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 6

8. คุณวุฒิวิชาชีพที่เกี่ยวข้อง (Related Professional Qualifications)

ไม่มี

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

รหัสหน่วยสมรรถนะ	**เนื้อหา**
41101	ธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์
41201	วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัยและสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ

10. ระดับคุณวุฒิ

10.1 สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาความมั่นคงปลอดภัยทางดิจิทัลและส่วนบุคคล อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 6

คุณลักษณะของผลการเรียนรู้ (Characteristics of Outcomes)

เป็นผู้มีสมรรถนะด้านการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ สามารถแก้ไขปัญหาในบริบทที่มีความซับซ้อนและเปลี่ยนแปลงตลอดเวลา โดยใช้องค์ความรู้หรือนวัตกรรมเพื่อการพัฒนาระบบงาน ให้คำปรึกษาด้วยประสบการณ์ที่มีความชำนาญด้านการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ โดยมีสมรรถนะในด้านธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์
วิศวกรรมซอฟต์แวร์ด้านความมั่งคงปลอดภัยและสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ

การเลื่อนระดับคุณวุฒิวิชาชีพ (Qualification Pathways)

1. คุณสมบัติของผู้ที่สามารถเข้ารับการประเมินคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 6

- มีประสบการณ์ทำงานด้านธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์ หรือที่เกี่ยวข้องไม่น้อยกว่า 10 ปี หรือ

- ผู้ที่สำเร็จการศึกษาระดับ ปริญญาตรี ในด้านธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์ หรือที่เกี่ยวข้อง หรือ

- ได้รับรองคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 5 แล้วเป็นระยะเวลาไม่น้อยกว่า 1 ปี

2. ผู้ที่จะผ่านการประเมินและได้รับการรับรองคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 6

- ผ่านเกณฑ์การประเมินตามหน่วยสมรรถนะของอาชีพอาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศระดับ 6 จำนวน 2 หน่วย

3. ในกรณีต่ออายุหนังสือรับรองมาตรฐานอาชีพให้เป็นไปตามคู่มือสำหรับผู้เข้ารับการประเมินหรือคู่มือเจ้าหน้าที่สอบ

หลักเกณฑ์การต่ออายุหนังสือรับรองมาตรฐานอาชีพ

N/A

กลุ่มบุคคลในอาชีพ (Target Group)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที

2131.70 ผู้เชี่ยวชาญด้านแคดแคม

หน่วยสมรรถนะ (หน่วยสมรรถนะทั้งหมดของคุณวุฒิวิชาชีพนี้)

41101 ธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์

41201 วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัยและสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ

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	41101	ธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์	41101.01	วางแผนเชิงกลยุทธ์
				41101.02	กำกับดูแลและการบริหารด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
				41101.03	ตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ
412	จัดหาระบบสารสนเทศอย่างมั่นคงปลอดภัย	41201	วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัยและสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ	41201.01	จัดหาระบบที่มีความมั่นคงปลอดภัย
				41201.02	วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัย
				41201.03	สถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ

คำอธิบาย

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

1. รหัสหน่วยสมรรถนะ 41101

2. ชื่อหน่วยสมรรถนะ ธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถกำกับดูแลทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ
รวมไปถึงสามารถวางแผนเชิงกลยุทธ์ทางด้านความมั่นคงปลอดภัยระบบสารสนเทศที่สอดคล้องกับองค์กร

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☑	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้บริหารเครือข่ายคอมพิวเตอร์ ผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ, ผู้บริหารด้านการจัดการความเสี่ยงของสารสนเทศ

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)
41101.01 วางแผนเชิงกลยุทธ์	1.1 ออกแบบกลยุทธ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศที่สอดคล้องกับแผนกลยุทธ์ขององค์กร 1.2 จัดทำแผนปฏิบัติที่สอดคล้องกับกลยุทธ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ ดำเนินการตามแผน และติดตามประเมินผลการดำเนินการตามแผน 1.3 ดำเนินการตรวจสอบผลของการดำเนินการตามแผนด้านความมั่นคงปลอดภัยระบบสารสนเทศ	การสัมภาษณ์ แฟ้มสะสมผลงาน
41101.02 กำกับดูแลและการบริหารด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	2.1 จัดการนโยบายด้านการรักษาความปลอดภัยสารสนเทศ 2.2 จัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ 2.3 จัดการโครงการทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ 2.4 จัดการบริการด้านความมั่นคงสารสนเทศ	การสัมภาษณ์ แฟ้มสะสมผลงาน

