หลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ
ผู้ปฏิบัติงานด้านเทคโนโลยี
(Cybersecurity for Technologist)

จัดโดย สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร

สารบัญ

โครงการฝึกอบรมการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ

ผู้ปฏิบัติงานด้านเทคโนโลยี

จัดโดยสำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร

หลักการและเหตุผล

หลักสูตรนี้เน้นให้เกิดความตระหนักถึงบทบาทหน้าที่ตามกฎหมายในเรื่องของการรักษาความมั่นคงปลอดภัย มีความรู้ความเข้าใจในการจัดการเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยและความเสี่ยงทางด้านเทคโนโลยีดิจิทัลที่กำลังเป็นปัญหาในการทำงานในยุคดิจิทัลได้อย่างมีประสิทธิภาพตามแนวทาง NIST Cybersecurity Framework โดยแบ่งเป็น 5 ขั้นตอนสำคัญ คือ identity, Protect, Detect, Response และ Recovery สำหรับช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ เนื้อหาในหลักสูตรจะเน้นให้ผู้เข้ารับการอบรมเกิดความตระหนักและเข้าใจในกระบวนการในการวางแผนรับมือกับภัยคุกคามและความเสี่ยงทางด้านเทคโนโลยีดิจิทัล การเข้าใจในกระบวนการจะทำให้เกิดการวางแผนที่ดีและยั่งยืนในการรับมือกับความเสี่ยงรูปแบบต่างๆ ที่เกิดขึ้นในปัจจุบันและอนาคตที่มีการเปลี่ยนแปลงทางด้านเทคโนโลยีอย่างรวดเร็ว การจัดการเรียนการสอนในหลักสูตรเน้นองค์ความรู้ทั้งภาคทฤษฎีและภาคปฏิบัติ

วัตถุประสงค์

1. เพื่อให้ผู้เข้าอบรมมีความตระหนักรู้ในการใช้งานเทคโนโลยีด้วยความมั่นคงปลอดภัย
2. เพื่อให้ผู้เข้าอบรมมีความรู้เกี่ยวกับกฎหมายในการรักษาความมั่นคงปลอดภัยและเข้าใจในบทบาทหน้าที่ที่ต้องปฏิบัติตามกฎหมาย
3. เพื่อให้ผู้เข้าอบรมมีความรู้และความเข้าใจกรอบในการักษาความปลอดภัยไซเบอร์ตามแนวทางของ NST Cybersecurity Framework
4. เพื่อให้ผู้เข้าอบรมสามารถวางแผนป้องกันและรับมือกับความมั่นคงปลอดภัยไซเบอร์ตามหลักการ
5. เพื่อให้ผู้เข้าอบรมมีการนำความรู้ไปประยุกต์ใช้ในการวางแผนรับมือเกี่ยวกับความเสี่ยงดิจิทัลในองค์กรได้

รูปแบบการฝึกอบรม

1) บรรยาย(Lecture)

2) การอภิปราย(Discussion)

3) อบรมเชิงปฏิบัติการ(Workshop)

รูปแบบและจำนวนชั่วโมงการฝึกอบรม ทั้งรูปแบบ Online และ On-Site ดังตาราง

การบรรยาย (Lecture) (ชั่วโมง)	การสาธิต (Demonstration) (ชั่วโมง)
13	17
จำนวนชั่วโมงอบรมในหลักสูตร รวม 30 ชั่วโมง (5 วัน)	

หมายเหตุ : อาจมีการเปลี่ยนแปลงตามความเหมาะสม

ระยะเวลาการฝึกอบรม

รุ่นที่	ช่วงเวลา	รูปแบบ	สถานที่
1	17 - 21 พฤษภาคม 2565	Onsite	สำนักดิจิทัลเทคโนโลยี มศก. จ.นครปฐม
2	13 – 17 สิงหาคม 2565	Onsite	สำนักดิจิทัลเทคโนโลยี มศก. จ.นครปฐม

