ที่ ศธ ๐๖๐๕/ ๓๔๕๕

สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา
ถนนรามอินทรา กม. ๕-๖ แขวงท่าแร้ง
เขตบางเขน กรุงเทพมหานคร ๑๐๒๓๐

๑ กันยายน ๒๕๖๙

เรื่อง ขอความอนุเคราะห์ส่งบุคลากรเข้ารับการอบรมโครงการอบรมเชิงปฏิบัติการการเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อพัฒนาสถานศึกษาอาชีวศึกษา (Build Total Cyber Resiliency from Pocket to Cloud)

เรียน ผู้อำนวยการสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษา

สิ่งที่ส่งมาด้วย โครงการอบรมฯ และตารางฝึกอบรม จำนวน ๑ ชุด

ตามที่สำนักงานคณะกรรมการการอาชีวศึกษา อนุมัติให้สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ดำเนินการโครงการอบรมเชิงปฏิบัติการการเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อพัฒนาสถานศึกษาอาชีวศึกษา (Build Total Cyber Resiliency from Pocket to Cloud) ให้กับครูผู้สอนและบุคลากรอาชีวศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษา จำนวน ๕๐ คน ระหว่างวันที่ ๑๔ - ๑๕ กันยายน ๒๕๖๙ ณ สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ถนนรามอินทรา กรุงเทพมหานคร นั้น

สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา จึงขอความอนุเคราะห์สถานศึกษาในสังกัดสำนักงานคณะกรรมการการอาชีวศึกษา ส่งครูผู้สอน และบุคลากรเข้ารับการอบรมโครงการดังกล่าว โดยสมัครเข้ารับการอบรมทาง QR Code ตั้งแต่บัดนี้ จนถึงวันที่ ๑๐ กันยายน ๒๕๖๙ และจะประกาศรายชื่อผู้เข้ารับการอบรมในระบบสารบรรณอิเล็กทรอนิกส์ โดยเบิกค่าใช้จ่ายในการเดินทางไปราชการของผู้เข้ารับการอบรม ค่าพาหนะ และค่าเบี้ยเลี้ยง เบิกจากสถานศึกษาต้นสังกัด (ค่าเบี้ยเลี้ยงในวันอบรม เบิกได้ ๑ ใน ๓ ส่วน) สำหรับที่พัก พักที่หอพักสำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ทั้งนี้ มอบหมายให้ นางสาวธณัทอร วรรณจรูญ หมายเลขโทรศัพท์ ๐๙ ๖๑๐๕ ๙๘๙๖ และนายอิสราพัส ศรัณย์พิชิตศึก หมายเลขโทรศัพท์ ๐๘ ๙๒๕๔ ๖๓๖๒ เป็นผู้ประสานงาน

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายเมืองมนต์ เนตรหาญ)
ผู้อำนวยการสำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา

เรียน ผู้อำนวยการ

ด้วย สสอ. ขอความอนุเคราะห์ส่งบุคลากรเข้ารับการอบรมโครงการอบรมเชิงปฏิบัติการเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ มาเพื่อ

/ เพื่อโปรดทราบ
เพื่อโปรดพิจารณา
/ เห็นควรแจ้ง รองฯ 4 ฝ่าย , บุคลากรทุกท่าน

นางสาวอัญชลี ธรรมศรีใจ
หัวหน้างานบริหารงานทั่วไป
2 ก.ย. 69

☐ ทราบ.....
☐ แจ้ง.....
☐ มอบ.....

(นายสมพงษ์ นันต๊ะภาพ)
รองผู้อำนวยการ รักษาการในตำแหน่ง
ผู้อำนวยการวิทยาลัยสารพัดช่างลำปาง
2 ก.ย. 69

กลุ่มนวัตกรรมการพัฒนาบุคลากร
โทร. ๐ ๒๕๐๙ ๓๖๕๔ - ๕ ต่อ ๑๓๐๑
โทรสาร ๐ ๒๙๔๓ ๖๐๒๐

การสมัครเข้ารับการอบรม

โครงการอบรมเชิงปฏิบัติการการเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์
เพื่อพัฒนาสถานศึกษาอาชีวศึกษา (Build Total Cyber Resiliency from Pocket to Cloud)
ระหว่างวันที่ ๑๔ – ๑๕ กันยายน ๒๕๖๙
ณ สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ถนนรามอินทรา กรุงเทพมหานคร

