มาตรฐานอาชีพและคุณวุฒิวิชาชีพ
Occupational Standard and Professional Qualifications

สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย

จัดทำโดย สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)
ร่วมกับ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

1. ชื่อมาตรฐานอาชีพ

สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย

2. ประวัติการปรับปรุงมาตรฐาน

ไม่มี

3. ทะเบียนอ้างอิง (Imprint)

ไม่มี

4. ข้อมูลเบื้องต้น

มาตรฐานสาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network & Security)
มีวัตถุประสงค์สำคัญเพื่อพัฒนาศักยภาพของบุคลากรในสาขาอาชีพ ICT ให้สามารถแข่งขันและเป็นที่ยอมรับในระดับสากล สนับสนุนบุคลากรในกลุ่มอาชีพให้มีสมรรถนะตรงตามความต้องการของผู้ว่าจ้าง มีทักษะทางเทคนิคในการปฏิบัติงาน

5. ประวัติการปรับปรุงมาตรฐานในแต่ละครั้ง

การทบทวนมาตรฐานอาชีพและคุณวุฒิวิชาชีพตามกรอบคุณวุฒิวิชาชีพ 8 ระดับ ครั้งที่ 1

6. ครั้งที่

1 (ปี พุทธศักราช 2563)

การเปลี่ยนแปลงที่สำคัญ

การทบทวนมาตรฐานอาชีพและคุณวุฒิวิชาชีพตามกรอบคุณวุฒิวิชาชีพ 8 ระดับ มีรายละเอียด ดังนี้

- ทบทวนคุณลักษณะผลการเรียนรู้ให้มีความสอดคล้องกับสมรรถนะของคุณวุฒิวิชาชีพ

- ทบทวนการเลื่อนระดับคุณวุฒิวิชาชีพสาขาวิชาชีพ

- ทบทวนสมรรถนะอาชีพ (หน่วยสมรรถนะ หน่วยสมรรถนะย่อย เกณฑ์การปฏิบัติงาน และรายละเอียดหน่วยสมรรถนะ)

- ทบทวนเครื่องมือประเมิน กระบวนการประเมิน คู่มือการประเมิน สัดส่วนคะแนน เกณฑ์การผ่านการประเมิน

กรอบคุณวุฒิ 7 ชั้น **จำนวน 5 อาชีพ 16 ชั้นคุณวุฒิ 37 หน่วยสมรรถนะ**	**กรอบคุณวุฒิ 8 ระดับ** **จำนวน 5 อาชีพ 16 ระดับคุณวุฒิ 36 หน่วยสมรรถนะ**
1. ช่างสนับสนุนด้านเทคนิค ชั้น 3 - 6	1. ช่างสนับสนุนด้านเทคนิค ระดับ 3 - 6
2. นักบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ชั้น 4 - 6	2. นักบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ระดับ 4 - 6
3. นักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ชั้น 4 - 6	3. นักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ระดับ 4 - 6
4. นักจัดการความมั่นคงระบบสารสนเทศ ชั้น 4 - 6	4. นักจัดการความมั่นคงระบบสารสนเทศ ระดับ 4 - 6
5. นักจัดการอุปกรณ์พกพาและเครือข่ายไร้สาย ชั้น 4 - 6	5. นักจัดการอุปกรณ์พกพาและเครือข่ายไร้สาย ระดับ 4 - 6

7. คุณวุฒิวิชาชีพที่ครอบคลุม (Professional Qualifications included)

สาขาวิชาชีพอุตสาหกรรมดิจิทัล

สาขาความมั่นคงปลอดภัยทางดิจิทัลและส่วนบุคคล

อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 5

8. คุณวุฒิวิชาชีพที่เกี่ยวข้อง (Related Professional Qualifications)

ไม่มี

9. หน่วยสมรรถนะทั้งหมดในมาตรฐานอาชีพ (List of All Units of Competence within this Occupational Standards)

รหัสหน่วยสมรรถนะ	**เนื้อหา**
41102	ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
41202	ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
41402	จัดการเหตุการณ์ทางไซเบอร์และสืบสวนทางไซเบอร์

10. ระดับคุณวุฒิ

10.1 สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาความมั่นคงปลอดภัยทางดิจิทัลและส่วนบุคคล อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 5

คุณลักษณะของผลการเรียนรู้ (Characteristics of Outcomes)

เป็นผู้มีสมรรถนะทางเทคนิคในการจัดการความมั่นคงปลอดภัยระบบสารสนเทศ สามารถแก้ไขปัญหาในบริบทที่มีการเปลี่ยนแปลงทั่วไป สามารถคิดวิเคราะห์และประเมินสถานการณ์ได้ด้วยตนเอง มีความเป็นผู้นำจัดการผลิตภาพการทำงาน ถ่ายทอดงาน สอนงาน และกำกับดูแลผู้ร่วมงานให้บรรลุงานตามแผนได้ โดยมีสมรรถนะในการปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ พัฒนาระบบสารสนเทศที่มีความมั่นคงปลอดภัย จัดการเหตุการณ์ทางไซเบอร์และสืบสวนทางไซเบอร์ ถ่ายทอด สอนงาน ฝึกอบรมเพื่อให้ความรู้และทักษะกับผู้อื่น