3	21 – 25 พฤศจิกายน 2565	Onsite	สำนักดิจิทัลเทคโนโลยี มศก. จ.นครปฐม

ตารางการฝึกอบรม

รายชื่อวิทยากรในการอบรม

1. อาจารย์ ดร.ณัฐโชติ พรหมฤทธิ์

2. ดร.จุมพฏ กาญจนกำธร

เวลา	หัวข้อ	เนื้อหา
	วันที่ 1	
09.00 – 12.00	ภาพรวมความมั่นคงปลอดภัยไซเบอร์ (Security Overview)	☐ Security Awareness การรู้เท่าทันการโจมตีและความมั่นคงปลอดภัยทางไซเบอร์ สถานการณ์ต่าง ๆ ที่เกิดขึ้นในองค์กรทั้งภาครัฐและเอกชน กรณีศึกษาต่าง ๆ ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ การเรียนรู้ถึงความเสียหายที่เกิดขึ้นจากภัยคุกคามไซเบอร์ ☐ Security Trend แนวโน้มของภัยคุกคามต่าง ๆ แนวโน้มของความมั่นคงปลอดภัยไซเบอร์ ☐ Information Security Concept: CIA แนวคิดพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ -Confidentiality คือ การรักษาความลับของไซเบอร์ -Integrity คือ ความถูกต้องของข้อมูลไซเบอร์ -Availability คือ ความพร้อมใช้งานของเทคโนโลยีไซเบอร์
13.00 – 16.00	กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Laws and Regulation)	☐ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ☐ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ☐ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ☐ กรณีศึกษาที่เกี่ยวข้องกับกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
	วันที่ 2	
09.00 – 10.30	การระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Identify)	☐ การศึกษาทำความเข้าใจบริบท ทรัพยากรและกิจกรรมงานสำคัญเพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบทรัพย์สิน ข้อมูล และขีดความสามารถ

เวลา	หัวข้อ	เนื้อหา
		☐ Indentity: Assessment and Auditing แนวทางและกรอบในการประเมินองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ และความเสี่ยง เพื่อวิเคราะห์ช่องว่าง (Gap Analysis) หรือจุดอ่อนของกระบวนการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ตัวอย่างของ Framework ในการประเมินองค์กรต่าง ๆ
10.30 – 12.00	การป้องกันด้านความมั่นคงปลอดภัยไซเบอร์ (Protection)	☐ การศึกษาแนวทางการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสม เพื่อการจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และการสร้างความตระหนักมาตรการควบคุมการเข้าถึงและมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ☐ การศึกษากรอบงานความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity framework) ☐ Protection: Security Design Principles ความรู้พื้นฐานและแนวทางการออกแบบระบบให้มีความมั่นคงปลอดภัย แนวทางการเลือกใช้วิธีการระบบหรือเทคโนโลยีเพื่อการรัษาความมั่นคงปลอดภัยในองค์กรเช่น ไฟร์วอล (Firewall) การป้องกันเครื่องอุปกรณ์ปลายทาง (Endpoint Security) การสำรองข้อมูล (Data backup) และฮาร์ดเดนนิง (Hardening) เพื่อให้เหมาะสมกับการใช้งานในองค์กร ☐ เทคโนโลยีในการรักษาความมั่นคงปลอดภัย
13.00 - 16.00	การเฝ้าระวังด้านความมั่นคงปลอดภัยไซเบอร์ (Detection)	☐ เรียนรู้การจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ☐ Detection: Security Monitoring การเรียนรู้แนวทางการวิเคราะห์ เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Monitoring) การวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามด้านความปลอดภัยไซเบอร์ (Security Monitoring) จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของเครื่องแม่ข่าย อุปกรณ์เครือข่ายและระบบงานต่าง ๆ

