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

อาชีพนักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ระดับ 5

8. คุณวุฒิวิชาชีพที่เกี่ยวข้อง (Related Professional Qualifications)

ไม่มี

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

รหัสหน่วยสมรรถนะ	**เนื้อหา**
40303	ควบคุมการเข้าถึงทรัพยากรของระบบเครือข่าย
40304	ติดตั้งใช้งานอุปกรณ์และเทคโนโลยีรักษาความมั่นคง
40305	ทดสอบและวิเคราะห์การรักษาความมั่นคงของระบบคอมพิวเตอร์และระบบเครือข่าย
40306	แก้ไขปัญหาด้านความมั่นคงสำหรับเครื่องแม่ข่ายและระบบเครือข่าย

10. ระดับคุณวุฒิ

10.1 สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาความมั่นคงปลอดภัยทางดิจิทัลและส่วนบุคคล
อาชีพนักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ระดับ 5

คุณลักษณะของผลการเรียนรู้ (Characteristics of Outcomes)

เป็นผู้มีสมรรถนะทางเทคนิคในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ สามารถแก้ไขปัญหาในบริบทที่มีการเปลี่ยนแปลงทั่วไป สามารถคิดวิเคราะห์และประเมินสถานการณ์ได้ด้วยตนเอง มีความเป็นผู้นำจัดการผลิตภาพการทำงาน ถ่ายทอดงาน สอนงาน และกำกับดูแลผู้ร่วมงานให้บรรลุงานตามแผนได้โดยมีสมรรถนะในการจัดการระบบความผิดพลาดของเครือข่าย บริการจัดการวัสดุอุปกรณ์เครือข่ายสำรอง และฝึกอบรมเพื่อให้ความรู้และทักษะกับผู้อื่น

การเลื่อนระดับคุณวุฒิวิชาชีพ (Qualification Pathways)

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

- มีประสบการณ์ทำงานด้านการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ หรือที่เกี่ยวข้องไม่น้อยกว่า 5 ปี หรือ

- ผู้ที่สำเร็จการศึกษาระดับ ปริญญาตรี ในด้านการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์หรือที่เกี่ยวข้อง หรือ

- ได้รับรองคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ระดับ 4 แล้วเป็นระยะเวลาไม่น้อยกว่า 1 ปี

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

- ผ่านเกณฑ์การประเมินตามหน่วยสมรรถนะของอาชีพนักทดสอบระบบ ระดับ 5 จำนวน 3 หน่วย

3. ในกรณีต่ออายุหนังสือรับรองมาตรฐานอาชีพให้เป็นไปตามคู่มือสำหรับผู้เข้ารับการประเมินหรือคู่มือเจ้าหน้าที่สอบ

หลักเกณฑ์การต่ออายุหนังสือรับรองมาตรฐานอาชีพ

N/A

กลุ่มบุคคลในอาชีพ (Target Group)

2131.30 ผู้บริหารระบบเครือข่าย

หน่วยสมรรถนะ (หน่วยสมรรถนะทั้งหมดของคุณวุฒิวิชาชีพนี้)

40303 ควบคุมการเข้าถึงทรัพยากรของระบบเครือข่าย

40304 ติดตั้งใช้งานอุปกรณ์และเทคโนโลยีรักษาความมั่นคง

40305 ทดสอบและวิเคราะห์การรักษาความมั่นคงของระบบคอมพิวเตอร์และระบบเครือข่าย

40306 แก้ไขปัญหาด้านความมั่นคงสำหรับเครื่องแม่ข่ายและระบบเครือข่าย

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
พัฒนาศักยภาพของบุคลากรในสาขาอาชีพ ICT ให้สามารถแข่งขันและเป็นที่ยอมรับในระดับสากล	40	ปฏิบัติงานด้าน เครือข่ายและความปลอดภัย ให้ได้ตามมาตรฐานอาชีพ	403	งานบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์

