

ข้อเสนอโครงการฝึกอบรม

หลักสูตรความมั่นคงปลอดภัยไซเบอร์พื้นฐาน

(Cybersecurity Fundamentals)

จัดโดย คณะเทคโนโลยีสารสนเทศและการสื่อสาร

มหาวิทยาลัยมหิดล

สารบัญ

	หน้าที่
<input checked="" type="checkbox"/> หลักการและเหตุผล	2
<input checked="" type="checkbox"/> วัตถุประสงค์	2
<input checked="" type="checkbox"/> รูปแบบการฝึกอบรม	3
<input checked="" type="checkbox"/> ระยะเวลาการฝึกอบรม	3
<input checked="" type="checkbox"/> ตารางการฝึกอบรม	4
<input checked="" type="checkbox"/> ค่าธรรมเนียมการฝึกอบรมของหลักสูตร	6
<input checked="" type="checkbox"/> เงื่อนไขการผ่านการฝึกอบรม	6
<input checked="" type="checkbox"/> สถานที่ฝึกอบรม	6
<input checked="" type="checkbox"/> สอบถามรายละเอียด	7
<input checked="" type="checkbox"/> ดำเนินการฝึกอบรมโดย	8

โครงการฝึกอบรมหลักสูตรความมั่นคงปลอดภัยไซเบอร์พื้นฐาน
(Cybersecurity Fundamentals)
จัดโดยคณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล

หลักการและเหตุผล

หลักสูตรนี้มุ่งเน้นให้ผู้เข้าอบรมได้ตระหนักรู้ความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งมีความรู้และความเข้าใจในภัยคุกคามไซเบอร์รูปแบบต่าง ๆ โดยเฉพาะที่กำลังเป็นประเด็นสำคัญในปัจจุบัน นอกจากนี้ยังส่งเสริมให้ผู้เข้ารับการอบรมมีความรู้เบื้องต้นในวิธีการป้องกันภัยคุกคามไซเบอร์ที่จะเกิดขึ้นในอนาคตได้อย่างถูกต้องและทันท่วงที รวมทั้งมีความเข้าใจเบื้องต้นเกี่ยวกับการบริหารความเสี่ยง (Risk Management) และการประเมินความเสี่ยง (Risk Assessment) ระบบสารสนเทศให้มีความมั่นคงปลอดภัยทางไซเบอร์

วัตถุประสงค์

- 1) เพื่อให้มีความตระหนักรู้ในความมั่นคงปลอดภัยไซเบอร์
- 2) เพื่อให้สามารถใช้เทคโนโลยีคอมพิวเตอร์ได้อย่างปลอดภัยและแก้ปัญหาเบื้องต้นได้เมื่อต้องพบกับภัยคุกคาม
- 3) เพื่อให้การประเมินความเสี่ยงด้านไซเบอร์โดยมีแนวทางการดำเนินงานที่ถูกต้องเหมาะสม



รูปแบบการฝึกอบรม

การฝึกอบรมในหลักสูตรฯ เป็นการผสมผสานหลายวิธี ได้แก่

- 1) บรรยาย (Lecture)
- 2) การอภิปราย (Discussion)
- 3) อบรมเชิงปฏิบัติการ (Workshop)

ซึ่งการผสมผสานรูปแบบการฝึกอบรมดังกล่าวข้างต้นจะทำให้ผู้เรียนมีกระบวนการเรียนรู้ และเกิดความคิด และสามารถวิเคราะห์ ซึ่งจะสามารถทำให้บรรลุตามวัตถุประสงค์ของหลักสูตรที่ได้กำหนดไว้ โดยสามารถอธิบายได้ดังภาพต่อไปนี้

ระยะเวลาการฝึกอบรม

การบรรยาย (Lecture) (ชั่วโมง)	การฝึกปฏิบัติ (Workshop) (ชั่วโมง)
4	8
จำนวนชั่วโมงอบรมในหลักสูตร รวม 12 ชั่วโมง (2 วัน)	

* อาจมีการเปลี่ยนแปลงตามความเหมาะสม

การจัดอบรมจำนวน 1 รุ่น รุ่นละไม่เกิน 40 คน จำนวน 2 วัน (วันละ 6 ชั่วโมง รวม 12 ชั่วโมง)

รุ่นที่ 1 อบรมระหว่างวันที่ 9-10 มิถุนายน 2565

ตารางการฝึกอบรม

วิทยากร

ดร. อธิพิณ รัชมีโรจน์ คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล

ดร. อัษฎารัตน์ คุรัตน์ คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล

รศ. ดร. สุตสงวน งามสุริยโรจน์ คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล

