สารบัญ

1. บทนำ

สำนักเทคโนโลยีสารสนเทศ กรมสุขภาพจิต มีความประสงค์จะดำเนินการจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ณ ศูนย์ข้อมูล (data center) เพื่อสนับสนุนนโยบายสำคัญของรัฐบาลตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องนั้นโดย กรมสุขภาพจิต มีแนวทางที่จะพัฒนาและจัดทำนโยบายความมั่นคงปลอดภัยของระบบสารสนเทศ อ้างอิงมาตรฐานสากล ISO/IEC 27001 ซึ่งเทียบเท่ามาตรฐานระดับพื้นฐานตามที่กฎหมายกำหนด ทั้งนี้เพื่อให้หน่วยงานสังกัดกรมสุขภาพจิตมีการปฏิบัติด้านความมั่นคงปลอดภัยได้อย่างถูกต้องตามกฎหมาย รองรับนโยบายการพัฒนาระบบสุขภาพจิต ดิจิทัลของกรมสุขภาพจิต ให้สามารถใช้งานระบบสารสนเทศอย่างมีคุณภาพ มีประสิทธิภาพ เสถียรภาพ และมีความพร้อมใช้งานและเข้าถึงข้อมูลได้อย่างรวดเร็ว ทุกที่ อย่างต่อเนื่อง เพื่อสร้างความเชื่อมั่นด้านความปลอดภัยในการเชื่อมโยงและการเข้าถึงระบบบริหารสุขภาพจิตของประชาชนและเพื่อป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้ข้อมูลสารสนเทศมีความถูกต้อง มีการรักษาความลับ และมีความพร้อมให้บริการอยู่ในระดับที่เหมาะสม

คู่มือระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual) ฉบับนี้ ถือเป็นส่วนหนึ่งของการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศสำหรับสำนักเทคโนโลยีสารสนเทศ กรมสุขภาพจิต เพื่อให้บริการสารสนเทศและการสื่อสาร ซึ่งอ้างถึงระบบบริหารความมั่นคงปลอดภัยสารสนเทศในภาพรวม ตามมาตรฐาน ISO/IEC 27001

2. ขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Scope of Information Security Management System)

สำนักเทคโนโลยีสารสนเทศ ได้ดำเนินการวิเคราะห์และประเมินเทคโนโลยีที่ใช้ของระบบที่มีความสำคัญต่อภารกิจและการบริการของสำนักฯ โดยระบุการขอรับรองระบบ ดังนี้

ขอบข่าย : ระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ณ ศูนย์ข้อมูล (data center)

ขอบเขต : สำนักเทคโนโลยีสารสนเทศ อาคาร 3 ชั้น 4 กรมสุขภาพจิต เลขที่ 88/20 หมู่ 4 ตำบลตลาดขวัญ อำเภอเมือง จังหวัดนนทบุรี 11000

3. นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Policy Statement)

เป้าหมายของนโยบายเพื่อป้องกันสินทรัพย์สารสนเทศ (Information Assets) ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศและการสื่อสารของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักเทคโนโลยีสารสนเทศ จากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้นทั้งที่โดยเจตนาหรือไม่เจตนาก็ตาม

เพื่อแสดงถึงข้อผูกพันด้านคุณภาพและความมุ่งมั่นของสำนักเทคโนโลยีสารสนเทศ ในการบริหารความมั่นคงปลอดภัยสารสนเทศ สำนักเทคโนโลยีสารสนเทศ จึงได้ประกาศนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) ดังนี้

“สำนักเทคโนโลยีสารสนเทศเป็นองค์กรที่เป็นศูนย์กลางในการดำเนินการและให้บริการด้านเทคโนโลยีดิจิทัล ที่มีความมั่งคงปลอดภัย และได้มาตรฐานสากล เพื่อสนับสนุนการดำเนินการตามพันธกิจของกรมสุขภาพจิต”

สำนักเทคโนโลยีสารสนเทศ ขอประกาศแนวทางปฏิบัติเพื่อให้สอดคล้องตามนโยบายมีดังนี้

1. กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และให้การสนับสนุนในเรื่องงบประมาณ ทรัพยากร ความรู้ความเข้าใจแก่บุคลากร

2. กำหนดแนวทางปฏิบัติที่เกี่ยวข้องในเรื่องของการรักษาความลับ (Confidentiality) โดยการทำสัญญารักษาความลับ, การรักษาความถูกต้อง ความสมบรูณ์ (Integrity) กำหนดสิทธิการเข้าถึงข้อมูลตามหน้าที่ที่เกี่ยวข้อง, ความพร้อมใช้งาน (Availability) มีระบบ อุปกรณ์สำรอง, การกำหนดสิทธิการเข้าออกพื้นที่เพื่อป้องกันการโจรกรรมข้อมูล กำหนดรหัสการเข้าใช้งาน และปรับปรุงตามนโยบายองค์กร

3. สื่อสาร ให้ความรู้ความเข้าใจด้านกฎหมาย ข้อบังคับ ข้อตกลงที่เกี่ยวข้องกับการให้บริการด้านเทคโนโลยีสารสนเทศ ความต่อเนื่อง ข้อมูลความปลอดภัย

4. แต่งตั้งคณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีการขับเคลื่อนนโยบายและรักษาระบบการบริหารงานเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

