



ข้อเสนอโครงการฝึกอบรม
หลักสูตรความมั่นคงปลอดภัยไซเบอร์พื้นฐาน
(Cybersecurity Fundamentals)

จัดโดย มหาวิทยาลัยสวนดุสิต

สารบัญ

	หน้าที่
<input checked="" type="checkbox"/> หลักการและเหตุผล	2
<input checked="" type="checkbox"/> วัตถุประสงค์	3
<input checked="" type="checkbox"/> รูปแบบการฝึกอบรม	3
<input checked="" type="checkbox"/> ระยะเวลาการฝึกอบรม	3
<input checked="" type="checkbox"/> ตารางการฝึกอบรม	4
<input checked="" type="checkbox"/> ค่าธรรมเนียมการฝึกอบรมของหลักสูตร	5
<input checked="" type="checkbox"/> เงื่อนไขการผ่านการฝึกอบรม	5
<input checked="" type="checkbox"/> สถานที่ฝึกอบรม	6
<input checked="" type="checkbox"/> สอบถามรายละเอียด	6
<input checked="" type="checkbox"/> ดำเนินการฝึกอบรมโดย	6

โครงการฝึกอบรม หลักสูตรความมั่นคงปลอดภัยไซเบอร์พื้นฐาน
(Cybersecurity Fundamentals)
จัดโดย มหาวิทยาลัยสวนดุสิต

หลักการและเหตุผล

ด้วยความก้าวหน้าทางเทคโนโลยีสารสนเทศที่เติบโตอย่างรวดเร็ว และสามารถเข้าถึงได้ง่าย สะดวก รวดเร็ว และครอบคลุมทุกอุปกรณ์สื่อสาร ซึ่งปัจจุบันเรามักจะพบข่าวเกี่ยวกับการหลอกลวง การล้วงข้อมูล การโจมตีระบบต่าง ๆ การขโมยข้อมูลทางอิเล็กทรอนิกส์มากขึ้นทุกวัน ซึ่งสิ่งเหล่านี้ล้วนเป็นภัยคุกคามทางไซเบอร์ทั้งสิ้น และเป็นสิ่งที่หลีกเลี่ยงได้ยากและปัจจุบันทวีความรุนแรงมากขึ้นเรื่อย ๆ ซึ่งอาจส่งผลกระทบต่อความเสียหายต่อทั้งระดับบุคคล ระดับองค์กร และระดับประเทศ ภัยคุกคามทางด้านไซเบอร์ในปัจจุบันมีเทคนิคการโจมตีที่หลากหลายและมีเพิ่มขึ้นอย่างรวดเร็ว ซึ่งส่งผลกระทบต่อความปลอดภัยในชีวิตประจำวันของทุกท่าน อย่างแน่นอน ซึ่งควรที่จะต้องมีการเรียนรู้ เพิ่มความรู้ทางด้านความปลอดภัยทางด้านไซเบอร์ตลอดเวลา จึงจำเป็นต้องมีกลไกสำหรับการบริหารจัดการความมั่นคงปลอดภัยสำหรับภัยคุกคามด้านไซเบอร์อย่างเป็นรูปธรรม โดยจำเป็นที่จะต้องมีการบริหารจัดการภัยคุกคามทางไซเบอร์ที่มีโอกาสเกิดขึ้นอย่างมีอาชีพ หลักสูตรนี้ จึงมีความต้องการให้ผู้เข้าร่วมฝึกอบรมมีความรู้ ความเข้าใจ ตลอดจนทักษะที่จำเป็นในประเด็นต่าง ๆ เกี่ยวกับ 1) สาระสำคัญของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (พรบ. ไซเบอร์) 2) สิ่งที่ต้องคำนึงต่อการดำเนินการให้สอดคล้องกับ พรบ. ไซเบอร์ 3) มาตรการที่จำเป็นต้องนำมาปฏิบัติเพื่อให้สอดคล้องกับความต้องการของ พรบ. ไซเบอร์ 4) มาตรฐาน ISO ที่เกี่ยวข้อง ตลอดจนการฝึกปฏิบัติเพื่อให้ผู้เข้าร่วมฝึกอบรมได้พัฒนาทักษะที่จำเป็นสำหรับการรับมือและบริหารจัดการภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เพื่อให้ผู้เข้าร่วมอบรมทุกท่านสามารถรับมือกับภัยไซเบอร์ต่าง ๆ ซึ่งเป็นภัยต่อทั้งตนเอง องค์กร และสังคม และเพื่อให้สามารถแก้ไขปัญหาต่าง ๆ ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์