แบบฟอร์มรับสมัครเข้าร่วมอบรม

ปิดรับสมัครในวันที่ ๑๐ กันยายน ๒๕๖๙ ประกาศรายชื่อผู้มีสิทธิ์เข้ารับการอบรม ในวันที่ ๑๑ กันยายน ๒๕๖๙
ทางสารบรรณอิเล็กทรอนิกส์

๑. ชื่อโครงการ

โครงการอบรมเชิงปฏิบัติการ การเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาสถานศึกษาอาชีวศึกษา (Build Total Cyber Resiliency from Pocket to Cloud)

๒. ผู้รับผิดชอบ

กลุ่มนวัตกรรมการพัฒนาบุคลากร สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ร่วมกับ บริษัท Lenovo (ประเทศไทย) จำกัด และบริษัท ซังฟอร์ เทคโนโลยี (ประเทศไทย) จำกัด (Sangfor Technologies (Thailand) Co., Ltd.)

๓. วันเวลาและสถานที่ดำเนินโครงการ

ระหว่างวันที่ ๑๔ - ๑๕ กันยายน ๒๕๖๙ ณ สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ถนนรามอินทรา กรุงเทพมหานคร

๔. หลักการและเหตุผล

ปัจจุบันเทคโนโลยีดิจิทัลได้เข้ามามีบทบาทสำคัญต่อการจัดการศึกษา การจัดการเรียนการสอน การบริหารสถานศึกษา ตลอดจนการให้บริการผู้เรียนและบุคลากรในทุกระดับ สถานศึกษาอาชีวศึกษามีการนำระบบเครือข่ายอินเทอร์เน็ต ระบบสารสนเทศ ห้องปฏิบัติการคอมพิวเตอร์ ระบบ Wi-Fi ระบบ Server ระบบกล้องวงจรปิด ระบบ Internet of Things (IoT) และระบบดิจิทัลอื่น ๆ มาใช้สนับสนุนภารกิจของสถานศึกษาเพิ่มมากขึ้น การเชื่อมโยงระบบและอุปกรณ์จำนวนมากดังกล่าว แม้จะช่วยเพิ่มประสิทธิภาพในการปฏิบัติงานและการจัดการเรียนรู้ แต่ในขณะเดียวกันก็ทำให้สถานศึกษามีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ที่มีรูปแบบและความซับซ้อนเพิ่มขึ้น

ภัยคุกคามทางไซเบอร์สามารถส่งผลกระทบต่อสถานศึกษาได้ทั้งในด้านการจัดการเรียนการสอน การบริหารงาน ระบบสารสนเทศ ข้อมูลของผู้เรียนและบุคลากร ตลอดจนความต่อเนื่องในการให้บริการของสถานศึกษา โดยเฉพาะกรณีการโจมตีด้วยมัลแวร์หรือ Ransomware การเข้าถึงระบบโดยไม่ได้รับอนุญาต การโจมตีระบบเครือข่าย การรั่วไหลของข้อมูล และการใช้ประโยชน์จากช่องโหว่ของอุปกรณ์หรือระบบสารสนเทศ หากสถานศึกษาไม่มีมาตรการในการป้องกัน ตรวจจับ วิเคราะห์ และตอบสนองต่อเหตุการณ์อย่างเป็นระบบ อาจก่อให้เกิดความเสียหายต่อข้อมูล ระบบงาน และภารกิจทางการศึกษาได้

