การฝึกยกระดับฝีมือ

หลักสูตร การรักษาความมั่นคงปลอดภัยไซเบอร์
(Cyber Security)
รหัสหลักสูตร 10120014220510
สาขาอาชีพ เทคโนโลยีดิจิทัล
ระดับหลักสูตร ระดับสูง (High)

สถาบันพัฒนาบุคลากรดิจิทัล
กรมพัฒนาฝีมือแรงงาน

ผู้อนุมัติหลักสูตร	นายถวัลย์ น้อยอุทัย ผู้อำนวยการสถาบันพัฒนาบุคลากรดิจิทัล	
วันที่อนุมัติ 2 ตุลาคม 2568	จำนวน 6 แผ่น	ปรับปรุงครั้งที่ .../...

การฝึกยกระดับฝีมือ
หลักสูตร การรักษาความมั่นคงปลอดภัยไซเบอร์
(Cyber Security)
รหัสหลักสูตร 10120014220510
สาขาอาชีพเทคโนโลยีดิจิทัล
ระดับหลักสูตร ระดับสูง (High)
สถาบันพัฒนาบุคลากรดิจิทัล กรมพัฒนาฝีมือแรงงาน

1. วัตถุประสงค์

เพื่อให้ผู้รับการฝึกอบรมมีความรู้ ทักษะ และมีความพร้อมในการประกอบอาชีพด้านความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนมีทัศนคติที่ดีในการประกอบอาชีพ โดยสามารถ

1.1 ปฏิบัติงานตามหลักการพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์

1.2 รักษาความปลอดภัยให้กับระบบเครือข่ายขององค์กรได้

1.3 เลือกและใช้งานเทคโนโลยี Endpoint Security ได้อย่างเหมาะสม

1.4 ประเมินช่องโหว่ของระบบ (Vulnerability Assessment) และการบริหารจัดการความเสี่ยง (Risk Management) ด้านไซเบอร์ขององค์กรได้

1.5 รับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Handling) ได้อย่างเหมาะสม

2. ระยะเวลาการฝึก

ผู้รับการฝึกจะได้รับการฝึกภาคทฤษฎี และภาคปฏิบัติ โดยหน่วยงานสังกัดกรมพัฒนาฝีมือแรงงาน หรือหน่วยงานอื่นที่เกี่ยวข้อง ระยะเวลาการฝึก จำนวน 30 ชั่วโมง

3. คุณสมบัติของผู้รับการฝึก

3.1 มีอายุตั้งแต่ 18 ปีขึ้นไป

3.2 มีความรู้พื้นฐานด้านการใช้งานคอมพิวเตอร์และอินเทอร์เน็ต หรือ มีประสบการณ์ในการทำงานด้านคอมพิวเตอร์และอินเทอร์เน็ต ไม่น้อยกว่า 6 เดือน

3.3 มีสุขภาพร่างกายแข็งแรง ไม่เป็นอุปสรรคต่อการฝึก และสามารถเข้ารับการฝึกได้ตลอดหลักสูตร

3.4 ไม่เป็นผู้ติดยาเสพติดให้โทษ และไม่เป็นโรคติดต่ออย่างร้ายแรง

4. วุฒิบัตร

ชื่อเต็ม : วุฒิบัตรพัฒนาฝีมือแรงงาน หลักสูตร การรักษาความมั่นคงปลอดภัยไซเบอร์

ชื่อย่อ : วพร. การรักษาความมั่นคงปลอดภัยไซเบอร์

ผู้รับการฝึกที่จะผ่านการอบรมจะต้องมีระยะเวลาการฝึกอบรมตามหลักสูตรไม่น้อยกว่าร้อยละ 80 และผ่านการประเมินผลตามเกณฑ์ไม่น้อยกว่าร้อยละ 70 ทั้งภาคทฤษฎีและปฏิบัติ จะได้รับวุฒิบัตรจากกรมพัฒนาฝีมือแรงงาน

