบ -สุ่มตรวจสอบฐานข้อมูลของระบบทดสอบและระบบที่ใช้งานจริง โดยให้ผู้ดูแลระบบแสดงฐานข้อมูลของระบบทดสอบกับฐานข้อมูลระบบจริง เพื่อแสดงให้เห็นว่ามีการแยกสองระบบนี้ออกจากกัน

เกณฑ์การประเมินความเสี่ยง

1. ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification)

ระดับ Level 1

-มีการสำรวจความต้องการ/หรือคำนึงถึงด้านความมั่นคงปลอดภัยของระบบที่พัฒนา

ระดับ Level 2

-การวิเคราะห์/ออกแบบระบบที่จะพัฒนา ได้แสดงให้เห็นถึงด้านความมั่นคงปลอดภัย

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยง ต่อภัยคุกคามในช่องโหว่ของระบบสารสนเทศที่หน่วยงานพัฒนา

1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการควบคุมสารสนเทศของหน่วยงาน อย่างน้อยตามที่กรมกำหนด

ระดับ Level 2

-เอกสารการวิเคราะห์ออกแบบระบบ แสดงให้เห็นว่าได้ปฏิบัติตามขั้นตอนในการควบคุมสารสนเทศของหน่วยงาน อย่างน้อยตามที่กรมกำหนด

-การพัฒนาระบบ ได้แสดงให้เห็นว่าได้ปฏิบัติตามขั้นตอนในการควบคุมสารสนเทศของหน่วยงาน อย่างน้อยตามที่กรมกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยง ของสารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศของหน่วยงานซึ่งมีการส่งผ่านเครือข่ายสาธารณะ

1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

ระดับ Level 1

-มีการกำหนดขั้นตอนปฏิบัติ/เงื่อนไขในการพัฒนาระบบสารสนเทศ ให้มีการป้องกันจากการรับ-ส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

ระดับ Level 2

-แสดงให้เห็นว่าสารสนเทศของบริการสารสนเทศ มีการป้องกันจากการรับ-ส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงต่อสารสนเทศของบริการสารสนเทศ

2. ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

ระดับ Level 1

-มีการกำหนดเกณฑ์สำหรับการพัฒนาซอฟแวร์และระบบต้องมีการกำหนดและปฏิบัติตามสำหรับการพัฒนาระบบขององค์กร อย่างน้อยเป็นไปตามที่กรมกำหนด เป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามเกณฑ์สำหรับการพัฒนาซอฟแวร์และระบบที่กำหนดไว้

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการพัฒนาซอฟแวร์

2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติในการควบคุมการเปลี่ยนแปลงระบบอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนการปฏิบัติในการควบคุมการเปลี่ยนแปลงระบบ
-มีการแต่งตั้งคณะทำงานดูแลการเข้าใช้งานระบบ และตั้งข้อปฏิบัติในการเข้าใช้งาน

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยง จากการเปลี่ยนแปลงระบบในช่วงวงจรการพัฒนาระบบ

2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติให้ต้องมีการทบทวนและทดสอบระบบเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานระบบที่สำคัญ

ระดับ Level 2

-มีการทบทวนและทดสอบระบบที่พัฒนาเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐาน เพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยขององค์กร

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐาน ระบบสำคัญ

2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

ระดับ Level 1

-มีการกำหนดขั้นตอนปฏิบัติในการควบคุมการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูป ตามที่กรมกำหนด

ระดับ Level 2

-มีการปฏิบัติในการควบคุมการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูป

-ผู้ปฏิบัติงานสามารถอธิบายวัตถุประสงค์และแนวทางปฏิบัติในการควบคุมการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูปได้อย่างถูกต้อง อย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติงานสามารถอธิบายวัตถุประสงค์และแนวทางปฏิบัติในการควบคุมการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูปได้อย่างถูกต้อง อย่างน้อย 3 คน

-ไม่พบปัญหา/ความเสี่ยงในการเปลี่ยนแปลงต่อซอฟแวร์สำเร็จรูป

2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

ระดับ Level 1

-มีการกำหนดขั้นตอนการวางแผนวิเคราะห์ออกแบบระบบตามหลักวิศวกรรมระบบที่คำนึงถึงด้านความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและมีการทบทวนปรับปรุงอย่างต่อเนื่อง อย่างน้อยตามที่กรมกำหนด

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนที่กำหนดไว้

-ผู้ปฏิบัติงานสามารถอธิบายถึงวิเคราะห์ออกแบบระบบตามหลักวิศวกรรมระบบที่คำนึงถึงด้านความมั่นคงปลอดภัยได้อย่างชัดเจน อย่างน้อย 1 คน

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงอันมาจากการจัดทำแบบแปลนโครงสร้างทางวิศวกรรมทั้งในปัจจุบันและอนาคต

2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

ระดับ Level 1

-มีการกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนที่กำหนดไว้ อย่างน้อยที่กรมกำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงของสภาพแวดล้อมของการพัฒนาระบบ

2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

ระดับ Level 1

-มีการกำหนดขั้นตอนปฏิบัติในการควบคุม-กำกับดูแล เฝ้าระวังและติดตามการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ

-เงื่อนไข(TOR)ในสัญญาจ้างมีกระบวนการในการควบคุม-กำกับดูแล เฝ้าระวังและติดตามการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการที่มีประสิทธิภาพ

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนปฏิบัติในการควบคุม-กำกับดูแล เฝ้าระวังและติดตามการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการและในเงื่อนไข(TOR)ในสัญญาจ้างมีกระบวนการในการควบคุม-กำกับดูแล เฝ้าระวังและติดตามการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ ที่มีประสิทธิภาพ

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการจ้างหน่วยงานภายนอกมาพัฒนาระบบ

2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

ระดับ Level 1

-มีการกำหนดขั้นตอนในการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่อยู่ในช่วงพัฒนาระบบ และต้องมีการกำหนดผลลัพธ์ที่ต้องการในการทดสอบด้านความมั่นคงปลอดภัย เป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนการปฏิบัติในการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบที่กำหนด

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยง ในการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบที่กำหนด

2.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

ระดับ Level 1

-มีการกำหนดแผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ สำหรับระบบใหม่ ระบบที่ปรับปรุงและระบบเวอร์ชั่นใหม่

ระดับ Level 2

-มีการปฏิบัติตามแผนการทดสอบระบบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยง ในการทดสอบระบบ

3. ข้อมูลสำหรับการทดสอบ (Test data)

3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)

ระดับ Level 1

-มีการกำหนดขั้นตอน/แนวทางปฏิบัติในการป้องกันข้อมูลที่นำไปใช้ในการทดสอบ

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอน/แนวทางปฏิบัติในการป้องกันข้อมูลที่นำไปใช้ในการทดสอบที่กำหนด อย่างน้อยที่กรมกำหนด คือ แยกระบบที่ทดสอบจากระบบที่ใช้งาน

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยง กับข้อมูลที่ใช้ในการทดสอบ

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
หมายเลขเอกสาร WI1101

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) ซึ่งได้ดำเนินการตรวจสอบการตกลงในการดำเนินการจ้างผู้รับจ้างภายนอกหน่วยงานมาดำเนินการให้เป็นไปอย่างถูกต้อง สามารถควบคุมกำกับ ตรวจสอบและประเมินผลการจ้างได้อย่างมีประสิทธิภาพ ประสิทธิผล

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการตกลงการจ้างผู้รับจ้างภายนอกมาดำเนินการ ดังนี้

(1) นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการ
(2) การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก
(3) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการ		
เพื่อให้มีการควบคุมความเสี่ยงในการจ้างงานผู้รับจ้างจากภายนอก	1.1 มีการกำหนดนโยบายเพื่อความปลอดภัยในการจ้างผู้รับจ้างจากภายนอก	-ตรวจสอบนโยบายว่าระบุเพื่อความปลอดภัยในการจ้างผู้รับจ้างจากภายนอกหรือไม่
	1.2 มีการแต่งตั้งคณะกรรมการที่ถูกต้องตามระเบียบพัสดุหรือไม่	-ตรวจสอบคำสั่งแต่งตั้งคณะกรรมการ -สัมภาษณ์กระบวนการในการกำหนดเงื่อนไขการจ้าง
	1.3 มีเอกสารประกอบการจัดจ้างถูกต้องตามระเบียบพัสดุ	-ตรวจสอบเอกสารประกอบการจัดจ้าง
2.การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก		
เพื่อไม่มีความเสี่ยงที่เกิดจากการกำหนดข้อตกลงการให้บริการของผู้รับจ้างภายนอก	2.1 มีการกำหนดเงื่อนไข/ข้อตกลงการให้บริการในการจ้างงานที่ครอบคลุมดังนี้ -การระบุสิทธิ-หน้าที่ของคู่สัญญา -การแบ่งชำระงวดเงิน หรือการชำระเงินที่เป็นการขจัดความเสี่ยงของผู้ว่าจ้าง -คุณลักษณะที่ต้องการของการจ้างงานหรือคุณลักษณะของที่ส่งมอบ -การควบคุม-กำกับ ติดตามและประเมินผลการปฏิบัติงานของผู้รับจ้างจากภายนอก -ความเป็นเจ้าของลิขสิทธิ์ในการจ้าง -การเยียวยาความเสียหายกันเมื่อมีการผิดสัญญา	-ตรวจสอบเอกสารเงื่อนไขในการจ้างว่ามีการระบุต้องครอบคลุมดังนี้ 1.การระบุสิทธิ-หน้าที่ของคู่สัญญา 2.การแบ่งชำระงวดเงิน หรือการชำระเงินที่เป็นการขจัดความเสี่ยงของผู้ว่าจ้าง 3.คุณลักษณะที่ต้องการของการจ้างงานหรือคุณลักษณะของที่ส่งมอบ 4.การควบคุม-กำกับ ติดตามและประเมินผลการปฏิบัติงานของผู้รับจ้างจากภายนอก 5.ความเป็นเจ้าของลิขสิทธิ์ในการจ้าง 6.การเยียวยาความเสียหายกันเมื่อมีการผิดสัญญา
3.ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก		
เพื่อให้มีกระบวนการควบคุม-กำกับติดตามและประเมินผลการให้บริการของผู้รับจ้างภายนอก	3.1 มีการกำหนดกระบวนการในการควบคุม-กำกับ ติดตามและประเมินผลการให้บริการของผู้รับจ้างภายนอก	-สัมภาษณ์กระบวนการในการควบคุม-กำกับ ติดตามและประเมินผลการให้บริการของผู้รับจ้างภายนอก -ตรวจสอบเอกสารประกอบการควบคุม-กำกับ ติดตามและประเมินผลการให้บริการของผู้รับจ้างภายนอก

เกณฑ์การประเมินความเสี่ยง

(1) นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการ

ระดับ Level 1

-มีการแต่งตั้งคณะกรรมการในการจัดจ้างถูกต้องตามระเบียบพัสดุ

-มีการจัดทำเอกสารประกอบและปฏิบัติตามกระบวนการจัดจ้างถูกต้องตามระเบียบพัสดุ

ระดับ Level 2

-มีการกำหนดนโยบายการจัดจ้างผู้รับจ้างจากภายนอก

ระดับ Level 3

-นโยบายมีความครอบคลุมและชัดเจนในการควบคุมความเสี่ยงจากการจ้างผู้รับจ้างมาดำเนินการ

(2) การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

ระดับ Level 1

-มีการกำหนดเงื่อนไข/ข้อตกลงการให้บริการในการจ้างงาน

ระดับ Level 2

-มีการกำหนดเงื่อนไข/ข้อตกลงการให้บริการในการจ้างงานที่ครอบคลุมดังนี้

1.การระบุสิทธิ-หน้าที่ของคู่สัญญา

2.การแบ่งชำระงวดเงิน หรือการชำระเงินที่เป็นการขจัดความเสี่ยงของผู้ว่าจ้าง

3.คุณลักษณะที่ต้องการของการจ้างงานหรือคุณลักษณะของที่ส่งมอบ

4.การควบคุม-กำกับ ติดตามและประเมินผลการปฏิบัติงานของผู้รับจ้างจากภายนอก

5.ความเป็นเจ้าของลิขสิทธิ์ในการจ้าง

6.การเยียวยาความเสียหายกันเมื่อมีการผิดสัญญา

ระดับ Level 3

-มีการกำหนดขอบเขต/บทบาทหน้าที่ในการเข้าถึงทรัพย์สินหน่วยงานมีมาตรการที่รัดกุมในการใช้ทรัพย์สินและข้อมูล

(3) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

ระดับ Level 1

-มีการกำหนดขั้นตอน/แนวทางปฏิบัติในการควบคุม-กำกับ ติดตามและประเมินผลการปฏิบัติงานของผู้รับจ้างภายนอก

-มีการจัดทำแผนงานการควบคุม-กำกับ ติดตามและประเมินผลการปฏิบัติงานของผู้รับจ้างภายนอก

ระดับ Level 2

-ปฏิบัติตามขั้นตอน/แนวทางปฏิบัติและแผนงานในการควบคุม-กำกับ ติดตามและประเมินผลการปฏิบัติงานของผู้รับจ้างภายนอกอย่างครบถ้วน

ระดับ Level 3

-มีการรายงานผลการปฏิบัติงานของผู้รับจ้างภายนอกเป็นระยะแก่ผู้บังคับบัญชา หรือตามที่ระเบียบพัสดุกำหนดไว้

-ไม่พบความเสี่ยงในการควบคุม-กำกับ ติดตามและประเมินผลการปฏิบัติงานของผู้รับจ้างภายนอก

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 12 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
(Information Security incident Management)
หมายเลขเอกสาร WI1201

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 12 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะดำเนินการตรวจสอบกระบวนการแก้ไขปัญหาหรือเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศ เพื่อให้การปฏิบัติงานกระบวนการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ ประสิทธิผล

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

1. มีการกำหนดผู้รับผิดชอบและขั้นตอนการปฏิบัติงานในการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงาน เพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผลและตามลำดับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
2. การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ
    1.1. มีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้
    1.2. การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses)
    1.3. การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)
3. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)
4. การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)
5. การเก็บรวบรวมหลักฐาน (Collection of evidence)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ		
เพื่อให้มีผู้รับผิดชอบและมีการกำหนดขั้นตอนการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย	1.1 หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติ -มีการกำหนดผู้รับผิดชอบในการแก้ไขปัญหา/แก้ไขเหตุการณ์ที่ไม่มั่นคงปลอดภัย -มีการกำหนดขั้นตอนการปฏิบัติในการแก้ไขปัญหา/แก้ไขเหตุการณ์ที่ไม่มั่นคงปลอดภัย -มีการสื่อสารประชาสัมพันธ์กระบวนการให้บริการ	-สัมภาษณ์กระบวนการบริหารจัดการแก้ไขปัญหา/แก้ไขเหตุการณ์ที่ไม่มั่นคงปลอดภัย -ตรวจสอบเอกสารประกอบการดำเนินการแก้ไขปัญหา/แก้ไขเหตุการณ์ที่ไม่มั่นคงปลอดภัย -สุ่มสอบถามผู้ใช้บริการเกี่ยวกับประสบการณ์ในการได้รับบริการแก้ไขปัญหา/แก้ไขเหตุการณ์ที่ไม่มั่นคงปลอดภัย
2.การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ		
เพื่อให้หน่วยงานมีการกำหนดช่องทางการรับการแจ้งเตือนจากปัญหาที่เกิดขึ้นและมีการรายงานเสนอผู้บังคับบัญชาอย่างเป็นระบบต่อเนื่อง	2.1มีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้ -มีการพัฒนาช่องทางการบริหารจัดการที่เหมาะสมรวดเร็ว -มีการรายงานต่อผู้บังคับบัญชาอย่างเป็นระบบและมีประสิทธิภาพ	-สุ่มตรวจสอบช่องทางการแจ้งเตือนปัญหาที่เกิดขึ้นและจับระยะเวลาในการรายงานว่ามีความรวดเร็วเหมาะสมอย่างไร -ตรวจสอบรายงานที่ผ่านมาเกี่ยวกับปัญหาหรือเหตุการณ์ความมั่นคงปลอดภัยที่เสนอต่อผู้บังคับบัญชา -สัมภาษณ์กระบวนการรายงานผ่านช่องทางต่างๆที่หน่วยงานกำหนด

