ประกาศจังหวัดร้อยเอ็ด
เรื่อง รายชื่อผู้ที่ผ่านการประเมินบุคคลเพื่อแต่งตั้งให้ดำรงตำแหน่งประเภทวิชาการ ระดับชำนาญการ
ของสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด

ตามหนังสือสำนักงาน ก.พ. ที่ นร ๑๐๐๖/ว ๑๔ ลงวันที่ ๑๑ สิงหาคม ๒๕๖๔ ได้กำหนดหลักเกณฑ์และวิธีการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งในตำแหน่งระดับควบ และมีผู้ครองตำแหน่งนั้นอยู่ โดยให้ผู้มีอำนาจสั่งบรรจุตามมาตรา ๕๗ หรือผู้ที่ได้รับมอบหมายเป็นผู้ประเมินบุคคลตามหลักเกณฑ์และวิธีการที่ อ.ก.พ. กรม กำหนด นั้น

จังหวัดร้อยเอ็ดได้คัดเลือกข้าราชการผู้ผ่านการประเมินบุคคลที่จะเข้ารับการประเมินผลงานเพื่อแต่งตั้งให้ดำรงตำแหน่งในระดับที่สูงขึ้น (ตำแหน่งระดับควบ) จำนวน ๑ ราย ดังนี้

ลำดับที่	ชื่อ-สกุล	ตำแหน่งที่ได้รับการคัดเลือก	ส่วนราชการ
๑.	นายพิพัฒน์พงษ์ ชุนประวัติ	นักวิชาการคอมพิวเตอร์ชำนาญการ	สำนักงานสาธารณสุขจังหวัดร้อยเอ็ด กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข

รายละเอียดแนบท้ายประกาศนี้

ทั้งนี้ ให้ผู้ผ่านการประเมินบุคคล เพื่อเลื่อนระดับสูงขึ้น จัดส่งผลงานประเมินตามจำนวนและเงื่อนไขที่คณะกรรมการประเมินผลงานกำหนด ภายใน ๑๘๐ วัน นับแต่วันที่ประกาศรายชื่อผู้ที่ผ่านการประเมินบุคคล หากพ้นระยะเวลาดังกล่าวแล้ว ผู้ที่ผ่านการประเมินบุคคลยังไม่ส่งผลงานจะต้องขอรับการประเมินบุคคลใหม่ อนึ่ง หากมีผู้ใดจะทักท้วงให้ทักท้วงได้ ภายใน ๓๐ วัน นับตั้งแต่วันประกาศ

ประกาศ ณ วันที่ ๒๕ มกราคม พ.ศ. ๒๕๖๗

(นายชัยวัฒน์ ชัยเวชพิสิฐ)
รองผู้ว่าราชการจังหวัด ปฏิบัติราชการแทน
ผู้ว่าราชการจังหวัดร้อยเอ็ด

บัญชีรายละเอียดแนบท้ายประกาศจังหวัดร้อยเอ็ด
เรื่อง รายชื่อผู้ที่ผ่านการประเมินบุคคลเพื่อแต่งตั้งให้ดำรงตำแหน่งประเภทวิชาการ ระดับชำนาญการ
ของสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด

ลำดับที่	ชื่อ - ชื่อสกุล	ส่วนราชการ/ตำแหน่งเดิม	ตำแหน่งเลขที่	ส่วนราชการ/ตำแหน่งที่ได้รับการคัดเลือก	ตำแหน่งเลขที่	หมายเหตุ
๑	นายพิพัฒน์พงษ์ ชุนประวัติ	สำนักงานสาธารณสุขจังหวัดร้อยเอ็ด กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข นักวิชาการคอมพิวเตอร์ ปฏิบัติการ	๒๔๒๒๐๕	สำนักงานสาธารณสุขจังหวัดร้อยเอ็ด กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข นักวิชาการคอมพิวเตอร์ ชำนาญการ	๒๔๒๒๐๕	เลื่อนระดับ ๑๐๐%
	ชื่อผลงานส่งประเมิน “การจัดการความปลอดภัยเครือข่ายคอมพิวเตอร์ในสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด (Network Security Management in Roi-Et Provincial Health Office)”					
	ชื่อแนวคิดในการพัฒนางาน “โครงการฝึกอบรมการรักษาความปลอดภัยทางไซเบอร์สำหรับผู้ปฏิบัติงาน”					
	รายละเอียดเค้าโครงผลงาน “แนบท้ายประกาศ”					