การเลื่อนระดับคุณวุฒิวิชาชีพ (Qualification Pathways)

1. คุณสมบัติของผู้ที่สามารถเข้ารับการประเมินคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 5

- มีประสบการณ์ทำงานด้านความมั่นคงปลอดภัยระบบสารสนเทศ หรือที่เกี่ยวข้องไม่น้อยกว่า 5 ปี หรือ
- ผู้ที่สำเร็จการศึกษาระดับ ปริญญาตรี ในด้านความมั่นคงปลอดภัยระบบสารสนเทศ หรือที่เกี่ยวข้อง หรือ
- ได้รับรองคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 4 แล้วเป็นระยะเวลาไม่น้อยกว่า 1 ปี

2. ผู้ที่จะผ่านการประเมินและได้รับการรับรองคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 5

- ผ่านเกณฑ์การประเมินตามหน่วยสมรรถนะของอาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศระดับ 5 จำนวน 3 หน่วย

3. ในกรณีต่ออายุหนังสือรับรองมาตรฐานอาชีพให้เป็นไปตามคู่มือสำหรับผู้เข้ารับการประเมินหรือคู่มือเจ้าหน้าที่สอบ

หลักเกณฑ์การต่ออายุหนังสือรับรองมาตรฐานอาชีพ

N/A

กลุ่มบุคคลในอาชีพ (Target Group)

2131.10 นักวิเคราะห์ระบบ

2131.30 ผู้เชี่ยวชาญด้านสื่อสารข้อมูล

2131.60 วิศวกรซอฟต์แวร์

2133 ผู้ประกอบวิชาชีพด้านคอมพิวเตอร์ที่มิได้จัดประเภทไว้ในที่อื่น

หน่วยสมรรถนะ (หน่วยสมรรถนะทั้งหมดของคุณวุฒิวิชาชีพนี้)

41102 ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

41202 ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

41402 จัดการเหตุการณ์ทางไซเบอร์และสืบสวนทางไซเบอร์

ตารางแผนผังแสดงหน้าที่

1. ตารางแสดงหน้าที่ 1

ประกาศใช้ ณ 03/03/2564

ตาราง 1 : FUNCTIONAL MAP แสดง KEY PURPOSE , KEY ROLES , KEY FUNCTION

ความมุ่งหมายหลัก Key Purpose		บทบาทหลัก Key Roles		หน้าที่หลัก Key Function	
คำอธิบาย	รหัส	คำอธิบาย	รหัส	คำอธิบาย	

คำอธิบาย ตารางแผนผังแสดงหน้าที่เป็นแผนผังที่ใช้วิเคราะห์หน้าที่งานเพื่อให้ได้หน้าที่หลัก (Key Function)

2. ตารางแสดงหน้าที่ 1 (ต่อ)

ประกาศใช้ ณ 03/03/2564

ตาราง 2 : FUNCTIONAL MAP แสดง KEY FUNCTION , UNIT OF COMPETENCE , ELEMENT OF COMPETENCE

หน้าที่หลัก Key Function		หน่วยสมรรถนะ Unit of Competence		หน่วยสมรรถนะย่อย Element of Competence	
รหัส	**คำอธิบาย**	**รหัส**	**คำอธิบาย**	**รหัส**	**คำอธิบาย**
411	บริหารจัดการด้านความมั่นคงปลอดภัยระบบสารสนเทศ	41102	ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	41102.01	ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
				41102.02	บริหารความต่อเนื่องทางธุรกิจ
				41102.03	จัดการองค์ความรู้
412	จัดหาระบบสารสนเทศอย่างมั่นคงปลอดภัย	41202	ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	41202.01	วางแผนความต้องการของระบบ
				41202.02	พัฒนาระบบ
				41202.03	ทดสอบและประเมินผล
414	ปกป้องคุ้มครองและสืบสวนทางไซเบอร์	41402	จัดการเหตุการณ์ทางไซเบอร์และสืบสวนทางไซเบอร์	41402.01	จัดการเหตุการณ์ทางไซเบอร์
				41402.02	วิเคราะห์ภัยคุกคาม
				41402.03	สืบสวนทางไซเบอร์และพิสูจน์หลักฐานดิจิทัล
				41402.04	กู้คืนระบบจากภัยพิบัติ

คำอธิบาย

ตารางแผนผังแสดงหน้าที่ (ต่อ) เป็นแผนผังที่ใช้วิเคราะห์หน้าที่งานหลังจากได้หน้าที่หลัก (Key Function) เพื่อให้ได้ หน่วยสมรรถนะ (Unit of Competence) และหน่วยสมรรถนะย่อย (Element of Competence)