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
เพื่อให้หน่วยงานมีการกำหนดหลักเกณฑ์ที่เหมาะสมในการปฏิบัติ	2.2การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ -มีการกำหนดหลักเกณฑ์ในการรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ ได้แก่ เกณฑ์ปัญหา/จุดอ่อนในระดับสูง ระดับปานกลาง ระดับต่ำ	-สัมภาษณ์และตรวจสอบการกำหนดหลักเกณฑ์ในการรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ ได้แก่ เกณฑ์ปัญหา/จุดอ่อนในระดับสูง ระดับปานกลาง ระดับต่ำ -สุ่มตรวจเอกสารการรายงานที่ผ่านมาว่าใช้หลักเกณฑ์ตามที่กำหนดหรือไม่
เพื่อให้หน่วยงานมีการกำหนดแนวทางปฏิบัติและ Work Flow ที่พิจารณาจากหลักเกณฑ์ในการรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานกำหนด	2.3การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ -แนวทางการปฏิบัติในการเฝ้าระวังระบบสารสนเทศและอุปกรณ์ เพื่อป้องกันการบุกรุก -มีการเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุกหรือโจมตีกรม เพื่อเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟวอลล์เป็นต้น -มีการบริหารจัดการ การบุกรุกระบบโดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับกรม และจัดทำวิธีปฏิบัติที่ถูกต้อง ให้กับกรมเพื่อป้องกันเหตุการณ์ที่เกิดขึ้นซ้ำ	-ตรวจสอบเอกสารแนวทางการปฏิบัติ 1.ในการเฝ้าระวังระบบสารสนเทศและอุปกรณ์ เพื่อป้องกันการบุกรุก 2.มีการเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุกหรือโจมตี 3.มีการบริหารจัดการ การบุกรุกระบบโดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้น 4.มีการจัดทำวิธีปฏิบัติที่ถูกต้อง เพื่อป้องกันเหตุการณ์ที่เกิดขึ้นซ้ำ -สัมภาษณ์แนวทางการปฏิบัติในการเฝ้าระวังระบบสารสนเทศและอุปกรณ์ เพื่อป้องกันการบุกรุก
3.การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ		
เพื่อให้หน่วยงานมีการปฏิบัติในการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบและชัดเจน	-มีการจัดทำขั้นตอนการปฏิบัติในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษร	-ตรวจสอบขั้นตอนการปฏิบัติในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานกำหนด -สัมภาษณ์การปฏิบัติในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศ
	-กรณีเกิดปัญหาให้รายงานเหตุการณ์ต่อผู้บังคับบัญชาทุกครั้ง	-สุ่มตรวจรายงานในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
4.การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ		
เพื่อให้หน่วยงานมีการวิเคราะห์ปัญหาและค้นหาสาเหตุ รวมทั้งแลกเปลี่ยนเรียนรู้ให้เกิดการต่อยอดความรู้เพื่อมิให้เกิดปัญหาซ้ำอีก	4.1มีการแจ้งเวียนเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นให้เจ้าหน้าที่ภายในหน่วยงานทราบ	-ตรวจสอบกระบวนการการวิเคราะห์ปัญหาและค้นหาสาเหตุ รวมทั้งแลกเปลี่ยนเรียนรู้ที่เกิดขึ้นในหน่วยงาน -สัมภาษณ์การวิเคราะห์ปัญหาและค้นหาสาเหตุ รวมทั้งแลกเปลี่ยนเรียนรู้
5.การเก็บรวบรวมหลักฐาน		
เพื่อให้หน่วยงานมีแนวทางขั้นตอนการเก็บหลักฐานสารสนเทศในสถานที่ปลอดภัย ข้อกำหนดการควบคุมนำมาใช้เพื่อไม่ให้เกิดการสูญหาย	มีแนวทางขั้นตอนการเก็บหลักฐานสารสนเทศในสถานที่ปลอดภัย ข้อกำหนดการควบคุมนำมาใช้เพื่อไม่ให้เกิดการสูญหาย	-ตรวจสอบแนวทางขั้นตอนการเก็บหลักฐานสารสนเทศในสถานที่ปลอดภัย ข้อกำหนดการควบคุมนำมาใช้เพื่อไม่ให้เกิดการสูญหาย -สัมภาษณ์กระบวนการเก็บหลักฐานสารสนเทศในสถานที่ปลอดภัย ข้อกำหนดการควบคุมนำมาใช้ ว่าได้ปฏิบัติตามแนวทาง/ขั้นตอนการเก็บหลักฐานสารสนเทศที่กำหนดไว้

<u>เกณฑ์การประเมินความเสี่ยง</u>

(1) มีการกำหนดผู้รับผิดชอบและขั้นตอนการปฏิบัติงานในการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงาน เพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผลและตามลำดับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

<u>ระดับ Level 1</u>

-มีการกำหนดผู้รับผิดชอบในการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงาน

-มีขั้นตอนการปฏิบัติงานในการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงาน

<u>ระดับ Level 2</u>

-มีขั้นตอนการปฏิบัติงานในการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงานมีความเหมาะสมในการแก้ไขปัญหาที่รวดเร็วมีประสิทธิภาพ

-มีการกำหนดผู้รับผิดชอบสำรองในกรณีฉุกเฉินที่ผู้รับผิดชอบหลักไม่สามารถปฏิบัติงานได้

<u>ระดับ Level 3</u>

-มีการปฏิบัติตามขั้นตอนการปฏิบัติงานในการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงานอย่างครบถ้วน

(2) การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ

2.1. มีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

ระดับ Level 1

-ไม่มีการกำหนดช่องทางการรายงานหรือแจ้งเตือนของระบบสารสนเทศที่ชัดเจน

-มีการรายงานต่อผู้บริหารเป็นครั้งคราว

ระดับ Level 2

-มีการกำหนดช่องทางการรายงานหรือแจ้งเตือนของระบบสารสนเทศที่ชัดเจน จำนวน 1 ช่องทาง

-มีการรายงานต่อผู้บริหารเป็นครั้งคราว

ระดับ Level 3

-มีการกำหนดช่องทางการรายงานหรือแจ้งเตือนของระบบสารสนเทศที่ชัดเจน มากกว่า 1 ช่องทาง

-มีการรายงานต่อผู้บริหารทุกครั้ง

2.2 การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses)

ระดับ Level 1

-มีการกำหนดเกณฑ์ในการประเมินจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ

ระดับ Level 2

-การกำหนดเกณฑ์ในการประเมินจุดอ่อนความมั่นคงปลอดภัยสารสนเทศถูกต้องและเหมาะสมกับการแก้ไขปัญหาที่เกิดขึ้นในองค์กร

ระดับ Level 3

-มีการปฏิบัติตามเกณฑ์ในการประเมินจุดอ่อนความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานกำหนดทุกครั้ง

2.3. การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

ระดับ Level 1

-มีการกำหนดขั้นตอนการประเมินและ Work Flow การตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ

ระดับ Level 2

-ขั้นตอนการประเมินและ Work Flow การตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศเหมาะสม

-มีการปฏิบัติในการประเมินและตัดสินใจเป็นไปตามที่หน่วยงานกำหนดแต่ไม่ทุกครั้ง

-มีระบบการเฝ้าระวังระบบสารสนเทศและอุปกรณ์ และจัดเก็บสถิติการบุกรุก

ระดับ Level 3

-มีการปฏิบัติในการประเมินและตัดสินใจเป็นไปตามที่หน่วยงานกำหนดทุกครั้ง

(3) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

ระดับ Level 1

-มีการจัดทำขั้นตอนการปฏิบัติในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

ระดับ Level 3

-มีการรายงานต่อผู้บังคับบัญชาทุกครั้ง

(4) การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

ระดับ Level 1

-มีการวิเคราะห์ปัญหาและค้นหาสาเหตุที่เกิดขึ้นในหน่วยงาน

ระดับ Level 2

-มีการแลกเปลี่ยนเรียนรู้หรือแจ้งเวียนปัญหาที่ได้รับจากการวิเคราะห์และค้นหาสาเหตุ/แนวทางการแก้ไขเรียบร้อยแล้ว เพื่อไม่ให้เกิดซ้ำอีก

ระดับ Level 3

-มีระบบแลกเปลี่ยนเรียนรู้ผ่านออนไลน์ที่รวดเร็วและมีประสิทธิภาพในการป้องกันการเกิดปัญหาซ้ำอีก

(5) การเก็บรวบรวมหลักฐาน (Collection of evidence)

ระดับ Level 1

-มีการกำหนดขั้นตอนการเก็บรวมรวมหลักฐานในเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนการเก็บรวมรวมหลักฐานในเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

ระดับ Level 3

-มีระบบสำรองและตรวจสอบการเก็บรวมรวมหลักฐานในเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 13 การบริหารความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ
(information security continuity)
หมายเลขเอกสาร WI1301

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 13 การบริหารความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

1. การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (planning information security continuity)
   - 1.1 การกำหนดรายการข้อมูลที่สำคัญที่ต้องสำรองข้อมูล
   - 1.2 การกำหนดขั้นตอนการสำรองข้อมูล
   - 1.3 การกำหนดผู้รับผิดชอบในการสำรองข้อมูล
   - 1.4 การกำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง
   - 1.5 การกำหนดแผนการบันทึกข้อมูลที่สำรอง
2. การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ
   - 2.1 การทดสอบข้อมูลที่สำรองไว้
   - 2.2 การกำหนดขั้นตอนวิธีการปฏิบัติในการทดสอบหรือการกู้คืนระบบมาใช้งาน
3. การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

   3.1 ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่

   3.2 กรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย

   3.3 การติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรองเพื่อให้สามารถค้นหาได้โดยเร็ว,เพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

   3.4 การอนุมัติเพื่อขอใช้งานสื่อบันทึกข้อมูลสำรอง

3.5 การกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว

4. การเตรียมการอุปกรณ์ประมวลผลสำรอง

4.1 มีการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือการประเมินผลกระทบของกระบวนงานหลัก

4.2 มีการกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

4.3 มีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

4.4 มีการกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

4.5 มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน

4.6 หน่วยงานที่เป็นหน่วยสำรองข้อมูลหรือจัดเก็บข้อมูลก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน

4.7 มีการทบทวนหรือปรับปรุงแผนฉุกเฉินและเก็บแผนฉุกเฉินไว้ในสถานที่มั่นคงปลอดภัย

4.8 ทดสอบการปฏิบัติตามแผนฉุกเฉิน

4.9 การสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับ

4.10 กรณีที่เกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ		
เพื่อให้หน่วยงานมีการสำรองข้อมูลที่สำคัญอย่างถูกต้อง	1.1 การกำหนดรายการข้อมูลที่สำคัญที่ต้องสำรองข้อมูล	-สัมภาษณ์กระบวนการกำหนดรายงานข้อมูลที่สำคัญที่ต้องสำรองข้อมูล
	1.2 การกำหนดขั้นตอนการสำรองข้อมูล -มีแนวทางขั้นตอนในการสำรองข้อมูลโดยมีรายละเอียดอย่างน้อยดังนี้ 1.ความถี่ในการสำรองข้อมูล 2.ประเภทสื่อที่ใช้ในการบันทึก 3.จำนวนที่สำรอง 4.รอบระยะเวลาในการสำรอง -มีการจดบันทึกการสำรองข้อมูลทุกครั้ง -มีการตรวจเช็คข้อมูลที่สำรองทุกครั้ง	-สัมภาษณ์ผู้ปฏิบัติเกี่ยวกับขั้นตอนการสำรองข้อมูล -ตรวจสอบแนวทาง/ขั้นตอนในการสำรองข้อมูล
	1.3 การกำหนดผู้รับผิดชอบในการสำรองข้อมูล	-ตรวจสอบการมอบหมาย/แต่งตั้งผู้รับผิดชอบในการสำรองข้อมูล
	1.4 การกำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง	-ตรวจสอบพื้นที่/สถานที่ที่เก็บรักษาข้อมูล -สัมภาษณ์การกำหนดพื้นที่/สถานที่ที่เก็บรักษาข้อมูล
	1.5 การกำหนดแผนการบันทึกข้อมูลที่สำรอง	-ตรวจสอบแผนการบันทึกข้อมูลที่สำรอง