5. กำหนดเป็นหัวข้อการอบรมปฐมนิเทศบุคลากรใหม่ และทบทวนในที่ประชุมสำนักเทคโนโลยีสารสนเทศประจำปี

6. ดำเนินการซักซ้อมแผนความต่อเนื่อง พัฒนา ปรับปรุง ทดสอบให้เหมาะสมและมั่นใจว่าพร้อมรับในทุกสถานการณ์

7. มีการทำข้อตกลงกับผู้ให้บริการภายนอก ผู้ขายอุปกรณ์ ในการให้ความร่วมมือเมื่อเกิดอุบัติการณ์ที่ส่งผลต่อความปลอดภัยด้านข้อมูลสารสนเทศในการให้บริการ และทบทวนข้อตกลงปีละ 1 ครั้ง

8. ผู้ที่เกี่ยวข้องทำการวางแผน และจัดการเรื่องความปลอดภัยของข้อมูล ระบบโครงข่าย เครื่องมือ และอุปกรณ์ให้อยู่ในระบบมาตรฐานซึ่งเป็นที่ยอมรับและเชื่อถือได้ รวมทั้งให้การดูแลเป็นพิเศษ

9. การเก็บรักษาความปลอดภัยของข้อมูล จะต้องระบุไว้เป็นส่วนหนึ่งในสัญญาบริการที่สำนักเทคโนโลยีสารสนเทศ ทำกับผู้ใช้บริการ ไม่ว่าจะเป็นการบริการประเภทใด ซึ่งจะต้องถือปฏิบัติโดยเคร่งครัด

10. มาตรการเกี่ยวกับความปลอดภัยของข้อมูล ถือเป็นหน้าที่ของบุคลากรของสำนักเทคโนโลยีสารสนเทศทุกคน จะต้องปฏิบัติตามและหากมีการฝ่าฝืน ให้ถือว่าเป็นการกระทำผิดวินัยอย่างร้ายแรง โดยสำนักเทคโนโลยีสารสนเทศถือเป็นหน้าที่ที่จะต้องแจ้งให้บุคลากรทุกคนทราบถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล

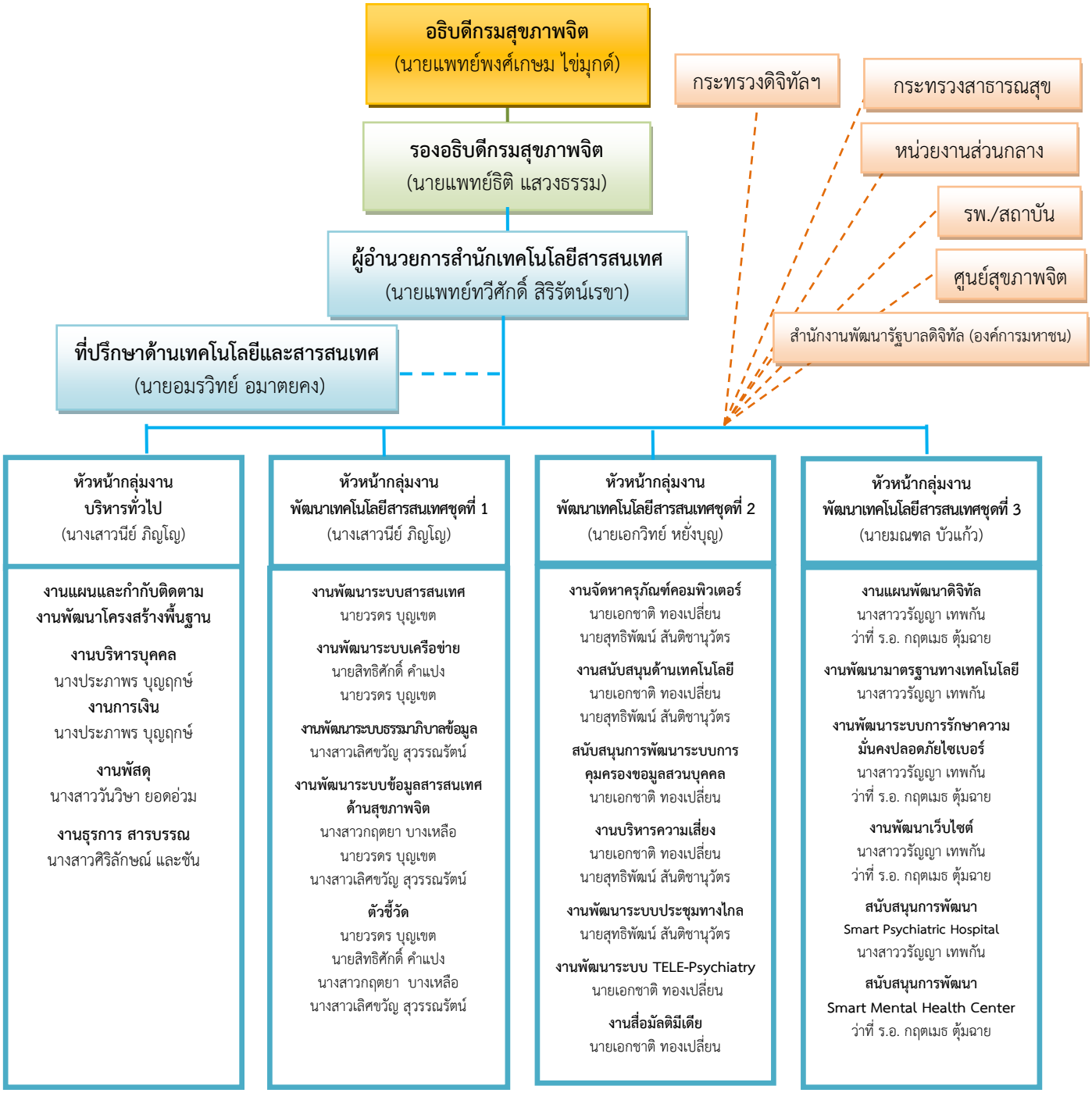
11. สำนักเทคโนโลยีสารสนเทศมีหน้าที่ในการจัดเก็บและเก็บรักษาข้อมูลของผู้ใช้บริการตามแบบ และวิธีการที่ได้ทำความตกลงร่วมกันไว้ระหว่างสำนักเทคโนโลยีสารสนเทศกับผู้ใช้บริการ รวมทั้งการไม่เปิดเผยข้อมูลใดๆ ที่มิได้รับความยินยอมจากผู้ใช้บริการสู่สาธารณชน หรือบุคคลภายนอก เพื่อไม่มีการรั่วไหล หรือการสูญหายของข้อมูลของผู้ใช้บริการ ไม่ว่าในกรณีใดๆ