เวลา	หัวข้อ	เนื้อหา
วันที่ 1		
09.00 -12.00	ความรู้เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศขององค์กร และกฎหมายที่เกี่ยวข้องในหน่วยงานรัฐ	<ul style="list-style-type: none">▪ พรบ. คุ้มครองข้อมูลส่วนบุคคล▪ พรบ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์▪ พื้นฐานการป้องกันภัยคุกคามไซเบอร์
	การวิเคราะห์กระบวนการทำงานขององค์กร	<ul style="list-style-type: none">▪ การวิเคราะห์กระบวนการทำงานขององค์กรเพื่อปรับปรุงหรือแก้ไขปัญหาการรักษาความปลอดภัยไซเบอร์
	แนวคิดด้านความมั่นคงปลอดภัยแบบZero Trust	<ul style="list-style-type: none">▪ แนวคิดด้านความมั่นคงปลอดภัยแบบZero Trust ระบบเครือข่ายทั้งหมดไม่ควรเชื่อถือซึ่งกันและกัน ไม่ใช่เฉพาะแค่การติดต่อกับระบบเครือข่ายภายนอกเท่านั้น แม้แต่ระบบภายในทั้งหมดเองก็ด้วยเช่นกัน และมีการวางมาตรการควบคุมโดยรอบข้อมูลหรือทรัพย์สินสารสนเทศเหล่านั้น เพื่อให้สามารถกำหนดและบังคับใช้นโยบายด้านความมั่นคงปลอดภัยในการเข้าถึงข้อมูลได้ทั้งหมด
13.00-16.00	เทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์	<ul style="list-style-type: none">▪ การตระหนักรูรูปแบบภัยคุกคามไซเบอร์(Cyber Security Awareness)▪ รูปแบบการโจมตีทางไซเบอร์และการป้องกัน▪ การรักษาความปลอดภัยไซเบอร์กับระบบเครือข่ายไร้สาย (Wireless LAN Security)
วันที่ 2		

เวลา	หัวข้อ	เนื้อหา
09.00 -12.00	การปรับแต่งคอมพิวเตอร์และโทรศัพท์มือถือด้านการรักษาความปลอดภัยทางไซเบอร์พื้นฐาน	<ul style="list-style-type: none"> ▪ การรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล ▪ การรักษาความปลอดภัยของเว็บเบราว์เซอร์ ▪ การรักษาความปลอดภัยการใช้สื่อสังคมออนไลน์
13.00-16.00	การประเมินความเสี่ยงมีแนวทางการดำเนินงานที่ถูกต้องเหมาะสมเมื่อเกิดภัยคุกคามไซเบอร์ขึ้น	<ul style="list-style-type: none"> ▪ ความรู้เบื้องต้นเกี่ยวกับการบริหารความเสี่ยง (Introduction to Risk Management) ▪ การประเมินความเสี่ยง (Risk Assessment) ระบบสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ ▪ ตัวอย่างการประเมิน- การประเมินตนเองตามมาตรฐานสากล ISO/IEC 27001:2013 ▪ กิจกรรมปฏิบัติ การประเมินตนเองตามมาตรฐานสากล ISO/IEC 27001:2013

หมายเหตุ :

1. พักรับประทานอาหารว่าง ช่วงเช้า เวลา 10.30 – 10.45 น. ช่วงบ่าย เวลา 14.30 – 14.45 น.
2. พักรับประทานอาหารกลางวัน เวลา 12.00 – 13.00 น.
3. กำหนดการอาจมีการเปลี่ยนแปลงตามความเหมาะสม

ค่าธรรมเนียมการฝึกอบรมของหลักสูตร

ค่าลงทะเบียนฝึกอบรมท่านละ **6,500** บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

หมายเหตุ:

ค่าลงทะเบียนข้างต้น **รวม** ค่าอาหารกลางวัน และอาหารว่าง

เงื่อนไขการผ่านการอบรมและได้รับประกาศนียบัตร

1. ทดสอบประเมินความรู้ภาคทฤษฎีด้วยแบบประเมินผลก่อนการฝึกอบรม (Pre-Test)
2. ทดสอบประเมินความรู้ภาคทฤษฎีด้วยแบบประเมินผลหลังการฝึกอบรม (Post-Test) เกณฑ์การผ่าน ไม่น้อยกว่าร้อยละ 70
3. ผู้เข้ารับการฝึกอบรมเข้ารับการฝึกอบรมไม่น้อยกว่าร้อยละ 80 ของระยะเวลาฝึกอบรมตลอดหลักสูตร

สถานที่ฝึกอบรม

คณะ ICT มหาวิทยาลัยมหิดล

999 ถนนพุทธมณฑลสาย 4 ตำบลศาลายา

อำเภอพุทธมณฑล จังหวัดนครปฐม 73170

TEL: (02) 441-0909 FAX: (02) 441-0808

ดำเนินการฝึกอบรมโดย

คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล

ที่อยู่ : 999 ถนนพุทธมณฑลสาย 4 ตำบลศาลายา อำเภอพุทธมณฑล, จังหวัดนครปฐม 73170

โทรศัพท์: (02) 441-0909

โทรสาร: (02) 441-0808

ไปรษณีย์อิเล็กทรอนิกส์: ict@mahidol.ac.th

เว็บไซต์: <https://www.ict.mahidol.ac.th>

หมายเหตุ: มหาวิทยาลัยขอสงวนสิทธิ์ในการคืนค่าลงทะเบียนการฝึกอบรมไม่ว่ากรณีใดๆ ยกเว้นกรณีมีเหตุสุดวิสัยไม่สามารถจัดฝึกอบรมได้