5. หัวข้อวิชา

รหัส	หัวข้อวิชา	ชั่วโมง	
		ทฤษฎี	ปฏิบัติ
10122232201	หลักการด้านความมั่นคงปลอดภัยไซเบอร์	1	2
10122232202	เทคโนโลยีการเข้ารหัสลับ	1	2
10122232203	การรักษาความปลอดภัยให้กับระบบเครือข่าย	1	2
10122232204	เทคโนโลยี Endpoint Security	1	2
10122232205	การป้องกันภัยคุกคามและการโจมตีรูปแบบต่าง ๆ	2	4
10122232206	การประเมินช่องโหว่ของระบบ	2	4
10122232207	การบริหารจัดการความเสี่ยง	1	2
10122232208	การรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	1	2
10122239901	การวัดและประเมินผล	0	0
รวม		**10**	**20**
		30	

6. เนื้อหาวิชา

10122232201 หลักการด้านความมั่นคงปลอดภัยไซเบอร์ **(1 : 2)**

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ เกี่ยวกับหลักการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Principles)

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับหลักการพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Principles) คำศัพท์เฉพาะทาง (Technical Term) ในสายอาชีพ การบริหารจัดการการเข้าถึงระบบ (Access Control) กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework)

ฝึกปฏิบัติเกี่ยวกับการบริหารจัดการการเข้าถึงระบบ ได้แก่ การจัดการสิทธิผู้ใช้ (User) บนระบบปฏิบัติการ จัดการการเข้าถึงระบบที่ประกอบไปด้วยการระบุตัวตน การพิสูจน์ตัวตน การจัดการสิทธิ การประยุกต์ใช้กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework)

10122232202 เทคโนโลยีการเข้ารหัสลับ **(1 : 2)**

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ เกี่ยวกับเทคโนโลยีการเข้ารหัสลับเพื่อรักษาความปลอดภัยให้กับข้อมูล

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับเทคโนโลยีการเข้ารหัสลับ (Cryptographic) การเข้ารหัสแบบสมมาตร (Symmetric Encryption) การเข้ารหัสแบบอสมมาตร (Asymmetric Encryption) การเข้ารหัสแบบทางเดียว (Hashing)

ฝึกปฏิบัติเกี่ยวกับการใช้เครื่องมือในการเข้ารหัสแบบแบบทางเดียว (Hashing) และเครื่องมือการเข้ารหัสแบบอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

10122232203 การรักษาความปลอดภัยให้กับระบบเครือข่าย (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ เกี่ยวกับระบบเครือข่ายและการรักษาความมั่นคงปลอดภัยให้กับระบบเครือข่ายทั้งแบบมีสายและแบบไร้สาย การเลือกใช้โปรโตคอล (Protocol) ภายในระบบเครือข่ายที่มีความมั่นคงปลอดภัย

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับหลักการออกแบบระบบเครือข่ายให้มีความมั่นคงปลอดภัย การแบ่งย่อยระบบเครือข่ายเพื่อความปลอดภัย อุปกรณ์ด้านความมั่นคงปลอดภัยระบบเครือข่าย

ฝึกปฏิบัติเกี่ยวกับการตั้งค่าอุปกรณ์ด้านความมั่นคงปลอดภัยระบบเครือข่าย การเลือกใช้อุปกรณ์ระบบเครือข่ายให้เหมาะสมกับความต้องการ

10122232204 เทคโนโลยี Endpoint Security (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ เกี่ยวกับเทคโนโลยี Endpoint Security ความแตกต่างของเทคโนโลยี Endpoint Security แต่ละประเภท การตั้งค่าความปลอดภัยให้กับระบบปฏิบัติการ

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับเทคโนโลยี Endpoint Security การตั้งค่าความปลอดภัยให้กับระบบปฏิบัติการ ความสำคัญของการอัปเดตระบบปฏิบัติการ

ฝึกปฏิบัติเกี่ยวกับการตั้งค่าความปลอดภัยให้กับอุปกรณ์ Endpoint ประเภทต่าง ๆ การตั้งค่าความปลอดภัยและการอัปเดตระบบปฏิบัติการ

0122232205 การป้องกันภัยคุกคามและการโจมตีรูปแบบต่าง ๆ (2 : 4)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ เกี่ยวกับการป้องกันภัยคุกคามและการโจมตีรูปแบบต่าง ๆ

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับประเภทของภัยคุกคาม ประเภทของการโจมตี วิธีการป้องกันภัยคุกคามและการโจมตีทางไซเบอร์

