

ข้อเสนอโครงการ

หลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี

(Cybersecurity for Technologist)

จัดโดยมหาวิทยาลัยหอการค้าไทย

สารบัญ

	หน้าที่
<input checked="" type="checkbox"/> หลักการและเหตุผล	2
<input checked="" type="checkbox"/> วัตถุประสงค์	2
<input checked="" type="checkbox"/> รูปแบบการฝึกอบรม	2
<input checked="" type="checkbox"/> ระยะเวลาการฝึกอบรม	3
<input checked="" type="checkbox"/> ตารางการฝึกอบรม	3
<input checked="" type="checkbox"/> ค่าธรรมเนียมการฝึกอบรมของหลักสูตร	4
<input checked="" type="checkbox"/> เงื่อนไขการผ่านการฝึกอบรม	4
<input checked="" type="checkbox"/> สถานที่ฝึกอบรม	5
<input checked="" type="checkbox"/> สอบถามรายละเอียด	5
<input checked="" type="checkbox"/> ดำเนินการฝึกอบรมโดย	5

โครงการฝึกอบรมหลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี (Cybersecurity for Technologist)

จัดโดยมหาวิทยาลัยหอการค้าไทย

หลักการและเหตุผล

การเปลี่ยนถ่ายไปสู่องค์กรดิจิทัลทำให้องค์กรสามารถตอบสนองอย่างรวดเร็วต่อการเปลี่ยนแปลงของความต้องการได้ องค์กรประกอบหนึ่งที่สำคัญอย่างยิ่งต่อองค์กรดิจิทัลคือ มีการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม ซึ่งจำเป็นต้องทำทั้งในระดับนโยบายและระดับปฏิบัติการ

โครงการนี้ได้เสนอหลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี เพื่อเป็นการส่งเสริมให้บุคลากรภาครัฐและ/หรือผู้ที่สนใจในระดับปฏิบัติการมีความตระหนักรู้และเน้นด้านองค์ความรู้ในเชิงปฏิบัติการเพื่อนำไปประยุกต์ใช้ในการวางแผนป้องกันและรับมือกับความเสี่ยงดิจิทัลในองค์กรได้

วัตถุประสงค์

1. เพื่อให้มีความตระหนักรู้ในการใช้งานเทคโนโลยีด้วยความมั่นคงปลอดภัยไซเบอร์
2. เพื่อให้มีความรู้เกี่ยวกับกฎหมายในการรักษาความมั่นคงปลอดภัยและเข้าใจในบทบาทหน้าที่ที่ต้องปฏิบัติตามกฎหมาย
3. เพื่อให้มีความรู้และความเข้าใจรอบในการรักษาความมั่นคงปลอดภัยไซเบอร์ตามแนวทางของ NIST Cybersecurity Framework
4. เพื่อให้สามารถวางแผนป้องกันและรับมือกับความมั่นคงปลอดภัยไซเบอร์ได้ตามหลักการ
5. เพื่อให้มีการนำความรู้ไปประยุกต์ใช้ในการวางแผนรับมือเกี่ยวกับความเสี่ยงดิจิทัลในองค์กรได้

รูปแบบการฝึกอบรม

การอบรมเป็นรูปแบบผสมผสานโดยมีการบรรยายและการอบรมเชิงปฏิบัติการรวมทั้งสิ้น 30 ชั่วโมง

ระยะเวลาการฝึกอบรม

การฝึกอบรมแบ่งเป็นรุ่นละไม่เกิน 30 คนโดยมีกำหนดในการฝึกอบรมดังนี้

- รุ่นที่ 1 ระหว่างวันที่ 30 พฤษภาคม – 3 มิถุนายน 2565
- รุ่นที่ 2 ระหว่างวันที่ 1 – 5 สิงหาคม 2565
- รุ่นที่ 3 ระหว่างวันที่ 19 – 23 ธันวาคม 2565

ตารางการฝึกอบรม

รายชื่อวิทยากรในการอบรม

1. ผศ.ดร. ศุภฤกษ์ มานิตพรสุทธิ์
2. ผศ. เจษฎา แก้ววิทย์

วันที่	เวลา	หัวข้อ
1	8.30 – 9.00 น.	ลงทะเบียน
	9.00 – 16.00 น.	ภาพรวมความมั่นคงปลอดภัยไซเบอร์ (Security Overview) - Security Awareness - Security Trend - Information Security Concept: CIA - ISO/IEC 27001 กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Laws and Regulation) - พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2560 - พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 - พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562 การระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Identification) - Identification: Assessment and Auditing แนวทางและกรอบในการประเมินองค์กร ด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยง
2	8.30 – 9.00 น.	ลงทะเบียน
	9.00 – 16.00 น.	การป้องกันด้านความมั่นคงปลอดภัยไซเบอร์ (Protection) - กรอบงานความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework)