12. สำนักเทคโนโลยีสารสนเทศจะต้องจัดทำเอกสารที่ระบุไว้อย่างชัดเจนว่าบุคลากรจะไม่นำข้อมูลของสำนักเทคโนโลยีสารสนเทศหรือข้อมูลของผู้ใช้บริการไปเปิดเผยแก่บุคคลภายนอก หรือที่ใดๆ หากมิได้รับความยินยอมจากสำนักเทคโนโลยีสารสนเทศหรือจากผู้ใช้บริการ

นโยบายและแนวปฏิบัตินี้ บุคลากรของสำนักเทคโนโลยีสารสนเทศจะต้องให้ความร่วมมือ และถือปฏิบัติร่วมกัน เพื่อให้มั่นใจว่าสำนักเทคโนโลยีสารสนเทศจะรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และมีการปรับปรุงประสิทธิภาพอย่างต่อเนื่อง

4. โครงสร้างคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Organization Structure)

โครงสร้างคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ของสำนักเทคโนโลยีสารสนเทศ ดังนี้



5. ความต้องการสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Requirements for ISMS)

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ต้องมีการกำหนดจัดตั้งนำมาใช้งาน บำรุงรักษาและปรับปรุงอย่างต่อเนื่อง โดยกำหนดจากความต้องการ และจุดประสงค์ ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ กระบวนการขององค์กรที่ใช้ ขนาดและโครงสร้างของ องค์กร ซึ่งสามารถเปลี่ยนแปลงได้ตลอดเวลา

6. บริบทขององค์กร (Context of the organization)

6.1 ความเข้าใจในองค์กรและบริบทขององค์กร (Understanding the organization and its context) องค์กรต้องกำหนดประเด็นทั้งภายในและภายนอกที่มีผลกระทบกับจุดประสงค์และความสามารถในการบรรลุถึงผลลัพธ์ตามเป้าหมายของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

6.2 ความเข้าใจในความต้องการ และความคาดหวังขององค์กรที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties) องค์กรต้องกำหนด

6.2.1 องค์กรที่เกี่ยวข้องซึ่งเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

6.2.2 ความต้องการขององค์กรที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

6.2.3 นำข้อกำหนดเหล่านั้นมาดำเนินการในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

หมายเหตุ ความต้องการขององค์กรที่เกี่ยวข้องอาจรวมถึงกฎหมาย กฎระเบียบ และภาระ ผูกพันตามสัญญา

6.3 การกำหนดขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system) องค์กรต้องกำหนดขอบเขตและการจัดตั้งขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยระบุเป็นลายลักษณ์อักษร

เมื่อกำหนดขอบเขต องค์กรจะพิจารณา

6.3.1 ประเด็นทั้งภายในและภายนอกองค์กร ซึ่งอ้างถึง 6.1

6.3.2 ความต้องการซึ่งอ้างถึง 6.2 และ

6.3.3 ความเชื่อมต่อกันและความเกี่ยวข้องระหว่างกิจกรรม ที่ดำเนินการโดยองค์กรและ โดยหน่วยงานอื่น

6.4 ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) องค์กรต้องจัดตั้งนำมาใช้งาน รักษาไว้ และพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

7. ความเป็นผู้นำ (Leadership)

7.1 ความเป็นผู้นำและความมุ่งมั่น (Leadership and commitment)

ผู้บริหารระดับสูง ได้ให้คำมั่นและแสดงให้เห็นถึงความเป็นผู้นำต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศโดย

7.1.1 รับรองว่านโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดขึ้นสอดคล้องกับทิศทางยุทธศาสตร์ขององค์กร

7.1.2 รับรองว่ามีการบูรณาการความต้องการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศในกระบวนการขององค์กร

7.1.3 รับรองว่าให้การสนับสนุนทรัพยากรที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

7.1.4 สื่อสารความสำคัญของประสิทธิภาพระบบบริหารความมั่นคงปลอดภัยสารสนเทศและสอดคล้องกับความต้องการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

7.1.5 ให้ทิศทางและสนับสนุนบุคลากรเพื่อให้ระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีประสิทธิภาพ