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
2.การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ		
เพื่อให้หน่วยงานมีการปฏิบัติเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ	2.1 การทดสอบข้อมูลที่สำรองไว้ -มีการกำหนดแผนในการทดสอบข้อมูลที่สำรองไว้ตามระยะเวลาที่เหมาะสม ทุก 4 เดือน	-ตรวจสอบแผนการทดสอบข้อมูลที่สำรอง -สัมภาษณ์กระบวนการจัดทำแผนการทดสอบข้อมูลที่สำรอง
	2.2 การกำหนดขั้นตอนวิธีการปฏิบัติในการทดสอบหรือการกู้คืนระบบมาใช้งาน -มีการกำหนดขั้นตอนการปฏิบัติในการทดสอบกู้คืนระบบ	-ตรวจสอบขั้นตอนวิธีการปฏิบัติในการทดสอบหรือกู้คืนระบบ -สัมภาษณ์เกี่ยวกับขั้นตอนวิธีการปฏิบัติในการทดสอบหรือกู้คืนระบบ
3.การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ		
เพื่อให้หน่วยงานมีการบริหารจัดการสื่อที่ใช้บันทึกข้อมูลที่สำรองไว้ได้อย่างมีประสิทธิภาพและมีประสิทธิผล ไม่เกิดความเสี่ยงต่อการเสียหาย สูญหายหรือการนำข้อมูลกลับมาใช้ไม่ได้ในอนาคต รวมทั้งเข้าถึงข้อมูลที่สำรองโดยผู้ได้รับอนุญาต	3.1 การจัดเก็บสื่อบันทึกข้อมูลสำรองพร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่	-สัมภาษณ์เกี่ยวกับสถานที่และการจัดเก็บสื่อบันทึกข้อมูลที่สำรองและสำเนาขั้นตอนหรือวิธีการปฏิบัติต่างๆ -ตรวจสอบสถานที่จัดเก็บสื่อบันทึกข้อมูลที่สำรองและสำเนาขั้นตอนหรือวิธีการปฏิบัติต่างๆ
	3.2 การนำข้อมูลกลับมาใช้งานในอนาคต	-สัมภาษณ์เกี่ยวกับการจัดเก็บเพื่อการนำข้อมูลกลับมาใช้งานในอนาคต
	3.3 การติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรองเพื่อให้สามารถค้นหาได้โดยเร็ว,เพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด	-สัมภาษณ์ถึงวิธีการจัดการและจัดเก็บสื่อที่ใช้ในการสำรองข้อมูล เพื่อการค้นหาที่รวดเร็วและป้องกันการใช้งานสื่อบันทึกผิดพลาด -สอบทานวิธีการจัดการและจัดเก็บสื่อที่ใช้ในการสำรองข้อมูล
	3.4 การอนุมัติเพื่อขอใช้งานสื่อบันทึกข้อมูลสำรอง	-สัมภาษณ์เกี่ยวกับขั้นตอนหรือวิธีปฏิบัติในกรณีมีผู้ขอใช้งานสื่อบันทึกข้อมูลที่สำรอง -สอบทานขั้นตอนหรือวิธีปฏิบัติในกรณีมีผู้ขอใช้งานสื่อบันทึกข้อมูลที่สำรอง
	3.5การกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว	-สัมภาษณ์เกี่ยวกับการกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว -สอบทานการปฏิบัติตามขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
4.การเตรียมการอุปกรณ์ประมวลผลสำรอง		
เพื่อให้มีการเตรียมอุปกรณ์ในการประมวลผลสำรองข้อมูล	4.1มีการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือการประเมินผลกระทบของกระบวนงานหลัก	-ตรวจสอบการประเมินความเสี่ยงและการประเมินผลกระทบของกระบวนงานหลักโดยการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน -สัมภาษณ์การประเมินความเสี่ยงของระบบงาน/กระบวนงาน
	4.2 การกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา	-สัมภาษณ์การกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
	4.3 ขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์	-สัมภาษณ์การกำหนดขั้นตอนการแก้ไขปัญหาในแต่ละสถานการณ์ -สอบทานขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์
	4.4 การกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ	-ตรวจสอบการมอบหมาย/แต่งตั้งเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจและขอบเขตอำนาจหน้าที่ที่กำหนดไว้
	4.5รายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน	-สัมภาษณ์การกำหนดรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน -สอบทานว่ามีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงานตามที่กำหนดไว้หรือมไม่ และมีสภาพความพร้อมใช้ในระดับใด
	4.6 หน่วยงานที่เป็นหน่วยสำรองข้อมูลหรือจัดเก็บข้อมูลก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน	-สอบทานการปฏิบัติและผลการปฏิบัติในการสำรองข้อมูลหรือจัดเก็บข้อมูล
	4.7 การทบทวนหรือปรับปรุงแผนฉุกเฉินและเก็บแผนฉุกเฉินไว้ในสถานที่มั่นคงปลอดภัย	-ตรวจสอบแผนฉุกเฉินและการทบทวนหรือปรับปรุงแผนฉุกเฉินและการเก็บแผนฉุกเฉินไว้ในสถานที่มั่นคงปลอดภัย -สัมภาษณ์กระบวนการจัดทำและทบทวน/ปรับปรุงแผนฉุกเฉินและการจัดเก็บแผนฉุกเฉิน

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	4.8 การทดสอบการปฏิบัติตามแผนฉุกเฉิน	-สัมภาษณ์วิธีการ/ขั้นตอนการทดสอบการปฏิบัติตามแผนฉุกเฉิน -สอบทานการปฏิบัติการทดสอบการปฏิบัติตามแผนฉุกเฉินที่ได้ปฏิบัติจริง
	4.9 การสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับ	-สัมภาษณ์กระบวนการการสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับ -สอบทานการการสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับ
	4.10 การบันทึกกรณีที่เกิดเหตุการณ์ฉุกเฉิน	-สัมภาษณ์การบันทึกกรณีที่เกิดเหตุการณ์ฉุกเฉิน -ตรวจสอบรายงานผลการปฏิบัติตามแผนฉุกเฉิน

เกณฑ์การประเมินความเสี่ยง

(1) การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (planning information security continuity)

1.1 การกำหนดรายการข้อมูลที่สำคัญที่ต้องสำรองข้อมูล

ระดับ Level 1

-มีการกำหนดรายการข้อมูลที่สำคัญที่ต้องสำรองข้อมูล

ระดับ Level 2

-มีการประเมินความเสี่ยงรายการข้อมูลที่สำคัญที่กำหนดไว้

ระดับ Level 3

-มีการจัดลำดับความสำคัญรายการข้อมูล ตามผลการประเมินความเสี่ยง

1.2 การกำหนดขั้นตอนการสำรองข้อมูล

ระดับ Level 1

-มีการกำหนดขั้นตอนการสำรองข้อมูล

ระดับ Level 2

-ขั้นตอนการสำรองข้อมูล ต้องมีรายละเอียดอย่างน้อยดังนี้

1.ความถี่ในการสำรองข้อมูล

2.ประเภทสื่อที่ใช้ในการบันทึก

3.จำนวนที่สำรอง

4.รอบระยะเวลาในการสำรอง

ระดับ Level 3

-มีการสำรองข้อมูลตามรายละเอียดที่กำหนดอย่างครบถ้วน

1.3 การกำหนดผู้รับผิดชอบในการสำรองข้อมูล

ระดับ Level 1

-การกำหนดผู้รับผิดชอบในการสำรองข้อมูล

ระดับ Level 2

-มีการกำหนดบทบาทหน้าที่ในการสำรองข้อมูลที่ชัดเจนเป็นลายลักษณ์อักษร

ระดับ Level 3

-มีการแต่งตั้ง/มอบหมายผู้รับผิดชอบสำรองไว้ กรณีที่ผู้รับผิดชอบหลักไม่สามารถปฏิบัติงานได้

1.4 การกำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง

ระดับ Level 1

-การกำหนดพื้นที่เก็บรักษาข้อมูลที่สำรอง

ระดับ Level 2

-การกำหนดพื้นที่เก็บรักษาข้อมูลที่สำรองที่ห่างไกลจากแหล่งข้อมูล

ระดับ Level 3

-การกำหนดพื้นที่เก็บรักษาข้อมูลที่สำรองที่ห่างไกลจากแหล่งข้อมูลมากกว่า 20 กม.ตามที่นโยบายกำหนดไว้

1.5 การกำหนดแผนการบันทึกข้อมูลที่สำรอง

ระดับ Level 1

-การกำหนดขั้นตอนให้มีการจัดทำแผนการบันทึกข้อมูลที่สำรอง และมีการบันทึกผลการปฏิบัติงานในการสำรองข้อมูลอย่างเป็นลายลักษณ์อักษร

ระดับ Level 2

-แผนการบันทึกข้อมูลที่สำรอง ต้องระบุเกี่ยวกับความถี่ในการสำรอง ประเภทของสื่อบันทึกในการสำรอง จำนวนที่สำรอง และระยะเวลาที่สำรอง รวมทั้งผู้รับผิดชอบในการสุ่มตรวจความถูกต้องในการสำรองข้อมูล

-มีการบันทึกผลการปฏิบัติงานในการสำรองข้อมูลอย่างเป็นลายลักษณ์อักษร แต่ไม่ตรงตามแผนงานที่กำหนด

-มีการสุ่มตรวจการปฏิบัติงานในการสำรองข้อมูลอย่างเป็นลายลักษณ์อักษร

ระดับ Level 3

-แผนการบันทึกข้อมูลที่สำรองได้รับการอนุมัติอย่างถูกต้องจากผู้บังคับบัญชาและสื่อสารให้ทีมงานทราบถือปฏิบัติ

-มีการบันทึกผลการปฏิบัติงานในการสำรองข้อมูลอย่างเป็นลายลักษณ์อักษรตรงตามแผนงานที่กำหนด

-มีการสุ่มตรวจการปฏิบัติงานในการสำรองข้อมูลอย่างเป็นลายลักษณ์อักษรและทุกครั้งที่มีการปฏิบัติงานตามแผนงานที่กำหนด

(2) การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

2.1 การทดสอบข้อมูลที่สำรองไว้

ระดับ Level 1

-มีการทดสอบข้อมูลที่สำรองไม่ตรงตามแผนการสำรองข้อมูล

ระดับ Level 2

-มีการทดสอบข้อมูลที่สำรองตรงตามแผนการสำรองข้อมูลและเป็นไปตามนโยบายกำหนดไว้

ระดับ Level 3

-มีการบันทึกผลการสำรองข้อมูลและรายงานผลการสำรองข้อมูลให้ผู้บังคับบัญชาทราบ

2.2 การกำหนดขั้นตอนวิธีการปฏิบัติในการทดสอบหรือการกู้คืนระบบมาใช้งาน

ระดับ Level 1

-มีการกำหนดขั้นตอนวิธีการทดสอบหรือการกู้คืนระบบ

ระดับ Level 2

-ผู้ปฏิบัติสามารถปฏิบัติตามขั้นตอนวิธีการทดสอบหรือกู้คืนระบบได้ตามระยะเวลาที่กำหนด อย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติสามารถปฏิบัติตามขั้นตอนวิธีการทดสอบหรือกู้คืนระบบได้ตามระยะเวลาที่กำหนด อย่างน้อย 3 คน

(3) การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

3.1 ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่

ระดับ Level 1

-มีการกำหนดแนวทางปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูลที่สำรองไว้นอกสถานที่

ระดับ Level 2

-ผู้ปฏิบัติสามารถบอกเกี่ยวกับแนวทางปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูลที่สำรองไว้นอกสถานที่ได้อย่างถูกต้อง อย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติสามารถบอกเกี่ยวกับแนวทางปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูลที่สำรองไว้นอกสถานที่ได้อย่างถูกต้อง อย่างน้อย 3 คน

-มีการปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูลที่สำรองไว้นอกสถานที่ตามที่กำหนดไว้

3.2 กรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย

ระดับ Level 1

-มีการกำหนดวิธีปฏิบัติ/แนวทางการนำข้อมูลที่เก็บในระยะเวลานาน เพื่อนำกลับมาใช้งานในอนาคต

ระดับ Level 2

-การกำหนดวิธีปฏิบัติ/แนวทางการนำข้อมูลที่เก็บในระยะเวลานาน เพื่อนำกลับมาใช้งานในอนาคตได้อย่างเหมาะสมและเป็นไปได้จริงในการปฏิบัติ

ระดับ Level 3

-มีการปฏิบัติตามวิธีปฏิบัติ/แนวทางการนำข้อมูลที่เก็บในระยะเวลานาน เพื่อนำกลับมาใช้งานในอนาคต

3.3 การติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรองเพื่อให้สามารถค้นหาได้โดยเร็ว,เพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

ระดับ Level 1

-มีการกำหนดวิธีปฏิบัติ/แนวการติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรองเพื่อให้สามารถค้นหาได้โดยเร็ว เพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

ระดับ Level 2

-การติดฉลากสื่อบันทึกข้อมูลสำรอง มีรายละเอียดชัดเจน

ระดับ Level 3

-การสืบค้นสื่อบันทึกข้อมูลที่สำรอง ตามวิธีการหรือแนวทางที่กำหนดได้อย่างรวดเร็วและมีประสิทธิภาพ

3.4 การอนุมัติเพื่อขอใช้งานสื่อบันทึกข้อมูลสำรอง

ระดับ Level 1

-มีการกำหนดกฎ ระเบียบในการขออนุมัติใช้งานสื่อบันทึกข้อมูลที่สำรองและระบุอำนาจในการอนุมัติที่เหมาะสมเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการปฏิบัติตามกฎ ระเบียบในการขออนุมัติใช้งานสื่อบันทึกข้อมูลที่สำรองในบางครั้ง

ระดับ Level 3

-มีการปฏิบัติตามกฎ ระเบียบในการขออนุมัติใช้งานสื่อบันทึกข้อมูลที่สำรองทุกครั้ง

3.5 การกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว

ระดับ Level 1

-มีการกำหนดขั้นตอนการทำลายข้อมูลและสื่อบันทึกข้อมูลที่ไม่ได้ใช้งานแล้ว

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอนการทำลายข้อมูลและสื่อบันทึกข้อมูลที่ไม่ได้ใช้งานแล้วเป็นบางครั้ง

ระดับ Level 3

-มีการปฏิบัติตามขั้นตอนการทำลายข้อมูลและสื่อบันทึกข้อมูลที่ไม่ได้ใช้งานแล้วทุกครั้ง
-ไม่พบปัญหา/ความเสี่ยงในข้อมูลที่อยู่ในสื่อบันทึกข้อมูลที่ไม่ได้ใช้งานแล้ว

(4) การเตรียมการอุปกรณ์ประมวลผลสำรอง

4.1 มีการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงานและระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือการประเมินผลกระทบของกระบวนงานหลัก

ระดับ Level 1

-มีแผนงานหรือขั้นตอนในการปฏิบัติการจัดทำประเมินความเสี่ยง ความสัมพันธ์และการกำหนดให้ความสำคัญของระบบ รวมทั้งกำหนดระยะเวลาในการกู้คืนระบบงาน พร้อม Work Flow ของแต่ละกระบวนงานที่สำคัญ

ระดับ Level 2

-มีเจ้าหน้าที่ดูแลระบบที่มีความสำคัญของหน่วยงาน

-มีการบันทึกเหตุการณ์การล่มของระบบทุกครั้ง

-สามารถกู้คืนระบบได้ตามระยะเวลาที่กำหนด

ระดับ Level 3

-มีการรายงานต่อหัวหน้างานและผู้อำนวยการทุกครั้งเมื่อมีเหตุการณ์ต้องกู้คืนระบบ

4.2 มีการกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

ระดับ Level 1

-มีการกำหนดขั้นตอน/วิธีการเผชิญกับสถานการณ์ โดยการจัดลำดับความสำคัญเมื่อเกิดเหตุการณ์ล่มของระบบและจัดแบ่งความรุนแรงของปัญหา รวมทั้งให้มีการจดบันทึกเหตุการณ์ที่เกิดความรุนแรงและต้องรายงานต่อหัวหน้างานและผู้อำนวยการทุกครั้งเมื่อมีเหตุการณ์ที่เกิดความรุนแรงขึ้น

ระดับ Level 2

-มีการปฏิบัติตามขั้นตอน/วิธีการเผชิญกับสถานการณ์ ที่หน่วยงานกำหนดไว้ แต่ยังไม่ครบถ้วน

ระดับ Level 3

-มีการปฏิบัติตามขั้นตอน/วิธีการเผชิญกับสถานการณ์ ที่หน่วยงานกำหนดไว้ ได้อย่างครบถ้วน

4.3 มีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

ระดับ Level 1

-มีการกำหนดแผนการปฏิบัติการแก้ไขปัญหาในแต่ละสถานการณ์ของระบบสารสนเทศ

ระดับ Level 2

-มีการแบ่งระดับชั้นในการแก้ไขปัญหา

ระดับ Level 3

-มีการรายงานต่อหัวหน้าหน่วยตามขั้นตอนที่กำหนด

4.4 มีการกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

ระดับ Level 1

-มีการมอบหมายหน้าที่ให้เจ้าหน้าที่ดูแลระบบสารสนเทศ และผู้มีอำนาจในการตัดสินใจกับปัญหาต่างๆไว้อย่างชัดเจนเป็นลายลักษณ์อักษร

ระดับ Level 2

-การมอบหมายหน้าที่ของเจ้าหน้าที่ที่ดูแลระบบสารสนเทศและผู้มีอำนาจในการตัดสินใจกับปัญหานั้น มีขอบเขตอำนาจหน้าที่ที่ชัดเจนและเหมาะสม

-มีการปฏิบัติตามการมอบหมายอย่างครบถ้วน

ระดับ Level 3

-มีการรายงานปัญหาและผลของการปฏิบัติในการแก้ไขปัญหา รวมทั้งปัญหา/อุปสรรคที่เกิดขึ้นไว้อย่างครอบคลุมและครบถ้วนทุกครั้ง

