หลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี

(Cybersecurity for Technologist)

จัดโดย มหาวิทยาลัยสุโขทัยธรรมาธิราช

ภายใต้การดำเนินงานของ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สารบัญ

โครงการฝึกอบรมหลักสูตรความมั่นคงปลอดภัยดิจิทัลสำหรับผู้บริหารภาครัฐ

จัดโดย มหาวิทยาลัยสุโขทัยธรรมาธิราช

หลักการและเหตุผล

หลักสูตรนี้เน้นให้เกิดความตระหนักถึงบทบาทหน้าที่ตามกฎหมายในเรื่องของการรักษาความมั่นคงปลอดภัย มีความรู้ความเข้าใจในการจัดการเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยและความเสี่ยงทางด้านเทคโนโลยีดิจิทัลที่กำลังเป็นปัญหาในการทำงานในยุคดิจิทัลได้อย่างมีประสิทธิภาพตามแนวทางของ NIST Cybersecurity Framework โดยแบ่งออกเป็น 5 ขั้นตอนสำคัญ คือ Identity, Protect, Detect, Response และ Recovery สำหรับช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ เนื้อหาในหลักสูตรจะเน้นให้ผู้เข้ารับการอบรมเกิดความตระหนักและเข้าใจในกระบวนการในการวางแผนรับมือกับภัยคุกคามและความเสี่ยงทางด้านเทคโนโลยีดิจิทัล การเข้าใจในกระบวนการจะทำให้เกิดการวางแผนที่ดีและยั่งยืนในการรับมือกับความเสี่ยงรูปแบบต่าง ๆ ที่เกิดขึ้นทั้งในปัจจุบันและอนาคตที่มีการเปลี่ยนแปลงทางด้านเทคโนโลยีอย่างรวดเร็ว การจัดการเรียนการสอนในหลักสูตรเน้นองค์ความรู้ทั้งภาคทฤษฎีและภาคปฏิบัติเพื่อให้ผู้ปฏิบัติงานเฉพาะด้านเทคโนโลยีดิจิทัล ได้นำความรู้และทักษะจากหลักสูตรไปประยุกต์ใช้ ในการวางแผนการรับมือกับภัยคุกคามและความเสี่ยงทางด้านดิจิทัลในองค์กรได้อย่างมีประสิทธิภาพ

วัตถุประสงค์

1 เพื่อให้มีความตระหนักรู้ในการใช้งานเทคโนโลยีด้วยความมั่นคงปลอดภัย

2 เพื่อให้มีความรู้เกี่ยวกับกฎหมายในการรักษาความมั่นคงปลอดภัยและเข้าใจในบทบาทหน้าที่ที่ต้องปฏิบัติตามกฎหมาย

3 เพื่อให้มีความรู้และความเข้าใจกรอบในการรักษาความมั่นคงปลอดภัยไซเบอร์ตามแนวทางของ NIST Cybersecurity Framework

4 เพื่อให้สามารถวางแผนป้องกันและรับมือกับความมั่นคงปลอดภัยไซเบอร์ได้ตามหลักการ

5 เพื่อให้มีการนำความรู้ไปประยุกต์ใช้ในการวางแผนรับมือเกี่ยวกับความเสี่ยงดิจิทัลในองค์กรได้