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
41101.03 ตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ	3.1 จัดทำกระบวนการตรวจสอบระบบสารสนเทศ 3.2 วางแผนการตรวจสอบ 3.3 ดำเนินการตรวจสอบและการติดตามผลของการตรวจสอบ 3.4 เขียนรายงานการตรวจสอบ	การสัมภาษณ์ แฟ้มสะสมผลงาน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. สามารถออกแบบกลยุทธ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศที่สอดคล้องกับแผนกลยุทธ์ขององค์กร
2. สามารถจัดทำแผนปฏิบัติที่สอดคล้องกับกลยุทธ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ ดำเนินการตามแผน และติดตาม ประเมินผลการดำเนินการตามแผน
3. สามารถดำเนินการตรวจสอบผลของการดำเนินการตามแผนด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างสม่ำเสมอ
4. สามารถจัดการนโยบายด้านการรักษาความปลอดภัยสารสนเทศและเอกสารอื่น ๆ ที่เกี่ยวข้อง
5. สามารถจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
6. สามารถจัดการโครงการทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ
7. สามารถจัดการบริการด้านความมั่นคงสารสนเทศ
8. สามารถจัดทำกระบวนการตรวจสอบระบบสารสนเทศ
9. สามารถวางแผนการตรวจสอบ
10. สามารถดำเนินการตรวจสอบและการติดตามผลของการตรวจสอบ
11. เขียนรายงานการตรวจสอบ

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ การออกแบบกลยุทธ์ และแผนปฏิบัติด้านความมั่นคงปลอดภัยระบบสารสนเทศ รวมทั้งหลักการตรวจสอบ
2. ความรู้เกี่ยวกับการติดตามแนวโน้มภัยคุกคามรูปแบบใหม่ทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ รวมทั้งเทคโนโลยีที่เกี่ยวข้อง
3. ความรู้เกี่ยวกับการจัดการความเสี่ยงสารสนเทศ
4. ความรู้เกี่ยวกับกฎหมาย กฎระเบียบ ข้อบังคับ และแนวปฏิบัติที่ดีทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ
5. ความรู้เกี่ยวกับระบบปฏิบัติการและระบบเครือข่าย
6. ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
7. ความรู้เกี่ยวกับการตรวจสอบระบบสารสนเทศ
8. ความรู้เกี่ยวกับกระบวนการทางธุรกิจ
9. ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
10. ความรู้เกี่ยวกับหลักการบริหารจัดการโครงการ
11. ความรู้เกี่ยวกับระบบสารสนเทศและระบบเครือข่าย
12. ความรู้เกี่ยวกับการประมวลผลข้อมูล
13. ความรู้เกี่ยวกับการตอบสนองต่อภัยคุกคามด้านไซเบอร์
14. ความรู้เกี่ยวกับการจัดการบริการทางด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของระบบสารสนเทศ

14. หลักฐานที่ต้องการ (Evidence Guide)

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

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. ทดสอบความรู้โดยใช้การสอบสัมภาษณ์

2. พิจารณาเพิ่มเติมจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. แฟ้มสะสมผลงาน ได้แก่ ใบผ่านงาน ประกาศนียบัตร วุฒิบัตร และเอกสารผลงานต่าง ๆ ที่เกี่ยวข้องกับความรู้ทางด้านธรรมาภิบาลความมั่นคงปลอดภัยระบบสารสนเทศและการวางแผนเชิงกลยุทธ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ผู้รับการประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบสัมภาษณ์

2. พิจารณาจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ในการปฏิบัติงานให้คำนึงถึงการวางแผนเชิงกลยุทธ์ การกำกับดูแลและการบริหารด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ การตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ

(ข) คำอธิบายรายละเอียด

1. การวางแผนเชิงกลยุทธ์ ควรมีการจัดทำกลยุทธ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศจะต้องศึกษาสิ่งต่าง ๆ ได้แก่ บริบทขององค์กร ศึกษาพันธกิจ เป้าหมายและกิจกรรมต่าง ๆ ภายในองค์กร ปัจจัยภายในและภายนอกที่มีผลกระทบต่อองค์กร เป็นต้น การจัดทำแผนปฏิบัติด้านความมั่นคงปลอดภัยระบบสารสนเทศต้องมีความสอดคล้องกับกลยุทธ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ โดยมีองค์ประกอบ ได้แก่ เป้าหมาย วัตถุประสงค์ ตัวชี้วัด กิจกรรมโครงการต่าง ๆ ระยะเวลา ผู้รับผิดชอบ เป็นต้น การตรวจสอบผลการดำเนินการตามแผนความมั่นคงปลอดภัยระบบสารสนเทศ จะต้องมีการติดตามทุก ๆ 3 เดือนและให้ทำการทบทวนผลการดำเนินการให้เป็นไปตามแผนที่วางไว้

2. การกำกับดูแลและการบริหารด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ การจัดการนโยบายด้านการรักษาความปลอดภัยสารสนเทศควรพิจารณาให้มีความสอดคล้องกับเป้าหมายในการดำเนินธุรกิจขององค์กร ในขณะเดียวกันจะต้องได้รับการอนุมัติจากผู้บริหารระดับสูง มีการประกาศใช้และสื่อสารไปให้คนภายในองค์กรรับทราบ การจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ควรพิจารณาความเสี่ยงทางด้านข้อมูล ที่องค์กรพบมีการเลือกวิธีการวิเคราะห์ความเสี่ยงที่เหมาะสม เลือกตัวควบคุมด้านความมั่นคงปลอดภัย รวมถึงระบุระดับการยอมรับความเสี่ยงที่องค์กรสามารถยอมรับได้ การจัดการโครงการทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ ให้พิจารณาประเด็นต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศที่แทรกเข้าไปอยู่ในขั้นตอนต่าง ๆ ของการจัดการโครงการ การจัดการบริการด้านความมั่นคงสารสนเทศให้พิจารณาแนวทางการจัดการความมั่นคงปลอดภัยของบริการสารสนเทศในมุมมองต่าง ๆ ครอบคลุมการรักษาความลับของข้อมูล การรักษาความคงสภาพของข้อมูล และการรักษาความพร้อมใช้ของข้อมูล

3. การตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ การจัดทำกระบวนการตรวจสอบระบบสารสนเทศ ควรพิจารณาถึงปัจจัยแวดล้อมต่าง ๆ เช่น รูปแบบของธุรกิจ จำนวนพนักงานในองค์กร วัฒนธรรมขององค์กร การวางแผนการตรวจสอบ ควรประเมินจากขอบเขตของระบบที่จะทำการตรวจสอบ รวมทั้งชนิดของการตรวจสอบเพื่อกำหนดแผนงาน ระยะเวลาที่ต้องใช้ รวมทั้งจำนวนผู้ตรวจสอบ การดำเนินการตรวจสอบและการติดตามผลของการตรวจสอบ ผู้ตรวจสอบควรปฏิบัติตามแผนการตรวจสอบอย่างเคร่งครัด มีจริยธรรมและจรรยาบรรณในการปฏิบัติงาน และติดตามผลของการตรวจสอบตามวงรอบที่เหมาะสม การเขียนรายงานการตรวจสอบ ควรมีลักษณะที่เป็นแบบแผนที่แน่นอน เข้าใจง่าย มีข้อมูลครบถ้วน

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะ 41101.01 วางแผนเชิงกลยุทธ์ ให้ทำการทดสอบโดยใช้แบบสัมภาษณ์และพิจารณาจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์

2. สมรรถนะ 41101.02 กำกับดูแลและการบริหารด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
ให้ทำการทดสอบโดยใช้แบบสัมภาษณ์และพิจารณาจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์

3. สมรรถนะ 41101.03 ตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ ให้ทำการทดสอบโดยใช้แบบสัมภาษณ์และพิจารณาจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์

1. รหัสหน่วยสมรรถนะ 41201

2. ชื่อหน่วยสมรรถนะ วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัยและสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ

3. ทบทวนครั้งที่ 1 / -

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถ จัดหาระบบที่มีความมั่นคงปลอดภัย วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัย สถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☑	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้บริหารเครือข่ายคอมพิวเตอร์ ผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ, ผู้บริหารด้านการจัดการความเสี่ยงของสารสนเทศ