ดังนั้น การรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานศึกษาจึงไม่ควรจำกัดอยู่เพียงการติดตั้งอุปกรณ์รักษาความปลอดภัยเท่านั้น แต่ควรพัฒนาให้เกิดความพร้อมในทุกมิติ ตั้งแต่การสร้างความรู้และทักษะของบุคลากร การออกแบบระบบเครือข่ายและโครงสร้างพื้นฐานที่ปลอดภัย การกำหนดสิทธิ์การเข้าถึง การแบ่งส่วนเครือข่าย การจัดเก็บและตรวจสอบ Log การเฝ้าระวังภัยคุกคาม การตรวจจับและวิเคราะห์เหตุการณ์ ตลอดจนการวางแผนตอบสนองและกู้คืนระบบเมื่อเกิดเหตุการณ์ผิดปกติ กำหนดแนวทางการพัฒนาการเรียนการสอนและศูนย์คอมพิวเตอร์ที่มีความมั่นคงปลอดภัยสำหรับสถานศึกษา เน้นการเรียนการสอน Cybersecurity และการบริหารจัดการศูนย์คอมพิวเตอร์และโครงสร้างพื้นฐานที่มั่นคงปลอดภัย ให้ความสำคัญกับการทำความเข้าใจแนวโน้มภัยคุกคาม ความต้องการกำลังคน และเส้นทางอาชีพด้าน Cybersecurity รวมถึงกรอบองค์ความรู้ด้าน Human and Regulatory, Attacks and Defences, Systems Security, Software and Platform Security และ Infrastructure Security ซึ่งสามารถนำไปเชื่อมโยงกับการจัดการเรียนการสอนในสาขาวิชาเทคโนโลยีสารสนเทศ คอมพิวเตอร์ อิเล็กทรอนิกส์ IoT และสาขาที่อื่นๆที่ เกี่ยวข้องได้ นอกจากนี้ ยังมีแนวทางการพัฒนาห้องปฏิบัติการด้าน Cybersecurity จาก Network Security Lab ไปสู่ Mini-SOC โดยใช้เทคโนโลยีและองค์ประกอบที่เกี่ยวข้อง เช่น NGFW, HCI, Server, L๓ Switch, Wi-Fi Controller, Network Sensor, NDR และ Cyber Command รวมทั้งการสาธิต Security Policy, Network Segmentation การตรวจจับการโจมตี และการวิเคราะห์ Alert เพื่อให้ผู้เข้าร่วมสามารถมองเห็นกระบวนการรักษาความมั่นคงปลอดภัยตั้งแต่ระดับห้องปฏิบัติการไปจนถึงระดับโครงสร้าง

พื้นฐาน...

พื้นฐานของสถานศึกษาในด้านการบริหารศูนย์คอมพิวเตอร์ ควรให้ความสำคัญกับภัยคุกคามที่อาจเกิดขึ้นกับห้องปฏิบัติการ Wi-Fi Server CCTV IoT และระบบควบคุม ตลอดจนความรู้ด้านกฎหมายและความรับผิดชอบของผู้ดูแลระบบ รวมถึงแนวทางการควบคุมสิทธิ์ การจัดเก็บ Log การคุ้มครองข้อมูล การตรวจสอบย้อนหลัง และการจัดการหลักฐาน

อีกทั้งยังนำเสนอแนวคิด Secure Technical College Architecture ซึ่งครอบคลุมการแบ่งส่วนเครือข่ายสำหรับ Staff, Student, Guest, Server, Computer Lab, CCTV/IoT และ Industrial Control Zone รวมถึงแนวทาง Mini-SOC และ Incident Response เพื่อให้สามารถเฝ้าระวัง วิเคราะห์ Alert ทำ Threat Hunting จัดทำ Incident Timeline และใช้ Incident Response Playbook เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

การอบรมยังมีการจำลองสถานการณ์ Ransomware แพร่จากห้องปฏิบัติการเข้าสู่เครือข่ายวิทยาลัย เพื่อให้ผู้เข้าร่วมเห็นภาพกระบวนการตั้งแต่การตรวจพบพฤติกรรมที่มีความเสี่ยง การวิเคราะห์ Traffic การระบุเครื่องต้นเหตุ การ Block และ Isolate การจำกัดการแพร่กระจาย การตรวจสอบผลกระทบต่อข้อมูล การจัดทำ Incident Timeline ตลอดจนการกู้คืนระบบและสรุปบทเรียนหลังเกิดเหตุการณ์ บริษัท เลอโนโว (ประเทศไทย) จำกัด ได้แสดงความประสงค์ในการเข้าจัดสัมมนาในวันที่ ๑๔ กันยายน ๒๕๖๙ ภายใต้หัวข้อ "Build Total Cyber Resiliency from Pocket to Cloud" โดยมีเป้าหมายเพื่อสร้างความรู้ความเข้าใจในการนำเทคโนโลยีดิจิทัลมาประยุกต์ใช้ในการปฏิบัติงานอย่างมีประสิทธิภาพและปลอดภัย พร้อมนำเสนอข้อมูลเกี่ยวกับแนวโน้มเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ เทคโนโลยีและนวัตกรรมด้านอุปกรณ์คอมพิวเตอร์สำหรับภาคการศึกษา รวมถึงผลิตภัณฑ์และโซลูชันล่าสุดของ Lenovo ด้วยเหตุผลดังกล่าว สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ร่วมกับ บริษัท เลอโนโว (ประเทศไทย) จำกัด จึงเห็นสมควรจัดโครงการอบรม "Build Total Cyber Resiliency from Pocket to Cloud" เพื่อพัฒนาความรู้ ความเข้าใจ และทักษะของครูและบุคลากรอาชีวศึกษาให้สามารถรับรู้และเข้าใจภัยคุกคามทางไซเบอร์ มีแนวทางในการออกแบบการเรียนการสอนด้าน Cybersecurity ตลอดจนสามารถนำความรู้ไปประยุกต์ใช้ในการดูแลระบบสารสนเทศและโครงสร้างพื้นฐานดิจิทัลของสถานศึกษา อันจะนำไปสู่การพัฒนาสถานศึกษาอาชีวศึกษาให้มีความพร้อมในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูระบบเมื่อเกิดภัยคุกคามทางไซเบอร์อย่างเป็นระบบ เป็นการเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อพัฒนาสถานศึกษาอาชีวศึกษา ให้ก้าวทันยุคแห่งการเปลี่ยนแปลงด้านเทคโนโลยีในอนาคตต่อไป