1. รหัสหน่วยสมรรถนะ 41102

2. ชื่อหน่วยสมรรถนะ ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☑	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้เชี่ยวชาญระบบเครือข่าย ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ นักวิเคราะห์ความมั่นคงปลอดภัยระบบสารสนเทศ ผู้บริหารด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ผู้บริหารเครือข่ายคอมพิวเตอร์

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที
2529 ผู้เชี่ยวชาญด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศและการสื่อสาร

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
41102.01 ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	1.1 ให้คำแนะนำผู้บริหารระดับสูงทางด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ประเมินความคุ้มค่าในการลงทุนทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ 1.2 ปฏิบัติเพื่อคงไว้ซึ่งความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร 1.3 จัดทำแผนงานด้านความมั่นคงปลอดภัยระบบสารสนเทศ	ข้อสอบข้อเขียน การสัมภาษณ์
41102.02 บริหารความต่อเนื่องทางธุรกิจ	2.1 จัดทำแผนบริหารความต่อเนื่องทางธุรกิจ 2.2 ทดสอบแผนบริหารความต่อเนื่องทางธุรกิจ 2.3 ทบทวนและปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ	ข้อสอบข้อเขียน การสัมภาษณ์
41102.03 จัดการองค์ความรู้	3.1 เก็บข้อมูลความต้องการของระบบจากผู้ใช้งาน 3.2 ออกแบบ จัดทำ และบำรุงรักษาระบบจัดการองค์ความรู้ 3.3 ติดตามการใช้งานระบบเพื่อให้เกิดการแลกเปลี่ยนองค์ความรู้ภายในองค์กร	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. สามารถให้คำแนะนำที่เหมาะสมในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบสารสนเทศแก่ผู้บริหาร
2. สามารถติดตามผลของการพิจารณาความเหมาะสมในการดำเนินโครงการด้านความมั่นคงปลอดภัยระบบสารสนเทศ
3. สามารถดำเนินการเพื่อคงไว้ซึ่งความมั่นคงปลอดภัยระบบสารสนเทศของระบบสารสนเทศขององค์กร
4. สามารถติดตามและทบทวนผลของการปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศของระบบสารสนเทศขององค์กร
5. สามารถจัดทำแผนงานทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ ได้รับการอนุมัติจากผู้บริหาร และมีการสื่อสารออกไปยังผู้ที่เกี่ยวข้อง
6. สามารถสื่อสารแผนงานด้านความมั่นคงปลอดภัยระบบสารสนเทศไปยังผู้ที่เกี่ยวข้อง
7. สามารถทบทวนแผนงานด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างสม่ำเสมอ

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
2. ความรู้เกี่ยวกับสถาปัตยกรรมทางด้านเทคโนโลยีสารสนเทศ
3. ความรู้เกี่ยวกับระบบเครือข่ายและระบบปฏิบัติการ
4. ความรู้เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศ
5. ความรู้เกี่ยวกับการบริหารความต่อเนื่องทางธุรกิจขององค์กร
6. ความรู้เกี่ยวกับการจัดการความเสี่ยง
7. ความรู้เกี่ยวกับการจัดการองค์ความรู้
8. ความรู้เกี่ยวกับการวางแผนและออกแบบระบบจัดการองค์ความรู้
9. ความรู้เกี่ยวกับการบำรุงรักษาระบบจัดการองค์ความรู้

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมินและควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. ผลจากการสังเกตการปฏิบัติงาน
2. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน
3. ข้อมูลจากแฟ้มสะสมงาน
4. ผลจาการทดสอบภาคปฏิบัติ

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. แฟ้มสะสมผลงาน ได้แก่ ใบผ่านงาน ประกาศนียบัตร วุฒิบัตร และเอกสารผลงานต่าง ๆ ที่เกี่ยวข้องกับความรู้ทางด้านธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์

(ค) คำแนะนำในการประเมินง

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ผู้รับการประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ในการปฏิบัติงานให้คำนึงถึงการปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ การบริหารความต่อเนื่องทางธุรกิจ การจัดการองค์ความรู้

(ข) คำอธิบายรายละเอียด

1. การปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ การให้คำแนะนำผู้บริหารระดับสูงทางด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ประเมินความคุ้มค่าในการลงทุนทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ ควรมีการติดตามผลของการดำเนินการตามคำแนะนำ เพื่อให้เกิดประสิทธิผลสูงสุด การปฏิบัติเพื่อคงไว้ซึ่งความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร ควรมีการติดตามผลการดำเนินงานเพื่อให้มีความสอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

รวมทั้งตรวจสอบความพร้อมทางระบบสารสนเทศขององค์ในมิติต่าง ๆ ไม่ว่าจะเป็นบุคลากร กระบวนการ และเทคโนโลยี
การจัดทำแผนงานด้านความมั่นคงปลอดภัยระบบสารสนเทศ ควรมีการวางแผนในระยะสั้น ระยะกลาง และระยะยาว
และมีการทบทวนแผนเป็นระยะเพื่อปรับแผนให้เหมาะสมกับสถานการณ์ความเป็นจริงมากที่สุด

