มาตรฐานอาชีพและคุณวุฒิวิชาชีพ
Occupational Standard and Professional Qualifications

สมรรถนะสนับสนุนการทำงานด้านดิจิทัลสำหรับข้าราชการ และบุคลากรภาครัฐ

จัดทำโดย สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)
ร่วมกับ มหาวิทยาลัยมหิดล

1. ชื่อมาตรฐานอาชีพ

สมรรถนะสนับสนุนการทำงานด้านดิจิทัลสำหรับข้าราชการ และบุคลากรภาครัฐ

2. ประวัติการปรับปรุงมาตรฐาน

ทบทวน ครั้งที่ 1 พ.ศ. 2567

3. ทะเบียนอ้างอิง (Imprint)

N/A

4. ข้อมูลเบื้องต้น

การทบทวนมาตรฐานสมรรถนะดิจิทัลสำหรับข้าราชการ และบุคลากรภาครัฐ มีวัตถุประสงค์เพื่อทบทวนมาตรฐานให้มีความทันสมัยสอดคล้องกับสถานการณ์ปัจจุบัน และสอดคล้องตามมติคณะรัฐมนตรีเมื่อวันที่ 12 มีนาคม พ.ศ.2567 เรื่อง แนวทางการพัฒนาบุคลากรภาครัฐ พ.ศ. 2566 – 2570 ซึ่งคณะรัฐมนตรีมีมติเห็นชอบแนวทางการพัฒนาบุคลากรภาครัฐ พ.ศ. 2566 – 2570 ตามมติคณะกรรมการข้าราชการพลเรือน (ก.พ.) ในการประชุมครั้งที่ 2/2566 เมื่อวันที่ 20 กุมภาพันธ์ 2566 โดยที่มาของแนวทางการพัฒนาบุคลากรภาครัฐ พ.ศ. 2566 – 2570 เริ่มต้นจากแนวทางการพัฒนาบุคลากรภาครัฐ พ.ศ.2563 – 2565 ที่มีเป้าหมายในการพัฒนากรอบความคิดและทักษะ ตามแนวทางการพัฒนา 1) Ecosystem 2) Skill set 3) Mindset ที่ขับเคลื่อนโดยการกำหนดบทบาทของหน่วยงานและบุคลากร และแนวทางการพัฒนาทักษะด้านดิจิทัล พ.ศ. 2561 – 2565 ที่มีเป้าหมายให้ภาครัฐมีกำลังคนที่มีทักษะด้านดิจิทัลที่เท่าทันการเปลี่ยนแปลง โดยมีแนวทางในการปรับบทบาทและพฤติกรรมเพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล (ทักษะดิจิทัล 7 กลุ่มทักษะ) เพื่อการขับเคลื่อนพัฒนาการปรับเปลี่ยนรูปแบบการดำเนินงาน และการให้บริการของหน่วยงานให้มีความทันสมัย โดยที่มีความเห็นจากส่วนราชการในการนำแนวทางทั้ง 2 แนวทางข้างต้นไปใช้ในการปรับปรุงแนวทางการพัฒนาบุคลากรภาครัฐ พ.ศ. 2566 – 2570 โดยมีวัตถุประสงค์เพื่อปรับให้กระชับเข้าใจง่ายมากขึ้น โดยการพัฒนาทักษะที่หลากหลาย ลดความซ้ำซ้อน สนับสนุนการพัฒนาให้ครอบคลุมทุกกลุ่มบุคลากร เพิ่มเติมการกำหนดให้มีการพัฒนาด้านคุณธรรม จริยธรรม โดยที่มีการกำหนดผลลัพธ์การพัฒนาที่ชัดเจน โดยทั้งนี้มีภาพรวมในการดำเนินงานคือการกำหนดให้การวางแผนกาลังคน และแผนการพัฒนามีความเชื่อมโยงกัน การส่งเสริมหน่วยงานต้นแบบในด้านต่าง ๆ เน้นการติดตามและประเมินผลการพัฒนาอย่างต่อเนื่อง และเป็นระบบ

โดยมาตรฐานสมรรถนะสนับสนุนการทำงานด้านดิจิทัลสำหรับข้าราชการและบุคลากรภาครัฐ ประกอบด้วยทักษะดิจิทัลที่เป็นทักษะพื้นฐานสำหรับทุกกลุ่มเป้าหมาย 3 ด้าน ได้แก่ ความเข้าใจและใช้เทคโนโลยีดิจิทัล (Digital Literacy) การปฏิบัติตามและใช้กฎหมายด้านดิจิทัล (Digital Governance) และความเป็นผู้นำด้านดิจิทัล (Digital Leadership) และ (ทักษะที่สามารถเลือกพัฒนาตามภารกิจหรืองานที่ได้รับมอบหมายโดยเชื่อมโยงกับแผนพัฒนาดิจิทัลของหน่วยงาน 4 ด้าน ได้แก่ การประยุกต์ใช้เทคโนโลยีเพื่อการพัฒนางาน (Digital Technology) การพัฒนานวัตกรรมเพื่อการบริการ (Digital Service) การใช้ประโยชน์และการใช้ข้อมูลร่วมกัน (Data Utilization and Sharing) ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) รวมทั้งสิ้น 7 ด้าน โดยจำแนกกลุ่มบุคลากรเป็น 2 กลุ่มหลัก คือ กลุ่มผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล (IT) และกลุ่มผู้ปฏิบัติงานที่ไม่เกี่ยวข้องกับด้านเทคโนโลยีดิจิทัลโดยตรง (Non-IT) โดยในแต่ละกลุ่มประกอบด้วย 3 ตำแหน่ง คือ กลุ่มผู้ปฏิบัติงาน กลุ่มผู้อำนวยการหรือหัวหน้างาน และกลุ่มผู้บริหาร หรือตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับกระทรวง กรม รวมหน่วยสมรรถนะทั้งสิ้น 44 หน่วยสมรรถนะ

5. ประวัติการปรับปรุงมาตรฐานในแต่ละครั้ง

ครั้งที่ 1 พ.ศ. 2567

6. ครั้งที่

1

7. คุณวุฒิวิชาชีพที่ครอบคลุม (Professional Qualifications included)

สมรรถนะสนับสนุนการทำงานด้านดิจิทัลสำหรับข้าราชการ และบุคลากรภาครัฐ

สำหรับผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล (IT)

ผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล (IT) ตำแหน่งประเภทผู้บริหาร หรือตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับกระทรวง กรม

8. คุณวุฒิวิชาชีพที่เกี่ยวข้อง (Related Professional Qualifications)

สมรรถนะสนับสนุนการทำงานด้านการใช้ดิจิทัล (Digital Literacy)

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

รหัสหน่วยสมรรถนะ	เนื้อหา
CS100	วิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
CS200	กำหนดมาตรการป้องกันภัยไซเบอร์ในระบบดิจิทัล
CS300	ตรวจจับภัยไซเบอร์ในสภาพแวดล้อมเครือข่าย
CS400	พัฒนาแผนการตอบสนองและกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์
CS500	กำกับ ดูแลด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

10. ระดับคุณวุฒิ

10.1 สมรรถนะสนับสนุนการทำงานด้านดิจิทัลสำหรับข้าราชการ และบุคลากรภาครัฐ สำหรับผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล (IT) ผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล (IT) ตำแหน่งประเภทผู้บริหาร หรือตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับกระทรวง กรม