7.1.6 ส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง

7.1.7 สนับสนุนอื่นๆ ที่แสดงถึงความเป็นผู้นำตามความรับผิดชอบ

7.2 นโยบาย (Policy)

ผู้บริหารระดับสูง จะกำหนดนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

7.2.1 เหมาะสมกับวัตถุประสงค์ขององค์กร

7.2.2 ครอบคลุมถึงวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ หรือเตรียมกรอบสำหรับจัดตั้งวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งอ้างถึง 8.1

7.2.3 ครอบคลุมถึงความมั่นคงในการบรรลุถึงความต้องการเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

7.2.4 ครอบคลุมถึงความมุ่งมั่นในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ อย่างต่อเนื่อง

7.2.5 มีการจัดทำข้อมูลเป็นเอกสารหรือเอกสารอิเล็กทรอนิกส์

7.2.6 มีการสื่อสารภายในองค์กร

7.2.7 มีการเผยแพร่ประชาสัมพันธ์ให้ผู้เกี่ยวข้อง ตามความเหมาะสม

7.3 บทบาทหน้าที่ ความรับผิดชอบและการมอบอำนาจ (Organizational roles, responsibilities and authorities)

ผู้บริหารระดับสูงจะต้องมั่นใจว่าความรับผิดชอบและอำนาจหน้าที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศได้ถูกมอบหมายและสื่อสารอย่างครบถ้วน ผู้บริหารระดับสูงจะต้องมอบหมายความรับผิดชอบและอำนาจหน้าที่โดย

7.3.1 ต้องมั่นใจว่าระบบบริหารความมั่นคงปลอดภัยสารสนเทศสอดคล้องกับความต้องการตามมาตรฐาน ISO/IEC 27001

7.3.2 มีการรายงานประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศต่อ ผู้บริหารระดับสูง

หมายเหตุ ผู้บริหารระดับสูงอาจมอบหมายความรับผิดชอบและอำนาจหน้าที่ในการรายงานประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศให้บุคลากรภายในองค์กร

8. การวางแผน (Planning)

8.1 ขั้นตอนในการระบุความเสี่ยงและโอกาส (Actions to address risks and opportunities)

8.1.1 บททั่วไป

เมื่อวางแผนสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ องค์กรจะต้องพิจารณาประเด็นที่อ้างถึงใน 6.1 และความต้องการที่อ้างถึงใน 6.2 และกำหนด ความเสี่ยงและโอกาสที่ต้องจัดการเพื่อ

8.1.1.1 ให้มั่นใจว่าระบบบริหารความมั่นคงปลอดภัยสารสนเทศสามารถบรรลุเป้าหมายตามที่ตั้งไว้

8.1.1.2 ป้องกันหรือลดผลกระทบที่ไม่ปรารถนา

8.1.1.3 บรรลุผลของการปรับปรุงอย่างต่อเนื่อง องค์กรจะต้องวางแผนดังนี้

8.1.1.4 ขั้นตอนการจัดการความเสี่ยงและโอกาส

8.1.1.5 วิธีการ

1) บูรณาการและการนำกระบวนการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศมาใช้งาน

2) ประเมินความมีประสิทธิผลของการดำเนินการ

8.1.2 การระบุความเสี่ยงของการรักษาความมั่นคงปลอดภัยสารสนเทศ องค์กรมีการกำหนดและประยุกต์ใช้กระบวนการจัดการความเสี่ยง

8.1.2.1 จัดตั้งและบำรุงรักษาเกณฑ์การประเมินความเสี่ยงของการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึง

1) เกณฑ์การยอมรับความเสี่ยง

2) เกณฑ์สำหรับการประเมินความเสี่ยง

8.1.2.2 เพื่อให้มั่นใจว่ากระบวนการประเมินความเสี่ยงสามารถทำซ้ำได้ โดยได้ผลลัพธ์แบบเดิม และผลลัพธ์สามารถเปรียบเทียบได้

8.1.2.3 การระบุความเสี่ยงของการรักษาความมั่นคงปลอดภัยสารสนเทศ

1) ประยุกต์ใช้กระบวนการประเมินความเสี่ยง เพื่อระบุความเสี่ยงที่เกี่ยวกับการทำให้สูญเสียความลับ (Confidential) ความถูกต้อง สมบูรณ์ (Integrity) และ ความพร้อมใช้ (Availability)

2) ระบุเจ้าของความเสี่ยง

8.1.2.4 การวิเคราะห์ความเสี่ยงของความปลอดภัยข้อมูล

1) ประเมินความเป็นไปได้ของผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงที่ระบุไว้ใน 8.1.2.3 1)

2) ประเมินความเป็นไปได้ที่เป็นจริงของการเกิดความเสี่ยงที่ระบุใน 8.1.2.3 1)

8.1.2.5 ประเมินความเสี่ยงของความปลอดภัยข้อมูล

1) เปรียบเทียบผลของการวิเคราะห์ความเสี่ยงตามเกณฑ์การประเมินความเสี่ยงที่กำหนดไว้ใน 8.1.2.1

2) จัดลำดับความเสี่ยงที่วิเคราะห์เพื่อจัดการความเสี่ยงองค์กรมีการเก็บรักษาเอกสารข้อมูลเกี่ยวกับกระบวนการประเมินความเสี่ยงของความมั่นคงปลอดภัยสารสนเทศ