2. การบริหารความต่อเนื่องทางธุรกิจ การจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ ควรมีการวิเคราะห์สภาพขององค์กร มีความรู้ความเข้าใจในบริบทขององค์กร กระบวนการทางธุรกิจ ระบุกระบวนการทางธุรกิจที่สำคัญ ประเมินความเสี่ยงที่ทำให้องค์กรหยุดชะงัก เขียนแผนบริหารความต่อเนื่องทางธุรกิจ
การทดสอบแผนบริหารความต่อเนื่องทางธุรกิจ ควรเลือกชนิดของการทดสอบที่เหมาะสม โดยหากองค์กรไม่เคยดำเนินการทดสอบแผนฯ มาก่อนอาจจะเลือกการทดสอบชนิด Table Top แต่หากเคยทดสอบมาแล้วอาจเลือกชนิดของการทดสอบแผนฯ เป็นแบบ Simulation
การทบทวนและปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจควรดำเนินการอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง หรือทุก ๆ ครั้งที่มีการเปลี่ยนแปลงโครงสร้างขององค์กร หรือพิจารณาแล้วเห็นว่ามีภัยคุกคามรูปแบบใหม่ที่องค์กรจำเป็นต้องเตรียมรับมือ

3. การจัดการองค์ความรู้ การเก็บข้อมูลความต้องการของระบบจากผู้ใช้งาน ควรมีการวางแผนการจัดเก็บ และกำหนดวิธีการจัดเก็บให้เหมาะสม เพื่อลดปัญหาความซ้ำซ้อนและเก็บข้อมูลได้ไม่ครบถ้วนเพื่อนำไปใช้งานต่อได้ การออกแบบ จัดทำ และบำรุงรักษาระบบจัดการองค์ความรู้ ควรคำนึงถึงความยืดหยุ่นในการใช้งานของระบบ การบำรุงรักษา รวมทั้งการใช้งานง่ายของผู้ใช้งานอีกด้วย
การติดตามการใช้งานระบบเพื่อให้เกิดการแลกเปลี่ยนองค์ความรู้ภายในองค์กร มีความสำคัญ เพื่อให้เกิดการใช้ข้อมูล การสร้างข้อมูล การแลกเปลี่ยนข้อมูลอย่างต่อเนื่อง จึงจำเป็นต้องจัดหามาตรการในการติดตาม และกระตุ้นให้เกิดการปฏิสัมพันธ์กับผู้ใช้งานอย่างสม่ำเสมอ

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้
1. สมรรถนะย่อย 41102.01 ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 41102.02 บริหารความต่อเนื่องทางธุรกิจ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
3. สมรรถนะย่อย 41102.03 จัดการองค์ความรู้ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

1. รหัสหน่วยสมรรถนะ 41202

2. ชื่อหน่วยสมรรถนะ ปฏิบัติการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

นักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถ วางแผนความต้องการของระบบ พัฒนาระบบ ทดสอบและประเมินผล

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☑	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้เชี่ยวชาญระบบเครือข่าย ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ นักวิเคราะห์ความมั่นคงปลอดภัยระบบสารสนเทศ
ผู้บริหารด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ผู้บริหารเครือข่ายคอมพิวเตอร์

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที
2529 ผู้เชี่ยวชาญด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศและการสื่อสาร

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
41202.01 วางแผนความต้องการของระบบ	1.1 ทำการวิเคราะห์ความเสี่ยง ศึกษาความเป็นไปได้ เพื่อกำหนด Functional requirements และ Specifications ประมาณราคาค่าใช้จ่ายของระบบ 1.2 กำหนดความต้องการของระบบ 1.3 บูรณาการนโยบายด้านการรักษาความมั่นคงปลอดภัยเพื่อให้มั่นใจในระบบที่พัฒนา	ข้อสอบข้อเขียน การสัมภาษณ์
41202.02 พัฒนาระบบ	2.1 วิเคราะห์ข้อจำกัดในการออกแบบ ข้อดีข้อเสียของระบบที่พัฒนา 2.2 ประยุกต์นโยบายด้านความมั่นคงปลอดภัยเข้าไปยังระบบที่ทำการพัฒนา ประเมินภัยคุกคาม ช่องโหว่ และความเสี่ยงของระบบ 2.3 พัฒนาซอฟต์แวร์ตามข้อกำหนดทางด้านความมั่นคงปลอดภัย 2.4 พัฒนาระบบการสำรองข้อมูลที่มีความมั่นคงปลอดภัย	ข้อสอบข้อเขียน การสัมภาษณ์