คุณลักษณะของผลการเรียนรู้ (Characteristics of Outcomes)

คุณลักษณะของผลการเรียนรู้ที่พึงประสงค์ของข้าราชการและบุคลากรภาครัฐ สำหรับผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล (IT) ในตำแหน่งผู้บริหารเทคโนโลยีดิจิทัลของหน่วยงานหรือผู้บริหารระดับกระทรวง กรม จะมีความสามารถในการใช้เครื่องมือดิจิทัลและใช้โปรแกรมพื้นฐานและโปรแกรมเสริมเพื่อการทำงานในสำนักงานการปฏิบัติและกำกับดูแลองค์กรให้มีการดำเนินงานตามกฎหมาย กรอบธรรมาภิบาล และหลักปฏิบัติด้านดิจิทัล สามารถประยุกต์ใช้กรอบการดำเนินงานร่วมกันสำหรับพัฒนารัฐบาลดิจิทัลปฏิบัติตามข้อตกลงระดับการให้บริการร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง สามารถบริหารความเสี่ยงดิจิทัล จัดทำ แก้ไขเพิ่มเติม หรือยกเลิกกฎหมายเพื่อการปรับเปลี่ยนไปสู่รัฐบาลดิจิทัล กำกับติดตามการพัฒนาข้อมูลในหน่วยงานให้เป็นไปตาม หลักธรรมาภิบาล มีความเข้าใจสถาปัตยกรรมองค์กรและการบูรณาการการทำงานข้ามหน่วยงานเพื่อรองรับการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล ผู้บริหารจะสามารถออกแบบ จัดเตรียมทรัพยากร ริเริ่ม และดำเนินโครงการดิจิทัลได้อย่างมีประสิทธิภาพ พร้อมทั้งทบทวนและปิดโครงการ รวมถึงการพัฒนาคนพันธุ์ใหม่ และขับเคลื่อนการเปลี่ยนแปลงสู่องค์กรดิจิทัลอย่างต่อเนื่อง เพื่อส่งเสริมการทำงานร่วมกันและการบริหารจัดการกระบวนการเปลี่ยนแปลงสู่องค์กรดิจิทัลที่มีประสิทธิภาพ

ทั้งนี้ข้าราชการและบุคลากรภาครัฐ สำหรับผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล (IT) ในตำแหน่งผู้บริหารเทคโนโลยีดิจิทัลของหน่วยงานหรือผู้บริหารระดับกระทรวง กรม สามารถเลือกพัฒนาสมรรถนะตามภารกิจหรืองานที่ได้รับมอบหมายโดยเชื่อมโยงกับแผนพัฒนาดิจิทัลของหน่วยงาน ที่จะสามารถใช้เทคโนโลยีดิจิทัลเพื่อสนับสนุนการเปลี่ยนผ่านสู่องค์กรดิจิทัล พัฒนาซอฟต์แวร์ตามแนวทางพลวัตร สามารถนำเทคโนโลยีปัญญาประดิษฐ์และ Generative AI มาใช้งานในการทำงาน มีความสามารถในการกำหนดกรอบการให้บริการ วางกลยุทธ์การให้บริการดิจิทัล และออกแบบนวัตกรรมบริการใหม่ๆ โดยสร้างเครือข่ายที่เสริมสร้างนวัตกรรมบริการดิจิทัล และพัฒนาบริการที่มีประสิทธิภาพและสามารถนำไปใช้งานได้จริงในระยะเวลาและทรัพยากรที่จำกัด ความรู้ในการบริหารจัดการข้อมูล การจัดทำบัญชีข้อมูล และการวิเคราะห์ข้อมูลเพื่อการนำไปใช้งานยังเป็นสิ่งจำเป็น พร้อมกับการวิเคราะห์ความมั่นคงปลอดภัยไซเบอร์และพัฒนามาตรการป้องกันภัยในสภาพแวดล้อมเครือข่าย และมีความสามารถในการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่องเพื่อรักษาความปลอดภัยของข้อมูลและระบบทั้งหมดในหน่วยงาน

การเลื่อนระดับคุณวุฒิวิชาชีพ (Qualification Pathways)

การเข้าสู่สมรรถนะสนับสนุนการทำงานด้านดิจิทัลสำหรับข้าราชการและบุคลากรภาครัฐสำหรับผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล (IT) ในตำแหน่งประเภทผู้บริหาร หรือตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับกระทรวง กรม สำหรับข้าราชการและบุคลากรภาครัฐที่ดำรงตำแหน่งประเภทบริหารที่ได้รับมอบหมายภารกิจที่เกี่ยวข้องกับงานด้านเทคโนโลยีดิจิทัลหรือดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับกระทรวง กรม ตามหนังสือสำนักงาน ก.พ. ที่ นร 1013/ว 8 ลงวันที่ 29 ธันวาคม 2563 เรื่องการปรับปรุงแนวทางการบริหารจัดการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐ

หลักเกณฑ์การต่ออายุหนังสือรับรองมาตรฐานอาชีพ

-

กลุ่มบุคคลในอาชีพ (Target Group)

ผู้ที่ปฏิบัติงานด้านเทคโนโลยีดิจิทัลในส่วนราชการ ซึ่งดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ เจ้าพนักงาน เครื่องคอมพิวเตอร์ หรือตำแหน่งในสายงานอื่นหรือประเภทอื่นที่ได้รับมอบหมายให้ปฏิบัติงานที่ต้องใช้ความรู้เชิงเทคนิคเกี่ยวกับเทคโนโลยีดิจิทัล

หน่วยสมรรถนะ (หน่วยสมรรถนะทั้งหมดของคุณวุฒิวิชาชีพนี้)

CS100 วิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

CS200 กำหนดมาตรการป้องกันภัยไซเบอร์ในระบบดิจิทัล

CS300 ตรวจจับภัยไซเบอร์ในสภาพแวดล้อมเครือข่าย

CS400 พัฒนาแผนการตอบสนองและกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์

CS500 กำกับ ดูแลด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

DG100 ปฏิบัติตามกฎหมายกรอบ ธรรมาภิบาลและหลักปฏิบัติที่ดีด้านดิจิทัล

DG200 กำกับและตรวจสอบการปฏิบัติตามกฎหมาย กรอบธรรมาภิบาล และหลักปฏิบัติที่ดีด้านดิจิทัล

DG300 ประยุกต์ใช้กรอบการดำเนินงานร่วมกันสำหรับพัฒนารัฐบาลดิจิทัล

DG400 ปฏิบัติตามข้อตกลงระดับการให้บริการร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง

DG500 บริหารความเสี่ยงดิจิทัล

DG600 จัดทำ แก้ไขเพิ่มเติม หรือยกเลิกกฎหมายเพื่อการปรับเปลี่ยนไปสู่รัฐบาลดิจิทัล

DG700 กำกับติดตามการพัฒนาข้อมูลในหน่วยงานให้เป็นไปตามหลักธรรมาภิบาล

DG800 เข้าใจสถาปัตยกรรมองค์กรเพื่อรองรับการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล

DG900 กำกับการใช้งานสถาปัตยกรรมองค์กร

DL100 กำหนดนโยบายเพื่อการบูรณาการ การทำงานข้ามหน่วยงาน

DL1000 บริหารจัดการกระบวนการเปลี่ยนแปลงสู่องค์กรดิจิทัล

DL200 ออกแบบองค์กรดิจิทัล

DL300 จัดเตรียมทรัพยากรเพื่อการบูรณาการสำหรับองค์กรดิจิทัล

DL400 ริเริ่มและวางแผนโครงการภายใต้รัฐบาลดิจิทัล

DL500 ดำเนินโครงการและควบคุมโครงการดิจิทัล

DL600 ทบทวนโครงการและปิดโครงการ

DL700 พัฒนาคนพันธุ์ใหม่สำหรับพัฒนาองค์กรดิจิทัล

DL800 พัฒนาการทำงานร่วมกันเป็นทีมแบบข้ามหน่วยงาน

DL900 ขับเคลื่อนการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล

DLit100 ใช้งานดิจิทัลขั้นต้น

DLit200 ใช้โปรแกรมพื้นฐานเพื่อการทำงานในสำนักงาน

DLit300 ใช้โปรแกรมเสริมเพื่อการทำงานในสำนักงาน

DS100 กำหนดกรอบการให้บริการแบบเชื่อมโยง

DS200 วางกลยุทธ์การให้บริการดิจิทัลและนำสู่การปฏิบัติ

DS300 ออกแบบนวัตกรรมบริการ

DS400 สร้างเครือข่ายเพื่อสร้างนวัตกรรมบริการดิจิทัล

DS500 สร้างนวัตกรรมบริการหลักที่ใช้การได้และสำเร็จได้

DS600 ปรับปรุงงานบริการรดิจิทัลเพื่อยกระดับอย่างต่อเนื่อง

DS700 บริหารประสิทธิภาพการบริการและการทำงานดิจิทัล

DT100 ใช้เทคโนโลยีดิจิทัล เพื่อสนับสนุนการเปลี่ยนผ่านสู่องค์กรดิจิทัล

DT200 ให้บริการด้วยเทคโนโลยีดิจิทัล

DT300 พัฒนาซอฟต์แวร์ตามแนวทางพลวัตรปรับต่อเนื่อง

DT400 เข้าใจพื้นฐานเทคโนโลยีปัญญาประดิษฐ์

DT500 ใช้งาน Generative AI เพื่อการทำงาน

DUS100 รู้หลักการบริหารจัดการข้อมูล

DUS200 จัดทำบัญชีข้อมูลและบริหารคุณภาพข้อมูล

DUS300 จัดทำคลังข้อมูลเพื่อการใช้งานภายใน และระหว่างหน่วยงาน

DUS400 วิเคราะห์ข้อมูลพื้นฐาน

DUS500 วิเคราะห์ข้อมูลขนาดใหญ่เพื่อการนำไปใช้งาน

ตารางแผนผังแสดงหน้าที่

1. ตารางแสดงหน้าที่ 1

ประกาศใช้ ณ 26/12/2567

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**
เพื่อการเปลี่ยนผ่านสู่รัฐบาล ดิจิทัลที่มีการบูรณาการเสมือนเป็นองค์กรเดียว (Connected and Open Government) ที่ประกอบด้วย การพัฒนาองค์กรดิจิทัลที่มีวัฒนธรรมดิจิทัล (Digital Culture/ Digital DNA) มีการเชื่อมโยงและบูรณาการกระบวนการทำงานและข้อมูล มีการให้บริการสาธารณะที่เป็นเลิศ โดยมีประชาชนเป็นศูนย์กลาง (Citizen Centric Excellence Service) ด้วยนวัตกรรม	01	ใช้เทคโนโลยีดิจิทัลอย่างรู้เท่าทัน	Dlit	นำประสบการณ์ด้านเทคโนโลยีดิจิทัลมาปรับใช้เพื่อการพัฒนางานและพัฒนาองค์กร ด้วยการประยุกต์ใช้เทคโนโลยีดิจิทัลอย่างถูกต้อง เหมาะสม และมีประสิทธิภาพ
	06	ใช้ประโยชน์ข้อมูลและการใช้ข้อมูลร่วมกัน (Data Utilization and Sharing)	DUS	สามารถวิเคราะห์ และใช้ประโยชน์ข้อมูล เพื่อประกอบการปฏิบัติงานหรือการพัฒนาหน่วยงาน รวมถึงแลกเปลี่ยน เชื่อมโยงข้อมูลในหน่วยงานและระหว่างหน่วยงาน
	02	กำกับดูแลการปฏิบัติตามกฎหมาย และมาตรฐานการจัดการดิจิทัล	DG	สื่อสาร ถ่ายทอด และประยุกต์ใช้ความรู้ความเข้าใจด้านนโยบาย กฎหมาย และมาตรฐานต่างๆ เพื่อการปฏิบัติงานหรือปรับปรุงแนวทางการทำงานให้ดีขึ้น
	03	ใช้เทคโนโลยีดิจิทัลเพื่อการประยุกต์และพัฒนาองค์กร	DS	ออกแบบและปรับปรุงกระบวนการทำงานหรือการให้บริการ โดยคำนึงถึงการอำนวยความสะดวกให้แก่ผู้รับบริการ เพิ่มความรวดเร็ว และลดข้อผิดพลาดต่างๆ โดยนำเทคโนโลยีดิจิทัลที่เหมาะสมมายกระดับคุณภาพงานบริการ
			DT	คัดสรร เลือก หรือนำเทคโนโลยีที่ทันสมัยมาใช้ในองค์กร เพื่อปรับเปลี่ยนรูปแบบ/กระบวนการดำเนินงานและการให้บริการให้อยู่ในรูปแบบดิจิทัล
	04	ใช้ดิจิทัลเพื่อการวางแผน บริหารจัดการและนำองค์กร	DL	DL มีภาวะผู้นำองค์กรดิจิทัล (Digital Leadership) ในมิติของการทำงานเป็น ทีม การบริหารจัดการทีมที่มีคุณภาพ การตัดสินใจที่มีคุณภาพการสื่อสารจูงใจและเจรจาต่อรอง การกระตุ้นการเรียนรู้ และการเป็นแบบอย่าง (Role model) การพัฒนาภาวะผู้นำให้แก่บุคลากร เพื่อมุ่งสู่การเป็นองค์กรดิจิทัล SPM กำหนดนโยบายทิศทางเพื่อพัฒนาองค์กรดิจิทัล ออกแบบองค์กรและจัดเตรียมทรัพยากรสำหรับองค์กรดิจิทัล ริเริ่มโครงการ วางแผนบริหารโครงการ การดำเนินโครงการ ติดตามและประเมิน โครงการ เพื่อการพัฒนารัฐบาลดิจิทัล
	05	ใช้เทคโนโลยีดิจิทัล เพื่อขับเคลื่อนการเปลี่ยนแปลงและสร้างสรรค์	DL	DTR ขับเคลื่อนองค์กรดิจิทัล ทั้งในมิติของการสร้าง/บริหารการเปลี่ยนแปลงองค์กรเพื่อไปสู่องค์กรดิจิทัล การสร้างวัฒนธรรมองค์กรดิจิทัล การสื่อสารองค์กร การสร้างแนวร่วม/การมีส่วนร่วมของบุคลากรในทุกระดับ
	07	ใช้ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)	CS	ตระหนัก เข้าใจ รับมือ ป้องกัน หรือบริหารจัดการต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์

คำอธิบาย ตารางแผนผังแสดงหน้าที่เป็นแผนผังที่ใช้วิเคราะห์หน้าที่งานเพื่อให้ได้หน้าที่หลัก (Key Function)