เวลา	หัวข้อ	เนื้อหา
		☐ เรียนรู้แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบ
	วันที่ 4	
09.00 – 12.00	การรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Response)	☐ เรียนรู้การจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง ☐ เรียนรู้เกี่ยวกับกระบวนการ “Incident Response” การตอบสอนงต่อสถานการณ์ไม่พึงประสงค์และไม่คาดคิดเพื่อให้องค์กรสามารถควบคุมสถานการณ์และมูลค่าความเสียหายที่เกิดขึ้นให้รวดเร็วทันการณ์และลดความเสียหาย ☐ กรณีศึกษาของการจัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan) ในองค์กรทั้งในและต่างประเทศ ☐ กระบวนการและขั้นตอนในการจัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan)
13.00 – 16.00	การกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์ (Recovery)	☐ เรียนรู้การกู้คืนระบบในกรณีเกิดการโจมตี การกู้คืนข้อมูล เรียนรู้ในวิธีการและแนวทางในการกู้คืนระบบให้กลับสู่สภาวะปกติและแก้สาเหตุที่ทำเกิดปัญหา ☐ กรณีศึกษา และตัวอย่างของการกู้คืนระบบ (Recovery) ที่เกิดขึ้นจากการโจมตีทางไซเบอร์
	วันที่ 5	
09.00 – 16.00	การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ (Incident Drill)	☐ Incident Drill การจำลอง Cyber Attack เพื่อให้องค์กรสามารถซ้อมรับมือกับการโจมตีที่อาจจะเกิดขึ้น เพื่อให้ได้มีส่วนร่วมและได้ลองปฏิบัติจริง ซึ่งจะต้องมีการซักซ้อมทำความเข้าใจและจำบองสถานการณ์ว่าเมื่อเกิดเหตุการณ์แล้วผู้ที่ตกเป็นเหยื่อ จะต้องดำเนินการอย่างไร เจ้าหน้าที่ในแผนกไอที และผู้มีส่วนเกี่ยวข้องจะต้องดำเนินการอย่างไร เพื่อให้สามารถตอบสนองต่อเหตุการณ์

เวลา	หัวข้อ	เนื้อหา
		ที่เกิดขึ้น (Incident response)ได้อย่างถูกต้อง รวดเร็ว และส่งผลให้เกิดผลกระทบกับองค์กรน้อยที่สุด

ค่าธรรมเนียมการฝึกอบรมของหลักสูตร

- ค่าลงทะเบียนฝึกอบรมแบบ Onsite ท่านละ 15,000 บาท (รวมภาษีมูลค่าเพิ่มแล้ว) ทั้งนี้ค่าลงทะเบียนข้างต้น รวม ค่าอาหารกลางวัน และอาหารว่าง

หมายเหตุ กรณีผู้เข้าอบรมมีจำนวนไม่ถึงตามที่กำหนดผู้จัดอบรมจะแจ้งให้ผู้สมัครเข้าร่วมอบรมทราบล่วงหน้า

เงื่อนไขการผ่านการอบรมและได้รับประกาศนียบัตร

1. ผู้เข้ารับการฝึกอบรมต้องทดสอบประเมินความรู้ภาคทฤษฎีด้วยแบบประเมินผลก่อนการฝึกอบรม (Pre-Test)
2. ผู้เข้ารับการฝึกอบรมต้องทดสอบประเมินความรู้ภาคทฤษฎีด้วยแบบประเมินผลหลังการฝึกอบรม (Post-Test) เกณฑ์การผ่านไม่น้อยกว่าร้อยละ 70
3. ผู้เข้ารับการฝึกอบรมจะต้องเข้าร่วมการฝึกอบรมไม่น้อยกว่าร้อยละ 80 ของระยะเวลาฝึกอบรม
4. การประเมินจากการฝึกปฏิบัติ

สถานที่ฝึกอบรม

- สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร
เลขที่ 6 ถนนราชมรรคาใน ตำบลพระปฐมเจดีย์
อำเภอเมือง จังหวัดนครปฐม
โทรศัพท์ : 0-3410-9686

สอบถามรายละเอียด

หากมีข้อสงสัย และ/หรือต้องการทราบรายละเอียดเพิ่มเติม สามารถติดต่อสอบถามได้ที่ นางณัฐสิรี นกแก้ว เบอร์โทร 081 290 4198

ดำเนินการฝึกอบรมโดย

สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร (Bureau Of Digital Technology)

ที่อยู่ เลขที่ 6 ถนนราชมรรคาใน ต.พระปฐมเจดีย์ อ.เมือง จ.นครปฐม 73000

โทร 034 109 686 ต่อ 217043

ไปรษณีย์อิเล็กทรอนิกส์ bdt-training@su.ac.th เว็บไซต์ https://bdt.su.ac.th