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
41202.03 ทดสอบและประเมินผล	3.1 กำหนดระดับของความมั่นคงปลอดภัยของซอฟต์แวร์ 3.2 วางแผนการทดสอบตามวัตถุประสงค์และข้อกำหนด 3.3 จัดทำสภาพแวดล้อมของการทดสอบและตรวจสอบทั้งฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์ต่อพ่วงของระบบ 3.4 ดำเนินการทดสอบระบบ 3.5 วิเคราะห์ผลการทดสอบ	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. สามารถทำการวิเคราะห์ความเสี่ยง ศึกษาความเป็นไปได้ เพื่อกำหนด Functional requirements และ Specifications ประมาณราคาค่าใช้จ่ายของระบบ
2. สามารถกำหนดความต้องการของระบบ
3. สามารถบูรณาการนโยบายด้านการรักษาความมั่นคงปลอดภัยเพื่อให้มั่นใจในระบบที่พัฒนา
4. สามารถวิเคราะห์ข้อจำกัดในการออกแบบ ข้อดีข้อเสีย ของระบบที่พัฒนา
5. สามารถประยุกต์นโยบายด้านความมั่นคงปลอดภัยเข้าไปยังระบบที่ทำการพัฒนา ประเมินภัยคุกคาม ช่องโหว่ และความเสี่ยงของระบบ
6. สามารถพัฒนาซอฟต์แวร์ตามข้อกำหนดทางด้านความมั่นคงปลอดภัย
7. สามารถพัฒนาระบบการสำรองข้อมูลที่มีความมั่นคงปลอดภัย
8. สามารถกำหนดระดับของความมั่นคงปลอดภัยของซอฟต์แวร์
9. สามารถวางแผนการทดสอบตามวัตถุประสงค์และข้อกำหนด
10. สามารถจัดทำสภาพแวดล้อมของการทอสอบและตรวจสอบทั้งฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์ต่อพ่วงเพื่อให้มั่นใจว่าสอดคล้องกับข้อกำหนดและความต้องการของระบบ
11. สามารถดำเนินการทดสอบระบบ
12. วิเคราะห์ผลการทดสอบ ให้คำแนะนำทางด้านความมั่นคงปลอดภัยตามผลการทดสอบที่ได้รับ

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย
2. ความรู้เกี่ยวกับวิศวกรรมซอฟต์แวร์
3. ความรู้เกี่ยวกับกระบวนการทางธุรกิจ
4. ความรู้เกี่ยวกับระบบปฏิบัติการและระบบเครือข่าย
5. ความรู้เกี่ยวกับวงจรชีวิตการพัฒนาระบบ
6. ความรู้เกี่ยวกับอัลกอริทึม
7. ความรู้เกี่ยวกับระบบฐานข้อมูล
8. ความรู้เกี่ยวกับการปฏิสัมพันธ์ระหว่างคอมพิวเตอร์และมนุษย์
9. ความรู้เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ
10. ความรู้เกี่ยวกับระบบปฏิบัติการและระบบเครือข่าย
11. ความรู้เกี่ยวกับระบบสารสนเทศขององค์กร
12. ความรู้เกี่ยวกับข้อกำหนดในการประเมินผลระบบสารสนเทศ
13. ความรู้เกี่ยวกับการประเมินความมั่นคงปลอดภัยระบบสารสนเทศ
14. ความรู้เกี่ยวกับระบบปฏิบัติการและระบบเครือข่าย
15. ความรู้เกี่ยวกับการทดสอบระบบชนิดต่าง ๆ

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมินและควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการสัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ผู้รับการประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ในการปฏิบัติงานให้คำนึงถึงการวางแผนความต้องการของระบบ การพัฒนาระบบ การทดสอบและประเมินผล

(ข) คำอธิบายรายละเอียด

1. การวางแผนความต้องการของระบบ การวิเคราะห์ความเสี่ยง ศึกษาความเป็นไปได้ เพื่อกำหนด Functional requirements และ Specifications ประมาณราคาค่าใช้จ่ายของระบบ ให้พิจารณาขอบเขตของระบบที่ต้องการพัฒนา พิจารณาภัยคุกคามที่เกี่ยวข้องโดยอาจพิจารณาจากภัยคุกคามที่เคยเจอ ภัยคุกคามที่อาจจะไม่เคยเกิดภายในองค์กรแต่เกิดกับผู้ที่อยู่ในธุรกิจเดียวกัน เป็นต้น ให้เลือกวิธีการประเมินความเสี่ยงที่เหมาะสม การกำหนดความต้องการของระบบให้พิจารณาเก็บข้อมูลให้รอบด้าน ด้วยเครื่องมือที่เหมาะสม การบูรณาการนโยบายด้านการรักษาความมั่นคงปลอดภัยเพื่อให้มั่นใจในระบบที่พัฒนา ให้พิจารณานโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร รวมทั้งกฎหมาย กฎระเบียบ ข้อบังคับ แนวทางปฏิบัติที่เกี่ยวข้องในการบูรณาการให้เหมาะสม