2. ตารางแสดงหน้าที่ 1 (ต่อ)

ประกาศใช้ ณ 26/12/2567

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**
CS	ตระหนัก เข้าใจ รับมือ ป้องกัน หรือบริหารจัดการต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์	CS100	วิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน	CS101	เข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร
				CS102	วิเคราะห์บริบทองค์กรเพื่อระบุความเสี่ยงด้านความมั่นคง ปลอดภัยไซเบอร์ขององค์กร
				CS103	ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร
		CS200	กำหนดมาตรการป้องกันภัยไซเบอร์ในระบบดิจิทัล	CS201	วิเคราะห์ความเสี่ยงจากการโจมตีทางไซเบอร์
				CS202	กำหนดมาตรการป้องกันไซเบอร์ที่เหมาะสม
		CS300	ตรวจจับภัยไซเบอร์ในสภาพแวดล้อมเครือข่าย	CS301	ตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้นในสภาพแวดล้อมเครือข่าย
				CS302	วิเคราะห์ข้อมูลเพื่อตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้น
		CS400	พัฒนาแผนการตอบสนองและกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์	CS401	วิเคราะห์ความเสี่ยงและผลกระทบของเหตุการณ์ผิดปกติ
				CS402	พัฒนาแผนการตอบสนองเมื่อ เกิดเหตุการณ์ผิดปกติ
				CS403	พัฒนาแผนการกู้คืนเมื่อเกิดเหตุการณ์ผิดปกติ
		CS500	กำกับ ดูแลด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง	CS501	ตรวจสอบและติดตามความมั่นคงปลอดภัยไซเบอร์ของระบบ คอมพิวเตอร์และเครือข่าย
				CS502	วิเคราะห์และประเมินผลข้อมูลเพื่อระบุและแก้ไขปัญหาด้าน ความมั่นคงปลอดภัยไซเบอร์
DG	สื่อสาร ถ่ายทอด และประยุกต์ใช้ความรู้ความเข้าใจด้านนโยบาย กฎหมาย และมาตรฐานต่างๆ เพื่อการปฏิบัติงานหรือปรับปรุงแนวทางการทำงานให้ดีขึ้น	N/A	N/A	N/A	N/A
DL	DL มีภาวะผู้นำองค์กรดิจิทัล (Digital Leadership) ในมิติของการทำงานเป็น ทีม การบริหารจัดการทีมที่มีคุณภาพ การตัดสินใจที่มีคุณภาพการสื่อสารจูงใจและเจรจาต่อรอง การกระตุ้นการเรียนรู้และการเป็นแบบอย่าง (Role model) การพัฒนาภาวะผู้นำให้แก่บุคลากรเพื่อมุ่งสู่การเป็นองค์กรดิจิทัล SPM กำหนดนโยบายทิศทางเพื่อพัฒนาองค์กรดิจิทัล ออกแบบองค์กรและจัดเตรียมทรัพยากรสำหรับองค์กรดิจิทัล ริเริ่มโครงการ วางแผนบริหารโครงการ การดำเนินโครงการ ติดตามและประเมินโครงการ เพื่อการพัฒนารัฐบาลดิจิทัล	N/A	N/A	N/A	N/A

หน้าที่หลัก Key Function		หน่วยสมรรถนะ Unit of Competence		หน่วยสมรรถนะย่อย Element of Competence	
รหัส	**คำอธิบาย**	**รหัส**	**คำอธิบาย**	**รหัส**	**คำอธิบาย**
DL	DTR ขับเคลื่อนองค์กรดิจิทัล ทั้งในมิติของการสร้าง/บริหารการเปลี่ยนแปลงองค์กรเพื่อไปสู่องค์กรดิจิทัล การสร้างวัฒนธรรมองค์กรดิจิทัล การสื่อสารองค์กร การสร้างแนวร่วม/การมีส่วนร่วมของบุคลากรในทุกระดับ	N/A	N/A	N/A	N/A
Dlit	นำประสบการณ์ด้านเทคโนโลยีดิจิทัลมาปรับใช้เพื่อการพัฒนางานและพัฒนาองค์กร ด้วยการประยุกต์ใช้เทคโนโลยีดิจิทัลอย่างถูกต้อง เหมาะสม และมีประสิทธิภาพ	N/A	N/A	N/A	N/A
DS	ออกแบบและปรับปรุงกระบวนการทำงานหรือการให้บริการ โดยคำนึงถึงการอำนวยความสะดวกให้แก่ผู้รับบริการ เพิ่มความรวดเร็ว และลดข้อผิดพลาดต่างๆ โดยนำเทคโนโลยีดิจิทัลที่เหมาะสมมายกระดับคุณภาพงานบริการ	N/A	N/A	N/A	N/A
DT	คัดสรร เลือก หรือนำเทคโนโลยีที่ทันสมัยมาใช้ในองค์กร เพื่อปรับเปลี่ยนรูปแบบ/กระบวนการดำเนินงานและการให้บริการให้อยู่ในรูปแบบดิจิทัล	N/A	N/A	N/A	N/A

หน้าที่หลัก Key Function		หน่วยสมรรถนะ Unit of Competence		หน่วยสมรรถนะย่อย Element of Competence	
รหัส	**คำอธิบาย**	**รหัส**	**คำอธิบาย**	**รหัส**	**คำอธิบาย**
DUS	สามารถวิเคราะห์ และใช้ประโยชน์ข้อมูล เพื่อประกอบการปฏิบัติงานหรือการพัฒนาหน่วยงานรวมถึงแลกเปลี่ยน เชื่อมโยงข้อมูลในหน่วยงาน และระหว่างหน่วยงาน	N/A	N/A	N/A	N/A

คำอธิบาย

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

1. รหัสหน่วยสมรรถนะ CS100

2. ชื่อหน่วยสมรรถนะ วิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

3. ทบทวนครั้งที่ N/A / 2567

4. สร้างใหม่ ☑ **ปรับปรุง** ☐

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

ผู้ที่ผ่านหน่วยสมรรถนะนี้ จะมีความรู้ความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร
สามารถวิเคราะห์บริบทองค์กรเพื่อระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร สามารถประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรได้

7. สำหรับระดับคุณวุฒิ

☑

8. กลุ่มอาชีพ (Sector)

ข้าราชการและบุคลากรภาครัฐ

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

N/A

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

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4. พระราชบัญญัติว่าด้วยการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
5. มาตรฐานและข้อกำหนด เช่น ISO/IEC 27001, NIST Cybersecurity Framework, และ CIS Controls

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
CS101 เข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร	ระบุบริบทในด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรได ระบุข้อมูลที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ขององค์กรได้ ระบุทรัพยากรที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ขององค์กรได้ ระบุระบบที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ขององค์กรได้	ข้อสอบข้อเขียน
CS102 วิเคราะห์บริบทองค์กรเพื่อระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร	ระบุปัจจัยที่มีผลต่อความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร ระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นในองค์กรได้ ระบุและประเมินทรัพย์สินทางไซเบอร์ได้ วิเคราะห์ผลกระทบของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อองค์กร	ข้อสอบข้อเขียน

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
CS103 ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร	วิเคราะห์ข้อมูลที่สำคัญสำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้ ระบุระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร ระบุผลการประเมินและแนวทางในการลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร ระบุแนวทางในการตรวจสอบและเฝ้าระวัง	ข้อสอบข้อเขียน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

มีความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์และการบริหารจัดการความเสี่ยง

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

- ทักษะในการวิเคราะห์และประเมินความเสี่ยง
- ทักษะในการใช้เครื่องมือและเทคโนโลยีที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
- ทักษะในการจัดการและเก็บรักษาข้อมูลที่เกี่ยวข้องกับการวิเคราะห์ความเสี่ยงได้อย่างเป็นระบบ
- ทักษะในการสื่อสารที่มีประสิทธิภาพ

(ข) ความต้องการด้านความรู้

- ความรู้ความเข้าใจในหลักการและวิธีการปกป้องข้อมูลและระบบจากภัยคุกคามไซเบอร์
- ความรู้ความเข้าใจในการทำงานของระบบเครือข่ายคอมพิวเตอร์ ระบบปฏิบัติการต่าง ๆ ที่ใช้ภายในองค์กร
- ความรู้ด้านกฎหมาย และข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
- ความรู้ด้านการบริหารจัดการความเสี่ยง

14. หลักฐานที่ต้องการ (Evidence Guide)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

- หลักฐานการวิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร
- เอกสารหรือรายงานที่แสดงถึงการวิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร

(ข) หลักฐานความรู้ (Knowledge Evidence)

- ใบวุฒิการศึกษา
- ประกาศนียบัตรต่าง ๆ จากการฝึกอบรมพัฒนาหรือการเรียนรู้ที่เกี่ยวข้อง

(ค) คำแนะนำในการประเมิน

- ตรวจประเมินหลักฐานโดยพิจารณาจากร่องรอยหลักฐานที่เกี่ยวข้องทั้งหลักฐานด้านปฏิบัติงานและ หลักฐานด้านความรู้

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

หน่วยความสามารถนี้ครอบคลุมการวิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรมีขอบเบตครอบคลุมโครงสร้างองค์กร การบริหารจัดการความเสี่ยง การใช้เทคโนโลยีสารสนเทศ และความต้องการขององค์กรการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์จะต้องพิจารณาจากปัจจัย
ต่าง ๆ เช่น ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นในองค์กร ผลกระทบของ ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อองค์กร และแนวทางในลดความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์จะต้องมีความแม่นยำและเชื่อถือได้
โดยพิจารณาจากข้อมูลที่มีอยู่และผลการวิเคราะห์

(ข) คำอธิบายรายละเอียด

- เข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร มีขอบเขตที่ครอบคลุมถึง การปกป้องระบบ เครือข่าย

และโปรแกรมขององค์กรจากการโจมตีทางไซเบอร์ที่อาจทำให้ข้อมูลสูญหาย ถูกขโมย
หรือถูกเข้าถึงโดยไม่ได้รับอนุญาตซึ่งการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรจะรวมถึง หลายๆ ด้าน ได้แก่

- การรักษาความลับของข้อมูล (Confidentiality): การป้องกันไม่ให้ข้อมูลสำคัญขององค์กรถูก เข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต

- การรักษาความถูกต้องของข้อมูล (Integrity): การป้องกันการแก้ไขหรือทำลายข้อมูล โดยไม่ได้รับอนุญาต ทำให้ข้อมูลมีความถูกต้องและน่าเชื่อถือ
- การรักษาความพร้อมใช้งานของระบบ (Availability): การทำให้ระบบและข้อมูลสามารถ เข้าถึงได้เสมอเมื่อต้องการใช้งาน
- การตรวจสอบและควบคุมการเข้าถึง (Access Control): การกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบเพื่อให้แน่ใจว่าบุคคลที่มีสิทธิ์เท่านั้นที่สามารถเข้าถึงข้อมูลได้
- การรักษาความปลอดภัยของเครือข่าย (Network Security): การป้องกันการเข้าถึงเครือข่ายของ องค์กรโดยไม่ได้รับอนุญาต การป้องกันไวรัสและมัลแวร์ และการป้องกันการโจมตีที่มาจากภายนอก
- การรักษาความปลอดภัยของแอปพลิเคชัน (Application Security): การป้องกันช่องโหว่และการโจมตีที่มาจากแอปพลิเคชันที่องค์กรใช้งาน
- การบริหารจัดการเหตุการณ์และการตอบสนอง (Incident Management and Response): การวางแผนและการดำเนินการตอบสนองต่อเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น รวมถึงการฟื้นฟูระบบหลังจากเหตุการณ์

16. หน่วยสมรรถนะร่วม (ถ้ามี)

N/A

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

N/A

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

สอบข้อเขียน

1. รหัสหน่วยสมรรถนะ CS200

2. ชื่อหน่วยสมรรถนะ กำหนดมาตรการป้องกันภัยไซเบอร์ในระบบดิจิทัล

3. ทบทวนครั้งที่ N/A / 2567

4. สร้างใหม่ ☑ **ปรับปรุง** ☐

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

ผู้ที่ผ่านหน่วยสมรรถนะนี้ จะสามารถวิเคราะห์ความเสี่ยงจากการโจมตีทางไซเบอร์โดยใช้เทคนิคการวิเคราะห์ความเสี่ยง สามารถระบุและประเมินความเสี่ยง รวมถึงกำหนดออกแบบ และพัฒนาแนวทางการป้องกันภัยไซเบอร์ได้อย่างเหมาะสม

7. สำหรับระดับคุณวุฒิ

☑

8. กลุ่มอาชีพ (Sector)

ข้าราชการและบุคลากรภาครัฐ

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

N/A

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

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4. พระราชบัญญัติว่าด้วยการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
5. มาตรฐานและข้อกำหนด เช่น ISO/IEC 27001, NIST Cybersecurity Framework, และ CIS Controls

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
CS201 วิเคราะห์ความเสี่ยงจากการโจมตีทางไซเบอร์	วิเคราะห์ความเสี่ยงจากการโจมตีทางไซเบอร์โดยใช้เทคนิคการวิเคราะห์ความเสี่ยง ระบุความเสี่ยงจากการโจมตีทางไซเบอร์ที่อาจเกิดขึ้น ประเมินความเสี่ยงจากการโจมตีทางไซเบอร์โดยใช้มาตรฐานความปลอดภัย	ข้อสอบข้อเขียน
CS202 กำหนดมาตรการป้องกันไซเบอร์ที่เหมาะสม	กำหนดมาตรการป้องกันไซเบอร์ที่เหมาะสมตามความเสี่ยงจากการโจมตีทางไซเบอร์ ออกแบบระบบป้องกันไซเบอร์ที่เหมาะสม พัฒนาแนวทางการป้องกันไซเบอร์ได้อย่างเหมาะสม	ข้อสอบข้อเขียน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ผู้ปฏิบัติงานต้องมีความรู้พื้นฐานด้านความปลอดภัยของข้อมูลและระบบไอที

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ
- ทักษะในการการวิเคราะห์ และประเมินความเสี่ยง
- ทักษะในการออกแบบระบบป้องกันไซเบอร์
- ทักษะในการตรวจสอบ และการตอบสนองต่อการบุกรุกทางไซเบอร์

(ข) ความต้องการด้านความรู้
- ความรู้พื้นฐานด้านความปลอดภัยของข้อมูล
- ความรู้พื้นฐานด้านระบบไอที
- ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์
- ความรู้ด้านกฎหมายและการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับความปลอดภัยไซเบอร์
- ความรู้ในการพัฒนาและบริหารจัดการนโยบายความปลอดภัยไซเบอร์ในองค์กร