วันที่	เวลา	หัวข้อ
		<ul style="list-style-type: none"> - Protection: Security Design Principles พื้นฐานและแนวทางการออกแบบระบบให้มีความมั่นคงปลอดภัย - เทคโนโลยีในการรักษาความมั่นคงปลอดภัยไซเบอร์ การเฝ้าระวังด้านความมั่นคงปลอดภัยไซเบอร์ (Detection) <ul style="list-style-type: none"> - Detection: Security Monitoring แนวทางการวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์
3	8.30 – 9.00 น.	ลงทะเบียน
	9.00 – 16.00 น.	การรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Response) <ul style="list-style-type: none"> - กระบวนการและขั้นตอนในการจัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan) - กรณีศึกษาการจัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan) ในองค์กรทั้งในและต่างประเทศ
4	8.30 – 9.00 น.	- ลงทะเบียน
	9.00 – 16.00 น.	การกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์ (Recovery) <ul style="list-style-type: none"> - การกู้คืนระบบในกรณีเกิดการโจมตี การกู้คืนข้อมูล วิธีการและแนวทางในการกู้คืนระบบให้กลับสู่สภาวะปกติและแก้ไขสาเหตุที่ทำให้เกิดปัญหา
5	8.30 – 9.00 น.	- ลงทะเบียน
	9.00 – 16.00 น.	การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ (Incident Drill) <ul style="list-style-type: none"> - กิจกรรมการซักซ้อมการโจมตีทางไซเบอร์ เพื่อทดสอบปฏิบัติและซ้อมรับมือการโจมตีที่อาจเกิดขึ้น

หมายเหตุ: กำหนดการและรายละเอียดการฝึกอบรม อาจเปลี่ยนแปลงได้ตามความเหมาะสม

ค่าธรรมเนียมการฝึกอบรมของหลักสูตร

ค่าลงทะเบียนฝึกอบรมแบบ On-Site ท่านละ 15,000 บาท (รวมภาษีมูลค่าเพิ่มแล้ว) ทั้งนี้ ค่าลงทะเบียนข้างต้นรวมค่าอาหารกลางวันและอาหารว่าง

ค่าลงทะเบียนฝึกอบรมแบบ Online ท่านละ 10,000 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

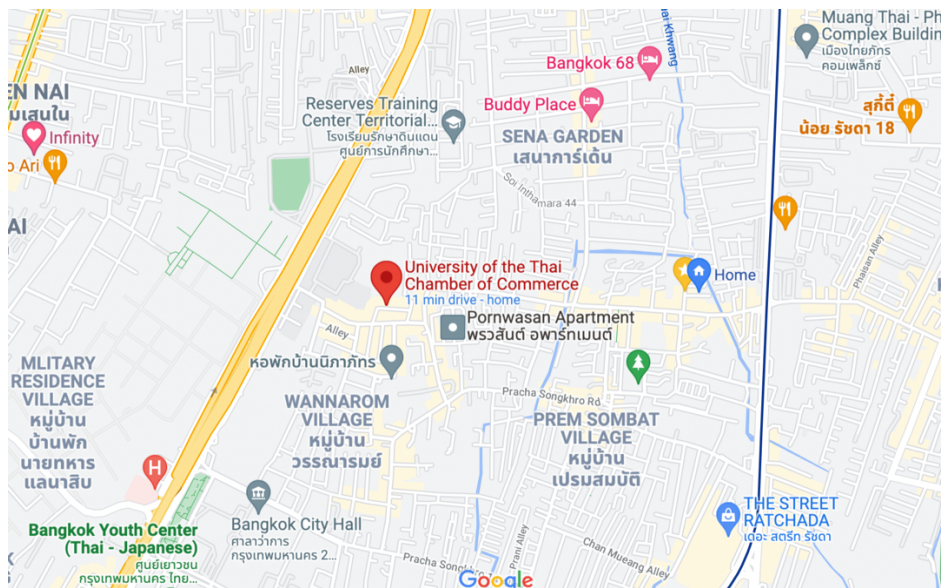
หมายเหตุ กรณีผู้เข้าอบรมมีจำนวนไม่ถึงตามที่กำหนด ผู้จัดอบรมจะแจ้งให้ผู้สมัครเข้าร่วมอบรมทราบล่วงหน้า

เงื่อนไขการผ่านการอบรมและได้รับประกาศนียบัตร

1. เวลาที่เข้าการอบรมไม่ต่ำกว่าร้อยละ 80
2. ผ่านการประเมินแบบทดสอบก่อนและหลังการอบรม (เกณฑ์การผ่านไม่น้อยกว่าร้อยละ 70)
3. ผ่านการประเมินจากการฝึกปฏิบัติ

สถานที่ฝึกอบรม

มหาวิทยาลัยหอการค้าไทย
เลขที่ 126/1 ซอยวิภาวดีรังสิต 2
ถนนวิภาวดีรังสิต แขวงรัชดาภิเษก
เขตดินแดง กรุงเทพมหานคร 10400



สอบถามรายละเอียด

สามารถสอบถามรายละเอียดเพิ่มเติมได้ที่ผศ.ดร. ศุภฤกษ์ มานิตพรสุทธิ์ สาขาวิชาวิศวกรรมคอมพิวเตอร์ และปัญญาประดิษฐ์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยหอการค้าไทย โทร. 062-236-8558 อีเมล suparerk_man@utcc.ac.th

ดำเนินการฝึกอบรมโดย

สาขาวิชาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยหอการค้าไทย
โทร. 062-236-8558, 02-697-6705
อีเมล suparerk_man@utcc.ac.th