2. การพัฒนาระบบ การวิเคราะห์ข้อจำกัดในการออกแบบ ข้อดีข้อเสีย ของระบบที่พัฒนา เป็นสิ่งที่จำเป็น และจำเป็นต้องมีการสื่อสารผลที่ได้จากการวิเคราะห์ไปให้กับผู้ที่เกี่ยวข้อง รวมทั้งผู้ใช้งานระบบด้วย การประยุกต์นโยบายด้านความมั่นคงปลอดภัยเข้าไปยังระบบที่ทำการพัฒนา ประเมินภัยคุกคาม ช่องโหว่ และความเสี่ยงของระบบ ควรมีการดำเนินการตั้งแต่ช่วงเริ่มต้นของการพัฒนาระบบ เนื่องจากจะทำให้มั่นใจได้ว่าระบบที่พัฒนาขึ้นได้มีการพิจารณาข้อกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร และเมื่อระบบถูกพัฒนาเสร็จสิ้นจะสอดคล้องกับนโยบายทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ รวมถึงเป้าหมายและกลยุทธ์ทางธุรกิจขององค์กร การพัฒนาซอฟต์แวร์ตามข้อกำหนดทางด้านความมั่นคงปลอดภัย แม้ว่าจะทำให้กระบวนการพัฒนาซอฟต์แวร์มีความล่าช้าลงไปบ้างเนื่องจากจำเป็นต้องมีการตรวจสอบเพิ่มเติม แต่จะทำให้มั่นใจได้ว่าซอฟต์แวร์ที่ถูกพัฒนาขึ้นนั้นไม่มีช่องโหว่ที่เป็นที่รู้จักในช่วงที่มีการพัฒนา และจะช่วยลดความเสียหายที่อาจจะเกิดขึ้นหลังจากที่ได้มีการนำเอาซอฟต์แวร์ดังกล่าวไปใช้งาน การพัฒนาระบบการสำรองข้อมูลที่มีความมั่นคงปลอดภัย อาจมีการพิจารณาการกำหนดการควบคุมการเข้าถึงและการนำเอาวิทยาการเข้ารหัสลับ มาใช้

3. การทดสอบและประเมินผล การกำหนดระดับของความมั่นคงปลอดภัยของซอฟต์แวร์ ให้พิจารณาถึงระดับระดับความลับของข้อมูล ระดับระดับความลับของผู้ใช้งาน การควบคุมการเข้าถึง รวมทั้งการควบคุมทางด้านความมั่นคงปลอดภัยสำหรับซอฟต์แวร์นั้น ๆ การวางแผนการทดสอบตามวัตถุประสงค์และข้อกำหนด ให้พิจารณาถึงแนวทางการทดสอบทางด้านความมั่นคงปลอดภัย นอกเหนือไปจากการทดสอบปรกติที่ได้มีการทำอยู่แล้ว เช่น การทดสอบช่องโหว่ การทดสอบการโจมตี เป็นต้น การจัดทำสภาพแวดล้อมของการทอสอบและตรวจสอบทั้งฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์ต่อพ่วงเพื่อให้มั่นใจว่าสอดคล้องกับข้อกำหนดและความต้องการของระบบ โดยปกติแล้วอาจจะไม่สามารถจำลองสภาพแวดล้อมให้เหมือนจริงได้ครบถ้วน แต่ให้พิจารณาการควบคุมปัจจัยหลักในการใช้งานระบบให้เหมาะสม การดำเนินการทดสอบระบบ ให้มีการควบคุมการทดสอบ และกำหนดตัวชี้วัดให้ชัดเจน การวิเคราะห์ผลการทดสอบ ให้คำแนะนำทางด้านความมั่นคงปลอดภัยตามผลการทดสอบที่ได้รับ โดยเทียบกับมาตรฐาน หรือแนวปฏิบัติที่ดี (Best Practice) ที่เป็นที่ยอมรับในภาคอุตสาหกรรม หรือได้รับคำแนะนำจากหน่วยงานที่เป็นที่ยอมรับ

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 41202.01 วางแผนความต้องการของระบบ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 41202.02 พัฒนาระบบ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
3. สมรรถนะย่อย 41202.03 ทดสอบและประเมินผล ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

1. รหัสหน่วยสมรรถนะ 41402

2. ชื่อหน่วยสมรรถนะ จัดการเหตุการณ์ทางไซเบอร์และสืบสวนทางไซเบอร์

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถจัดการเหตุการณ์ทางไซเบอร์ วิเคราะห์ภัยคุกคาม สืบสวนทางไซเบอร์และพิสูจน์หลักฐานดิจิทัล กู้คืนระบบจากภัยพิบัติ

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☑	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้เชี่ยวชาญระบบเครือข่าย ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ นักวิเคราะห์ความมั่นคงปลอดภัยระบบสารสนเทศ ผู้บริหารด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ผู้บริหารเครือข่ายคอมพิวเตอร์

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที
2529 ผู้เชี่ยวชาญด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศและการสื่อสาร