14. หลักฐานที่ต้องการ (Evidence Guide)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)
- หลักฐานการกำหนดมาตรการป้องกันภัยไซเบอร์ในระบบดิจิทัล
- เอกสารหรือรายงานที่แสดงถึงการกำหนดมาตรการป้องกันภัยไซเบอร์ในระบบดิจิทัล

(ข) หลักฐานความรู้ (Knowledge Evidence)
- ใบวุฒิการศึกษา
- ประกาศนียบัตรต่าง ๆ จากการฝึกอบรมพัฒนาหรือการเรียนรู้ที่เกี่ยวข้อง

(ค) คำแนะนำในการประเมิน
- ตรวจประเมินหลักฐานโดยพิจารณาจากร่องรอยหลักฐานที่เกี่ยวข้อง ทั้งหลักฐานด้านปฏิบัติงานและหลักฐานด้านความรู้

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

หน่วยความสามารถนี้ครอบคลุมถึงการกำหนดมาตรการป้องกันไซเบอร์ในระบบไอทีที่หลากหลาย รวมถึงระบบเครือข่าย ระบบฐานข้อมูล ระบบปฏิบัติการ และระบบอื่น ๆ ที่เกี่ยวข้องกับความปลอดภัยของข้อมูล ผู้ปฏิบัติงานต้องสามารถวิเคราะห์ความเสี่ยงและการกำหนดมาตรการป้องกันไซเบอร์ที่เหมาะสมสำหรับระบบไอทีที่หลากหลาย โดยคำนึงถึงมาตรฐานความปลอดภัยและข้อกำหนดขององค์กร ผู้ปฏิบัติงานต้องสามารถทำงานร่วมกับทีมงานและผู้เกี่ยวข้องอื่น ๆ เพื่อประกันความปลอดภัยของข้อมูลและระบบไอที

(ข) คำอธิบายรายละเอียด

- วิเคราะห์ความเสียงจากการโจมตีทางไซเบอร์

มีขอบเขตที่ครอบคุลมถึงกระบวนการในการประเมินและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ต่อระบบข้อมูลหรือโครงสร้างพื้นฐานทางเทคโนโลยีขององค์กร โดยจะพิจารณาถึงความเสี่ยงที่อาจเกิดจากภัยคุกคามที่อาจทำให้เกิดความเสียหายต่อข้อมูล ความเสียหายทางการเงิน หรือการหยุดชะงักในการดำเนินงานขององค์กร กระบวนการนี้จะช่วยให้สามารถระบุความเสี่ยงที่มีความสำคัญและจัดทำแผนเพื่อการจัดการและบรรเทาความเสี่ยงได้อย่างมีประสิทธิภาพ

- กำหนดมาตรการป้องกันไขเบอร์ที่เหมาะสม มีขอบเขตที่ครอบคลุมถึงการวางแผนและดำเนินการเพื่อปกป้องระบบและข้อมูลในองค์กรจากภัยคุกคามทางไซเบอร์ เช่น การแฮกข้อมูล การโจมตีจากไวรัส หรือการรั่วไหลของข้อมูลที่เหมาะสม ตามความเสียงจากการโจมตีทางไซเบอร์

16. หน่วยสมรรถนะร่วม (ถ้ามี)

N/A

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

N/A

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

สอบข้อเขียน

1. รหัสหน่วยสมรรถนะ CS300

2. ชื่อหน่วยสมรรถนะ ตรวจจับภัยไซเบอร์ในสภาพแวดล้อมเครือข่าย

3. ทบทวนครั้งที่ 1 / 2567

4. สร้างใหม่ ☑ **ปรับปรุง** ☐

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

ผู้ที่ผ่านหน่วยสมรรถนะนี้ จะมีความรู้ความสามารถในการตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้นในสภาพแวดล้อมเครือข่าย สามารถวิเคราะห์ข้อมูลและตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้น รวมทั้งสามารถดำเนินการตามขั้นตอนในการจัดการภัยไซเบอร์ได้อย่างเหมาะสม

7. สำหรับระดับคุณวุฒิ

☑

8. กลุ่มอาชีพ (Sector)

ข้าราชการและบุคลากรภาครัฐ

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

N/A

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

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4. พระราชบัญญัติว่าด้วยการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
5. มาตรฐานและข้อกำหนด เช่น ISO/IEC 27001, NIST Cybersecurity Framework, และ CIS Controls

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
CS301 ตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้นในสภาพแวดล้อมเครือข่าย	วิเคราะห์ข้อมูลเพื่อตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้น ตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้นในระบบดิจิทัล ดำเนินการตามขั้นตอนในการจัดการภัยไซเบอร์ที่ตรวจจับได้	ข้อสอบข้อเขียน
CS302 วิเคราะห์ข้อมูลเพื่อตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้น	วิเคราะห์ข้อมูลลักษณะของภัยไซเบอร์ที่อาจเกิดขึ้น วิเคราะห์ข้อมูลลักษณะของระบบเครือข่ายที่ อาจเกิดขึ้น วิเคราะห์ข้อมูลลักษณะของระบบความมั่นคงที่อาจเกิดขึ้น	ข้อสอบข้อเขียน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ผู้ปฏิบัติงานต้องมีความรู้ความสามารถในการใช้งานระบบเครือข่ายและระบบความมั่นคง

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ
- ทักษะการวิเคราะห์ภัยคุกคาม
- ทักษะในการใช้เครื่องมือและเทคโนโลยีการรักษาความปลอดภัย
- ทักษะในการระบุเหตุการณ์การรักษาความปลอดภัย
- ทักษะการสื่อสาร และการประสานงาน

(ข) ความต้องการด้านความรู้
- ความรู้ความสามารถในการใช้งานระบบเครือข่าย
- ความรู้ความสามารถในการใช้งานระบบความมั่นคง
- ความรู้ความสามารถในการวิเคราะห์ข้อมูล
- ความรู้ด้านมาตรฐานและนโยบายความปลอดภัยไซเบอร์
- ความรู้ด้านเทคนิคการบุกรุก และการป้องกัน
- ความรู้ด้านกฎหมาย และข้อกำหนดด้านความเป็นส่วนตัวและการคุ้มครองข้อมูล

14. หลักฐานที่ต้องการ (Evidence Guide)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)
- หลักฐานการตรวจจับภัยไซเบอร์ในระบบดิจิทัล
- เอกสารหรือรายงานที่แสดงถึงการตรวจจับภัยไซเบอร์ในระบบดิจิทัล

(ข) หลักฐานความรู้ (Knowledge Evidence)
- ใบวุฒิการศึกษา
- ประกาศนียบัตรต่าง ๆ จากการฝึกอบรมพัฒนาหรือการเรียนรู้ที่เกี่ยวข้อง

(ค) คำแนะนำในการประเมิน
- ตรวจประเมินหลักฐานโดยพิจารณาจากร่องรอยหลักฐานที่เกี่ยวข้อง ทั้งหลักฐานด้านปฏิบัติงานและหลักฐานด้านความรู้