๕. วัตถุประสงค์

๕.๑ เพื่อพัฒนาความรู้ ความเข้าใจเกี่ยวกับสถานการณ์ แนวโน้ม และรูปแบบภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อสถานศึกษาอาชีวศึกษา

๕.๒ เพื่อเสริมสร้างความรู้เกี่ยวกับกรอบองค์ความรู้ด้าน Cybersecurity ทั้งในมิติของ Human and Regulatory, Attacks and Defences, Systems Security, Software and Platform Security และInfrastructure Security

๕.๓ เพื่อพัฒนาศักยภาพครูผู้สอนในการออกแบบรายวิชา กิจกรรมการเรียนรู้ และ Cybersecurity Lab ให้สอดคล้องกับบริบทของการจัดการอาชีวศึกษา

๕.๔ เพื่อให้ครูผู้สอนสามารถเชื่อมโยงความรู้ด้าน Cybersecurity กับสาขาวิชา IT, Computer, Electronics, IoT และระบบไฟฟ้าได้อย่างเหมาะสม

๕๕ เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับการออกแบบและพัฒนา Network Security Lab และ Mini-SOC สำหรับสถานศึกษาอาชีวศึกษา

๕.๖ เพื่อให้ผู้เข้ารับการอบรมเข้าใจแนวทางการใช้เทคโนโลยี เช่น NGFW, HCI, NDR และ Cyber Command เพื่อสนับสนุนการเรียนการสอนและการรักษาความมั่นคงปลอดภัยของระบบ

๕.๗ เพื่อเสริมสร้าง...

๕.๗ เพื่อเสริมสร้างความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับศูนย์คอมพิวเตอร์ ห้องปฏิบัติการ ระบบ Wi-Fi Server CCTV IoT และระบบควบคุมของสถานศึกษา

๕.๘ เพื่อสร้างความเข้าใจเกี่ยวกับหน้าที่ ความรับผิดชอบ การกำกับดูแล และกฎหมายที่เกี่ยวข้องกับการบริหารจัดการระบบสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

๕.๙ เพื่อให้บุคลากรสามารถนำแนวคิด Network Segmentation, Mini-SOC และIncident Response ไปประยุกต์ใช้ในการวางแผนพัฒนาระบบของสถานศึกษา

๕.๑๐ เพื่อสร้างความตระหนักถึงความสำคัญของการป้องกัน ตรวจจับ วิเคราะห์ ตอบสนอง และฟื้นฟูระบบเมื่อเกิดเหตุการณ์ด้าน Cybersecurity

๕.๑๑ เพื่อสร้างเครือข่ายความร่วมมือระหว่างสำนักงานคณะกรรมการการอาชีวศึกษา สถานศึกษา และภาคเอกชนในการพัฒนาบุคลากรและระบบเทคโนโลยีด้าน Cybersecurity

๖. ตัวชี้วัดความสำเร็จ

๖.๑ เชิงปริมาณ

๖.๑.๑ มีครูและบุคลากรอาชีวศึกษาเข้าร่วมโครงการไม่น้อยกว่าจำนวนเป้าหมายที่กำหนด

๖.๑.๒ ผู้เข้าร่วมโครงการไม่น้อยกว่าร้อยละ ๘๐ เข้าร่วมกิจกรรมครบตามระยะเวลาที่กำหนด