(นายนราธร สุขธิประภา)
หัวหน้ากลุ่มงานบริหารทรัพยากรบุคคล

<u>ส่วนที่ ๒</u> ผลงานที่เป็นผลการปฏิบัติงานหรือผลสำเร็จของงาน

๑. เรื่อง การจัดการความปลอดภัยเครือข่ายคอมพิวเตอร์ ในสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด

(Network Security Management in Roi-Et Provincial Health Office)

๒. ระยะเวลาที่ดำเนินการ เดือนธันวาคม ๒๕๖๖ - มกราคม ๒๕๖๗

๓. ความรู้ ความชำนาญงาน หรือความเชี่ยวชาญและประสบการณ์ที่ใช้ในการปฏิบัติงาน

ในยุคปัจจุบันการรักษาความปลอดภัยของข้อมูลทางสารสนเทศต่างๆ นั้น มีความสำคัญต่อองค์กรภาครัฐต่างๆ เป็นอย่างมาก ไม่ว่าจะเป็นเรื่องฐานข้อมูลภายในองค์กรเอง ซึ่งถ้าไปตกอยู่กับผู้ไม่ประสงค์ดีและถูกเผยแพร่ออกไป ย่อมที่จะเป็นผลเสียหายต่อองค์กรเป็นอย่างมาก ซึ่งความเสียหายนั้นเกิดได้จากหลายรูปแบบด้วยกัน ไม่ว่าจะเป็นการรู้เท่าไม่ถึงการณ์ของบุคคลากรภายในองค์กรเอง หรือการเข้าใช้งานภายในเครือข่ายอินเทอร์เน็ต การเข้าเยี่ยมชมเว็บไซต์ที่ไม่มีความปลอดภัย เช่น เว็บไซต์ที่ใช้ในการปลอมการใช้งานให้ถูกต้องโดยวิธีการแครก (crack) แน่นอนว่า เมื่อผู้ใช้งานภายในองค์กรเองเข้าไปแล้วย่อมที่จะนำสิ่งที่ไม่พึงประสงค์ติดมาเก็บไว้ที่เครือข่ายภายในขององค์กรด้วย หรือจากเข้าใช้งานอีเมล์โดยความไม่ปลอดภัย (Spam mail) ซึ่งดังที่กล่าวมาข้างต้นจึงเป็นความเสี่ยงทั้งหมดที่อยู่ภายในเครือข่าย ทั้งสิ้น ดังนั้นระบบสารสนเทศจึงจำเป็นที่จะต้องมีระบบรักษาความปลอดภัยภายในเครือข่าย ที่มีความแข็งแกร่ง และพร้อมที่จะรับมือกับภัยคุกคามต่างๆ เหล่านั้นได้

๔. สรุปสาระสำคัญ ขั้นตอนการดำเนินงาน และเป้าหมายของงาน

สรุปสาระสำคัญ

ในปัจจุบันสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด ได้นำระบบเทคโนโลยีเข้ามาใช้ภายในองค์กร ทำให้ผู้ใช้งานเข้าถึงข้อมูลต่างๆ ไม่ว่าจะเป็นฐานข้อมูล อีเมล์ เว็บไซต์ไฟล์ภาพ เพลงในอินเตอร์เน็ต ผู้ใช้งานอาจรู้เท่าไม่ถึงการณ์ อาจจะดาวน์โหลดไฟล์ เหล่านั้นมา ซึ่งอาจจะเป็นการสร้างปัญหาและนำความเสียหายมาสู่ภายในองค์กร และกระทบต่อการทำงานของแอพพลิเคชั่นหลักของผู้ใช้งาน ทำให้การทำงานมีความล่าช้า หรือทำงานไม่ได้เลย และเมื่อคอมพิวเตอร์ของผู้ใช้งานภายในองค์กรติดไวรัสคอมพิวเตอร์ ผลมาจากการเข้าใช้งานเว็บไซต์ที่ไม่มีความน่าเชื่อถือ หรือเว็บที่มีไวรัส จะนำความเสียหายมาให้ผู้ใช้งานอื่นๆ ในองค์กรที่ใช้เครือข่ายเดียวกัน จึงได้ศึกษาระบบรักษาความปลอดภัยของระบบสารสนเทศที่เป็นมาตรฐานและนิยมใช้งานมาประยุกต์ใช้งานภายในองค์กร จัดหาเครื่องมือที่เป็นระบบรักษาความปลอดภัยให้กับระบบสารสนเทศ เพื่อเป็นการหยุด และสกัดกั้นการโจมตีของ Hacker และไวรัส พร้อมทั้งจัดทำนโยบายความปลอดภัยในการเข้าใช้งานระบบสารสนเทศ