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

หน่วยความสามารถนี้ครอบคลุมถึงการตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้นในสภาพแวดล้อมเครือข่ายทุกประเภท รวมทั้งระบบเครือข่ายที่ใช้งานในองค์กร ระบบเครือข่ายที่ใช้งานในภาครัฐ และระบบเครือข่ายที่ใช้งานในภาคเอกชน หน่วยความสามารถนี้ยังครอบคลุมถึงการตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้นในสภาพแวดล้อมเครือข่ายที่มีความซับซ้อนและความเสี่ยงสูง รวมทั้งระบบเครือข่ายที่มีการเชื่อมต่อกับระบบอื่นๆ หน่วยความสามารถนี้จะช่วยให้ผู้ปฏิบัติงานสามารถตรวจจับภัยไซเบอร์ได้อย่างรวดเร็วและแม่นยำ รวมทั้งสามารถลดความเสี่ยงของภัยไซเบอร์ที่อาจเกิดขึ้นในสภาพแวดล้อมเครือข่าย

(ข) คำอธิบายรายละเอียด

- ตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้นในระบบดิจิทัล มีขอบเขตที่ครอบคลุมถึง กระบวนการหรือเทคนิคในการค้นหาและระบุพฤติกรรมหรือกิจกรรมที่อาจเป็นอันตรายต่อระบบคอมพิวเตอร์หรือเครือข่าย โดยจะมีการใช้เครื่องมือและเทคนิคต่าง ๆ เช่น การวิเคราะห์การเข้าใช้งานระบบ การตรวจสอบกิจกรรมที่ผิดปกติ การใช้ซอฟต์แวร์ป้องกันไวรัส หรือการใช้ระบบตรวจจับการบุกรุก (IDS) เพื่อป้องกันและตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้นอย่างทันท่วงที
- วิเคราะห์ข้อมูลเพื่อตรวจจับภัยไซเบอร์ที่อาจเกิดขึ้น มีขอบเขตที่ครอบคลุมถึง กระบวนการที่ใช้ในการสำรวจและตรวจสอบข้อมูลจากแหล่งต่าง ๆ เพื่อตรวจจับพฤติกรรมหรือเหตุการณ์ที่อาจบ่งชี้ถึงภัยคุกคามหรือการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต รวมถึงการวิเคราะห์พฤติกรรมของผู้ใช้หรือระบบเพื่อตรวจจับการเปลี่ยนแปลงที่อาจบ่งชี้ถึงการโจมตี และการตรวจสอบการรับส่งข้อมูลในเครือข่ายเพื่อตรวจจับกิจกรรมที่ผิดปกติหรือไม่ปกติ

16. หน่วยสมรรถนะร่วม (ถ้ามี)

N/A

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

N/A

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

สอบข้อเขียน

1. รหัสหน่วยสมรรถนะ CS400

2. ชื่อหน่วยสมรรถนะ พัฒนาแผนการตอบสนองและกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์

3. ทบทวนครั้งที่ N/A / 2567

4. สร้างใหม่ ☑ **ปรับปรุง** ☐

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

ผู้ที่ผ่านหน่วยสมรรถนะนี้ จะสามารถวิเคราะห์ความเสี่ยงและผลกระทบของเหตุการณ์ผิดปกติ รวมทั้งสามารถพัฒนาแผนการตอบสนองและแผนการกู้คืนเมื่อเกิดเหตุการณ์ผิดปกติได้

7. สำหรับระดับคุณวุฒิ

☑

8. กลุ่มอาชีพ (Sector)

ข้าราชการและบุคลากรภาครัฐ

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

N/A

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

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
3. พระราชบัญญัติว่าด้วยการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
4. มาตรฐานและข้อกำหนด เช่น ISO/IEC 27001, NIST Cybersecurity Framework, และ CIS Controls
5. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
CS401 วิเคราะห์ความเสี่ยงและผลกระทบของเหตุการณ์ผิดปกติ	วิเคราะห์ความเสี่ยงและผลกระทบของเหตุการณ์ผิดปกติ ระบุความเสี่ยงและผลกระทบที่อาจเกิดขึ้น ประเมินความเสี่ยงและผลกระทบของเหตุการณ์ผิดปกติ	ข้อสอบข้อเขียน
CS402 พัฒนาแผนการตอบสนองเมื่อ เกิดเหตุการณ์ผิดปกติ	พัฒนาแผนการตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติ ระบุวิธีการตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติ ประเมินความเหมาะสมของแผนการตอบสนอง	ข้อสอบข้อเขียน
CS403 พัฒนาแผนการกู้คืนเมื่อเกิดเหตุการณ์ผิดปกติ	พัฒนาแผนการกู้คืนเมื่อเกิดเหตุการณ์ผิดปกติ ระบุวิธีการกู้คืนเมื่อเกิดเหตุการณ์ผิดปกติ ประเมินความเหมาะสมของแผนการกู้คืน	ข้อสอบข้อเขียน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ผู้ปฏิบัติงานต้องมีความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อย 2 ปี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ
- ทักษะในการวิเคราะห์ความเสี่ยงและผลกระทบ
- ทักษะในการพัฒนาแผนการตอบสนองและแผนการกู้คืน

(ข) ความต้องการด้านความรู้
- ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์
- ความรู้เกี่ยวกับเหตุการณ์และการตอบสนองต่อเหตุการณ์ไซเบอร์
- ความรู้เกี่ยวกับกฎหมาย และข้อกำหนดด้านไซเบอร์
- ความรู้เกี่ยวกับเทคโนโลยี และเครื่องมือที่ใช้ในการตรวจจับ ป้องกัน และกู้คืนจากการโจมตีไซเบอร์
- ความรู้ความเข้าใจในการสร้างและปรับปรุงนโยบายเพื่อตอบสนองและจากเหตุการณ์ไซเบอร์

14. หลักฐานที่ต้องการ (Evidence Guide)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)
- หลักฐานการพัฒนาแผนการตอบสนองและกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์
- เอกสารหรือรายงานที่แสดงถึงการพัฒนาแผนการตอบสนองและกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์

(ข) หลักฐานความรู้ (Knowledge Evidence)
- ใบวุฒิการศึกษา
- ประกาศนียบัตรต่าง ๆ จากการฝึกอบรมพัฒนาหรือการเรียนรู้ที่เกี่ยวข้อง

(ค) คำแนะนำในการประเมิน
- ตรวจประเมินหลักฐานโดยพิจารณาจากร่องรอยหลักฐานที่เกี่ยวข้อง ทั้งหลักฐานด้านปฏิบัติงานและหลักฐานด้านความรู้

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ผู้ปฏิบัติงานต้องสามารถวิเคราะห์ความเสี่ยงและผลกระทบของเหตุการณ์ผิดปกติได้อย่างถูกต้องและเหมาะสมรวมทั้งพัฒนาแผนการตอบสนองและแผนการกู้คืนเพื่อลดผลกระทบและฟื้นฟูระบบให้กลับมาเป็นปกติได้ภายในเวลาที่เหมาะสม โดยผู้ปฏิบัติงานต้องสามารถทำงานร่วมกับทีมและผู้เกี่ยวข้องได้อย่างมีประสิทธิภาพรวมทั้งสามารถปรับตัวและแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็วและเหมาะสม