8.1.3 การจัดการความเสี่ยง

องค์กรมีการกำหนดและประยุกต์ใช้กระบวนการจัดการความเสี่ยง

8.1.3.1 เลือกแนวทางในการจัดการความเสี่ยงที่เหมาะสมตามผลของการประเมินความเสี่ยง

8.1.3.2 กำหนดมาตรการทั้งหมดที่จำเป็นในการนำแนวทางในการจัดการความเสี่ยงมาใช้

8.1.3.3 เปรียบเทียบมาตรการที่ระบุใน 8.1.3.2 กับมาตรการของมาตรฐาน Annex A และตรวจสอบว่าไม่มีมาตรการที่จำเป็นถูกละเว้น

8.1.3.4 จัดทำคำประกาศการนำไปใช้งาน (Statement of Applicability – SOA) ซึ่งประกอบด้วยมาตรการที่จำเป็น (ตามที่ระบุใน 8.1.3.2 และ 8.1.3.3) และการให้เหตุผลสำหรับมาตรการที่ใช้และมาตรการที่ละเว้นจาก Annex A

8.1.3.5 กำหนดแผนการจัดการความเสี่ยงของระบบริหารความมั่นคงปลอดภัยสารสนเทศ

8.1.3.6 กำหนดเจ้าของความเสี่ยงและอนุมัติแผนการจัดการความเสี่ยง และยอมรับความเสี่ยงที่ยังคงหลงเหลือ

ทั้งนี้ในการบริหารความเสี่ยงของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) จะเป็นไปตามแนวทางการประเมินความเสี่ยงสารสนเทศ (Risk Assessment Approach) ในวิธีปฏิบัติงาน (Work Instruction) เรื่อง แนวทางการประเมินความเสี่ยงสารสนเทศ (Risk Assessment Approach)

8.2 วัตถุประสงค์และการวางแผน เพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security objectives and planning to achieve them) องค์กรจะจัดตั้ง วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในฟังก์ชั่นและระดับที่เกี่ยวข้อง วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศจะต้อง

- สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
- สามารถวัดผลได้ (หากปฏิบัติได้)

- คำนึงถึงความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และผลจากการประเมินความเสี่ยงและการจัดการความเสี่ยง

- มีการสื่อสารกับผู้ที่เกี่ยวข้อง

- มีการปรับปรุงตามความเหมาะสม องค์กรมีการเก็บรักษาข้อมูลเอกสารหลักฐานเกี่ยวกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

8.3 การวางแผนการเปลี่ยนแปลง

เมื่อองค์กรกำหนดความจำเป็นในการเปลี่ยนแปลงระบบความมั่นคงปลอดภัยสารสนเทศ การเปลี่ยนแปลงต้องดำเนินการตามแผนที่วางไว้

9. การสนับสนุน (Support)

9.1 ทรัพยากร (Resources)

9.2 องค์กรมีการระบุและเตรียมทรัพยากรที่จำเป็นในการจัดตั้งระบบบริหารความมั่นคงปลอดภัย นำมาใช้งาน บำรุงรักษา และพัฒนาอย่างต่อเนื่อง

9.3 ความสามารถ (Competence)

องค์กรดำเนินการดังนี้

9.3.1 ระบุความสามารถของบุคลากรที่จำเป็นในการปฏิบัติงานภายใต้มาตรการที่มีผลกับประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

9.3.2 ทำให้มั่นใจว่าบุคลากรมีความสามารถพื้นฐานที่เหมาะสมด้านการศึกษา การฝึกอบรม และประสบการณ์

9.3.3 ดำเนินการให้ได้รับความสามารถที่จำเป็นในการปฏิบัติงาน และประเมินผล ประสิทธิภาพของการดำเนินการตามความเหมาะสม

9.3.4 เก็บรักษาเอกสารหลักฐานของความสามารถนั้น ๆ

หมายเหตุ ตัวอย่างการดำเนินการที่เหมาะสม เช่น วางแผนการฝึกอบรม การให้คำปรึกษา หรือมอบหมายงานให้บุคลากรที่มีอยู่ หรือว่าจ้างผู้ที่มีความสามารถนั้น

9.4 ความตระหนัก (Awareness) บุคลากรที่ปฏิบัติงานภายใต้มาตรการขององค์กรจะต้องตระหนักถึง

9.4.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

9.4.2 บุคลากรให้การสนับสนุนเพื่อให้ระบบบริหารความมั่นคงปลอดภัยมีประสิทธิภาพ รวมถึงประโยชน์ที่จะได้รับเมื่อสามารถปรับปรุงประสิทธิภาพของระบบบริหารความ มั่นคงปลอดภัยสารสนเทศได้

9.4.3 การดำเนินการที่ไม่สอดคล้องกับความต้องการของระบบบริหารความมั่นคงปลอดภัย สารสนเทศ

9.5 การติดต่อสื่อสาร (Communication)

องค์กรระบุความจำเป็นของทั้งการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับระบบ บริหารความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นไปตามวิธีปฏิบัติงาน (Work Instruction) เรื่อง การสื่อสารขององค์กร โดยคลอบคลุมสิ่งต่อไปนี้

9.5.1 สิ่งที่จะสื่อสาร

9.5.2 เวลาที่จะสื่อสาร

9.5.3 ผู้ที่จะสื่อสาร

9.5.4 ผู้ที่รับหน้าที่ผู้สื่อสาร

9.5.5 กระบวนการ ของการสื่อสารที่มีประสิทธิภาพ

9.6 เอกสารหลักฐาน (Documented information)