4.5 มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน

ระดับ Level 1

-หน่วยงานมีการกำหนดรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงานไว้เป็นลายลักษณ์อักษร

-หน่วยงานมีการสื่อสารถึงความจำเป็นและรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงานให้ทีมงานที่เกี่ยวข้องทราบอย่างชัดเจน

-มีการชี้แจงถึงอุปกรณ์ชนิดนั้นๆ ว่าควรใช้เมื่อเกิดเหตุการณ์ประเภทใด

ระดับ Level 2

-ผู้ปฏิบัติงาน/ทีมงาน อธิบายถึงความจำเป็นและรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงานได้อย่างชัดเจน อย่างน้อย 1 คน

-มีการปฏิบัติตามการกำหนดรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงานไว้อย่างครบถ้วน

ระดับ Level 3

-ผู้ปฏิบัติงาน/ทีมงาน อธิบายถึงความจำเป็นและรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงานได้อย่างชัดเจน อย่างน้อย 3 คน

-การจดบันทึกการใช้งานอุปกรณ์และสาเหตุของเหตุการณ์การใช้งาน

-มีการรายงานหรือสรุปผลการใช้งานอุปกรณ์ต่างๆตามข้อกำหนด

4.6 หน่วยงานที่เป็นหน่วยสำรองข้อมูลหรือจัดเก็บข้อมูลก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน

ระดับ Level 1

-มีแผนการสำรองข้อมูลภายนอกหน่วยงาน

ระดับ Level 2

-ข้อมูลที่สำคัญของหน่วยงานมีการสำรองไว้นอกจากสถานที่ทำงาน

-มีการจดบันทึกการนำข้อมูลไปสำรองไว้ที่ภายนอกหน่วยงาน

ระดับ Level 3

-มีการรายงานปัญหาหรือข้อมูลให้หัวหน้าหน่วยงานทราบ

4.7 มีการทบทวนหรือปรับปรุงแผนฉุกเฉินและเก็บแผนฉุกเฉินไว้ในสถานที่มั่นคงปลอดภัย

ระดับ Level 1

-มีแผนการเผชิญกับสถานการณ์ฉุกเฉิน

ระดับ Level 2

-แผนการเผชิญกับสถานการณ์ฉุกเฉินมีการทบทวนให้เป็นปัจจุบันและเหมาะสมกับสถานการณ์

ระดับ Level 3

-การเก็บรักษาแผนในการรับมือสถานการณ์ฉุกเฉินไม่เหมาะสม

4.8ทดสอบการปฏิบัติตามแผนฉุกเฉิน

ระดับ Level 1

-แผนการเผชิญกับสถานการณ์ฉุกเฉิน โดยระบุให้ทดสอบแบบจำลองสถานการณ์จริง

ระดับ Level 2

-มีการปฏิบัติตามแผนการเผชิญกับสถานการณ์ฉุกเฉิน โดยจำลองสถานการณ์จริงขึ้นมาใช้ในการทดสอบ/กู้คืนระบบ

ระดับ Level 3

-มีการรายงานผลการทดสอบหรือกู้คืนระบบอย่างเป็นลายลักษณ์อักษร ต่อผู้บังคับบัญชา

4.9 การสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับ

ระดับ Level 1

-มีการวิเคราะห์และวางแผนการสื่อสารประชาสัมพันธ์ให้เหมาะสมกับกลุ่มเป้าหมาย

ระดับ Level 2

-มีการสื่อสารประชาสัมพันธ์แผนการเผชิญกับสถานการณ์ฉุกเฉิน อย่างน้อย 1 ช่องทาง

-แบ่งแยกระดับการรับข่าวสาร

-ผู้ปฏิบัติงาน/ทีมงาน อธิบายถึงแผนการเผชิญกับสถานการณ์ฉุกเฉินได้อย่างชัดเจน อย่างน้อย 1 คน

ระดับ Level 3

-ผู้ปฏิบัติงาน/ทีมงาน อธิบายถึงแผนการเผชิญกับสถานการณ์ฉุกเฉินได้อย่างชัดเจน อย่างน้อย 3 คน

-มีรายงานการประเมินผลการสื่อสารแผนการเผชิญกับสถานการณ์ฉุกเฉิน

4.10 กรณีที่เกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหาและวิธีการแก้ไขปัญหาไว้ด้วย

ระดับ Level 1

-มีการจดบันทึกเหตุการณ์ของรายละเอียดที่เกิดเหตุการณ์ สาเหตุของปัญหาที่เกิดขึ้น

ระดับ Level 2

-มีการบันทึกวิธีการแก้ไขปัญหา

ระดับ Level 3

-มีการรายงานต่อผู้บังคับบัญชาเป็นลายลักษณ์อักษร

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ
หมวดที่ 14 การปฏิบัติงานที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ
หมายเลขเอกสาร WI1401

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

1.0 วัตถุประสงค์

วิธีการปฏิบัติงานฉบับนี้ เป็นแนวทางการปฏิบัติในการตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ หมวดที่ 14 การปฏิบัติงานที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ

2.0 ขอบข่าย

ระเบียบปฏิบัติฉบับนี้ ครอบคลุมการสอบทานกระบวนการนำนโยบายสู่การปฏิบัติ ดังนี้

2.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

2.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)

2.1.1.1 มีการปฏิบัติตามข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศ เพื่อป้องกันมิให้เจ้าหน้าที่ของกรมสนสังกัดกรมสนับสนุนบริการสุขภาพละเมิดข้อกำหนดของกฎหมาย

2.1.1.2 มีการการทำนิติกรรมสัญญาทางด้านเทคโนโลยีสารสนเทศต้องส่งให้นิติกรตรวจสอบดูความถูกต้องของสัญญาให้เป็นไปตามที่กฎหมายกำหนด

2.1.1.3 มีการจัดตั้งคณะกรรมการจัดทำข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการเพื่อรวมข้อกำหนดที่มีผลทางกฎหมายด้านระเบียบ

2.1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

2.1.3 การป้องกันข้อมูล (Protection of records)

2.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)

2.1.5 ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of cryptographic controls)

2.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

2.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

2.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)

2.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

3.0 ขั้นตอนการปฏิบัติ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
1.การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)		
เพื่อป้องกันมิให้เจ้าหน้าที่ของกรมสนสังกัดกรมสนับสนุนบริการสุขภาพละเมิดข้อกำหนดของกฎหมาย	1.1 มีการปฏิบัติตามข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศ โดย -หน่วยงานต้องมีการวิเคราะห์กระบวนการปฏิบัติที่เสี่ยงต่อการละเมิดกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง -หน่วยงานต้องจัดระบบควบคุมภายในโดยมีจุดการควบคุมความเสี่ยงต่อการละเมิดกฎหมาย ฯลฯ -หน่วยงานต้องกำหนดขั้นตอน/แนวทางปฏิบัติงานในการควบคุมจุดเสี่ยงต่อการละเมิดกฎหมาย -หน่วยงานต้องมีการอบรมหรือชี้แจงระบบควบคุมภายใน/มาตรการในการควบคุมความเสี่ยงในการปฏิบัติงานให้ถือปฏิบัติ -หน่วยงานต้องมีการติดตามประเมินผลการปฏิบัติงานเป็นระยะ	-สัมภาษณ์กระบวนการวิเคราะห์กระบวนการปฏิบัติงานที่เสี่ยงต่อการละเมิดกฎหมาย ฯลฯ -ตรวจสอบรายงานการวิเคราะห์กระบวนการปฏิบัติที่เสี่ยงต่อการละเมิดกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องและการจัดระบบการควบคุมจุดเสี่ยง รวมทั้งการอบรมหรือชี้แจงระบบควบคุมภายใน/มาตรการในการควบคุมความเสี่ยงในการปฏิบัติงานที่ให้ถือปฏิบัติและกระบวนการในการติดตามประเมินผลการปฏิบัติงานตามระยะเวลาที่กำหนด

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
	1.2 การจัดทำนิติกรรมสัญญาทางด้านเทคโนโลยีสารสนเทศ โดย -หน่วยงานต้องมีการจัดทำนิติกรรมสัญญาที่ครอบคลุมเนื้อหาดังนี้ (1) สิทธิ-หน้าที่ของคู่สัญญา (2) การแบ่งชำระงวดเงิน หรือการชำระเงินที่เป็นการขจัดความเสี่ยงของผู้ว่าจ้าง (3) คุณลักษณะที่ต้องการของการจ้างงาน/ของที่จะให้ส่งมอบ (4) ลิขสิทธิ์ในการจ้าง (5) การเยียวยาความเสียหายในกรณีถ้ามีการผิดสัญญา (6) ขั้นตอน/แนวทางปฏิบัติในการควบคุม-กำกับ ติดตาม ประเมินผลการปฏิบัติงานของผู้รับจ้าง	-สัมภาษณ์กระบวนการจัดทำนิติกรรมสัญญาทางด้านเทคโนโลยีสารสนเทศ -ตรวจสอบการจัดทำนิติกรรมสัญญาที่ต้องครอบคลุมเนื้อหาดังนี้ (1) สิทธิ-หน้าที่ของคู่สัญญา (2) การแบ่งชำระงวดเงิน หรือการชำระเงินที่เป็นการขจัดความเสี่ยงของผู้ว่าจ้าง (3) คุณลักษณะที่ต้องการของการจ้างงาน/ของที่จะให้ส่งมอบ (4) ลิขสิทธิ์ในการจ้าง (5) การเยียวยาความเสียหายในกรณีถ้ามีการผิดสัญญา (6) ขั้นตอน/แนวทางปฏิบัติในการควบคุม-กำกับ ติดตาม ประเมินผลการปฏิบัติงานของผู้รับจ้าง
เพื่อรวมข้อกำหนดที่มีผลทางกฎหมาย ด้านระเบียบ	1.3 การจัดตั้งคณะกรรมการจัดทำข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการ ที่ต้องครอบคลุมประเด็นดังนี้ -ระเบียบการใช้คอมพิวเตอร์ -ระเบียบการใช้ soft ware ที่ถูกต้องตามกฎหมาย -การกำหนดสิทธิและการให้สิทธิในการเข้าถึงข้อมูล -การป้องกันความปลอดภัยของข้อมูลและ ระบบต่างๆ อุปกรณ์ต่างๆ ทางด้านเทคโนโลยีสารสนเทศ -การกำหนดแนวทางการใช้ข้อมูล -การป้องกันข้อมูลส่วนตัว ฯลฯ	-สัมภาษณ์กระบวนการจัดตั้งคณะกรรมการจัดทำข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการ -สัมภาษณ์กระบวนการข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการ -ตรวจสอบข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการที่ต้องครอบคลุมประเด็นดังนี้ 1.ระเบียบการใช้คอมพิวเตอร์ 2.ระเบียบการใช้ soft ware ที่ถูกต้องตามกฎหมาย 3.การกำหนดสิทธิและการให้สิทธิในการเข้าถึงข้อมูล 4.การป้องกันความปลอดภัยของข้อมูลและ ระบบต่างๆ อุปกรณ์ต่างๆ ทางด้านเทคโนโลยีสารสนเทศ 5.การกำหนดแนวทางการใช้ข้อมูล 6.การป้องกันข้อมูลส่วนตัว ฯลฯ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
2.สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)		
เพื่อให้มั่นใจว่ามีความสอดคล้องกับความต้องการของกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างที่ว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์	2.1 มีขั้นตอนการปฏิบัติงานที่เหมาะสมไม่ละเมิดกฎหมาย ระเบียบข้อบังคับ รวมทั้งสัญญาจ้าง ที่ว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์	-ตรวจสอบการกำหนดขั้นตอนการปฏิบัติงานและสัญญาจ้าง ว่าไม่มีจุดเสี่ยงต่อการละเมิดกฎหมาย ระเบียบข้อบังคับ -สัมภาษณ์กระบวนการปฏิบัติงานและการจัดทำสัญญาจ้าง เพื่อได้ความชัดเจนในกระบวนการปฏิบัติงานและสัญญาจ้างที่ไม่ละเมิดกฎหมาย ระเบียบข้อบังคับ
	2.2 มีสัญญาข้อตกลงระหว่างผู้ให้บริการกับผู้ใช้บริการอย่างชัดเจนในการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์	-ตรวจสอบสัญญาข้อตกลงระหว่างผู้ให้บริการกับผู้ใช้บริการเกี่ยวกับความชัดเจนในการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ -สัมภาษณ์การใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์และสัญญาข้อตกลงระหว่างผู้ให้บริการกับผู้ใช้บริการ
3.การป้องกันข้อมูล (Protection of records)		
	3.1 การกำหนดแนวทางการจัดทำสัญญาจ้างกับเอกชน อย่างน้อยระบุถึง (1) ประเด็นห้ามนำข้อมูลของกรมไปเผยแผ่ ทำหาย หรือทำลาย ปลอมแปลงโดยไม่ได้รับอนุญาต (2) การเข้าออกห้องเก็บข้อมูลต้องมีระบบรักษาความปลอดภัยอย่างเข้มงวด (3) มีการเก็บสำรองข้อมูลและกำหนดสิทธิการเข้าถึงข้อมูลด้วยusernameและpassword	-ตรวจสอบแนวทางการจัดทำสัญญาจ้างกับเอกชนของหน่วยงาน ต้องมีการให้กำหนดอย่างน้อยระบุถึง (1) ประเด็นห้ามนำข้อมูลของกรมไปเผยแผ่ ทำหาย หรือทำลาย ปลอมแปลงโดยไม่ได้รับอนุญาต (2) การเข้าออกห้องเก็บข้อมูลต้องมีระบบรักษาความปลอดภัยอย่างเข้มงวด (3) มีการเก็บสำรองข้อมูลและกำหนดสิทธิการเข้าถึงข้อมูลด้วยusernameและpassword -ตรวจสอบสัญญาจ้างกับเอกชนของหน่วยงานว่าได้ระบุครอบคลุมตามแนวทางการจัดทำสัญญาจ้างข้างต้นหรือไม่ -สัมภาษณ์ผู้ปฏิบัติงานถึงขอบเขตประเด็นสำคัญที่ต้องระบุในสัญญาจ้างกับเอกชนและวัตถุประสงค์ที่ต้องกำหนดไว้