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**
403	งานบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์	40303	ควบคุมการเข้าถึงทรัพยากรของระบบเครือข่าย	40303.01	บริหารจัดการการเข้าถึงของผู้ใช้
				40303.02	กำหนดหน้าที่รับผิดชอบของผู้ใช้งาน
				40303.03	ควบคุมการเข้าถึงทางกายภาพ ระบบปฏิบัติการ เครือข่าย และสารสนเทศ
				40303.04	ควบคุมอุปกรณ์สื่อสารประเภทพกพาและการใช้งานจากภายนอก
		40304	ติดตั้งใช้งานอุปกรณ์และเทคโนโลยีรักษาความมั่นคง	40304.01	ทำ Hardening ระบบปฏิบัติการเครือข่าย
				40304.02	รักษาความปลอดภัยเครือข่ายการสื่อสาร
		40305	ทดสอบและวิเคราะห์การรักษาความมั่นคงของระบบคอมพิวเตอร์และระบบเครือข่าย	40305.01	ใช้เครื่องมือในการทดสอบเจาะระบบเพื่อตรวจสอบหาช่องโหว่และหยุดยั้ง
				40305.02	ทดสอบโจมตีผ่านแอพพลิเคชั่น
				40305.03	ทดสอบโจมตีจากรูปแบบการติดต่อสื่อสารในระบบเครือข่าย
		40306	แก้ไขปัญหาด้านความมั่นคงสำหรับเครื่องแม่ข่ายและระบบเครือข่าย	40306.01	วิเคราะห์ข้อมูลการใช้งานระบบ
				40306.02	ตรวจสอบการบุกรุก
				40306.03	สำรองและกู้คืนข้อมูล
				40306.04	ตรวจสอบและวิเคราะห์หลักฐานทางดิจิทัล

คำอธิบาย

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

1. รหัสหน่วยสมรรถนะ 40303

2. ชื่อหน่วยสมรรถนะ ควบคุมการเข้าถึงทรัพยากรของระบบเครือข่าย

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถบริหารจัดการการเข้าถึงของผู้ใช้ กำหนดหน้าที่รับผิดชอบของผู้ใช้งาน ควบคุมการเข้าถึงทางกายภาพ ระบบปฏิบัติการ เครือข่าย และสารสนเทศ ควบคุมอุปกรณ์สื่อสารประเภทพกพา และ การใช้งานจากภายนอก

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☑	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้ประกอบวิชาชีพด้านเทคโนโลยีสารสนเทศและการสื่อสาร

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที
2529 ผู้ประกอบวิชาชีพด้านฐานข้อมูลและเครือข่าย

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

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
40303.01 บริหารจัดการการเข้าถึงของผู้ใช้	1.1 บริหารจัดการการเข้าถึงของผู้ใช้ให้มีความมั่นคงปลอดภัย 1.2 กำหนดหน้าที่รับผิดชอบของผู้ใช้งานเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต	ข้อสอบข้อเขียน การสัมภาษณ์
40303.02 กำหนดหน้าที่รับผิดชอบของผู้ใช้งาน	2.1 กำหนดหน้าที่รับผิดชอบของผู้ใช้งาน 2.2 กำหนดหน้าที่รับผิดชอบของผู้ใช้งานเพื่อป้องกันการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ	ข้อสอบข้อเขียน การสัมภาษณ์
40303.03 ควบคุมการเข้าถึงทางกายภาพ ระบบปฏิบัติการเครือข่าย และสารสนเทศ	3.1 ควบคุมการเข้าถึงทางกายภาพ ระบบปฏิบัติการเครือข่าย 3.2 ควบคุมการเข้าถึงทางกายภาพ ระบบสารสนเทศ	ข้อสอบข้อเขียน การสัมภาษณ์
40303.04 ควบคุมอุปกรณ์สื่อสารประเภทพกพาและการใช้งานจากภายนอก	4.1 ควบคุมอุปกรณ์สื่อสารประเภทพกพาและการใช้งานจากภายนอก 4.2 ควบคุมการเข้าถึงในด้านต่าง ๆ ต่อไปนี้ให้เกิดความมั่นคงปลอดภัย	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. ความสามารถในด้านการทำเอกสารแสดงการบริหารจัดการการเข้าถึงของผู้ใช้
2. ความสามารถในด้านการทำเอกสารแสดงการกำหนดควบคุมการเข้าถึงทางกายภาพ ระบบปฏิบัติการ เครือข่าย และสารสนเทศ
3. ความสามารถในด้านการทำเอกสารการดำเนินงานเพื่อการควบคุมอุปกรณ์สื่อสารประเภทพกพาและการใช้งานจากภายนอก