ขั้นตอนการดำเนินงาน

เนื่องจากในอดีตสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด ระบบคอมพิวเตอร์ภายในสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด ไม่มีระบบ Firewall ใช้สำหรับป้องกันเครือข่ายคอมพิวเตอร์ ทำให้ง่ายต่อการโจมตี ระบบเครือข่ายต่างๆ แยกออกจากกัน ทำให้การบริหารจัดการของเครือข่ายทำได้อย่างลำบาก การตรวจสอบความผิดปกติของเครือข่ายทำได้ยาก ไม่มีระบบการรักษาความปลอดภัยเลย และไม่มีนโยบายความปลอดภัยในส่วนต่างๆ ของระบบ ซึ่งนโยบายที่รัดกุมเป็นส่วนช่วยทำให้ลดความเสี่ยงที่จะเกิดขึ้น การจัดหาระบบและติดตั้งระบบป้องกันสารสนเทศ ได้นำระบบ Fortinet Firewall เข้ามาเป็นเครื่องมือรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ตให้กับองค์กร หลังจากปรับระบบคอมพิวเตอร์ภายในสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด มีระบบ Firewall ที่แบ่งออกเป็น ๓ โซน คือ

๑. โซน WAN เป็นช่องทางสำหรับให้ User ใช้ในการออกเครือข่ายอินเตอร์เน็ต

๒. โซน DMZ เป็นโซนที่ เครื่อง Server ให้บริการทางเครือข่ายต่างๆ

๓. โซน User เป็นโซนที่ แบ่ง user แต่ละฝ่ายอย่างชัดเจน เช่น โซนการเงิน โซนควบคุมโรค ฯลฯ และได้จัดทำนโยบายการรักษาความปลอดภัยของระบบคอมพิวเตอร์นี้ เป็นไปตามขั้นตอน ดังนี้

๑. เสนอการจัดทำนโยบายให้หัวหน้าศูนย์เทคโนโลยีสารสนเทศรับทราบเสนอผู้บริหารสูงสุด เพื่อขออนุมัติจัดทำนโยบาย

๒. ร่างนโยบายข้อกำหนดต่างๆ เพื่อให้สอดคล้องกับการรักษา ความปลอดภัยในระบบสารสนเทศ

๓. จัดทำแบบสอบถามเพื่อนำผลที่ได้จากแบบสอบถามมาจัดทำนโยบาย

๔. นำร่างนโยบายให้กลุ่มกฎหมายตรวจสอบ

๕. ปรับปรุงแก้ไขร่างนโยบาย

๖. ผู้บริหารสูงสุดเซ็นต์อนุมัตินโยบาย ประกาศ จัดอบรมให้เจ้าหน้าที่กลุ่มงานต่างๆ รับทราบและปฏิบัติ

๗. ติดตาม ตรวจสอบการปฏิบัติตามข้อกำหนดในส่วนต่างๆ ของนโยบาย

๘. ทบทวน แก้ไขปรับปรุงนโยบายให้สอดคล้องกับเหตุการณ์ปัจจุบันเหมาะสมกับภัยคุกคามที่เปลี่ยนแปลงไป

เป้าหมายงาน

เพื่อศึกษาระบบรักษาความปลอดภัยของระบบสารสนเทศ ที่เป็นมาตรฐานและนิยมใช้งาน มาประยุกต์ใช้งานภายในองค์กร จัดหาระบบและติดตั้งระบบป้องกันสารสนเทศ พร้อมทั้งจัดทำนโยบาย ความปลอดภัยในการเข้าใช้งานระบบสารสนเทศ

๕. ผลสำเร็จของงาน (เชิงปริมาณ/คุณภาพ)

๕.๑ ระบบเครือข่ายคอมพิวเตอร์ได้รับการปรับปรุงให้มีระบบ Internet/Intranet สำรอง มีความปลอดภัย และความเสถียรภาพมากขึ้น