9.6.1 บททั่วไป

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กรจะครอบคลุมถึง

9.6.1.1 ข้อมูลเอกสารที่ต้องการตามมาตรฐาน ISO/IEC 27001

9.6.1.2 ข้อมูลเอกสารที่ระบุโดยองค์กรว่ามีความจำเป็นต่อประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

9.6.2 การจัดทำและปรับปรุง

เมื่อมีการจัดทำและปรับปรุงข้อมูลเอกสาร องค์กรจะต้องมั่นใจว่า

9.6.2.1 มีการระบุและคำอธิบาย (เช่น หัวเรื่อง วันที่ ผู้จัดทำ หรือหมายเลขอ้างอิง)

9.6.2.2 จัดรูปแบบ (เช่น ภาษา ซอฟต์แวร์เวอร์ชั่น กราฟฟิก) และสื่อ เช่น กระดาษ อิเล็กทรอนิกส์)

9.6.2.3 มีการทบทวนและอนุมัติตามเหมาะสม

9.6.3 การควบคุมเอกสาร

ข้อมูลเอกสารที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีการควบคุมเพื่อให้มั่นใจว่า

9.6.3.1 พร้อมใช้และเหมาะสมสำหรับการใช้งานในสถานที่ และเมื่อจำเป็น

9.6.3.2 มีการป้องกันอย่างพอเพียง (เช่น จากการเปิดเผยความลับ การใช้งานอย่างไม่เหมาะสม หรือขาดความสมบูรณ์) ในการควบคุมเอกสาร องค์กรจะระบุกิจกรรมดังต่อไปนี้

9.6.3.3 การแจกจ่าย การเข้าถึง การแก้ไข และการใช้งาน

9.6.3.4 การจัดเก็บและการป้องกัน รวมถึงการดำรงไว้ซึ่งความชัดเจน

9.6.3.5 การควบคุมการเปลี่ยนแปลง (เช่น การควบคุมเวอร์ชั่น)

9.6.3.6 การเก็บรักษาและการทำลาย

เอกสารที่มาจากภายนอก มีการกำหนดตามความจำเป็นสำหรับการวางแผนและการปฏิบัติงานสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ จะต้องมีการระบุและควบคุมตามความเหมาะสม

การเข้าถึง หมายถึง การตัดสินใจในการให้สิทธิ์ในการดูเอกสารเท่านั้น หรือการให้สิทธิ์และอำนาจในการดูแลแก้ไขเอกสาร

เอกสารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) รวมถึง แบบฟอร์ม และรูปแบบการบันทึกข้อมูลต่างๆ จะต้องมีการป้องกัน ควบคุม บำรุงรักษา และจัดการเอกสารให้เป็นไปตามระเบียบการปฏิบัติงาน (Quality Procedure) เรื่องการควบคุมเอกสาร

10. การดำเนินการ (Operation)

10.1 การวางแผนและควบคุมการดำเนินการ (Operational planning and control)

องค์กรจะต้องวางแผน จัดทำ และควบคุมกระบวนการที่จำเป็น เพื่อให้เป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศและปฏิบัติตามข้อ 8.1 องค์กรจะต้องมีแผนการจัดทำเพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดในข้อ 8.2

- จัดทำเกณฑ์สำหรับกระบวนการ
- ดำเนินการควบคุมกระบวนการตามเกณฑ์ที่กำหนด

องค์กรจะเก็บเอกสารข้อมูลให้เป็นความตามขอบเขตที่จำเป็นเพื่อให้กระบวนการต่างๆ เป็นไปตามแผนงานที่วางไว้

หน่วยงานจะต้องควบคุมการปรับแผนและทบทวนผลของการเปลี่ยนแปลงที่ไม่ได้เจตนา เพื่อจัดการผลกระทบที่อาจจะเกิดขึ้น ตามความจำเป็น

องค์กรต้องมั่นใจว่ากระบวนการจ้างหน่วยงานอื่นดำเนินการจะมีการกำหนดและควบคุม

10.2 การประเมินความเสี่ยง (Information security risk assessment)

องค์กรจะต้องจัดทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามที่ได้ วางแผนไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ หรือเกิดขึ้นโดยคำนึงถึงเกณฑ์ที่กำหนดไว้ในข้อ 8.1.2.1

องค์กรจะต้องเก็บรักษาเอกสารข้อมูลของผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

10.3 การจัดการความเสี่ยง (Information security risk treatment)

องค์กรจะต้องนำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศมาใช้งาน องค์กรจะต้องเก็บรักษาเอกสารข้อมูลของผลการจัดการความเสี่ยงด้านความมั่นคงปลอดภัย

11. การประเมินผลการดำเนินการ (Performance evaluation)

11.1 การเฝ้าระวัง การวัดผล การวิเคราะห์และประเมินผล (Monitoring, measurement, analysis and evaluation) องค์กรจะต้องประเมินผลการปฏิบัติงานด้านความมั่นคงปลอดภัย สารสนเทศและประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

องค์กรจะต้องกำหนด

11.1.1 ความจำเป็นในการเฝ้าระวัง และวัดผล รวมถึงกระบวนการและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ

11.1.2 วิธีการเฝ้าระวัง วัดผล วิเคราะห์ และประเมินผล ตามความเหมาะสม เพื่อให้ได้ผลที่ถูกต้อง