รูปแบบการฝึกอบรม

1. การบรรยาย 13 ชั่วโมง
2. การฝึกปฏิบัติ 17 ชั่วโมง

ระยะเวลาการฝึกอบรม

รุ่นที่ 1 วันที่ 18-22 เมษายน 2565

รุ่นที่ 2 วันที่ 9 - 13 พฤษภาคม 2565

ตารางการฝึกอบรม : อาจารย์ ดร.ศรันย์ นาคถนอม และอาจารย์ ดร.เตชค์ฐสิณป์ เพียซ้าย

เวลา	หัวข้อ	เนื้อหา
		วันที่ 1 (อาจารย์ ดร.เตชค์ฐสิณป์ เพียซ้าย)
9.01 – 10.00	ภาพรวมความมั่นคงปลอดภัยไซเบอร์ (Security Overview)	- Security Awareness การรู้เท่าทันการโจมตีและความมั่นคงปลอดภัยทางไซเบอร์ สถานการณ์ต่าง ๆ ที่เกิดขึ้นในการองค์กรทั้งภาครัฐและเอกชน กรณีศึกษาต่าง ๆ ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ การเรียนรู้ถึงความเสียหายที่เกิดขึ้นจากภัยคุกคามไซเบอร์ - Security Trend แนวโน้มของภัยคุกคามต่าง ๆ แนวโน้มของความมั่นคงปลอดภัย ไซเบอร์ - Information security Concept: CIA แนวคิดพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ ▪Confidentiality คือ การรักษาความลับของ ไซเบอร์ ▪Integrityคือความถูกต้องของข้อมูลไซเบอร์ ▪Availability คือความพร้อมใช้งานของเทคโนโลยีไซเบอร์
10.01-12.00	กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไซเบอร์ (Laws and Regulation)	▪ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2560 ▪ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ▪ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
13.01-14.00	กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไซเบอร์ (Laws and Regulation)	กรณีศึกษาที่เกี่ยวข้องกับกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
14.01-16.00	การระบุความเสี่ยงด้านความมั่นคงปลอดภัย ไซเบอร์ (Identify)	- การศึกษาทำความเข้าใจบริบท ทรัพยากรและกิจกรรมงานสำคัญเพื่อบริหารจัดการความเสี่ยงตามฐานความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ - Identity: Assessment and Auditing แนวทางและกรอบในการการประเมินองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ และความเสี่ยงเพื่อวิเคราะห์ช่องว่าง (Gap Analysis) หรือจุดอ่อนของกระบวนการ

เวลา	หัวข้อ	เนื้อหา
		ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ตัวอย่างของ Framework ในการประเมินขององค์กรต่าง ๆ
		วันที่2 (อาจารย์ ดร.เตชค์ฐสิณป์ เพียซ้าย)
9.01-12.00	การป้องกันด้านความมั่นคงปลอดภัยไซเบอร์ (Protection)	- การศึกษาแนวทางการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสม เพื่อการจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และการสร้างความตระหนักมาตรการควบคุมการเข้าถึงและมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ - การศึกษากรอบงานความมั่นคงปลอดภัยทาง ไซเบอร์ (Cybersecurity framework) - Protection: Security Design Principles ความรู้พื้นฐานและแนวทางการออกแบบระบบให้มีความมั่นคงปลอดภัย แนวทางการเลือกใช้วิธีการ ระบบหรือเทคโนโลยีเพื่อการรักษาความมั่นคงปลอดภัยในองค์กร เช่น ไฟร์วอล (Firewall) การป้องกันเครื่องอุปกรณ์ปลายทาง (Endpoint Security) การสำรองข้อมูล (Data backup) และ ฮาร์ดเดนนิง (Hardening) เพื่อให้เหมาะสมกับการใช้งานในองค์กร - เทคโนโลยีในการรักษาความมั่นคงปลอดภัย ไซเบอร์
13.01-16.00	การเฝ้าระวังด้านความมั่นคงปลอดภัยไซเบอร์ (Detection)	-เรียนรู้การจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น - Detection: Security Monitoring การเรียนรู้แนวทางการวิเคราะห์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Monitoring Service) การวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามด้านความปลอดภัยไซเบอร์ (Security Monitoring) จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของเครื่องแม่ข่าย อุปกรณ์เครือข่ายและระบบงานต่าง ๆ - เรียนรู้แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบ
		วันที่3 (อาจารย์ ดร.ศรันย์ นาคถนอม)
9.01-12.00	การรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Response)	- เรียนรู้การจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