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับ การควบคุมการเข้าถึงทรัพยากรต่าง ๆ ของระบบเครือข่าย (ACL: Access Control List)
2. ความรู้เกี่ยวกับ การรักษาความมั่นคงปลอดภัยระบบเครือข่ายเบื้องต้น (Introduction to Network Security)

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมิน และควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. ผลจากการสังเกตการปฏิบัติงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการ สัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ผู้รับการประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ไม่มี

(ข) คำอธิบายรายละเอียด

1. บริหารจัดการควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ได้รับอนุญาตแล้วและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยประกอบไปด้วย

- การลงทะเบียนพนักงาน
- การบริหารจัดการสิทธิการใช้งานระบบตามความจำเป็น
- การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
- การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

2. กำหนดหน้าที่รับผิดชอบของผู้ใช้งานเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ โดยประกอบไปด้วย

- การกำหนดวิธีปฏิบัติที่ดีในการใช้งานรหัสผ่าน
- การป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าใช้งานอุปกรณ์ที่ไม่มีผู้ดูแล
- ป้องกันการทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย

3. ควบคุมการเข้าถึงในด้านต่าง ๆ ต่อไปนี้ให้เกิดความมั่นคงปลอดภัย

- สร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

- ควบคุมการเข้าถึงระบบปฏิบัติการในด้านการใช้งานโปรแกรมประเภทยูทิลิตี้

- ควบคุมการเข้าถึงเครือข่ายด้วยระบบพิสูจน์ตัวตน เพื่อเข้าถึงทรัพยากรที่แบ่งแยกตามความจำเป็น เช่น พอร์ต การแบ่งแยกเครือข่าย การควบคุมการเชื่อมต่อข้ามเครือข่าย

- ควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ และแยกระบบสารสนเทศตามความสำคัญควบคุมอุปกรณ์สื่อสารประเภทพกพาเช่น คอมพิวเตอร์พกพา โทรศัพท์มือถือ แท็บเล็ต เพื่อไม่ให้เกิดความเสี่ยงกับสารสนเทศขององค์กร

4. ควบคุมการเข้าใช้งานสารสนเทศจากภายนอกของบุคลากรเพื่อให้เกิดความมั่นคงปลอดภัย ด้วยการกำหนดสิทธิการใช้งาน การเข้ารหัสการติดต่อสื่อสาร

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 40303.01 บริหารจัดการการเข้าถึงของผู้ใช้ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 40303.02 กำหนดหน้าที่รับผิดชอบของผู้ใช้งาน) ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
3. สมรรถนะย่อย 40303.03 ควบคุมการเข้าถึงทางกายภาพระบบปฏิบัติการเครือข่ายและสารสนเทศ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
4. สมรรถนะย่อย 40303.04 ควบคุมอุปกรณ์สื่อสารประเภทพกพาและการใช้งานจากภายนอก ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

1. รหัสหน่วยสมรรถนะ 40304

2. ชื่อหน่วยสมรรถนะ ติดตั้งใช้งานอุปกรณ์และเทคโนโลยีรักษาความมั่นคง

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

อาชีพนักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถทำ Hardening ระบบปฏิบัติการเครือข่าย และรักษาความปลอดภัยเครือข่ายการสื่อสาร