หมายเหตุ วิธีการที่เลือกจะต้องสามารถเปรียบเทียบผลลัพธ์ได้ และทำซ้ำได้ผลลัพธ์ที่ถูกต้อง

11.1.3 ช่วงเวลาในการเฝ้าระวังและวัดผล

11.1.4 ผู้เฝ้าระวังและวัดผล

11.1.5 ผลที่ได้จากการเฝ้าระวังและวัดผลแล้ว จะต้องมีการวิเคราะห์และประเมินผล

11.1.6 ผู้ที่วิเคราะห์และประเมินผล องค์กรจะเก็บรักษาเอกสารข้อมูลการเฝ้าระวังและวัดผลไว้เป็นหลักฐาน

11.2 การตรวจสอบภายใน (Internal audit)

องค์กรจะดำเนินการตรวจติดตามภายในตามรอบระยะเวลาที่กำหนดไว้ เพื่อเตรียมข้อมูล ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ดังนี้

11.2.1 เพื่อให้สอดคล้องกับ

- ความต้องการด้านระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร
- ข้อกำหนดในมาตรฐาน ISO/IEC 27001

11.2.2 มีการนำมาใช้งานและบำรุงรักษาอย่างมีประสิทธิภาพ

11.2.3 มีการวางแผน จัดตั้ง นำมาใช้งานและบำรุงรักษาแผนการตรวจติดตาม รวมถึงความถี่ วิธีการ ความรับผิดชอบ ความต้องการของแผนและการรายงาน แผนการตรวจ ติดตามที่จะพิจารณาถึงความสำคัญของกระบวนการที่เกี่ยวข้องและผลจากการตรวจติดตามครั้งก่อน

11.2.4 กำหนดเกณฑ์และขอบเขตการตรวจติดตาม

11.2.5 เลือกผู้ตรวจติดตามและตรวจติดตามเพื่อให้มั่นใจว่าเป็นไปตามวัตถุประสงค์และ ความยุติธรรมของกระบวนการตรวจติดตาม

11.2.6 ทำให้มั่นใจว่าผลของการตรวจติดตามได้รับการรายงานต่อผู้บริหารที่เกี่ยวข้อง

11.2.7 การเก็บรักษาข้อมูลเอกสารแผนการตรวจติดตามและผลการตรวจติดตามไว้เป็น หลักฐาน

11.3 การทบทวนของฝ่ายบริหาร (Management review)

ผู้บริหารระดับสูงต้องทบทวนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มีการดำเนินการที่เหมาะสมพอเพียงและสัมฤทธิ์ผล การทบทวนของฝ่ายบริหารจะต้องพิจารณาดังนี้

11.3.1 สถานะของการดำเนินการทบทวนของฝ่ายบริหารครั้งก่อน

11.3.2 การเปลี่ยนแปลงทั้งภายในและภายนอกที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

11.3.3 การเปลี่ยนแปลงความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียที่เกี่ยวระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

11.3.4 ข้อเสนอแนะเพื่อดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศรวมถึงแนวโน้ม ดังต่อไปนี้

- การไม่เป็นไปตามข้อกำหนด (Nonconformities) และการแก้ไข (Corrective Action)
- ผลการเฝ้าระวังและวัดผล
- ผลการตรวจติดตาม
- การบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

11.3.5 ข้อเสนอแนะจากผู้ที่เกี่ยวข้อง

11.3.6 ผลจากการประเมินความเสี่ยงและสถานะของแผนการจัดการความเสี่ยง

11.3.7 โอกาสในการพัฒนาอย่างต่อเนื่อง ผลลัพธ์ของการทบทวนของฝ่ายบริหารจะรวมถึงการตัดสินใจที่เกี่ยวข้องกับโอกาสในการพัฒนาอย่างต่อเนื่องและความจำเป็นในการเปลี่ยนแปลงระบบบริหารความมั่นคงปลอดภัยสารสนเทศ องค์กรจะเก็บรักษาเอกสารข้อมูลการทบทวนของฝ่ายบริหารไว้เป็นหลักฐาน

12. การปฏิบัติการแก้ไข (Improvement)

12.1 ความไม่สอดคล้องกับข้อกำหนดและการปฏิบัติการแก้ไข (Nonconformity and corrective action)

เมื่อเกิดความไม่สอดคล้องกับข้อกำหนด องค์กรจะต้อง

12.1.1 ดำเนินการกับความไม่สอดคล้องกับข้อกำหนดอย่างเหมาะสม

- ดำเนินการเพื่อควบคุมและแก้ไข
- ดำเนินการกับผลลัพธ์

12.1.2 ประเมินการดำเนินการกำจัดสาเหตุของความไม่สอดคล้องกับข้อกำหนด เพื่อไม่ให้เกิดซ้ำหรือเกิดที่อื่นอีก

- ทบทวนความไม่สอดคล้อง
- ระบุสาเหตุของความไม่สอดคล้อง

- ระบุหากเกิดความไม่สอดคล้องคล้ายกับที่เคยเกิดขึ้นหรืออาจจะเกิดขึ้นได้

12.1.3 ดำเนินการตามความจำเป็น

12.1.4 ทบทวนประสิทธิผลของการแก้ไข

12.1.5 ปรับเปลี่ยนระบบบริหารความมั่นคงปลอดภัย หากจำเป็น การปฏิบัติการแก้ไขจะต้องเหมาะสมกับผลของความไม่สอดคล้องที่พบ โดยองค์กรจะเก็บรักษาเอกสารข้อมูลดังต่อไปนี้ไว้เป็นหลักฐาน