๕.๒ ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ สามารถตรวจจับความผิดปกติของเครือข่ายคอมพิวเตอร์ได้รวดเร็ว ทันเหตุการณ์

๕.๓ มีระบบความปลอดภัยของระบบ Server โดยแยกส่วนออกมาอย่างชัดเจนกับส่วนผู้ใช้ (Client) ส่วนออก Internet

๕.๔ ผู้บริหารมีความเชื่อมั่น ไว้วางใจ ในการเก็บรักษาข้อมูลผู้ป่วย

๕.๕ ผู้ปฏิบัติงาน (Client) มีความรู้ตระหนักในเรื่องของความปลอดภัยของข้อมูล

๖. การนำไปใช้ประโยชน์/ผลกระทบ

๖.๑ ผู้ดูแลระบบสามารถบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ได้ง่าย

๖.๒ ระบบเครือข่ายคอมพิวเตอร์ มีระบบการป้องกันและบริหารจัดการ มีความปลอดภัยในการจัดเก็บข้อมูลของผู้ป่วย

๖.๓ มีระบบเครือข่ายและระบบสำรองในการใช้งาน

๖.๔ ผู้ดูแลระบบต้องมีความเข้าใจในการจัดการระบบ และผู้ใช้ต้องมีความรู้และตระหนักถึงความปลอดภัยของข้อมูล

๗. ความยุ่งยากและซับซ้อนในการดำเนินการ

๗.๑ ผู้ดูแลระบบต้องได้รับการฝึกอบรมให้เกิดความเชี่ยวชาญ และเข้าใจระบบเครือข่ายคอมพิวเตอร์ในการออกแบบระบบความปลอดภัยที่ซับซ้อนมากขึ้น

๗.๒ ผู้ใช้ (user) มีความรู้เบื้องต้น ทักษะในเรื่องเครือข่ายคอมพิวเตอร์ ต่างกัน

๗.๓ อุปกรณ์ที่มี มีอายุการใช้งานนาน ไม่สามารถ set ระบบให้มีความปลอดภัยเพียงพอกับเทคโนโลยีที่มีการเปลี่ยนแปลง

๘. **ปัญหาและอุปสรรคในการดำเนินการ**

๘.๑ การให้ความสำคัญกับระบบความปลอดภัยด้านเครือข่ายคอมพิวเตอร์

๘.๒ ความรู้ ทักษะ ผู้ดูแลระบบ ในการจัดการความปลอดภัยของเครือข่ายคอมพิวเตอร์

๘.๓ ความรู้ ความเข้าใจ ผู้ใช้ระบบ (User) ในเรื่องระบบความปลอดภัยของเครือข่ายคอมพิวเตอร์

๙. **ข้อเสนอแนะ**

๙.๑ ควรมีการฝึกอบรมผู้ดูแลระบบ ให้เกิดความรอบรู้ การโจมตีทางเครือข่ายคอมพิวเตอร์

๙.๒ ปรับปรุงระบบ อุปกรณ์ให้ทันสมัย

๙.๓ อบรมผู้ใช้ระบบให้ตระหนัก เข้าใจเรื่องความปลอดภัยทางเครือข่ายคอมพิวเตอร์

๑๐. **การเผยแพร่ผลงาน (ถ้ามี)** ไม่มี

๑๑. **ผู้มีส่วนร่วมในผลงาน (ถ้ามี)**

๑) นายพิพัฒน์พงษ์ ชุนประวัติ สัดส่วนของผลงาน ๑๐๐ %

ขอรับรองว่าผลงานดังกล่าวเป็นความจริงทุกประการ

(ลงชื่อ) .....

(นายพิพัฒน์พงษ์ ชุนประวัติ)

(ตำแหน่ง) นักวิชาการคอมพิวเตอร์ปฏิบัติการ

(วันที่) ๑๗/ มกราคม /๒๕๖๗

ผู้ขอประเมิน

ขอรับรองว่าผลงานดังกล่าวเป็นความจริงทุกประการ

รายชื่อผู้มีส่วนร่วมในผลงาน	ลายมือชื่อ
นายพิพัฒน์พงษ์ ชุนประวัติ	

ได้ตรวจสอบแล้วขอรับรองว่าผลงานดังกล่าวข้างต้นถูกต้องตรงกับความเป็นจริงทุกประการ

(ลงชื่อ) .....