๖.๑.๓ ผู้เข้าร่วมโครงการไม่น้อยกว่าร้อยละ ๘๐ ผ่านเกณฑ์การประเมินความรู้ความเข้าใจด้าน Cybersecurity หลังการอบรมตามเกณฑ์ที่โครงการกำหนด

๖.๑.๔ ผู้เข้าร่วมโครงการไม่น้อยกว่าร้อยละ ๘๐ สามารถระบุแนวทางการนำความรู้จากการอบรมไปประยุกต์ใช้กับการเรียนการสอนหรือการบริหารจัดการระบบสารสนเทศของสถานศึกษาได้

๖.๑.๕ ผู้เข้าร่วมโครงการไม่น้อยกว่าร้อยละ ๘๕ มีความพึงพอใจต่อเนื้อหา วิทยากร รูปแบบการจัดกิจกรรม และประโยชน์ที่ได้รับ อยู่ในระดับมากขึ้นไป

๖.๒ เชิงคุณภาพ

๖.๒.๑ ผู้เข้าร่วมโครงการสามารถอธิบายสถานการณ์และแนวโน้มภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับสถานศึกษาอาชีวศึกษาได้

๖.๒.๒ ครูผู้สอนสามารถนำกรอบองค์ความรู้ด้าน Cybersecurity ไปใช้เป็นแนวทางในการออกแบบรายวิชากิจกรรม หรือ Lab-based Learning ได้

๖.๒.๓ บุคลากรสามารถอธิบายหลักการพื้นฐานของ Network Security Lab, Network Segmentation, Mini-SOC และ Incident Response ได้

๖.๒.๔ บุคลากรศูนย์คอมพิวเตอร์มีความเข้าใจเกี่ยวกับหน้าที่และความรับผิดชอบ รวมถึงแนวทางการจัดการระบบให้สอดคล้องกับกฎหมายและมาตรการด้านความมั่นคงปลอดภัย

๖.๒.๕ ผู้เข้าร่วมโครงการสามารถวิเคราะห์แนวทางการรับมือเหตุการณ์จำลอง เช่น Ransomware และสามารถอธิบายลำดับการดำเนินงานตั้งแต่การตรวจจับ การวิเคราะห์ การจำกัดเหตุการณ์ การกู้คืน และการสรุปบทเรียนได้

๖.๒.๖ สถานศึกษามีบุคลากรที่มีความรู้และความตระหนักด้าน Cybersecurity เพิ่มขึ้น และสามารถนำความรู้ไปวางแผนพัฒนาระบบที่มีความมั่นคงปลอดภัยมากยิ่งขึ้น

๗. หลักสูตรในการอบรม ระยะเวลา ๒ วัน จำนวน ๑๔ ชั่วโมง

วันที่ ๑ หัวข้อ Transform Learning Inspire future

- Lenovo AI in Education
- AI Driven Classroom Transformation
- Digital Workplace Solution for Education

วันที่ ๒ ...

วันที่ ๒ การจัดการเรียนการสอน Cybersecurity ด้วยระบบ Sangfor

- Cybersecurity Workforce and Education Landscape แนวโน้มภัยคุกคามความต้องการกำลังคน และเส้นทางอาชีพด้าน Cybersecurity

- Cybersecurity Knowledge Areasกรอบองค์ความรู้ด้าน Human and Regulatory, Attacks and Defences, Systems Security, Software and Platform Security และ Infrastructure Security

- กรณีศึกษาหลักสูตร Cybersecurity ของ PIM โครงสร้างรายวิชา การเรียนภาคปฏิบัติ โครงงาน การฝึกงาน

- การออกแบบห้องปฏิบัติการด้วย NGFW, HCI, Server, L๓ Switch, Wi-Fi Controller, Network Sensor, NDR และ Cyber Command

- สาธิต Security Policy, Network Segmentation, การตรวจจับการโจมตี และการวิเคราะห์

๘. วิทยากร

วิทยากรภาคเอกชน จากบริษัท Lenovo (ประเทศไทย) จำกัด และบริษัท ซังฟอร์ เทคโนโลยี (ประเทศไทย) จำกัด (Sangfor Technologies (Thailand) Co., Ltd.)