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
4.ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)		
เพื่อให้หน่วยงานมีการดำเนินการสอดคล้องกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง เพื่อป้องกันข้อมูลส่วนบุคคลและความเป็นส่วนตัว	4.1 หน่วยงานต้องมีการกำหนดให้ข้อมูลส่วนตัวต้องมีการเข้ารหัสหรือขออนุญาตจากเจ้าของเรื่อง ให้เป็นไปตามข้อบังคับ	-ตรวจสอบข้อมูลส่วนตัวว่ามีการเข้ารหัสหรือไม่ โดยให้ผู้ปฏิบัติงานเปิดฐานข้อมูลที่มีข้อมูลส่วนบุคคลจัดเก็บไว้ ว่ามีการเข้ารหัสไว้หรือไม่ -สัมภาษณ์เกี่ยวกับการจัดเก็บข้อมูลส่วนตัว/ข้อมูลส่วนบุคคลว่ามีการจัดเก็บดูแลรักษาอย่างไร และหากต้องการการเข้าถึงมีวิธีการหรือขั้นตอนการปฏิบัติอย่างไร เพื่อวิเคราะห์หาความเสี่ยงในการปฏิบัติต่อข้อมูลส่วนบุคคล
	4.2 หน่วยงานต้องกำหนดให้ข้อมูลที่เป็นส่วนบุคคล เจ้าของข้อมูลสามารถกำหนดวิธีการเข้ารหัสได้ด้วยตัวเอง	-สัมภาษณ์การกำหนดให้ข้อมูลที่เป็นส่วนบุคคล เจ้าของข้อมูลสามารถกำหนดวิธีการเข้ารหัสได้ด้วยตัวเอง เพื่อทราบรายละเอียดวิธีการเข้ารหัสได้ด้วยตนเอง -ตรวจสอบระบบที่ดำเนินการให้เจ้าของข้อมูลสามารถกำหนดวิธีการเข้ารหัสได้ด้วยตนเอง
5.ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of cryptographic controls)		
เพื่อให้มีการกำหนดมาตรการควบคุม ขั้นตอนการเข้าถึงฐานข้อมูลในแต่ละระดับชั้นความสำคัญ	5.1 มีมาตรการควบคุม ขั้นตอนการเข้าถึงฐานข้อมูลในแต่ละระดับชั้นความสำคัญ	-ตรวจสอบมาตรการควบคุม ขั้นตอนการเข้าถึงฐานข้อมูลในแต่ละระดับชั้นความสำคัญ -สัมภาษณ์และให้ผู้ปฏิบัติงาน/ผู้ดูแลระบบที่รับตรวจปฏิบัติตามมาตรการควบคุม ขั้นตอนการเข้าถึงฐานข้อมูลในแต่ละระดับชั้นความสำคัญ เพื่อค้นหาความเสี่ยงที่อาจเกิดขึ้นในกระบวนการปฏิบัติงานในการเข้ารหัสข้อมูล
-เพื่อให้ระบบสารสนเทศของหน่วยงานได้รับการตรวจประเมินและลดความเสี่ยงที่อาจเกิดความเสี่ยงหาในระบบสารสนเทศของหน่วยงาน	5.2 มีการการตรวจประเมิน ให้คณะกรรมการจัดทำข้อกำหนด จัดทำมาตรฐานการตรวจสอบประเมินระบบสารสนเทศ โดย -มีการแต่งตั้งคณะกรรมการในการจัดทำมาตรฐานการตรวจสอบประเมินระบบสารสนเทศ -มีการกำหนดขั้นตอน/มาตรฐานการตรวจสอบประเมินระบบสารสนเทศ	-ตรวจสอบคำสั่งแต่งตั้ง/มอบหมายงานของคณะกรรมการจัดทำมาตรฐานการตรวจสอบประเมินระบบสารสนเทศ ว่ามีการแต่งตั้งและกำหนดอำนาจหน้าที่ครอบคลุมการตรวจประเมินระบบสารสนเทศหรือไม่ เพื่อหาความเสี่ยงในการตรวจประเมินหรือการละไม่ตรวจประเมินบางส่วนของระบบสารสนเทศ -ตรวจสอบกำหนดขั้นตอน/มาตรฐานการตรวจสอบประเมินระบบสารสนเทศ -สัมภาษณ์เกี่ยวกับการกำหนดขั้นตอนและวิธีการตรวจสอบประเมินระบบสารสนเทศ

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
6.การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)		
1.เพื่อให้การปฏิบัติสอดคล้องกับนโยบายและมาตรฐานความปลอดภัย 2.เพื่อให้มีการกำหนดให้มีการประชุมพิจารณาขั้นตอนการปฏิบัติสอดคล้องกับนโยบายและมาตรฐานความปลอดภัย	6.1 เมื่อมีการเปลี่ยนแปลงกรม คณะทำงานสามารถประชุมเพื่อทบทวนมาตรการ ขั้นตอนความมั่นคงปลอดภัยได้ตลอดเวลา 6.2 มีวิธีการในการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและการปฏิบัติของกรม ต้องมีการทบทวนอย่างอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือมีการเปลี่ยนแปลงกรมที่มากเกิดขึ้น	-ตรวจสอบข้อกำหนด/แนวทางปฏิบัติของหน่วยงาน ที่กำหนดให้มีการทบทวนด้านความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน เมื่อกรมฯมีการเปลี่ยนแปลง เช่น นโยบาย หรือ ยุทธศาสตร์ หรือโครงสร้างองค์กร เป็นต้น ที่ส่งผลกระทบต่อกระบวนงานด้านเทคโนโลยีสารสนเทศและระบบสารสนเทศของหน่วยงาน -สัมภาษณ์การปฏิบัติตามแนวทางปฏิบัติที่กำหนดไว้ข้างต้น -สุ่มสอบถามว่าในช่วงระยะเวลาภายใน 1 ปีที่ผ่านมา มีเหตุการณ์ที่ส่งผลต่อการทบทวนด้านความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานหรือไม่ และหน่วยงานดำเนินการอย่างไร โดยมีวัตถุประสงค์อย่างไร
7.ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)		
เพื่อให้หน่วยงานมีการปฏิบัติที่สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย	7.1หน่วยงานต้องมีการกำหนดขั้นตอน/แนวทางปฏิบัติในการทบทวนระบบให้สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างชัดเจนเป็นลายลักษณ์อักษร 7.2 หน่วยงานมีการดำเนินทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลสารสนเทศและขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบาย มาตรฐานและความต้องการด้านความมั่นคงปลอดภัย	-ตรวจสอบขั้นตอนการปฏิบัติตามนโยบายและมาตรฐานความมั่นคงปลอดภัยที่หน่วยงานต้องกำหนดขึ้นใช้ในการปฏิบัติงานว่ามีครอบคลุมตามที่นโยบาย/มาตรฐานความมั่นคงปลอดภัยหรือไม่ และการกำหนดดังกล่าวเหมาะสมและครอบคลุมความเสี่ยงหรือไม่ -ตรวจสอบว่าหน่วยงานมีการดำเนินการทบทวนเกี่ยวกับการประมวลผลสารสนเทศและขั้นตอนการปฏิบัติงานโดยเทียบกับนโยบาย มาตรฐานและความต้องการด้านความมั่นคงปลอดภัยอย่างเป็นระยะที่เหมาะสมหรือไม่ และค้นหาความเสี่ยงในการทบทวนดังกล่าว -สัมภาษณ์กระบวนการทบทวนดังกล่าวถึงวิธีการปฏิบัติในการทบทวนและการเปรียบเทียบกับนโยบาย มาตรฐานและความต้องการด้านความมั่นคงปลอดภัย รวมทั้งการกำหนดระยะเวลาที่ทบทวนอย่างไร

วัตถุประสงค์ของการควบคุม	วิธีการหรือขั้นตอนการควบคุม	ขั้นตอนการตรวจสอบ
8.การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)		
	8.1หน่วยงานมีการกำหนดขั้นตอน/แนวทางปฏิบัติในการทบทวนทางเทคนิคในระบบสารสนเทศหรือระบบการปฏิบัติงานด้าน IT ให้สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างชัดเจนเป็นลายลักษณ์อักษร	-ตรวจสอบขั้นตอน/แนวทางปฏิบัติในการทบทวนทางเทคนิคในระบบสารสนเทศหรือระบบการปฏิบัติงานด้าน IT ให้สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างชัดเจนเป็นลายลักษณ์อักษรว่ามีหรือไม่ และถ้ามีครอบคลุมเหมาะสมหรือไม่ ค้นหาความเสี่ยงในกระบวนการดังกล่าว -สัมภาษณ์กระบวนการและขั้นตอนการปฏิบัติในการทบทวนทางเทคนิคในระบบสารสนเทศหรือระบบการปฏิบัติงานด้าน IT ให้สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

เกณฑ์การประเมินความเสี่ยง

(1) ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)

1.1.1 มีการปฏิบัติตามข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศ เพื่อป้องกันมิให้เจ้าหน้าที่ของกรมสนสังกัดกรมสนับสนุนบริการสุขภาพละเมิดข้อกำหนดของกฎหมาย

ระดับ Level 1

-มีการกำหนดแนวทางปฏิบัติ/ขั้นตอนการปฏิบัติตามข้อกำหนดทางกฎหมาย

-มีการอบรมหรือชี้แจงความเสี่ยงในการละเมิดต่อข้อกำหนดทางกฎหมาย

ระดับ Level 2

-ผู้ปฏิบัติงานมีความรู้ความเข้าใจความเสี่ยงในการละเมิดต่อข้อกำหนดทางกฎหมาย โดยสามารถอธิบายและตอบคำถามเกี่ยวกับความเสี่ยงในการละเมิดต่อข้อกำหนดทางกฎหมายได้อย่างครบคลุมครบถ้วน อย่างน้อย 1 คน

-มีการปฏิบัติตามแนวทางปฏิบัติ/ขั้นตอนการปฏิบัติตามข้อกำหนดทางกฎหมาย

ระดับ Level 3

-ไม่พบปัญหาหรือความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่กรมฯที่ละเมิดข้อกำหนดทางกฎหมาย

1.1.2 มีการการทำนิติกรรมสัญญาทางด้านเทคโนโลยีสารสนเทศต้องส่งให้นิติกรตรวจสอบดูความถูกต้องของสัญญาให้เป็นไปตามที่กฎหมายกำหนด

ระดับ Level 1

-มีการกำหนดแนวทางปฏิบัติและขั้นตอนการจัดทำนิติกรรมสัญญาทางด้านเทคโนโลยีสารสนเทศ ครอบคลุมในประเด็นสำคัญ อย่างน้อยตามที่กำหนดไว้

ระดับ Level 2

-มีระบบการตรวจสอบ ควบคุม-กำกับตามที่กรมกำหนด

ระดับ Level 3

ไม่พบปัญหา/ความเสี่ยงในการจัดทำนิติกรรมสัญญาทางด้านเทคโนโลยีสารสนเทศที่มีความผิดพลาด หรือหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย

1.1.3 มีการจัดตั้งคณะกรรมการจัดทำข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการเพื่อรวมข้อกำหนดที่มีผลทางกฎหมายด้านระเบียบ

ระดับ Level 1

-มีการจัดตั้งคณะกรรมการจัดทำข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการ เพื่อรวมข้อกำหนดที่มีผลทางกฎหมาย ด้านระเบียบ

ระดับ Level 2

-มีการกำหนดแนวทางปฏิบัติที่สอดคล้องตามข้อกำหนดทางกฎหมาย

ระดับ Level 3

-มีการปฏิบัติตามแนวทางปฏิบัติที่สอดคล้องตามข้อกำหนดทางกฎหมายที่กรมกำหนดไว้
-ไม่พบปัญหา/ความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่กรมที่มีการละเมิดข้อกำหนดทางกฎหมาย

1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

ระดับ Level 1

-มีขั้นตอนการปฏิบัติที่เหมาะสม เพื่อให้มั่นใจว่ามีความสอดคล้องกับความต้องการของกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง ที่ว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์
-มีสัญญาข้อตกลงระหว่างผู้ให้บริการกับผู้ใช้บริการอย่างชัดเจนในการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์

ระดับ Level 2

-มีระบบการเฝ้าระวังติดตามดูแลการไม่ละเมิดสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์

ระดับ Level 3

-มีการปฏิบัติตามแผนการเฝ้าระวังติดตามการไม่ละเมิดสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์และมีรายงานผลการปฏิบัติในการดำเนินการเฝ้าระวังดังกล่าว เพื่อนำสู่การปรับปรุงวางแผนการปฏิบัติ
-ไม่พบปัญหา/ความเสี่ยงในการละเมิดสิทธิในทรัพย์สินทางปัญญา

1.3. การป้องกันข้อมูล (Protection of records)

ระดับ Level 1

-มีการกำหนดแนวทางการจัดทำสัญญาจ้างกับเอกชน อย่างน้อยระบุถึง

1. ประเด็นห้ามนำข้อมูลของกรมไปเผยแผ่ ทำหาย หรือทำลาย ปลอมแปลงโดยไม่ได้รับอนุญาต
2. การเข้าออกห้องเก็บข้อมูลต้องมีระบบรักษาความปลอดภัยอย่างเข้มงวด
3. มีการเก็บสำรองข้อมูลและกำหนดสิทธิการเข้าถึงข้อมูลด้วยusernameและpassword

ระดับ Level 2

-มีการปฏิบัติตามแนวทางที่กำหนด แต่ไม่ครบทุกประเด็น

ระดับ Level 3

-มีการปฏิบัติตามแนวทางที่กำหนด ครอบคลุมครบทุกประเด็น

-ไม่พบปัญหา/ความเสี่ยงในการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

1.4. ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)

ระดับ Level 1

-มีการกำหนดแนวทางปฏิบัติในการป้องกันข้อมูลส่วนตัว โดยมีการดำเนินการสอดคล้องกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

ระดับ Level 2

-มีการปฏิบัติตามแนวทางปฏิบัติในการป้องกันข้อมูลส่วนตัวที่กำหนด แต่ไม่ครบถ้วน

ระดับ Level 3

-มีการปฏิบัติตามแนวทางปฏิบัติในการป้องกันข้อมูลส่วนตัวที่กำหนดอย่างครบถ้วน

-ไม่พบปัญหา/ความเสี่ยงต่อข้อมูลส่วนบุคคล

1.5. ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of cryptographic controls)

ระดับ Level 1

-มีการแต่งตั้ง/มอบหมายให้คณะกรรมการจัดทำข้อกำหนด จัดทำมาตรฐานการตรวจสอบประเมินระบบสารสนเทศ

ระดับ Level 2

-มีการกำหนดแนวทางการตรวจประเมินของคณะกรรมการเกี่ยวกับมาตรฐานการตรวจสอบประเมินระบบสารสนเทศและมาตรการควบคุม ขั้นตอนการเข้าถึงฐานข้อมูลในแต่ละระดับชั้นความสำคัญ

-มีการปฏิบัติตามมาตรการควบคุม ขั้นตอนการเข้าถึงฐานข้อมูลในแต่ละระดับชั้นความสำคัญ

ระดับ Level 3

-มีการปฏิบัติตามแนวทางการตรวจประเมินของคณะกรรมการเกี่ยวกับมาตรฐานการตรวจสอบประเมินระบบสารสนเทศอย่างครบถ้วน

-ไม่พบปัญหา/ความเสี่ยงของข้อมูลมิให้เกิดการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

2. การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

2.1. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

ระดับ Level 1

-มีการกำหนดให้มีการทบทวนมาตรการ ขั้นตอนและการบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญของกรม

ระดับ Level 2

-มีการปฏิบัติทบทวนมาตรการ ขั้นตอนและการบริหารจัดการความมั่นคงปลอดภัยอย่างครอบคลุมและสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญของกรม

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในมาตรการ ขั้นตอนและการบริหารจัดการความมั่นคงปลอดภัย หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญของกรม

2.2. ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)

ระดับ Level 1

-มีการกำหนดให้มีการประชุมพิจารณาวิเคราะห์ขั้นตอนการปฏิบัติงานให้สอดคล้องกับนโยบายและมาตรฐานความปลอดภัย

ระดับ Level 2

-มีการปฏิบัติสอดคล้องกับนโยบายและมาตรฐานความปลอดภัย

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการปฏิบัติงานอันเนื่องมาจากการปฏิบัติไม่สอดคล้องกับนโยบายและมาตรฐานความปลอดภัย

2.3. การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

ระดับ Level 1

-มีการกำหนดขั้นตอน/แนวทางปฏิบัติในการทบทวนระบบให้สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างชัดเจนเป็นลายลักษณ์อักษร