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
41402.01 จัดการเหตุการณ์ทางไซเบอร์	1.1 ระบุกระบวนการจัดการต่อเหตุการณ์ทางไซเบอร์ประสานและให้การสนับสนุนในด้านการตอบสนองต่อเหตุการณ์ทางไซเบอร์ 1.2 ตรวจดูข้อมูลจากแหล่งข้อมูลภายนอกเพื่อตรวจสอบภัยคุกคามที่อาจส่งผลกระทบต่อองค์กร 1.3 เลือกแนวทางตอบสนองต่อเหตุการณ์	ข้อสอบข้อเขียน การสัมภาษณ์
41402.02 วิเคราะห์ภัยคุกคาม	2.1 วิเคราะห์ภัยคุกคามทางไซเบอร์ 2.2 วิเคราะห์การโจมตีทางไซเบอร์	ข้อสอบข้อเขียน การสัมภาษณ์
41402.03 สืบสวนทางไซเบอร์และพิสูจน์หลักฐานดิจิทัล	3.1 สืบสวนทางไซเบอร์ 3.2 พิสูจน์หลักฐานดิจิทัล	ข้อสอบข้อเขียน การสัมภาษณ์
41402.04 กู้คืนระบบจากภัยพิบัติ	4.1 จัดทำแผนกู้คืนระบบจากภัยพิบัติ 4.2 ติดตั้งและตั้งค่าศูนย์คอมพิวเตอร์สำรอง 4.3 ทดสอบแผนกู้คืนระบบจากภัยพิบัติ	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. สามารถระบุกระบวนการจัดการต่อเหตุการณ์ทางไซเบอร์ ประสานและให้การสนับสนุนในด้านการตอบสนองต่อเหตุการณ์ทางไซเบอร์
2. สามารถตรวจดูข้อมูลจากแหล่งข้อมูลภายนอกเพื่อตรวจสอบภัยคุกคามที่อาจส่งผลกระทบต่อองค์กร
3. สามารถเลือกแนวทางตอบสนองต่อเหตุการณ์อย่างเหมาะสม
4. สามารถวิเคราะห์ภัยคุกคามทางไซเบอร์
5. สามารถวิเคราะห์การโจมตีทางไซเบอร์
6. สามารถสืบสวนทางไซเบอร์
7. สามารถพิสูจน์หลักฐานดิจิทัล
8. สามารถจัดทำแผนกู้คืนระบบจากภัยพิบัติ
9. สามารถติดตั้งและตั้งค่าศูนย์คอมพิวเตอร์สำรอง
10. สามารถทดสอบแผนกู้คืนระบบจากภัยพิบัติ

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับการสำรองข้อมูล ชนิดของการสำรองข้อมูล และเครื่องมือที่ใช้ในการกู้ข้อมูล
2. ความรู้เกี่ยวกับบริการเครือข่ายและโพรโทคอล
3. ความรู้เกี่ยวกับชนิดของเหตุการณ์ การตอบสนองต่อเหตุการณี
4. ความรู้เกี่ยวกับโพรโทคอลสื่อสารบนเครือข่าย
5. ความรู้เกี่ยวกับการวิเคราะห์ระดับแพ็กเก็ต
6. ความรู้เกี่ยวกับเครื่องมือวิเคราะห์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ
7. ความรู้เกี่ยวกับภัยคุกตามรูปแบบต่าง ๆ
8. ความรู้เกี่ยวกับเทคนิคการเจาะระบบ
9. ความรู้เกี่ยวกับแนวทางการหาช่องโหว่ของระบบ
10. ความรู้เกี่ยวกับช่องโหว่และภัยคุกคามระบบและเครือข่าย
11. ความรู้เกี่ยวกับการดำเนินการสืบสวนทางไซเบอร์
12. ความรู้เกี่ยวกับการพิสูจน์หลักฐานทางดิจิทัล ไม่ว่าจะเป็นการสืบสวนจากคอมพิวเตอร์ ข้อมูลบนเครือข่าย เป็นต้น
13. ความรู้เกี่ยวกับชนิดของหลักฐานที่ได้ดำเนินการจัดเก็บ
14. ความรู้เกี่ยวกับเครื่องมือที่ใช้ในการพิสูจน์หลักฐาน
15. ความรู้เกี่ยวกับกู้คืนระบบจากภัยพิบัติ
16. ความรู้เกี่ยวกับการจัดตั้งศูนย์คอมพิวเตอร์หรือศูนย์ข้อมูลสำรอง
17. ความรู้เกี่ยวกับการจัดทำแผนทดสอบการกู้คืนระบบ

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมินและควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการสัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ผู้รับการประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ในการปฏิบัติงานให้คำนึงถึงการจัดการเหตุการณ์ทางไซเบอร์ การวิเคราะห์ภัยคุกคาม การสืบสวนทางไซเบอร์และพิสูจน์หลักฐานดิจิทัล การกู้คืนระบบจากภัยพิบัติ