๙. กลุ่มเป้าหมาย

ครูและบุคลากรทางการศึกษาในสังกัดสำนักงานคณะกรรมการการอาชีวศึกษา โดยเน้นผู้ที่มีบทบาทเกี่ยวข้องกับการจัดการเรียนการสอนด้านเทคโนโลยี การบริหารระบบสารสนเทศ และการดูแลโครงสร้างพื้นฐานดิจิทัลของสถานศึกษา

๑๐. คุณสมบัติของผู้เข้ารับการอบรม

๑๐.๑ ครูผู้สอนและบุคลากรอาชีวศึกษา สาขาวิชาเทคโนโลยีสารสนเทศ เทคโนโลยีคอมพิวเตอร์ เทคนิคคอมพิวเตอร์ เทคโนโลยีธุรกิจดิจิทัล คอมพิวเตอร์ธุรกิจ หรือสาขาที่เกี่ยวข้องกับหลักสูตร

๑๐.๒ มีความตั้งใจ มุ่งมั่นเพื่อพัฒนาความรู้พื้นฐานการรักษาความมั่นคงปลอดภัยไซเบอร์นำความรู้ที่ได้ไปใช้ในชีวิตประจำวัน และถ่ายทอดให้กับนักเรียน

๑๑. วิธีการวัดและประเมินผล

๑๑.๑ วิธีการวัดและการประเมินผล

๑) ประเมินผลโดยใช้แบบทดสอบก่อนการอบรมและหลังการอบรม เพื่อวัดความรู้ ความเข้าใจในเนื้อหาวิชาที่เข้ารับการอบรม

๒) แบบประเมินผลโครงการหลังการฝึกอบรมและฝึกปฏิบัติ เพื่อวัดผลความพึงพอใจของผู้เข้ารับการอบรมและการบริหารจัดการโครงการในภาพรวม

๑๑.๒ เกณฑ์การผ่านการฝึกอบรมและพัฒนาวัดจากในห้องเรียน

๑) มีเวลาเข้าอบรมไม่น้อยกว่า ร้อยละ ๘๐

๒) สอบผ่านแบบทดสอบหลังเรียน ร้อยละ ๘๐

๑๒. งบประมาณ

บริษัท Lenovo (ประเทศไทย) จำกัด เป็นผู้รับผิดชอบ ค่าอาหารเช้า ค่าอาหารกลางวัน ค่าอาหารว่างและเครื่องดื่ม สำหรับค่าเบี้ยเลี้ยง (เบิกได้ ๒ ใน ๓ ส่วน เฉพาะวันที่มีการอบรม) ในส่วนของค่าพาหนะให้เบิกจากสถานศึกษาต้นสังกัด ส่วนที่พัก พักที่หอพักสำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ถนนรามอินทรา กรุงเทพมหานคร โดยไม่มีค่าใช้จ่าย

ตารางโครงการอบรมเชิงปฏิบัติการการเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์
เพื่อพัฒนาสถานศึกษาอาชีวศึกษา (Build Total Cyber Resiliency from Pocket to Cloud)
ระหว่างวันที่ ๑๔ - ๑๕ กันยายน ๒๕๖๙
ณ สำนักพัฒนาสมรรถนะครูและบุคลากรอาชีวศึกษา ถนนรามอินทรา กรุงเทพมหานคร

วัน / เวลา	๐๙.๐๐ - ๑๐.๐๐ น.	๑๐.๐๐ – ๑๒.๐๐ น.	๑๒.๐๐ - ๑๓.๐๐ น.	๑๓.๐๐ – ๑๕.๐๐ น.	๑๕.๐๐ – ๑๗.๐๐ น.
วันที่ ๑๔ กันยายน ๒๕๖๙	บรรยาย เรื่อง Lenovo AI in Education	บรรยาย เรื่อง AI-Driven Classroom Transformation	พักกลางวัน	บรรยาย เรื่อง บรรยาย เรื่อง Classroom modernization : Powerful specialist computer	
วันที่ ๑๕ กันยายน ๒๕๖๙	บรรยาย เรื่อง Choose Your Own Device Program	บรรยาย เรื่อง Digital Workplace Solution for Education	พักกลางวัน	บรรยาย เรื่อง Microsoft Digital Classroom & Learning Management	Q&A and Closing

หมายเหตุ ๑. ตารางอบรมอาจเปลี่ยนแปลงตามความเหมาะสม
๒. รับประทานอาหารว่างและเครื่องดื่ม เช้า ๑๐.๐๐ - ๑๐.๑๕ น. บ่าย ๑๕.๐๐ - ๑๕.๑๕ น.
๓. รับประทานอาหารเช้า ๐๗.๐๐ - ๐๘.๓๐ น. รับประทานอาหารกลางวัน ๑๒.๐๐ – ๑๓.๐๐ น.