(นายสุวิทย์ กิริยะ)

(ตำแหน่ง) นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ

(วันที่) ๒๕/ มกราคม /๒๕๖๗

ผู้บังคับบัญชาที่กำกับดูแล

(ลงชื่อ) .....

(นายนิสิต บุญอะรัญ)

(นายแพทย์ชำนาญการพิเศษ (ด้านเวชกรรม))

(ตำแหน่ง) รก.นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)

ปฏิบัติราชการแทน นายแพทย์สาธารณสุขจังหวัดร้อยเอ็ด

(วันที่) ..... 24 ม.ค. 2567 .....

ผู้บังคับบัญชาที่เหนือขึ้นไป

หมายเหตุ : คำรับรองจากผู้บังคับบัญชาอย่างน้อยสองระดับ คือ ผู้บังคับบัญชาที่กำกับดูแล และผู้บังคับบัญชาที่เหนือขึ้นไปอีกหนึ่งระดับ เว้นแต่ในกรณีที่ผู้บังคับบัญชาดังกล่าวเป็นบุคคลคนเดียวกัน ก็ให้มีคำรับรองหนึ่งระดับได้

แบบเสนอแนวคิดการพัฒนาหรือปรับปรุงงาน

(ระดับ ชำนาญการ)

๑. เรื่อง โครงการฝึกอบรมการรักษาความปลอดภัยทางไซเบอร์สำหรับผู้ปฏิบัติงาน

๒. หลักการและเหตุผล

ในปัจจุบันการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารส่งผลให้เกิดการพัฒนาทั้งทางเศรษฐกิจและสังคมอย่างก้าวกระโดด เนื่องจากปัจจุบันมีการพัฒนาแอปพลิเคชั่นและซอฟแวร์ที่มีประสิทธิภาพสูง ทำให้ผู้ใช้งานทั่วไปสามารถเข้าถึงข้อมูลและบริการได้สะดวกและรวดเร็ว หน่วยงานของรัฐทุกระดับต่างตระหนักถึงศักยภาพของเทคโนโลยีสารสนเทศและการสื่อสารหรือเทคโนโลยีดิจิทัล และได้พยายามใช้ประโยชน์จากเทคโนโลยีเหล่านี้ในการยกระดับการทำงานและการให้บริการประชาชนมาอย่างต่อเนื่อง อย่างไรก็ตามแม้ว่าเทคโนโลยีสารสนเทศและการสื่อสารจะมีประโยชน์สำหรับการปฏิบัติงานของหน่วยงานของรัฐในหลากหลายมิติ แต่ในขณะเดียวกันหน่วยงานของรัฐกลับต้องเผชิญกับภัยคุกคามไซเบอร์ (Cyber Threat) มากขึ้นอย่างไม่เคยปรากฏมาก่อน ภัยคุกคามเหล่านี้เป็นภัยคุกคามใหม่ที่มีศักยภาพสูงในการสร้างความเสียหายให้แก่หน่วยงานของรัฐทั้งในระดับบุคคล หน่วยงาน และประเทศ รวมทั้งสร้างความเสียหายต่อประชาชนผู้รับบริการอีกด้วย ดังนั้น หน่วยงานของรัฐ จึงจำเป็นต้องเร่งเตรียมความพร้อมในทุกมิติเพื่อรับมือภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ โดยการพัฒนาบุคลากรหน่วยงานของรัฐให้มีศักยภาพเพียงพอในการรับมือภัยคุกคามไซเบอร์ได้ ซึ่งถือเป็นการวางรากฐานที่สำคัญยิ่งในการรักษาความปลอดภัยไซเบอร์ (Cyber Security)

สำนักงานสาธารณสุขจังหวัดร้อยเอ็ด จึงเล็งเห็นประเด็นความสำคัญในการพัฒนาบุคลากรผู้ปฏิบัติงานในสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด เพื่อให้ผู้เข้ารับการฝึกอบรมตระหนักถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์ สามารถป้องกันภัยคุกคามไซเบอร์ที่จะเกิดขึ้นในอนาคตได้อย่างถูกต้องและทันท่วงที และมีแนวทางการดำเนินงานที่ถูกต้องเหมาะสมเมื่อเกิดภัยคุกคามทางไซเบอร์รวมทั้งเพื่อให้ผู้เข้ารับการอบรมมีความรู้และความเข้าใจด้านความปลอดภัยทางไซเบอร์สำหรับผู้ปฏิบัติงาน