(ข) คำอธิบายรายละเอียด

1. การจัดการเหตุการณ์ทางไซเบอร์ การระบุกระบวนการจัดการต่อเหตุการณ์ทางไซเบอร์ ประสานและให้การสนับสนุนในด้านการตอบสนองต่อเหตุการณ์ทางไซเบอร์ ควรมีการออกแบบกระบวนการ ฝึกอบรมบุคลากร รวมทั้งมีการประสานหน่วยงานทั้งภายในและภายนอก และวางแผนการฝึกเพื่อเตรียมรับมือกับภัยทางด้านไซเบอร์ การตรวจดูข้อมูลจากแหล่งข้อมูลภายนอกเพื่อตรวจสอบภัยคุกคามที่อาจส่งผลกระทบต่อองค์กร ทำการประสานงานกับหน่วยงานทั้งภายในและภายนอก รวมทั้งองค์กรภาครัฐที่มีขีดความสามารถทางด้านไซเบอร์ การเลือกแนวทางตอบสนองต่อเหตุการณ์อย่างเหมาะสม จัดทำแผนเผชิญเหตุหรือแผนรับมือกับเหตุการณ์ทางไซเบอร์ โดยพิจารณาถึงภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงสูงที่สุดเป็นลำดับแรก ๆ และ ดำเนินการทดสอบแผนอย่างสม่ำเสมอ

2. การวิเคราะห์ภัยคุกคาม การวิเคราะห์ภัยคุกคาม เก็บข้อมูลที่เกี่ยวข้องกับภัยคุกคามและข้อมูลการโจมตีจากอุปกรณ์ดักจับข้อมูลต่าง ๆ เช่น ระบบตรวจจับการบุรุก ข้อมูลล็อก เป็นต้น จัดหมวดหมู่ของภัยคุกคามและการโจมตีตามชนิด และระดับความรุนแรง การวิเคราะห์การโจมตี ทำการวิเคราะห์ภัยคุกคามและการโจมตีเพื่อศึกษาพฤติกรรมและหาแนวทางการป้องกันและแก้ไขปัญหาและลดผลกระทบที่เกิดขึ้น

3. การสืบสวนทางไซเบอร์และพิสูจน์หลักฐานดิจิทัล การสืบสวนทางไซเบอร์ มีความเข้าใจเกี่ยวกับภัยคุกคามรวมทั้งอาชญากรรมทางไซเบอร์ ดำเนินการจัดทำแนวทางและแผนสืบสวนทางไซเบอร์ แม้กระทั่งแนวคิดทางด้านอาชญวิทยา การพิสูจน์หลักฐานดิจิทัล ระบุหลักฐานที่สามารถสืบค้นและจัดเก็บเพื่อนำมาวิเคราะห์ในภายหลัง ดำเนินการจัดเก็บหลักฐานทางดิจิทัลด้วยวิธีการที่ได้รับการยอมรับเป็นมาตรฐาน ดำเนินการขนส่งหลักฐานมายังห้องปฏิบัติการเพื่อทำการวิเคราะห์ วิเคราะห์ผลของการพิสูจน์หลักฐานทางดิจิทัล จัดทำรายงานสรุปพร้อมนำเสนอ หรืออาจจะขึ้นให้การเป็นพยานผู้เชี่ยวชาญในระดับศาล

4. การกู้คืนระบบจากภัยพิบัติ การจัดทำแผนกู้คืนระบบจากภัยพิบัติ เก็บข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร ผ่านทางการสัมภาษณ์ การตอบแบบสอบถาม และอื่น ๆ เพื่อพิจารณาถึงระบบสารสนเทศที่มีความสำคัญต่อองค์กร เขียนแผนกู้คืนระบบจากภัยพิบัติโดยกำหนดสถานการณ์ภัยพิบัติที่ส่งผลกระทบต่อระบบสารสนเทศ การติดตั้งและตั้งค่าศูนย์คอมพิวเตอร์สำรอง แนวทางการเลือกใช้ศูนย์คอมพิวเตอร์สำรองนั้นให้พิจารณาจากแผนการกู้คืน ซึ่งระบุระยะเวลาที่ยอมให้ระบบล่ม และระยะเวลาที่ยอมให้ข้อมูลสูญหาย ข้อมูลเหล่านี้จะถูกนำมาใช้ในการวางกลยุทธ์การกู้คืนระบบและการกู้คืนข้อมูลต่อไป การทดสอบแผนกู้คืนระบบจากภัยพิบัติ ทำการทดสอบแผนกู้คืนระบบจากภัยพิบัติ ปรับปรุงแผนกู้คืนระบบจากภัยพิบัติจากผลการทดสอบ หลังจากนั้นจึงดำเนินการประกาศใช้แผนกู้คืนระบบจากภัยพิบัติต่อไป

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้
1. สมรรถนะย่อย 41402.01 จัดการเหตุการณ์ทางไซเบอร์ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 41402.02 วิเคราะห์ภัยคุกคาม ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
3. สมรรถนะย่อย 41402.03 สืบสวนทางไซเบอร์และพิสูจน์หลักฐานดิจิทัล ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
4. สมรรถนะย่อย 41402.04 กู้คืนระบบจากภัยพิบัติ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์