เวลา	หัวข้อ	เนื้อหา
		- เรียนรู้เกี่ยวกับกระบวนการ “Incident Response”การตอบสนองต่อสถานการณ์ไม่พึงประสงค์และไม่คาดคิดเพื่อให้องค์กรสามารถควบคุมสถานการณ์และมูลค่าความเสียหายที่เกิดขึ้นให้รวดเร็วทันการณ์และลดความเสียหาย
13.01-16.00	การรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Response)	- กรณีศึกษาของการจัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan) ในองค์กรทั้งในและต่างประเทศ - กระบวนการและขั้นตอนในการจัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan)
		วันที่4 (อาจารย์ ดร.ศรันย์ นาคถนอม)
9.01-12.00	การกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์ (Recovery)	เรียนรู้การกู้คืนระบบในกรณีเกิดการโจมตี การกู้คืนข้อมูล เรียนรู้ในวิธีการและแนวทางในการกู้คืนระบบให้กลับสู่สภาวะปกติและแก้ไขสาเหตุที่ทำให้เกิดปัญหา
13.01-16.00	การกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์ (Recovery)	กรณีศึกษาและตัวอย่างของการกู้คืนระบบ(Recovery) ที่เกิดขึ้นจากการโจมตีทางไซเบอร์
		วันที่5
9.01-12.00	การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ (Incident Drill)	Incident Drill การจำลอง Cyber Attack เพื่อให้องค์กรสามารถซ้อมรับมือกับการโจมตีที่อาจจะเกิดขึ้น เพื่อให้ได้มีส่วนร่วมและได้ลองปฏิบัติจริง ซึ่งจะต้องมีการซักซ้อมทำความเข้าใจและจำลองสถานการณ์ว่าเมื่อเกิดเหตุการณ์แล้วผู้ที่ตกเป็นเหยื่อ จะต้องดำเนินการอย่างไร เจ้าหน้าที่ในแผนกไอทีและผู้มีส่วนเกี่ยวข้องจะต้องดำเนินการอย่างไร เพื่อให้สามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้น (Incident response) ได้อย่างถูกต้อง รวดเร็ว และส่งผลให้เกิดผลกระทบกับองค์กรน้อยที่สุด
13.01-16.00	การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ (Incident Drill)	Incident Drill การจำลอง Cyber Attack เพื่อให้องค์กรสามารถซ้อมรับมือกับการโจมตีที่อาจจะเกิดขึ้น เพื่อให้ได้มีส่วนร่วมและได้ลองปฏิบัติจริง ซึ่งจะต้องมีการซักซ้อมทำความเข้าใจและจำลองสถานการณ์ว่าเมื่อเกิดเหตุการณ์แล้วผู้ที่ตกเป็นเหยื่อ จะต้องดำเนินการอย่างไร เจ้าหน้าที่ในแผนกไอทีและผู้มีส่วนเกี่ยวข้องจะต้องดำเนินการอย่างไร เพื่อให้สามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้น (Incident response) ได้อย่างถูกต้อง รวดเร็ว และส่งผลให้เกิดผลกระทบกับองค์กรน้อยที่สุด

ค่าธรรมเนียมการฝึกอบรมของหลักสูตร

ค่าลงทะเบียนฝึกอบรมรูปแบบ Onsite 15,500 บาท/คน

ค่าลงทะเบียนฝึกอบรมรูปแบบ Online 9,700 บาท/คน

เงื่อนไขการผ่านการอบรมและได้รับประกาศนียบัตร

1. แบบทดสอบความรู้ความเข้าใจก่อน-หลัง การอบรม
2. ประเมินการมีส่วนร่วมในการอภิปรายระหว่างเรียน
3. การประเมินจากการทดสอบการประมวลความรู้

สถานที่ฝึกอบรม

ห้องปฏิบัติการคอมพิวเตอร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

สอบถามรายละเอียด

1.	อาจารย์ ดร.ศรันย์ นาคถนอม	เบอร์โทร 080-039-7788
2.	อาจารย์ ดร.เตชค์ฐสิณป์ เพียซ้าย	เบอร์โทร 099-393-6519
3.	ผู้ช่วยศาตราจารย์ฐากร พฤกษวันประสุต	เบอร์โทร 089-660-3335
4.	นางสาวนพวรรณ ชื่นอารมณ์	เบอร์โทร 089-814-0799

ดำเนินการฝึกอบรมโดย

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

เลขที่ 9/9 หมู่ 9 ต.บางพูด อ.ปากเกร็ด จ.นนทบุรี 11120