ระดับ Level 2

-มีการทบทวนระบบให้สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

ระดับ Level 3

-ไม่พบปัญหา/ความเสี่ยงในการพัฒนาหรือปรับปรุงละเมิดต่อนโยบายและกฎหมาย

วิธีปฏิบัติงาน Work Instruction
เรื่อง การตรวจสอบ คุณภาพการให้บริการงานเทคโนโลยีสารสนเทศ
กรมสนับสนุนบริการสุขภาพ
หมายเลขเอกสาร WI1501

☑ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

ขั้นตอนการทำงาน

เกณฑ์คะแนนในการประเมินมาตรฐาน ITITL

0=ไม่มี
1=มีแต่ไม่มีการปฏิบัติหรือไม่มีแต่มีการปฏิบัติอยู่
2=มีไม่ครบถ้วนทุกกระบวนการและมีการปฏิบัติไม่สม่ำเสมอ
3=มีไม่ครบถ้วนทุกกระบวนการและมีการปฏิบัติอย่างสม่ำเสมอหรือมีความครบถ้วนแต่ปฏิบัติไม่สม่ำเสมอ
4=มีครบถ้วนทุกกระบวนการและมีการปฏิบัติอย่างสม่ำเสมอ

หมวดที่ 1 Strategy Generation

วัตถุประสงค์ : เพื่อให้ฝ่ายบริหารทราบเหตุผลในโครงการต่างๆ ที่จำเป็นต่อการบริการงานด้านไอที มีการสำรวจยุทธศาสตร์ การกำหนดวัตถุประสงค์ วิเคราะห์คู่แข่ง เป็นต้น

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.1 มีการประชุมคณะกรรมการหรือทีมงาน IT เพื่อกำหนด -วัตถุประสงค์การให้บริการ -วิสัยทัศน์ พันธกิจและกลยุทธ์การให้บริการที่เหมาะสมสอดคล้องในการขับเคลื่อนเป้าหมายของหน่วยงาน -กำหนดแผนงานค่าเป้าหมายระยะปานกลางที่สอดคล้องกับวิสัยทัศน์ พันธกิจและกลยุทธ์ที่กำหนดไว้ รวมทั้งแผนแม่บทด้าน IT ของกรม -กำหนดแผนงานด้าน IT ระยะสั้น 1 ปีและโครงการที่ชัดเจน โดยระบุถึงวัตถุประสงค์ ตัวชี้วัด ที่ชัดเจน			

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.2 มีกระบวนการในการสื่อสารวิสัยทัศน์ด้าน IT พันธกิจ และ กลยุทธ์ที่กำหนดไว้ และแผนงานระยะสั้นและปานกลางที่เหมาะสมอย่างน้อย 3 ช่องทาง ได้แก่ เว็บไซต์ ที่ประชุมประจำเดือนระดับองค์กร บันทึกแจ้งเวียน			
1.3 มีกระบวนการในการควบคุม-กำกับ ติดตามความก้าวหน้าในการดำเนินงานตามแผนงาน(Action plan) แสดงให้เห็นถึงการควบคุมกำกับทั้งกิจกรรมและการใช้จ่ายเงินตามแผนงาน/โครงการที่ชัดเจน รวมทั้งการประเมินผลเมื่อสิ้นสุดโครงการ			
1.4 มีกระบวนการรวบรวมผลการดำเนินงานด้าน IT ทั้งผลการดำเนินงานตามแผนงานและปัญหา/อุปสรรคที่เกิดขึ้นในกระบวนการดำเนินงาน นำข้อมูลดังกล่าวเข้าสู่การพิจารณาวิเคราะห์ทบทวนกลยุทธ์และค่าเป้าหมายในระยะปานกลางในปีถัดไป ได้อย่างเหมาะสมต่อเนื่องเป็นระบบ			

หมวดที่ 2 Financial Management (FM)

วัตถุประสงค์ : การจัดการบริหารการเงินกับการให้บริการด้านไอที เพื่อรองรับการจัดการมูลค่าได้อย่างมีประสิทธิภาพ เช่น ทรัพย์สินด้านไอที และ ทรัพยากรที่ถูกใช้ในการให้บริการเพื่อสร้างความมั่นใจให้ลูกค้าและรองรับข้อมูลอย่างแม่นยำเพื่อนำไปสู่การลงทุนเพื่อให้สามารถบริหารจัดการเงินที่ต้องใช้กับอุปกรณ์ทางด้านไอทีและที่ต้องใช้กับการบริการทางด้านไอทีได้อย่างมีประสิทธิภาพ

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
Budgeting Process: คือการบริหารจัดงบประมาณด้านIT			
1.มีจัดทำกระบวนการบริหารจัดการงบประมาณตามระเบียบราชการที่ดี มาใช้ในการบริหารจัดการ ควบคุม กำกับ การเบิกจ่ายงบประมาณ			
2.มีการกำหนดให้มีการรายงานการเบิกจ่ายงบประมาณในระยะเวลาที่เหมาะสม			
3.มีการประชุมคณะผู้บริหารขององค์กรติดตามความก้าวหน้าและแจ้งเตือนการเบิกจ่ายงบประมาณที่ไม่เหมาะสมและไม่ตรงเวลาในการใช้จ่ายตามแผนที่ตั้งไว้ หรือมีแนวโน้มการใช้จ่ายเงินงบประมาณ และแจ้งปัญหาอุปสรรค ร่วมกันแก้ไขปัญหาล่วงหน้าเพื่อให้การเบิกจ่ายตรงตามแผนงานที่กำหนด			

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
4.มีการประเมินผลสรุปวิเคราะห์ผลการเบิกจ่ายงบประมาณรายไตรมาสอย่างเป็นลายลักษณ์อักษรและแจ้งเข้าที่ประชุมการใช้จ่ายงบประมาณเป็นระยะ			
5.มีแผนการเบิกจ่ายงบประมาณตามโครงการและระบุตัวชี้วัดของแต่ละโครงการวัดประเมินผลทั้งประสิทธิภาพและประสิทธิผล			
IT Accounting: คือการจัดทำบัญชีสำหรับงานบริการทางด้านIT			
6.มีการกำหนดเป็นนโยบายให้มีการลงบัญชีที่ถูกต้องและมีกระบวนการตรวจสอบความถูกต้องอย่างสม่ำเสมอเป็นรูปธรรม			
7.มีการลงบันทึกบัญชีคุมการใช้จ่ายงบประมาณอย่างครบถ้วน แต่หากมีความผิดพลาดสามารถหาสาเหตุและแก้ไขปัญหาที่เกิดขึ้นได้			
Cost Model: คือเป็นกรอบการทำงานในรูปแบบของการคำนวณภาพรวมของความจำเป็นของค่าใช้จ่ายในงานบริการทางด้านไอที			
8.กำหนดเป็นนโยบายให้มีการสร้างCost Modelอย่างเป็นรูปธรรม อย่างน้อยให้ควรมีการรายงานผลการเบิกจ่ายเป็นหมวดหมู่ตามที่องค์กรกำหนด			
9.การคำนวณภาพรวมของความจำเป็นของค่าใช้จ่ายในงานบริการทางด้านไอที			

หมวดที่ 3 Service Portfolio Management

วัตถุประสงค์ : เป็นการดูแลการลงทุนในการจัดการบริการที่มีรูปแบบไดนามิกที่มีการข้ามโครงสร้างภายในองค์กรและการจัดการมูลค่า จะทำให้เกิดประโยชน์

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีกระบวนการในการกำหนดการให้บริการของหน่วยงานที่ชัดเจน			
2.มีการแสดงข้อกำหนดการให้บริการที่สอดคล้องกับความต้องการลูกค้าไว้อย่างชัดเจน			
3.มีการปรับปรุงรายละเอียดการให้บริการ เมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบต่อระบบการให้บริการ			
4.มีการทบทวนรายละเอียดการให้บริการ อย่างน้อยปีละ 1 ครั้ง			

หมวดที่ 4 Demand Management

วัตถุประสงค์ : เพื่อให้ผู้รับผิดชอบบริการด้านไอที ใช้ทรัพยากรที่มีอยู่ได้อย่างมีประสิทธิภาพมากที่สุด

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการกำหนดผู้รับผิดชอบในการบริการด้าน IT ไว้อย่างชัดเจน			
2.มีการประเมินความรู้ ความสามารถ และสมรรถนะของทรัพยากร รวมทั้งบุคลากรที่รับผิดชอบดูแลระบบอย่างเป็นระบบและเป็นลายลักษณ์อักษร			
3.มีการนำผลการประเมินทั้งด้านขีดสมรรถนะของอุปกรณ์ เครื่องมือ ระบบและบุคลากรมาเป็นแนวทางในการวางแผนทรัพยากรให้เกิดความคุ้มค่า รวมทั้งวางแผนในการพัฒนาบุคลากรด้าน IT			
4.มีการดำเนินการพัฒนาและปรับปรุงระบบตามที่วางแผนไว้			
5.มีการตรวจสอบ ติดตาม ประเมินผลการใช้ทรัพยากร รวมทั้งประเมินผลการปฏิบัติงานของบุคลากรเป็นระยะ			
6.มีการสรุปผลการประเมินในการใช้ทรัพยากร			

หมวดที่ 5 Service Catalogue Management

วัตถุประสงค์ : คือ คำอธิบายหน้าที่บริการต่อธุรกิจ เพื่อให้บริการ Catalogue การผลิตและการเก็บมีข้อมูลที่ถูกต้องในการปฏิบัติงานด้านบริการ และมีการเตรียมการเพื่อใช้ให้สามารถใช้งาน Service Catalogue Management ได้และเป็นการให้ข้อมูลสำคัญสาหรับทุกบริการอื่นๆ รวมถึงการจัดการกระบวนการรายละเอียด Service สถานะปัจจุบันและจุดที่ให้บริการในด้านต่างๆ

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการกำหนดคำอธิบายหน้าที่การให้บริการด้านเทคโนโลยีสารสนเทศ			
2.มีการจัดทำรายละเอียดการให้บริการ			
3.มีการปรับปรุงรายละเอียดการให้บริการและมีการทบทวนอย่างสม่ำเสมอและเมื่อมีการเปลี่ยนแปลงเหตุการณ์สำคัญขององค์กร			

หมวดที่ 6 Service Level Agreement

วัตถุประสงค์ : Service Level Management (SLM) เพื่อการเจรจาข้อตกลงระดับบริการกับลูกค้า และการบริการออกแบบตามออกแบบตามเป้าหมายที่ตกลงกัน โดยในการให้บริการจะแบ่งระดับการให้บริการออกเป็น Service Level Management ยังรับผิดชอบในการตรวจสอบให้แน่ใจว่าปฏิบัติระดับข้อตกลง และการหนุนสัญญาที่เหมาะสมกับการตรวจสอบและรายงานระดับบริการ มีความชัดเจนสามารถวัดผลการดำเนินงานด้านสารสนเทศจากระดับการให้บริการ

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
6.1 กระบวนการการได้มาซึ่งข้อตกลง			
1.มีการสำรวจความต้องการผู้ใช้ระบบและนำข้อมูลเข้าสู่การพิจารณาข้อตกลงกับตัวแทนผู้ใช้งาน หรือคณะกรรมการพัฒนาระบบฯ ปีละ 1ครั้ง โดยการประชุม หรือจัดทำแบบสอบถาม หรือการสัมภาษณ์ หรือการ Focus Group เป็นต้น			
2.มีการสรุปข้อตกลงการให้บริการ โดยกำหนดตัวชี้วัด แต่ละข้อตกลงให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้งประกาศให้ลูกค้าผู้ใช้บริการทราบทั่วกัน			
6.2 กระบวนการติดตามผลการดำเนินงานที่เป็นไปตามข้อตกลง			
3.มีการกำหนดแผนงาน/โครงการ/กิจกรรม/มาตรการในการดำเนินงานให้สอดคล้องเพื่อให้การดำเนินงานเป็นไปตามข้อตกลงการให้บริการอย่างครบถ้วน			
4.มีการกำหนดแผนการติดตามผลการดำเนินงานโดยจัดประชุมคณะกรรมการพัฒนาระบบฯ อย่างน้อย ปีละ 3 ครั้ง			
6.3 มีกระบวนการหรือการวัดผลการดำเนินงานเปรียบเทียบกับเป้าหมายข้อตกลง			
5.มีการประชุมติดตามผลของทีมงานหรือคณะกรรมการพัฒนาระบบฯ และมีการนำข้อมูลในการเข้าที่ประชุมอย่างน้อยการประชุมแต่ละครั้งต้องมีดังนี้ -รายงานผลการดำเนินงาน ปัญหา/อุปสรรค -พิจารณาหาแนวทางแก้ไขปัญหาร่วมกันเพื่อให้การดำเนินงานเป็นไปตามข้อตกลง -เปรียบเทียบกิจกรรมวัดผลกับเป้าหมายข้อตกลง			
6.4 มีกระบวนการทบทวนข้อตกลงในการให้บริการ			
6.มีการจัดประชุมสรุปผลการดำเนินงานและทบทวนข้อตกลงทุกสิ้นปีงบประมาณและรายงานการวางแผนเป็นข้อเสนอในงบประมาณใหม่พร้อมทั้งข้อตกลงในการดำเนินงานในอนาคต			

หมวดที่ 7 Capacity Management

วัตถุประสงค์ : เพื่อให้มั่นใจว่าผู้ให้บริการดำเนินการได้ตามที่ต้องการเช่น เวลา ความสามารถของระบบ โดยรองรับการทำงานได้ในปัจจุบันและอนาคตตามข้อตกลงที่ลูกค้าต้องการ และ เป็นการบริหารจัดการทรัพยากรที่เหมาะสมเกี่ยวข้องกับขีดความสามารถในการรองรับระบบการให้บริการสำหรับขีดความสามารถในการรองรับของระบบในปัจจุบันและอนาคต

ขอบเขต

มุ่งเน้นที่ประสิทธิภาพของทรัพยากรและกระบวนการที่เกี่ยวข้องกับขีดความสามารถของระบบ ซึ่งจะต้องประกอบด้วยส่วนปฏิบัติ(Operation) และการพัฒนา (Development) อันได้แก่

- ฮาร์ดแวร์ (Hardware) ได้แก่ Debase Server และ Web Server
- อุปกรณ์ของระบบเครือข่าย(Network Equipment) ได้แก่อุปกรณ์LAN, WAN ,Switch, Hub, Router, Modem,Frill wall
- ซอฟแวร์ (Software) ระบบปฏิบัติการและNetwork Software รวมทั้งโปรแกรมที่พัฒนาขึ้นภายในองค์กรหรือโปรแกรมสำเร็จรูปที่จัดซื้อมา ได้แก่ โปรแกรมระบบงานผ่านเครือข่ายอินเทอร์เน็ต โปรแกรมMYSQL ,โปรแกรมLinux,โปรแกรม mrtg,โปรแกรมPHP, โปรแกรม Apahe,โปรแกรม MySQL Front ,โปรแกรม winscp371 เป็นต้น
- บุคลากร(Human Resource) ได้แก่เจ้าหน้าที่ที่เกี่ยวข้อง