๓. บทวิเคราะห์/แนวความคิด/ข้อเสนอ และข้อจำกัดที่อาจเกิดขึ้นและแนวทางแก้ไข

วัตถุประสงค์

๑. เพื่อให้ผู้เข้ารับการฝึกอบรมมีความตระหนักรู้ในการใช้งานเทคโนโลยีอย่างปลอดภัย

๒. เพื่อให้ผู้เข้ารับการฝึกอบรมสามารถวางแผนป้องกันและรับมือกับความปลอดภัยไซเบอร์ได้ตามหลักการ

๓. เพื่อให้ผู้เข้ารับการฝึกอบรมสามารถนำความรู้ไปประยุกต์ใช้ในการวางแผนรับมือเกี่ยวกับความเสี่ยงทางไซเบอร์ในองค์กรได้

กลุ่มเป้าหมาย

ผู้ปฏิบัติงานในสำนักงานสาธารณสุขจังหวัดร้อยเอ็ด จำนวน ๑๗๘ คน

แนวทางการฝึกอบรม

การจัดการเรียนการสอนในหลักสูตรเน้นองค์ความรู้ทั้งภาคทฤษฎีและภาคปฏิบัติเพื่อให้ผู้ปฏิบัติงาน ได้นำความรู้และทักษะจากหลักสูตรไปประยุกต์ใช้ในการวางแผนการรับมือกับภัยคุกคามและความเสี่ยงทางด้านไซเบอร์ในองค์กรได้อย่างมีประสิทธิภาพ

ระยะเวลาการฝึกอบรม

ระยะเวลาในการอบรมต่อรุ่นจำนวน ๕ วัน

เนื้อหาการฝึกอบรม

- ภาพรวมความปลอดภัยไซเบอร์
- การระบุความเสี่ยงด้านความปลอดภัยไซเบอร์
- การป้องกันด้านความปลอดภัยไซเบอร์
- การรับมือด้านความปลอดภัยไซเบอร์
- การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์

๔. ผลที่คาดว่าจะได้รับ

๑. ผู้เข้ารับการฝึกอบรมสามารถอธิบายถึงความสำคัญของการรักษาความปลอดภัยไซเบอร์ และแนวคิดพื้นฐานของการรักษาความมั่นคงปลอดภัยสารสนเทศได้

๒. ผู้เข้ารับการฝึกอบรมเข้าใจกระบวนการในการระบุความเสี่ยงด้านความปลอดภัย และสามารถประเมินวิเคราะห์ความปลอดภัยไซเบอร์ในองค์กรได้

๓. ผู้เข้ารับการฝึกอบรมสามารถอธิบายแนวทางการจัดทำมาตรการในการรักษาความปลอดภัยไซเบอร์ และสามารถวิเคราะห์วิธีการในการรักษาความปลอดภัยไซเบอร์หรือเทคโนโลยีที่เหมาะสมได้

๔. ผู้เข้ารับการฝึกอบรมเข้าใจแนวทางการดำเนินการในการเฝ้าระวังความปลอดภัยไซเบอร์ แนวทางในการวิเคราะห์การตรวจจับเหตุการณ์ผิดปกติทางไซเบอร์เบื้องต้น

๕. ผู้เข้ารับการฝึกอบรมมีความรู้เกี่ยวกับกระบวนการจัดทำแผนการรับมือความปลอดภัยไซเบอร์ และสามารถจัดทำแผนการตอบสนองภัยคุกคามได้

๖. ผู้เข้ารับการฝึกอบรมสามารถสรุปวิเคราะห์แนวทางที่เหมาะสมในการวางแผนการตอบสนองภัยคุกคามระบบได้

๕. ตัวชี้วัดความสำเร็จ

๑. ผู้เข้ารับการฝึกอบรมมีความรู้ ความเข้าใจเกี่ยวกับการใช้งานเทคโนโลยีอย่างปลอดภัยไม่น้อยกว่าร้อยละ ๘๐

๒. ผู้เข้ารับการฝึกอบรมสามารถวางแผนป้องกันและรับมือกับความปลอดภัยไซเบอร์ได้ตามหลักการไม่น้อยกว่าร้อยละ ๘๐

(ลงชื่อ) .....
(นายพิพัฒน์พงษ์ ชุนประวัติ)
(ตำแหน่ง) นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(วันที่) ...../...../.....
ผู้ขอประเมิน