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☑	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้ประกอบวิชาชีพด้านเทคโนโลยีสารสนเทศและการสื่อสาร

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที
2529 ผู้ประกอบวิชาชีพด้านฐานข้อมูลและเครือข่าย

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

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
40304.01 ทำ Hardening ระบบปฏิบัติการเครือข่าย	1.1 ทำ Hardening ระบบปฏิบัติการเครือข่ายเพื่อไม่ให้สิ่งที่ไม่จำเป็นแสดงออกไปสู่ภายนอก 1.2 ติดตั้ง Antivirus ,Firewalls เพื่อไม่ให้สิ่งที่ไม่จำเป็นแสดงออกไปสู่ภายนอก	ข้อสอบข้อเขียน การสัมภาษณ์
40304.02 รักษาความปลอดภัยเครือข่ายการสื่อสาร	2.1 รักษาความปลอดภัยเครือข่ายการสื่อสาร 2.2 การรักษาความปลอดภัยเครือข่ายการสื่อสารโดยใช้ GPG เพื่อ Encrypt และ Sign E-Mail ,Secure Shell, Secure Copy , Certificates และ SSL, IPsec	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ
1. ความสามารถในด้านการทำเอกสารการทำ Hardening
2. ความสามารถในด้านการทำเอกสารและทักษะการใช้งานเครื่องมือการรักษาความปลอดภัยเครือข่ายการสื่อสาร
(ข) ความต้องการด้านความรู้
1. มีความรู้เรื่อง Prevention
2. มีความรู้เรื่องการทำ Hardening
3. มีความรู้เรื่องการรักษาความปลอดภัยเครือข่ายการสื่อสาร

14. หลักฐานที่ต้องการ (Evidence Guide)

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

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. ผลจากการสังเกตการปฏิบัติงาน

(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

ไม่มี

(ข) คำอธิบายรายละเอียด

1. ทำ Hardening ระบบปฏิบัติการเครือข่ายเพื่อไม่ให้สิ่งที่ไม่จำเป็นแสดงออกไปสู่ภายนอก โดยประกอบไปด้วย

1.1 ทำ Hardening ระบบปฏิบัติการ

1.2 ติดตั้งและใช้งานโปรแกรม Antivirus

1.3 ติดตั้งและใช้งาน Firewalls

2. รักษาความปลอดภัยเครือข่ายการสื่อสาร โดยประกอบไปด้วย

2.1 ใช้ GPG เพื่อ Encrypt และ Sign E-Mail

2.2 Secure Shell (SSH)

2.3 ใช้ Secure Copy (SCP)

2.4 ใช้ Certificates และ SSL

2.5 ใช้ IPsec

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 40304.01 ทำ Hardening ระบบปฏิบัติการเครือข่าย ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

2. สมรรถนะย่อย 40304.02 รักษาความปลอดภัยเครือข่ายการสื่อสาร (Securing Network Communications) ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

1. รหัสหน่วยสมรรถนะ 40305

2. ชื่อหน่วยสมรรถนะ ทดสอบและวิเคราะห์การรักษาความมั่นคงของระบบคอมพิวเตอร์และระบบเครือข่าย

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถใช้เครื่องมือในการทดสอบเจาะระบบเพื่อตรวจสอบหาช่องโหว่และหยุดยั้งทดสอบโจมตีผ่านแอพพลิเคชั่น และทดสอบโจมตีจากรูปแบบการติดต่อสื่อสารในระบบเครือข่าย

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☑	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้ประกอบวิชาชีพด้านเทคโนโลยีสารสนเทศและการสื่อสาร

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที
2529 ผู้ประกอบวิชาชีพด้านฐานข้อมูลและเครือข่าย