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
7.1การวางแผนเพิ่มขีดความสามารถของระบบ(Capacity planning)			
1.เมื่อมีความต้องการในการพัฒนาระบบเกิดขึ้นต้องกำหนดให้มีการประเมินทรัพยากรสำหรับเครื่องเซิร์ฟเวอร์ที่จำเป็นต้องจัดเตรียมเพิ่มเติมเพื่อให้รองรับกับระบบงานใหม่ที่เกิดขึ้น			
2.การคำนวณขนาดของหน่วยความจำสามารถประเมินได้จากขนาดของหน่วยความจำ = A x B x C โดยที่ A = จำนวนตัวแปรทั้งหมดของแอพพลิเคชันที่จำเป็นต้องใช้ B = ขนาดเฉลี่ยของตัวแปรของเหล่านั้น C = จำนวนผู้ใช้งานทั้งหมดที่ประเมินไว้			
7.2 การวางแผนเพิ่มขีดความสามารถของระบบ(Capacity planning)			
3.การคำนวณขนาดพื้นที่ดิสก์สามารถประเมินได้จาก ขนาดพื้นที่ดิสก์ = M x N x O โดยที่ M = จำนวนRecord ของTableที่ประเมินไว้ N = ขนาดของRecord O = จำนวน Tableทั้งหมดที่ประเมินไว้			
7.3 การจัดการทรัพยากรเพื่อให้สอดคล้องกับความต้องการทางธุรกิจ(Business capacity management)			
4.การวางแผนในการจัดซื้อจัดหา ทรัพยากรของระบบ ต้องมีการนำข้อมูลสถิติการรองรับขีดความสามารถของระบบมาวางแผนร่วมด้วย			

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
7.4 การติดตามประสิทธิภาพเพื่อให้เป็นในตามระดับการให้บริการ(resource capacity management)			
5.จัดทำแผนการเฝ้าระวังความพร้อมใช้การบริการอย่างต่อเนื่องโดยมี 1.แผนการตรวจสอบติดตามสถานภาพการให้บริการระบบเครือข่ายคอมพิวเตอร์ 2.มีวิธีขั้นตอนการตรวจสอบการใช้งานเครือข่ายที่ผิดปกติ			
6.มีการกำหนดค่าThreshold สำหรับทรัพยากรดังกล่าวเช่นอาจกำหนดไว้ที่ 60-80 เปอร์เซ็นต์ของทรัพยากรแต่ละอย่างเพื่อแจ้งเตือนเมื่อมีปริมาณการใช้งานถึงค่าที่			
7.5 การคาดการณ์ความต้องการทรัพยากรเพิ่มเติมในอนาคต (Modeling)			
7.กำหนดขั้นตอนปฏิบัติในการคาดการณ์ความต้องการทรัพยากรเพิ่มเติมในอนาคตและกำหนดไว้เป็นส่วนหนึ่งของนโยบายความมั่นคงปลอดภัย			

หมวดที่ 8 Availability Management

วัตถุประสงค์ : เพื่อกำหนดการวิเคราะห์แบบแผนวัดและปรับปรุงในทุกด้านให้พร้อมทั้งการบริการด้านไอที ให้มีการจัดการรับผิดชอบ เพื่อให้มั่นใจว่าโครงสร้างพื้นฐานไอที ทั้งหมดกระบวนการ เครื่องมือ ฯลฯ ให้เหมาะสมสำหรับการตกลง ซึ่งเป้าหมายหลักก็ เพื่อการเตรียมความพร้อมในทุกด้านของไอที และทำให้ทราบถึงการออกแบบโครงสร้างเพื่อรองรับความพร้อม ความเชื่อถือ ความถูกต้อง และ ความปลอดภัย และเป็นการบริหารจัดการกระบวนการเทคโนโลยีสารสนเทศของระบบทั้งหมดเพื่อให้มั่นใจได้ว่าการบริหารที่ให้กับผู้ใช้บริการมีความต่อเนื่องพร้อมใช้ในให้บริการทุกสถานการณ์

ขอบเขต

มุ่งประเด็นที่ความพร้อมใช้งานของทรัพยากรกระบวนการใดๆที่ส่งผลกระทบต่อความพร้อมใช้ในการให้บริการโดยมีรายละเอียดที่ต้องครอบคลุมดังนี้

1. การบำรุงรักษาและพัฒนาทรัพยากรได้แก่

1.1 ฮาร์ดแวร์)Hardware) ได้แก่ Debase Server และ Web Server

1.2 อุปกรณ์ของระบบเครือข่าย)Network Equipment) ได้แก่ อุปกรณ์ LAN ,WAN ,Switch ,Hub ,Router ,Modem ,Frill wall

1.3 ซอฟแวร์)Software) ระบบปฏิบัติการและNetwork Software รวมทั้งโปรแกรมที่พัฒนาขึ้นภายในองค์กรหรือโปรแกรมสำเร็จรูปที่จัดซื้อมาได้แก่โปรแกรมระบบรายงานระบบติดตามและเฝ้าระวังผู้ติดยาเสพติดผ่านเครือข่ายอินเทอร์เน็ต) บสต, (.โปรแกรมMYSQL,โปรแกรมLinux, โปรแกรมmrtg,โปรแกรมPHP ,โปรแกรมApahe ,โปรแกรมMySQL Front ,โปรแกรม winscp371 เป็นต้น

1.4บุคลากร(Human Resource) ได้แก่เจ้าหน้าที่ที่เกี่ยวข้อง

การเฝ้าระวังและป้องกันการเกิดเหตุการณ์ที่ไม่คาดคิดอันเป็นภัยคุกคามต่อการให้บริการต่อเนื่องกระบวนการในการกู้คืนระบบการให้บริการต่อเนื่องให้กลับมาใช้โดยรวดเร็วที่สุด

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการจัดทำแผนการเฝ้าระวังความพร้อมใช้การบริการอย่างต่อเนื่องโดยมี 1.1 แผนการตรวจสอบติดตามสถานภาพการให้บริการระบบเครือข่ายคอมพิวเตอร์			
1.2 มีวิธีขั้นตอนการตรวจสอบการใช้งานเครือข่ายที่ผิดปกติ			
2. มีแผนการบำรุงรักษาอุปกรณ์เครือข่ายคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง			
3.มีการกำหนดอุปกรณ์ที่สำคัญและจำเป็นต่อการให้บริการที่ครอบคลุมสอดคล้องกับแผนงานบำรุงรักษาอุปกรณ์			

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
4.มีการจัดทำขั้นตอนการบำรุงรักษาแต่ละอุปกรณ์เพื่อเป็นแนวทางผู้ปฏิบัติครบถ้วนทุกชิ้น			
5.มีการกำหนดขั้นตอนวิธีการแก้ไขการใช้งานเครือข่ายที่ผิดปกติอย่างชัดเจน ตามหมวด Incident & Problem & Service Deskเพื่อลดการใช้ดุลพินิจในการแก้ไขปัญหาระบบเครือข่ายผิดปกติและมีกระบวนการที่เป็นมาตรฐานชัดเจน			

หมวดที่ 9 IT Service Continuity Management

วัตถุประสงค์ : เพื่อรองรับการจัดการแผนธุรกิจต่อเนื่องโดยรวม และมั่นใจได้ว่าโครงสร้างพื้นฐานและ บริการสามารถครอบคลุมความต้องการและตอบรับกับข้อตกลงของเวลาในการดำเนินการของธุรกิจทำให้ธุรกิจที่ใช้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องจากภัยพิบัติ และเหตุการณ์ผิดปกติ ลดความเสียหายของการดำเนินงานองค์กร มีแผนรับมือความเสี่ยงที่จะเกิดและสร้างความพร้อมของทีมงานเมื่อเกิดภัยพิบัติขึ้น

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีกำหนดนโยบายหรือการปฏิบัติในการกู้คืนระบบกำหนดเพียงแต่ข้อตกลงที่ผู้ดูแลระบบต้องกู้คืนระบบภายในกี่วันที่เหมาะสมและสอดคล้องกับข้อตกลงการให้บริการ			
2.จัดทำแผนงานการกู้คืนข้อมูล			
3.มีการซักซ้อมอย่างน้อยปีละครั้ง			
4.มีเอกสารประกอบวิธีการสำรองข้อมูลที่ถูกต้องเป็นแนวทางการปฏิบัติงาน			
5.มีการฝึกอบรมบุคคลกรให้มีความตระหนักถึงกระบวนการสำรองและกู้คืนระบบรวมทั้งเอกสารการกู้คืนระบบที่สำคัญต่างๆ			

หมวดที่ 10 Information Security Management

วัตถุประสงค์ : เพื่อให้งานบริการมีความมั่นคงและปลอดภัยตามหลัก CIA (Certified Internal Auditor) โดยมีการจัดทำนโยบายมาตรฐานและขั้นตอนการปฏิบัติเพื่อทราบถึงความเสี่ยงในปัจจุบัน ลดช่องโหว่จากภัยคุกคามต่างๆ

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการประเมินความเสี่ยงระบบรักษาความปลอดภัย			
2.การประเมินความเสี่ยงต่อทรัพย์สินเทคโนโลยีสารสนเทศและข้อมูลข่าวสารขององค์การอย่างครบถ้วนและมีการจัดลำดับความเสี่ยง			
3.มีระบบมาตรการการรักษาความปลอดภัยเช่นจัดลำดับสิทธิการใช้งานเข้าถึงข้อมูล ความครบถ้วน ถูกต้อง ความพร้อมใช้งานของข้อมูล			
4.ระบบการควบคุม ได้แก่ นโยบายในการควบคุมความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้พนักงานและลูกค้าปฏิบัติตาม ,กำหนดบทบาทหน้าที่การบริหารจัดการความปลอดภัยเทคโนโลยีสารสนเทศ ,ระบวนการติดตาม ตรวจสอบ ควบคุมกำกับ ประเมินผล ดูแลบำรุงรักษา ผลของนโยบายนั้น,มีการอบรมทบทวนการรักษาความปลอดภัย, มีการประเมินความเสี่ยงและดำเนินการควบคุม พร้อมใช้ในการให้บริการ ,ผลการปฏิบัติในการควบคุมไม่ควรเปลี่ยนแปลงผลที่ได้ตกลงไว้ ,ปัญหาที่พบควรลงในรายงานตามระเบียบปฏิบัติของการแก้ไขป้องกันปัญหา			
5.การจัดทำเอกสารและการบันทึกผลการปฏิบัติและผลการควบคุมกำกับในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ			

หมวดที่ 11 Supplier Management

วัตถุประสงค์ : เพื่อให้มั่นใจว่าทุกสัญญาที่ทำกับซัพพลายเออร์ (Supplier) จะสนับสนุนความต้องการของธุรกิจและซัพพลายเออร์ทั้งหมดจะต้องทำตามสัญญาข้อผูกพันของบริษัท ให้ได้รับบริการที่มีคุณภาพจากผู้ให้บริการที่มีความพร้อม และ เหมาะสม กับความต้องการขององค์กร เพื่อประสิทธิภาพการติดต่อกับผู้ให้บริการ เพิ่มประสิทธิภาพของระบบงานเนื่องจากได้ผู้ให้บริการที่มีความเหมาะสม

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการกำหนดขั้นตอนการจัดซื้อจัดจ้าง ตามระเบียบทางราชการ แต่รูปแบบการกำหนดเงื่อนไข TOR ที่เป็นมาตรฐาน โดยเน้นให้ครอบคลุมดังนี้ 1.1 สิทธิ-หน้าที่ของคู่สัญญา 1.2 การแบ่งชำระงวดเงิน หรือการชำระเงินที่เป็นการขจัดความเสี่ยงของผู้ว่าจ้าง 1.3 คุณลักษณะที่ต้องการของการจ้างงาน/ของที่จะให้ส่งมอบ 1.4 ลิขสิทธิ์ในการจ้างทำของนั้นเป็นของใคร 1.5 ถ้ามีการผิดสัญญาจะเยียวยาความเสียหายกันอย่างไร			
2.มีการแต่งตั้ง/มอบหมายให้มีผู้ประสานงาน			
3.มีการวัดผลการปฏิบัติที่ไม่เป็นไปตามข้อกำหนดที่ครบถ้วน โดยเฉพาะมีขั้นตอนกระบวนการควบคุม-กำกับที่เหมาะสมและชัดเจน			

หมวดที่ 12 Transition Planning and Support

วัตถุประสงค์ : เพื่อการวางแผนและประสานงานทรัพยากรรวมถึงการปรับใช้หลัก Release เข้ามาภายใต้ต้นทุนที่คาดการณ์ ไว้ที่เวลาและการประเมินคุณภาพไว้แล้ว ได้แผนงานที่มีประสิทธิภาพก่อนที่จะดำเนินการ

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
มีการวางแผนการการพัฒนาและแผนการโอนถ่ายระบบที่พัฒนาสู่การปฏิบัติงานจริง			
1.มีการวิเคราะห์ความเป็นไปได้ในการพัฒนาระบบด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยประกอบด้วย 1.1 ด้านเทคนิค 1.2 ด้านปฏิบัติการ 1.3 ด้านการลงทุนหรือการตั้งงบประมาณ			
2.มีการนำผลการวิเคราะห์ความเป็นไปได้มานำเสนอต่อผู้บริหารหรือคณะกรรมการในการพัฒนาระบบ			
3.มีการวางแผนการพัฒนาและการถ่ายโอนระบบสู่การปฏิบัติงานจริงอย่างเป็นลายลักษณ์อักษรและมีความเป็นไปได้ในทางการปฏิบัติ			
4.มีการวิเคราะห์และประเมินความเสี่ยง รวมทั้งจัดทำแผนบริหารจัดการความเสี่ยงในการพัฒนาระบบและโอนถ่ายระบบสู่การปฏิบัติจริง			
5.มีการสรุปวิเคราะห์ผลการพัฒนาและแผนการโอนถ่ายระบบที่พัฒนาสู่การปฏิบัติงานจริง			

หมวดที่ 13 Service Asset and Configuration Management

วัตถุประสงค์ : เพื่อกำหนดและควบคุมส่วนประกอบของบริการและโครงสร้างพื้นฐาน มีการบำรุงรักษา และจัดทำเวอร์ชั่นในการกำหนดการติดตั้ง และเพื่อจัดหารวบรวมทรัพย์สินสารสนเทศและเหตุการณ์ปัญหาการเปลี่ยนแปลงและวิธีการจัดการที่มีอยู่ทั้งหมดให้เกิดความถูกต้องเชื่อถือได้ในการนำไปใช้กับทุกกระบวนการจัดการกับบริการต่างๆโดยการระบุควบคุมบำรุงรักษาและตรวจสอบ Version ของทุกConfiguration Item ที่มีอยู่และกำหนดการควบคุมส่วนประกอบต่างๆของService และInfrastructure รวมทั้งการดูแลรักษาความถูกต้องของ Configuration information

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการจัดทำแผนการบริหารจัดการองค์ประกอบพื้นฐานที่เกี่ยวข้องกับการให้บริการอย่างเป็นรูปธรรม			
2.มีการวิเคราะห์ออกแบบการจัดเก็บเป็นฐานข้อมูลที่แต่ละหัวข้อมีความสัมพันธ์กันเพื่อให้การจัดทำระบบข้อมูลนี้มีความสอดคล้องกับวิธีปฏิบัติ			
3.มีกระบวนการในการควบคุมองค์ประกอบพื้นฐานฯ เช่นการบันทึก ปรับปรุงแก้ไขเปลี่ยนแปลง ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต			
4.มีการรายงานสถานภาพขององค์ประกอบพื้นฐานฯอาจประกอบด้วย -ข้อมูลปัจจุบันและอดีตขององค์ประกอบพื้นฐานฯในระบบข้อมูล -มาตรฐานการตั้งค่าคอนฟิกกูเรชันของฮาร์ดแวร์หรือซอฟต์แวร์ต่างๆ -เวอร์ชันต่างๆของซอฟต์แวร์ที่ได้มีการปรับปรุง -ผู้รับผิดชอบในการเปลี่ยนแปลง -ประวัติการเปลี่ยนแปลงขององค์ประกอบหนึ่ง -ประวัติของปัญหาหรือIncident ที่เกิดขึ้นกับองค์ประกอบหนึ่ง			
5.มีการสำรวจข้อมูลนี้ให้มีความสอดคล้องกับข้อเท็จจริงหลังจากทำการสำรวจข้อมูลทั้งหมด เช่น สำรวจปีละ 1 ครั้ง			