1. เพื่อให้ผู้เข้าร่วมฝึกอบรมมีความรู้และความเข้าใจในสาระสำคัญของ พรบ. ไซเบอร์ และปฏิบัติตามความต้องการของ พรบ. ไซเบอร์ ได้อย่างสอดคล้อง
2. เพื่อให้ผู้เข้าร่วมฝึกอบรมมีความรู้และความเข้าใจในมาตรการที่จำเป็น สามารถจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย และจัดเตรียมทรัพยากรที่จำเป็นสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ได้
3. เพื่อให้ผู้เข้ารับการฝึกอบรมฝึกวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ได้

รูปแบบการฝึกอบรม

การอบรมในรูปแบบการบรรยาย และกรณีศึกษา

ระยะเวลาการฝึกอบรม

การจัดอบรม รุ่นละไม่เกิน 30 คน จำนวน 2 วัน (วันละ 6 ชั่วโมง รวม 12 ชั่วโมง)
ระยะเวลาการอบรม ระหว่างวันที่ 23 – 24 เมษายน พ.ศ. 2565

หมายเหตุ กำหนดการอาจมีการเปลี่ยนแปลงตามความเหมาะสม

ตารางการฝึกอบรม

วิทยากร

1. ผู้ช่วยศาสตราจารย์ ดร.สุระสิทธิ์ ทรงม้า
2. ผู้ช่วยศาสตราจารย์วัชรภรณ์ เนตรหาญ
3. อาจารย์ณรงค์ฤทธิ์ ภิรมย์นง

เวลา	หัวข้อ	เนื้อหา
วันที่ 1		
09.00-12.00	<ul style="list-style-type: none">● แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์● ภัยคุกคามและแนวโน้มภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	<ul style="list-style-type: none">- แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์- วิวัฒนาการของการรักษาความปลอดภัยระบบสารสนเทศ- ความหมายของการรักษาความปลอดภัยสารสนเทศ- องค์ประกอบการรักษาความปลอดภัยระบบสารสนเทศ- ภัยคุกคามความมั่นคงของสารสนเทศในชีวิตประจำวัน- ระดมสมองและแลกเปลี่ยนเรียนรู้ กรณีศึกษา ภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
13.00-16.00	<ul style="list-style-type: none">● รูปแบบและเทคนิคการบุกรุกการรักษาความมั่นคงปลอดภัยไซเบอร์● การวิเคราะห์กระบวนการทำงานขององค์กรเพื่อปรับปรุงและแก้ไขปัญห ความมั่นคงปลอดภัย	<ul style="list-style-type: none">- รูปแบบและเทคนิคในการบุกรุกระบบสารสนเทศในชีวิตประจำวัน- การวิเคราะห์จุดอ่อนและความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์- การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ- การกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์

เวลา	หัวข้อ	เนื้อหา
	ไซเบอร์	
วันที่ 2		
9.00 -12.00	<ul style="list-style-type: none"> ● เครื่องมือในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ● การกู้คืนสารสนเทศ 	<ul style="list-style-type: none"> - เครื่องมือสำหรับความมั่นคงปลอดภัยไซเบอร์ - เครื่องมือป้องกันไวรัส - การใช้งานไฟล်วอลล์ - ระบบป้องกันและตรวจจับการบุกรุก - การเข้ารหัส - ฝึกปฏิบัติการการตั้งค่าการรักษาความมั่นคงปลอดภัยไซเบอร์
13.00-16.00	<ul style="list-style-type: none"> ● กฎหมายด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับหน่วยงานรัฐ 	<ul style="list-style-type: none"> - กฎหมายที่เกี่ยวข้องกับหน่วยงานภาครัฐ - พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ - พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล - ระดมสมองและแลกเปลี่ยนเรียนรู้

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 **5,900 บาท** (รวมภาษีมูลค่าเพิ่มแล้ว) สำหรับ Onsite (ค่าลงทะเบียนข้างต้น รวม ค่าอาหารกลางวัน และอาหารว่าง)

ค่าลงทะเบียนฝึกอบรมท่านละ **4,900 บาท** (รวมภาษีมูลค่าเพิ่มแล้ว) สำหรับ Online

หมายเหตุ: ขอสงวนสิทธิ์กรณีที่จำนวนผู้เข้าอบรมไม่ถึงตามเกณฑ์ขั้นต่ำที่กำหนด
จำนวนผู้เข้าอบรมขั้นต่ำ 15 คน