12.1.6 ลักษณะของความไม่สอดคล้องและการดำเนินการในภายหลัง

12.1.7 ผลการของปฏิบัติการแก้ไข

12.2 การปรับปรุงอย่างต่อเนื่อง (Continual improvement) องค์กรจะต้องคงไว้ซึ่งการปรับปรุงอย่างต่อเนื่องเพื่อความเหมาะสมพอเพียงและสัมฤทธิ์ผลของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ตารางแสดงความสัมพันธ์ของเอกสารที่สอดคล้องกับข้อกำหนด ISO/IEC 27001

Document No.	Name of Document	Ref. Req	Department					
			ISMR	DC	กลุ่มงานบริหารทั่วไป	กลุ่มงานพัฒนาเทคโนโลยีสารสนเทศ ชุดที่ 1	กลุ่มงานพัฒนาเทคโนโลยีสารสนเทศ ชุดที่ 2	กลุ่มงานพัฒนาเทคโนโลยีสารสนเทศ ชุดที่ 3
SD-01	วิเคราะห์บริบทองค์กร	4.1, 6.1	⊕	X	X	X	X	X
SD-02	วิเคราะห์ผู้มีส่วนได้ส่วนเสีย	4.2, 6.1	⊕	X	X	X	X	X
ISMS-01	คู่มือระบบการจัดการความปลอดภัยสารสนเทศ	4.3, 4.4,6.3	⊕	O	X	X	X	X
	นโยบาย	5.2, 7.3	⊕	X	X	X	X	X
	ประกาศแต่งตัวแทนฝ่ายบริหารระบบบริหารการให้บริการ	5.3	⊕	X	X	X	X	X
QP-01	การควบคุมเอกสาร	7.5.1-7.5.3	X	⊕	X	X	X	X
QP-02	การบริหารจัดการทรัพย์สิน	6.1.3, Annex A	X	X	⊕	O	O	X
QP-03	การขอเข้าพื้นที่ควบคุม	6.1.3, Annex A	X	X	O	X	⊕	X
QP-04	การสำรองและทดสอบกู้คืนข้อมูล	6.1.3, Annex A	X	X	X	X	X	⊕
QP-05	การติดตามการใช้งาน	6.1.3, Annex A	O	X	X	⊕	O	⊕
QP-06	การลงทะเบียนผู้ใช้งาน	6.1.3, Annex A	X	X	X	X	O	⊕
QP-07	การควบคุมการเปลี่ยนแปลง	6.1.3, Annex A	O	O	O	O	⊕	O
QP-08	การบริหารจัดการอุบัติการณ์ที่ส่งผลต่อการให้บริการ	6.1.3, Annex A	O	X	X	X	X	⊕
QP-09	การประเมินความเสี่ยงปลอดภัยของข้อมูลสารสนเทศ	6.1.1, 6.1.2, 6.1.3, 8.1, 8.2, 8.3	O	O	O	O	⊕	O
QP-10	การตรวจติดตามภายใน	9.2	O	⊕	O	O	O	O

Document No.	Name of Document	Ref. Req	Department					
			ISMR	DC	กลุ่มงานบริหารทั่วไป	กลุ่มงานพัฒนาเทคโนโลยีสารสนเทศชุดที่ 1	กลุ่มงานพัฒนาเทคโนโลยีสารสนเทศชุดที่ 2	กลุ่มงานพัฒนาเทคโนโลยีสารสนเทศชุดที่ 3
QP-11	การปฏิบัติการแก้ไขและป้องกัน	9.3	O	⌖	O	O	O	O
QP-12	การกำหนดวัตถุประสงค์ ประชุมทบทวนฝ่ายบริหารและการสื่อสาร	6.2, 7.3, 7.4, 9.1	O	⌖	O	O	O	O
QP-13	การบริหารจัดการความต่อเนื่องในการดำเนินงานขององค์กร	6.1.3, Annex A	O	O	O	O	O	⌖
QP-14	การสรรหาและฝึกอบรม	7.1, 7.2, 7.3	X	X	⌖	X	X	X
QP-15	การควบคุมผู้ให้บริการภายนอก	6.1.3, Annex A	X	X	⌖	X	X	X
QP-16	การออกแบบและพัฒนาระบบ	6.1.3, Annex A	X	X	X	⌖	X	X
QP-17	การติดตามประเมินความสอดคล้องกฎหมายคอมพิวเตอร์	6.1.3, Annex A	O	O	O	⌖	O	O
SD-03	แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมสุขภาพจิต	Annex A	O	O	O	⌖	O	O
SD-04	มาตรฐานเว็บไซต์ภาครัฐ	Annex A	X	X	X	O	O	⌖
SD-05	มาตรฐานแอพพลิเคชันภาครัฐสำหรับอุปกรณ์เคลื่อนที่	Annex A	X	X	X	⌖	O	O

<u>หมายเหตุ</u>

⌖ หมายถึง เกี่ยวข้องโดยตรงและเป็นผู้รับผิดชอบควบคุมการบันทึกข้อมูลในเอกสาร

O หมายถึง เกี่ยวข้องโดยตรง

X หมายถึง เกี่ยวข้องโดยอ้อม