หมวดที่ 14 Change Management

วัตถุประสงค์ : เพื่อมั่นใจว่าวิธีการมาตรฐาน และขั้นตอนปฏิบัติได้ถูกใช้อย่างมีประสิทธิภาพ และพร้อมการรับมือกับการเปลี่ยนแปลงโดยต้องได้รับผลกระทบต่อคุณภาพน้อยที่สุด

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการกำหนดให้นิยามระบุถึงเหตุการณ์ใดเป็นการเปลี่ยนแปลงที่มีผลกระทบต่อการให้บริการการของระบบเทคโนโลยีสารสนเทศที่ต้องมีการควบคุม โดยระบุถึงนิยามระดับและประเภทของการเปลี่ยนแปลงให้สอดคล้องกับการกำหนดขั้นตอนอำนาจการอนุมัติการเปลี่ยนแปลง			
2.มีการจดบันทึกเมื่อมีเหตุการณ์การเปลี่ยนแปลงแต่ละประเภท			
3.มีการประเมินผลกระทบ/การประเมินความเสี่ยง ก่อนการอนุมัติการเปลี่ยนแปลงอย่างเป็นรูปธรรมและลายลักษณ์อักษรและมีการกำหนดระดับอำนาจในการเปลี่ยนแปลงแต่ละประเภท			
4.มีการวางแผนการบริหารจัดการเปลี่ยนแปลงด้วยการนำข้อมูลสถิติมาวิเคราะห์ประกอบการวางแผนเพื่อความคุ้มค่า และต้องมีการประเมินและสรุปผลการดำเนินงานตามแผนงานที่ผ่านมาตามความเหมาะสมอย่างน้อยปีละ 1 ครั้ง			
5.มีการจัดเตรียมแผนถอยหลังกลับ (Back-out procedures) ในกรณีดำเนินการไม่สำเร็จ จะดำเนินการย้อนกลับอย่างไร			
6.มีการกำหนดบทบาทอำนาจหน้าที่ความรับผิดชอบแต่ละระดับอย่างชัดเจนเป็นลายลักษณ์อักษร โดยมีการจัดแบ่งระดับการเปลี่ยนแปลงตามข้อตกลงของทีมงาน เช่น การเปลี่ยนแปลงตามปกติ (Normal Change) ซึ่งไม่ใช่กรณีเร่งด่วน ผู้รับผิดชอบในการอนุมัติคือใคร แนวทางปฏิบัติอย่างไรอย่างย่อ ส่วนการเปลี่ยนแปลงเร่งด่วน(Emergency Change) ผู้รับผิดชอบในการอนุมัติคือใคร แนวทางปฏิบัติอย่างไรอย่างย่อ			
7.มีระเบียบขั้นตอนปฏิบัติในการอนุมัติตามกระบวนการการเปลี่ยนแปลงแต่ละระดับและทบทวนระเบียบปฏิบัติอย่างน้อยปีละ 1 ครั้ง			
8.มีการกลไกหรือกระบวนการควบคุมและการประสานงานการกระทำการเปลี่ยนแปลงที่ชัดเจนอย่างเป็นระบบและลายลักษณ์อักษร			

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
9.มีแนวทางการค้นหาสาเหตุและการแก้ไขในแต่ละระดับ การเปลี่ยนแปลงที่ไม่เป็นไปตามข้อกำหนดที่กำหนดไว้และต้องมีแนวทางในการแก้ไขการดำเนินการที่ไม่เป็นไปตามข้อกำหนดเพื่อลดความเสี่ยงในการสูญเสีย			
10.มีกระบวนการตรวจสอบ ควบคุมกำกับกระบวนการเฝ้าระวัง และการจัดเก็บผลการเปลี่ยนแปลงที่เกิดขึ้นรายงานต่างๆ เกี่ยวกับการเปลี่ยนแปลงที่เกิดขึ้น			

หมวดที่ 15 Release and Deployment Management

วัตถุประสงค์ : เพื่อวางแผนตารางเวลาและควบคุมการเคลื่อนไหวของเวอร์ชั่นที่จะทดสอบและสภาพแวดล้อม (Environment) ที่จะใช้ซึ่งเป็นเป้าหมายหลักของการจัดการ

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการกำหนดนโยบายและกระบวนการพัฒนาระบบที่เป็นขั้นตอน และเป็นลายลักษณ์อักษร (System development life cycle) ซึ่งประกอบด้วยการเริ่มต้นการพัฒนา การวิเคราะห์ การออกแบบ การพัฒนา การทดสอบ และการนำระบบงานขึ้นสู่การใช้งานจริง (Deployment/Release)มีกระบวนการการบริหารจัดการการวิเคราะห์ออกแบบ การพัฒนา ทดสอบ และติดตั้งโอนย้าย อย่างเป็นระบบและมีแผนโครงการบริหารจัดการการพัฒนาควบคุมกำกับและการขออนุมัติต่างๆอัน -กำหนดความถี่และชนิดของ Release -กำหนดบทบาทหน้าที่และภาระหน้าที่ของผู้ปฏิบัติ Release Management -การกำหนดสิทธิในการอนุญาตในการทำ Release -การกำหนดชื่อ และรายละเอียดของ Release -กำหนดวิธีการ group change เข้าไปในการทำ Release -กำหนดวิธีการ Build, installation, release distribution process -การตรวจสอบและการยอมรับการ Release -ประกาศใช้ทราบทั่วกัน			

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
2.มีการกำหนดให้มีการวิเคราะห์ ออกแบบระบบอย่างเป็นรูปธรรม โดยมีเอกสารที่เกี่ยวข้องกับการวิเคราะห์ออกแบบระบบ ตามวิธีการที่ผู้พัฒนาเลือกปฏิบัติตอนส่งมอบงาน			
3.เมื่อพัฒนาระบบงานเสร็จในเบื้องต้น มีการประกาศแจ้งผู้ใช้งานทราบอย่างเป็นทางการ			
4.มีแผนการอบรมสำหรับผู้ใช้งาน และต้องมีการปรับหลักสูตรอย่างต่อเนื่อง			
5.มีวิธีการประเมินหรือทดสอบหลังการติดตั้งระบบ			
6.มีกระบวนการแก้ไขปัญหาแนวทางปฏิบัติแก่ผู้ปฏิบัติงานที่ชัดเจนและกำหนดให้มีการบันทึกจดปัญหา สาเหตุ และแนวทางแก้ไขเป็นลายลักษณ์อักษร โดยเฉพาะกรณีมีการเปลี่ยนแปลงของระบบที่มีผลกระทบต่อองค์กรและผู้ใช้งานระบบมาก			

หมวดที่ 16 Service Validation and Testing Evaluation

วัตถุประสงค์ : เพื่อให้แน่ใจว่าการติดตั้งและบริการมีผลเป็นไปตามความคาดหวังของลูกค้าและยืนยันว่าการดำเนินงานไอที สามารถรองรับบริการใหม่ที่เกิดขึ้นมาได้

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.การวางแผนการทดสอบระบบและกำหนดวิธีการทดสอบระบบไว้เป็นลายลักษณ์อักษรอย่างเป็นรูปธรรมชัดเจนโดย -กำหนดวิธีการตรวจสอบผลและความสามารถ -ควรกำหนดบทบาทและความรับผิดชอบสำหรับการนำออกมาใช้งานเพื่อทดสอบการยอมรับและสภาพแวดล้อมที่ดีขึ้น -มีการกำหนดให้มีการรายงานผลการทดสอบระบบอย่างเป็นลายลักษณ์อักษรและส่งมอบเป็นทางการ			
2.มีแผนการติดตั้งระบบสู่การใช้งานจริงและแผนการทดสอบระบบอย่างเป็นทางการ			
3.มีการจัดทำเอกสารอธิบายบทบาท และขอบเขตหน้าที่ความรับผิดชอบและการทดสอบติดตั้งระบบงาน			
4.กำหนดระบุคุณลักษณะ เฉพาะและรายละเอียดของทุกรุ่นที่นำออกมาใช้งานและการจัดเก็บรวมทั้งการจัดกลุ่มการเปลี่ยนแปลง			
5.การติดตั้งระบบมีแผนสำรองแก้ไขปัญหาฉุกเฉินรองรับ หรือมีแผนถอยหลังกลับอย่างเป็นลายลักษณ์อักษร			

หมวดที่ 17 Knowledge Management

วัตถุประสงค์ : เพื่อรวบรวมวิเคราะห์ จัดเก็บและแบ่งปันความรู้ และข้อมูลภายในองค์กร หรือเป็นการจัดการความรู้เพื่อปรับปรุงประสิทธิภาพ โดยการลดความจำเป็นในการที่จะต้องทำการค้นหาความรู้อีกครั้ง และให้เป็นศูนย์รวมความรู้ทั้งหมด ทุกคนในองค์กรเข้ามาหาความรู้ได้ ซึ่งจะเป็นประโยชน์ ในการตอบปัญหาของ Service ที่ได้เปิดให้บริการอีกทางด้วย

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการจัดทำระบบ/หรือบันทึก ในการรวบรวมวิเคราะห์ จัดเก็บและแบ่งปันความรู้ และข้อมูลภายในองค์กร			
2.มีการนำปัญหาที่พบมาแลกเปลี่ยนเรียนรู้ โดยผ่านทางระบบอินเทอร์เน็ต หรือผ่านการจัดการประชุม สภากาแฟ พี่สอนน้อง เป็นต้น			
3.นำผลการแลกเปลี่นเรียนรู้มาปรับปรุงพัฒนางานด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ			

หมวดที่ 18 Service Operation

หมายถึง แนวทางและสถานะของวงจรการบริการ พื้นฐานและขบวนการงานบริการ การประยุกต์ใช้การจัดการโครงสร้าง การจัดการขบวนการ ปัจจัยความสำเร็จและความเสี่ยงในงานบริการ ประกอบด้วยกุญแจสำคัญ ได้แก่

- Event Management เพื่อตรวจสอบเหตุการณ์ โดยดูความเหมาะสมของเหตุการณ์ และพิจารณากิจกรรมควบคุมที่เหมาะสมเพื่อดำเนินการ Event Management และเพื่อใช้ในการกรองการจัดกลุ่มงาน และการตัดสินใจในการดำเนินการที่เหมาะสม

- Request Fulfillment เพื่อการปฏิบัติงานด้านการให้บริการคำร้องโดยให้เป็นมาตรฐานการเปลี่ยนแปลง เช่นขอเปลี่ยนรหัสผ่าน หรือขอข้อมูลต่างๆ

- Access management เพื่อให้ผู้ใช้สิทธิในการใช้บริการในขณะที่มีการป้องกันการเข้าถึงที่ไม่อนุญาตให้ผู้ใช้บริการอื่นเข้าใช้ได้ ใช้นโยบายที่กำหนดใน IT Security Management เข้า Management เป็นบางครั้งเรียกว่า Rights Management หรือ Identity Management

- Service Desk เป็น “ศูนย์กลางในการติดต่อ” Single Point Of Contact (SPOC) ในการรับแจ้งปัญหา (Incident) ที่เกิดขึ้นจากผู้ใช้บริการไอที โดยแจ้งผ่านทางโทรศัพท์ เว็บ อีเมล และ เป็นศูนย์กลางในการติดต่อสื่อสารและประสานงานระหว่างผู้ใช้งานไอที กับ IT Groups และทีมงาน Support เพื่อทำการแก้ไขปัญหาต่างๆ ที่ เกิดขึ้นให้สามารถใช้งานได้เป็นปกติโดยเร็วที่สุดเท่าที่จะเป็นไปได้

- Incident Management เป็นกระบวนการเกี่ยวกับการจัดการ Incident ทั้งหมด ตั้งแต่การรับปัญหา Incident ข้อผิดพลาดของระบบงานบริการไอที ต่างๆ ที่เกิดขึ้น การตอบคำถาม หรือข้อซักถามต่าง ๆ จากผู้ใช้งาน การแก้ไขปัญหา การส่งต่อการติดตามความคืบหน้าของปัญหา Incident ที่เกิดขึ้นเพื่อกู้คืน Service ให้กลับคืนสู่สภาวะปกติให้เร็วที่สุดเท่าที่จะทำได้และลดผลกระทบที่ส่งผลต่อการดำเนินทางธุรกิจให้น้อยที่สุด และต้องอยู่ภายในระดับการให้บริการที่ตกลงไว้ (SLA)

- Problem Management เพื่อใช้ในการจัดการวงจรของปัญหาทั้งหมด และการจัดการปัญหาในแง่ป้องกันเหตุการณ์ที่เกิดขึ้น และเพื่อการลดผลกระทบของเหตุการณ์ที่ไม่สามารถทำให้เชิงรุก วิเคราะห์ปัญหาการจัดการบันทึกเหตุการณ์และใช้ข้อมูลที่เก็บรวบรวมโดย IT Service Management กระบวนการเพื่อระบุแนวโน้มหรือปัญหาสำคัญต่างๆ

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
1.มีการกำหนดขั้นตอนและกระบวนการให้บริการในการรับปัญหาความช่วยเหลือที่ชัดเจนเป็นลายลักษณ์อักษรและแจ้งเวียนให้ทราบทั่วกัน			
2.มีการกำหนดเกณฑ์ระดับของปัญหาโดยคำนึงถึงความเร่งด่วนและผลกระทบ และกำหนดแนวทางการแก้ไขปัญหาในแต่ละระดับตามเกณฑ์ที่กำหนดอย่างชัดเจนเป็นลายลักษณ์อักษร			
3.มีการจัดลำดับความสำคัญในการแก้ไขปัญหาก่อน-หลัง			

หัวข้อหลักมาตรฐาน	กระบวนการในปัจจุบัน	คำแนะนำ/ข้อเสนอแนะ	คะแนนที่ได้
4.กำหนดให้มีการแยกแยะปัญหาและจัดลำดับความสำคัญของปัญหาที่ชัดเจนโดยให้คำนึงถึงความเร่งด่วนและผลกระทบของปัญหานั้นๆ			
5.มีการจดบันทึกปัญหาและเวลา ผู้รับเรื่อง และหากหาสาเหตุและวิธีการแก้ไขได้แล้วต้องมีการจดบันทึกและควรมีกระบวนการให้ทีมงานทราบทั่วกันในปัญหาเดิมๆ			
6.มีการนำข้อมูลสถิติปัญหาและการแก้ไขปัญหาไปวิเคราะห์และจัดทำแผนหาแนวทางป้องกันในอนาคต			
7.มีกระบวนการนำปัญหาที่หาทางแก้ไขได้แล้วนำไปจัดทำเป็นองค์ความรู้เผยแพร่ให้ทีมงาน			

คณะผู้จัดทำ
ชุมชนนักปฏิบัติผู้ตรวจสอบภายในงานเทคโนโลยีสารสนเทศ
กลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ

1.	นางกิ่งกาญจน์	ภู่ทองตระกูล	ผู้อำนวยการกลุ่มตรวจสอบภายใน
2.	นางณัฐณิชา	กลัมพสุต	นักวิชาการตรวจสอบภายในชำนาญการ
3.	นางสาววันเพ็ญ	กุลศรีชัย	นักวิชาการตรวจสอบภายใน
4.	นายชาริต	ตาลซาย	นักวิชาการตรวจสอบภายใน
5.	นายณัฐวุฒิ	พลอยสุข	เจ้าหน้าที่งานคอมพิวเตอร์

ภาคผนวก