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

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
40305.01 ใช้เครื่องมือในการทดสอบเจาะระบบเพื่อตรวจสอบหาช่องโหว่และหยุดยั้ง	1.1 ใช้เครื่องมือในการทดสอบเจาะระบบเพื่อตรวจสอบหาช่องโหว่และหยุดยั้ง 1.2 ใช้เครื่องมือในการตรวจสอบเพื่อหยุดยั้ง	ข้อสอบข้อเขียน การสัมภาษณ์
40305.02 ทดสอบโจมตีผ่านแอพพลิเคชั่น	2.1 ทดสอบโจมตีผ่านแอพพลิเคชั่นและหยุดยั้ง 2.2 ทดสอบโจมตีผ่านแอพพลิเคชั่น โดยใช้ Web SQL Injection, Web Browser Exploits, E-Mail System Exploits	ข้อสอบข้อเขียน การสัมภาษณ์
40305.03 ทดสอบโจมตีจากรูปแบบการติดต่อสื่อสารในระบบเครือข่าย	3.1 ทดสอบโจมตีจากรูปแบบการติดต่อสื่อสารในระบบเครือข่ายและหยุดยั้ง 3.2 ทดสอบโจมตีผ่านแอพพลิเคชั่น โดยใช้ Trojan Attacks , Man-in-the-Middle Attack, Steganography	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. ความสามารถในด้านการทำเอกสารและทักษะการใช้เครื่องมือในการทดสอบเจาะระบบเพื่อตรวจสอบหาช่องโหว่และหยุดยั้ง
2. ความสามารถในด้านการทำเอกสารและทักษะการใช้เครื่องมือทดสอบโจมตีผ่านแอพพลิเคชั่นเพื่อตรวจสอบหาช่องโหว่และหยุดยั้ง
3. ความสามารถในด้านการทำเอกสารและทักษะการใช้เครื่องมือทดสอบโจมตีจากรูปแบบการติดต่อสื่อสารในระบบเครือข่ายเพื่อตรวจสอบหาช่องโหว่และหยุดยั้ง

(ข) ความต้องการด้านความรู้

1. มีความรู้เรื่อง Vulnerabilities and Threats
2. มีความรู้เรื่อง โจมตีผ่านแอพพลิเคชั่น
3. มีความรู้เรื่อง โจมตีจากรูปแบบการติดต่อสื่อสารในระบบเครือข่าย

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

ไม่มี

(ข) คำอธิบายรายละเอียด

1. ใช้เครื่องมือในการทดสอบเจาะระบบเพื่อตรวจสอบหาช่องโหว่และหยุดยั้ง โดยประกอบไปด้วย

- สแกน IP Address และ Port , Service Identity Determination
- GUI-Based Vulnerability Scanners
- Researching System Vulnerabilities
- ใช้ Metasploit
- Password Cracking

2. ทดสอบโจมตีผ่านแอพพลิเคชั่น โดยประกอบไปด้วย

- Web SQL Injection

- Web Browser Exploits

- E-Mail System Exploits

3. ทดสอบโจมตีผ่านแอพพลิเคชั่น โดยประกอบไปด้วย

- Trojan Attacks

- Man-in-the-Middle Attack

- Steganography

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 40305.01

ใช้เครื่องมือในการทดสอบเจาะระบบเพื่อตรวจสอบหาช่องโหว่และหยุดยั้งให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

2. สมรรถนะย่อย 40305.02 ทดสอบโจมตีผ่านแอพพลิเคชั่น (Attacks Against Applications) ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

3. สมรรถนะย่อย 40305.03 ทดสอบโจมตีจากรูปแบบการติดต่อสื่อสารในระบบเครือข่ายให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

1. รหัสหน่วยสมรรถนะ 40306

2. ชื่อหน่วยสมรรถนะ แก้ไขปัญหาด้านความมั่นคงสำหรับเครื่องแม่ข่ายและระบบเครือข่าย

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถวิเคราะห์ข้อมูลการใช้งานระบบ ตรวจสอบการบุกรุก สำรองและกู้คืนข้อมูล ตรวจสอบและวิเคราะห์หลักฐานทางดิจิทัล