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)
41201.01 จัดหาระบบที่มีความมั่นคงปลอดภัย	1.1 จัดทำนโยบายทางด้าน supply chain security และนโยบายด้านการจัดการความเสี่ยง 1.2 ประเมินประสิทธิผลของงานจัดซื้อในส่วนที่เกี่ยวข้องกับความต้องการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการประเมินความเสี่ยงของ supply chain 1.3 ตรวจสอบเพื่อให้มั่นใจว่ากระบวนการจัดซื้อทั้งหมดสอดคล้องกับความต้องการทางด้านความมั่นคงปลอดภัยระบบสารสนเทศและเป้าหมายขององค์กร	การสัมภาษณ์ แฟ้มสะสมผลงาน
41201.02 วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัย	2.1 วิเคราะห์ความต้องการของผู้ใช้และความต้องการของซอฟต์แวร์ 2.2 แปลงความต้องการทางด้านความมั่นคงปลอดภัยเป็นข้อกำหนดในการออกแบบระบบ 2.3 พัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย 2.4 ตรวจหาช่องโหว่ในระหว่างการพัฒนาโปรแกรมและแก้ไขทบทวนชุดคำสั่ง	การสัมภาษณ์ แฟ้มสะสมผลงาน
41201.03 สถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ	3.1 วางแผนสถาปัตยกรรมของระบบ 3.2 ออกแบบความมั่นคงปลอดภัย	การสัมภาษณ์ แฟ้มสะสมผลงาน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. สามารถจัดทำนโยบายทางด้าน supply chain security และนโยบายด้านการจัดการความเสี่ยง
2. สามารถประเมินประสิทธิผลของงานจัดซื้อในส่วนที่เกี่ยวข้องกับความต้องการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการประเมินความเสี่ยงของ supply chain
3. สามารถตรวจสอบเพื่อให้มั่นใจว่ากระบวนการจัดซื้อทั้งหมดสอดคล้องกับความต้องการทางด้านความมั่นคงปลอดภัยระบบสารสนเทศและเป้าหมายขององค์กร
4. สามารถวิเคราะห์ความต้องการของผู้ใช้และความต้องการของซอฟต์แวร์
5. สามารถแปลงความต้องการทางด้านความมั่นคงปลอดภัยเป็นข้อกำหนดในการออกแบบระบบ
6. สามารถพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย
7. สามารถตรวจหาช่องโหว่ในระหว่างการพัฒนาโปรแกรมและแก้ไข ทบทวนชุดคำสั่ง (Source code review)
8. สามารถวางแผนสถาปัตยกรรมของระบบให้สอดคล้องกับความต้องการของผู้ใช้
9. สามารถออกแบบความมั่นคงปลอดภัยของระบบให้สอดคล้องกับความต้องการ

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับการจัดการทรัพยากร รวมทั้งความต้องการทรัพยากรของระบบ
2. ความรู้เกี่ยวกับการจัดการความเสี่ยง
3. ความรู้เกี่ยวกับ Supply Chain
4. ความรู้เกี่ยวกับกฎหมายที่เกี่ยวข้องกับ Supply Chain
5. ความรู้เกี่ยวกับการพัฒนาระบบสารสนเทศ
6. ความรู้เกี่ยวกับระบบปฏิบัติการและระบบเครือข่าย
7. ความรู้เกี่ยวกับการตั้งค่าระบบอย่างมั่นคงปลอดภัย
8. ความรู้เกี่ยวกับวิศวกรรมซอฟต์แวร์
9. ความรู้เกี่ยวกับสถาปัตยกรรมคอมพิวเตอร์
10. ความรู้เกี่ยวกับสถาปัตยกรรมความมั่นคงปลอดภัยขององค์กร
11. ความรู้เกี่ยวกับระบบฐานข้อมูล
12. ความรู้เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ
13. ความรู้เกี่ยวกับการตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศ
14. ความรู้เกี่ยวกับ Access Control Model ต่าง ๆ

14. หลักฐานที่ต้องการ (Evidence Guide)

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

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน
2. ข้อมูลจากแฟ้มสะสมงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการสัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ผู้รับการประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบสัมภาษณ์
2. พิจารณาจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ในการปฏิบัติงานให้คำนึงถึงการจัดหาระบบที่มีความมั่นคงปลอดภัย วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัย สถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ

(ข) คำอธิบายรายละเอียด

1. การจัดหาระบบที่มีความมั่นคงปลอดภัย การจัดทำนโยบายทางด้าน supply chain security และนโยบายด้านการจัดการความเสี่ยง ควรต้องได้รับการอนุมัติจากผู้บริหารระดับสูง มีการประกาศใช้อย่างเป็นทางการ และสื่อสารไปยังผู้ที่เกี่ยวข้องให้รับทราบโดยทั่วกัน การประเมินประสิทธิผลของงานจัดซื้อในส่วนที่เกี่ยวข้องกับความต้องการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการประเมินความเสี่ยงของ supply chain ให้มีการดำเนินการอย่างต่อเนื่องตามวงรอบ มีการกำหนดตัวชี้วัดที่แน่นอน การตรวจสอบเพื่อให้มั่นใจว่ากระบวนการจัดซื้อทั้งหมดสอดคล้องกับความต้องการทางด้านความมั่นคงปลอดภัยระบบสารสนเทศและเป้าหมายขององค์กร ควรดำเนินการโดยผู้ที่ไม่มีส่วนได้ส่วนเสียกับการจัดซื้อ และมีการตรวจสอบอย่างสม่ำเสมอ

2. วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัย การวิเคราะห์ความต้องการของผู้ใช้และความต้องการของซอฟต์แวร์ ให้พิจารณาดำเนินการวิเคราะห์ทั้งความต้องการของผู้ใช้ และความต้องการของซอฟต์แวร์ ในด้านต่าง ๆ ให้รอบด้าน โดยใช้เครื่องมือในการเก็บข้อมูลที่เหมาะสม การแปลงความต้องการทางด้านความมั่นคงปลอดภัยเป็นข้อกำหนดในการออกแบบระบบ ให้เลือกเครื่องมือหรือรูปแบบการแปลงที่เหมาะสม การพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย ให้พิจารณาแนวทางการนำเอาแนวคิดทางด้านความมั่นคงปลอดภัยมาพิจารณาในทุกเฟสของการพัฒนาซอฟต์แวร์ การตรวจหาช่องโหว่ในระหว่างการพัฒนาโปรแกรมและแก้ไข ทบทวนชุดคำสั่ง (Source code review) อาจมีการพิจารณาดำเนินการทั้งในช่วงของการพัฒนาซอฟต์แวร์ และการทดสอบตั้งแต่ Unit Testing ไปจนถึง User Acceptance Testing

3. สถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ การวางแผนสถาปัตยกรรมของระบบให้สอดคล้องกับความต้องการของผู้ใช้ ควรมีการศึกษาสถาปัตยกรรมของระบบ รวมทั้งประเด็นทางด้านความมั่นคงปลอดภัยระบบสารสนเทศแบบต่าง ๆ ที่ได้มีการประยุกต์ใช้ เพื่อเลือกแนวทางที่เหมาะสมกับองค์กร การออกแบบความมั่นคงปลอดภัยของระบบให้สอดคล้องกับความต้องการ เป็นขั้นตอนที่มีความสำคัญ หลังจากที่ได้มีการเก็บข้อมูล และวางแผนสถาปัตยกรรมทางด้านความมั่นคงปลอดภัยของระบบแล้ว จึงดำเนินการออกแบบ เพื่อประยุกต์สถาปัตยกรรมทางด้านความมั่นคงปลอดภัยระบบสารสนเทศที่เหมาะสมสำหรับองค์กร หลังจากนั้นจึงดำเนินการตามสถาปัตยกรรมทางด้านความมั่นคงปลอดภัยระบบสารสนเทศที่ได้เลือกใช้ และมีการติดตาม ทบทวนผลของการดำเนินการตามสถาปัตยกรรมทางด้านความมั่นคงปลอดภัยระบบ

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 41201.01 จัดหาระบบที่มีความมั่นคงปลอดภัยให้ทำการทดสอบโดยใช้แบบสัมภาษณ์และพิจารณาจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์
2. สมรรถนะย่อย 41201.02 วิศวกรรมซอฟต์แวร์ด้านความมั่นคงปลอดภัยให้ทำการทดสอบโดยใช้แบบสัมภาษณ์และพิจารณาจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์
3. สมรรถนะย่อย 41201.03 สถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ ให้ทำการทดสอบโดยใช้แบบสัมภาษณ์และพิจารณาจากแฟ้มสะสมผลงานได้แก่ ใบผ่านงาน ประกาศนียบัตร ใบวุฒิบัตร ภาพถ่ายผลงาน และเอกสารต่าง ๆ ที่แสดงถึงประสบการณ์