ฝึกปฏิบัติเกี่ยวกับวิธีการป้องกันภัยคุกคามและการโจมตีทางไซเบอร์

10122232206 การประเมินช่องโหว่ของระบบ (2 : 4)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ เกี่ยวกับกระบวนการประเมินช่องโหว่ของระบบ (Vulnerability Assessment)

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับกระบวนการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) การใช้เครื่องมือประเมินช่องโหว่ของระบบทั้งแบบ Opensource และ แบบ Commercial วิธีการแก้ไขช่องโหว่ของระบบ

ฝึกปฏิบัติเกี่ยวกับการใช้เครื่องมือประเมินช่องโหว่ของระบบทั้งแบบ Opensource และแบบ Commercial วิธีการแก้ไขช่องโหว่ของระบบ

10122232207 การบริหารจัดการความเสี่ยง (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ เกี่ยวกับการบริหารจัดการความเสี่ยง (Risk Management) การเลือกกลยุทธ์ในการรับมือกับความเสี่ยง

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับกระบวนการในการบริหารจัดการความเสี่ยง (Risk Management) กลยุทธ์ในการรับมือกับความเสี่ยง กรอบ (Framework) และแนวปฏิบัติที่ดี (Best Practice) ในการบริหารจัดการความเสี่ยง แผนกู้คืนภัยพิบัติ (DR Plan) และแผนบริหารความต่อเนื่อง (BCP Plan)

ฝึกปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยง (Risk Management) กลยุทธ์ในการรับมือกับความเสี่ยง กรอบ (Framework) และแนวปฏิบัติที่ดี (Best Practice)

10122232208 การรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ เกี่ยวกับการรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Handling) กฎหมาย ระเบียบ มาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ การพิสูจน์พยานหลักฐานทางดิจิทัลขั้นพื้นฐาน (Digital Forensic Concept)

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับกระบวนการรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Handling) กฎหมาย ระเบียบ มาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ การพิสูจน์พยานหลักฐานทางดิจิทัลขั้นพื้นฐาน (Digital Forensic Concept)

10122232209 การวัดและประเมินผล (0 : 0)

ประเมินความรู้และทักษะของผู้เข้ารับการฝึก ระหว่างการฝึกอบรม และช่วงท้ายของการฝึกอบรม โดยใช้วิธีถามตอบ การสังเกตพฤติกรรมและการมีส่วนร่วมในกิจกรรม รวมถึงการประเมินจากผลงานหรือการนำเสนอผลงาน

คณะผู้จัดทำหลักสูตร

1.	นายจเร รัตนพิทักษ์	วิทยากร บริษัท เออาร์ไอที จำกัด
2.	นางสาวเพ็ญพร ฉิมพลีย์	วิทยากร บริษัท เออาร์ไอที จำกัด
3.	นางสาวอรอนงค์ หลิมเจริญ	วิทยากร บริษัท เออาร์ไอที จำกัด
4.	นายชาติชาย เทียมสนิท	นักวิชาการพัฒนาฝีมือแรงงานชำนาญการ สถาบันพัฒนาบุคลากรดิจิทัลข
5.	นายทวีศักดิ์ เจริญศิลป์	นักวิชาการพัฒนาฝีมือแรงงานชำนาญการ สถาบันพัฒนาบุคลากรดิจิทัล
6.	นายถวัลย์ น้อยอุทัย	นักวิชาการพัฒนาฝีมือแรงงานชำนาญการพิเศษ สถาบันพัฒนาบุคลากรดิจิทัล

อินทุอร

ลงนาม.....ผู้เสนอหลักสูตร

(นางสาวอินทุอร พุทธรัตน์)

ตำแหน่ง นักวิชาการพัฒนาฝีมือแรงงาน

ลงนาม.....ผู้เห็นชอบหลักสูตร

(นายทวีศักดิ์ เจริญศิลป์)

ตำแหน่ง นักวิชาการพัฒนาฝีมือแรงงานชำนาญการ

ลงนาม.....ผู้อนุมัติหลักสูตร

(นายถวัลย์ น้อยอุทัย)

ตำแหน่ง ผู้อำนวยการสถาบันพัฒนาบุคลากรดิจิทัล