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☑	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้ประกอบวิชาชีพด้านเทคโนโลยีสารสนเทศและการสื่อสาร

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2133 ผู้ประกอบวิชาชีพด้านคอมพิวเตอร์ที่มิได้จัดประเภทไว้ในที่อื่น

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

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
40306.01 วิเคราะห์ข้อมูลการใช้งานระบบ	1.1 วิเคราะห์ข้อมูลการใช้งานระบบเพื่อการเตรียมรองรับการโจมตี 1.2 วิเคราะห์ข้อมูลการใช้งานระบบเพื่อให้ทราบความแตกต่างระหว่างสภาวะปกติและเกิดเหตุโดนโจมตี หรือมีการละเมิดสิทธิ์	ข้อสอบข้อเขียน การสัมภาษณ์
40306.02 ตรวจสอบการบุกรุก	2.1 ใช้งานระบบตรวจจับการบุกรุกได้ 2.2 ใช้ Snort ติดตั้งบนระบบปฏิบัติการแล้วทำการทดสอบโจมตีและแก้ไขช่องโหว่ที่ค้นพบ	ข้อสอบข้อเขียน การสัมภาษณ์
40306.03 สำรองและกู้คืนข้อมูล	3.1 สำรองข้อมูล 3.2 คืนข้อมูล	ข้อสอบข้อเขียน การสัมภาษณ์
40306.04 ตรวจสอบและวิเคราะห์หลักฐานทางดิจิทัล	4.1 ตรวจสอบหลักฐานทางดิจิทัล 4.2 วิเคราะห์หลักฐานทางดิจิทัล	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. ความสามารถในด้านการทำเอกสารการเก็บข้อมูลและผลการวิเคราะห์การใช้งาน
2. ความสามารถในด้านการทำเอกสารและทักษะการใช้งานระบบตรวจจับการบุกรุก
3. ความสามารถในด้านการทำเอกสารและทักษะการสำรองและกู้คืนข้อมูล
4. ความสามารถในด้านการเอกสารและทักษะการตรวจสอบและวิเคราะห์หลักฐานทางดิจิทัล

(ข) ความต้องการด้านความรู้

1. มีความรู้เรื่อง Preparing for and Detecting Attacks
2. มีความรู้เรื่อง Digital Forensics

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมิน และควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. ผลจากการสังเกตการปฏิบัติงาน

(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

ไม่มี

(ข) คำอธิบายรายละเอียด

1. วิเคราะห์ข้อมูลการใช้งานระบบเพื่อให้ทราบความแตกต่างระหว่างสภาวะปกติและเกิดเหตุโดนโจมตี หรือมีการละเมิดสิทธิ์

2. ใช้งานระบบตรวจจับการบุกรุก อาทีใช้ Snort ติดตั้งบนระบบปฏิบัติการแล้วทำการทดสอบโจมตีและ สร้างกฎขึ้นมาแก้ไขช่องโหว่ที่ค้นพบ

3. สำรองและกู้คืนข้อมูลในแบบต่าง ๆ ต่อไปนี้

3.1 Full Backup

3.2 Incremental Backup

3.3 Differential Backup

4. ตรวจสอบและวิเคราะห์หลักฐานทางดิจิทัล0 ในปแบบต่าง ๆ ต่อไปนี้

4.1 Live Analysis: Incident Determination

4.2 Acquiring the Data

4.3 Forensic Analysis

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 40306.01 วิเคราะห์ข้อมูลการใช้งานระบบ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 40306.02 ตรวจสอบการบุกรุก ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
3. สมรรถนะย่อย 40306.03 สำรองและกู้คืนข้อมูล ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
4. สมรรถนะย่อย 40306.04 ตรวจสอบและวิเคราะห์หลักฐานทางดิจิทัล ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์