(ข) คำอธิบายรายละเอียด

- วิเคราะห์ความเสี่ยงและผลกระทบของเหตุการณ์ผิดปกติ มีขอบเขตที่ครอบคลุมถึง กระบวนการที่ช่วยในการประเมินความเสียงและผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ด้านความปลอดภัยไซเบอร์ที่อาจเกิดขึ้นระบบสารสนเทศหรือเครือข่ายขององค์กร
- พัฒนาแผนการตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติ มีขอบเขตที่ครอบคลุมถึงการสร้างแผนและขั้นตอนที่ชัดเจนสำหรับการจัดการกับเหตุการณ์ที่อาจเกิดขึ้นเกี่ยวกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย เช่น การโจมตีทางไขเบอร์ หรือการละเมิดข้อมูล เป็นต้น
- พัฒนาแผนการกู้คืนเมื่อเกิดเหตุการณ์ผิดปกติ มีขอบเขตที่ครอบคลุมถึง การสร้างแผนงานที่ชัดเจนสามารถระบุวิธีการกู้คืนเมื่อเกิดเหตุการณ์ผิดปกติ สามามารถประเมินความเหมาะสมของแผนการกู้คืน และมีการจัดเตรียมไว้ล่วงหน้าเพื่อรับมือกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ เช่น การโจมตีจากแฮกเกอร์ การรั่วไหลของข้อมูล หรือการระงับการทำงานของระบบ

16. หน่วยสมรรถนะร่วม (ถ้ามี)

N/A

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

N/A

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

สอบข้อเขียน

1. รหัสหน่วยสมรรถนะ CS500

2. ชื่อหน่วยสมรรถนะ กำกับ ดูแลด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

3. ทบทวนครั้งที่ N/A / 2567

4. สร้างใหม่ ☑ **ปรับปรุง** ☐

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

ผู้ที่ผ่านหน่วยสมรรถนะนี้จะสามารถตรวจสอบและติดตามความมั่นคงปลอดภัยไซเบอร์ของระบบคอมพิวเตอร์และเครือข่ายเครือข่ายอย่างต่อเนื่อง เพื่อป้องกันและตรวจสอบภัยไซเบอร์ รวมถึงสามารถวิเคราะห์ข้อมูลเพื่อระบุปัญหาและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์

7. สำหรับระดับคุณวุฒิ

☑

8. กลุ่มอาชีพ (Sector)

ข้าราชการและบุคลากรภาครัฐ

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

N/A

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

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4. พระราชบัญญัติว่าด้วยการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
5. มาตรฐานและข้อกำหนด เช่น ISO/IEC 27001, NIST Cybersecurity Framework, และ CIS Controls

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
CS501 ตรวจสอบและติดตามความมั่นคงปลอดภัยไซเบอร์ของระบบคอมพิวเตอร์และเครือข่าย	ตรวจสอบระบบคอมพิวเตอร์และเครือข่ายเพื่อระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ติดตามและวิเคราะห์ข้อมูลเพื่อระบุและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ตรวจสอบและประเมินผลการทำงานของระบบคอมพิวเตอร์และเครือข่ายเพื่อความมั่นคงปลอดภัยไซเบอร์	ข้อสอบข้อเขียน
CS502 วิเคราะห์และประเมินผลข้อมูลเพื่อระบุและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์	วิเคราะห์ข้อมูลเพื่อระบุและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ประเมินผลข้อมูลเพื่อระบุและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ สร้างรายงานผลการวิเคราะห์และประเมินผลข้อมูลเพื่อระบุและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์	ข้อสอบข้อเขียน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

- มีความรู้และทักษะในการใช้งานระบบคอมพิวเตอร์และเครือข่ายรวมถึงความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ
- ทักษะในการใช้งานระบบคอมพิวเตอร์และเครือข่าย
- ทักษะในการวิเคราะห์และประเมินผลข้อมูล
- ทักษะในการตรวจจับ และตอบสนองต่อเหตุการณ์ไซเบอร์
- ทักษะในการประเมินและจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

(ข) ความต้องการด้านความรู้
- ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์
- ความรู้ด้านมาตรฐาน และนโยบายความปลอดภัยไซเบอร์
- ความรู้เกี่ยวกับกฎหมายและข้อบังคับที่เกี่ยวข้องกับความปลอดภัยของข้อมูล
- ความรู้เกี่ยวกับการป้องกันและตรวจสอบความปลอดภัย และการป้องกันภัยคุกคาม

14. หลักฐานที่ต้องการ (Evidence Guide)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)
- หลักฐานการกำกับ ดูแลด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง
- เอกสารหรือรายงานที่แสดงถึงการกำกับ ดูแลด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

(ข) หลักฐานความรู้ (Knowledge Evidence)
- ใบวุฒิการศึกษา
- ประกาศนียบัตรต่าง ๆ จากการฝึกอบรมพัฒนาหรือการเรียนรู้ที่เกี่ยวข้อง

(ค) คำแนะนำในการประเมิน
- ตรวจประเมินหลักฐานโดยพิจารณาจากร่องรอยหลักฐานที่เกี่ยวข้อง ทั้งหลักฐานด้านปฏิบัติงานและหลักฐานด้านความรู้

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

หน่วยความสามารถนี้ครอบคลุมถึงการตรวจสอบและติดตามความมั่นคงปลอดภัยไซเบอร์ของระบบคอมพิวเตอร์และเครือข่ายทุกประเภท รวมถึงระบบคอมพิวเตอร์เดสก์ท็อป ระบบคอมพิวเตอร์แล็ปท็อป ระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายทุกประเภท รวมถึงระบบเครือข่ายไร้สาย ระบบเครือข่าย LAN การตรวจสอบและติดตามความมั่นคงปลอดภัยไซเบอร์จะต้องดำเนินการอย่างต่อเนื่องเพื่อป้องกันและตรวจสอบ ภัยคุกคามทางไซเบอร์รวมถึงการตรวจสอบและวิเคราะห์ข้อมูลเพื่อระบุและแก้ไขปัญหาด้านความมั่นคง ปลอดภัยไซเบอร์

(ข) คำอธิบายรายละเอียด

- ตรวจสอบและติดตามความมั่นคงปลอดภัยไซเบอร์ของระบบคอมพิวเตอร์และเครือข่าย มีขอบเขตที่ ครอบคลุมถึง กระบวนการและกิจกรรมที่มีวัตถุประสงค์เพื่อประเมิน ตรวจสอบระบบคอมพิวเตอร์และ เครือข่ายเพื่อระบุความเสียงด้านความมั่นคงปลอดภัยไซเบอร์ ติดตามและวิเคราะห์ข้อมูลเพื่อระบุและ แก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ตรวจสอบและประเมินผลการทำงานของระบบ คอมพิวเตอร์และเครือข่ายเพื่อความมั่นคงปลอดภัยไซเบอร์ และควบคุมการปกป้องข้อมูลและทรัพยากรทางคอมพิวเตอร์จากภัยคุกคามและการโจมตีทางไซเบอร์
- วิเคราะห์และประเมินผลข้อมูลเพื่อระบุและแก้ไขปัญหา ด้านความมั่นคงปลอดภัยไซเบอร์ มีขอบเขตที่ ครอบคลุมถึงการใช้ข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์เพื่อ ระบุปัญหาการวิเคราะห์ข้อมูล เพื่อค้นหาไว้เป็นหรือหลักรรมที่ยายเป็นสัญญาณของภัยคุกคามข่องโหว่ด้านควานความความปลอดภัย ประเมินผลกระทบความรุนแรงและผลกระทบที่อาจเกิดขึ้นจากปัญหาเหล่านั้น และพัฒนาและ ดำเนินการแก้ไขสร้างแผนและมาตรการในการป้องกันหรือแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์

16. หน่วยสมรรถนะร่วม (ถ้ามี)

N/A

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

N/A

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

สอบข้อเขียน