เอกสารหมายเลข 2

ข้อเสนอโครงการ

หลักสูตรความมั่นคงปลอดภัยทางดิจิทัลสำหรับผู้บริหารภาครัฐ

(Digital Security for Government Executives)

จัดโดย สำนักบริการคอมพิวเตอร์

มหาวิทยาลัยเกษตรศาสตร์

สารบัญ

		หน้าที่
☑	หลักการและเหตุผล	1
☑	วัตถุประสงค์	1
☑	รูปแบบการฝึกอบรม	1
☑	ระยะเวลาการฝึกอบรม	1
☑	ตารางการฝึกอบรม	2
☑	ค่าธรรมเนียมการฝึกอบรมของหลักสูตร	4
☑	เงื่อนไขการผ่านการฝึกอบรม	4
☑	สถานที่ฝึกอบรม	5
☑	สอบถามรายละเอียด	5
☑	ดำเนินการฝึกอบรมโดย	5

โครงการฝึกอบรมหลักสูตรความมั่นคงปลอดภัยทางดิจิทัลสำหรับผู้บริหารภาครัฐ

จัดโดยสำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์

หลักการและเหตุผล

ปัจจุบันการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) สำคัญอย่างยิ่ง เนื่องจากองค์กร ไม่ว่าจะเป็ภาครัฐหรือเอกชนต่างรวบรวม ประมวลผลและจัดเก็บข้อมูลจำนวนมากบนคอมพิวเตอร์และอุปกรณ์อื่น ๆ ซึ่งข้อมูลเหล่านั้นอาจเป็นข้อมูลที่ค่อนข้างละเอียดอ่อนไม่ว่าจะเป็นทรัพย์สินทางปัญญา ข้อมูลทางการเงิน ข้อมูลส่วนบุคคล หรือข้อมูลประเทศอื่น ๆ ที่บุคคลอื่นสามารถเข้าถึงหรือเปิดเผยได้โดยไม่ได้รับอนุญาตอาจส่งผลกระทบด้านลบกับองค์กรได้ เพราะองค์กรมักส่งข้อมูลที่มีความสำคัญข้ามเครือข่ายและอุปกรณ์ ซึ่งข้อมูลเหล่านั้นควรได้รับการปกป้องจากการโจมตีทางไซเบอร์

ผู้บริหารองค์กรจำเป็นต้องพัฒนาความปลอดภัยทางไซเบอร์ให้ดีขึ้น โดยเริ่มจากการใช้กลยุทธ์ประเมินและวางโครงสร้าง IT เพื่อความปลอดภัยทางไซเบอร์ในระยะยาวขององค์กร สร้างความตระหนักรู้ถึงความสำคัญของความปลอดภัยทางไซเบอร์ให้กับบุคลากรภายในองค์กรอย่างทั่วถึง เพื่อให้ทุกคนในองค์กรเล็งเห็นถึงข้อสำคัญนี้และมีส่วนร่วมในการสร้างความปลอดภัยทางดิจิทัลให้กับองค์กร ต่อไป

วัตถุประสงค์

1. เพื่อให้มีความรู้และความเข้าใจพื้นฐานในหลักการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์
2. เพื่อให้สามารถออกแบบและจัดทำนโยบายหรือยุทธศาสตร์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
3. เพื่อให้มีความรู้เกี่ยวกับกฎหมายและมาตรฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

รูปแบบการฝึกอบรม

การฝึกอบรมในหลักสูตร ประกอบไปด้วย การบรรยาย (Lecture) การอภิปราย (Discussion) และกรณีศึกษา (Case Study)

ระยะเวลาการฝึกอบรม

การจัดอบรมจำนวน 1 รุ่น รุ่นละ 30 คน อบรมระหว่างวันที่ 10-11 พฤษภาคม 2565
จำนวน 2 วัน (วันละ 6 ชั่วโมง รวม 12 ชั่วโมง) เวลา 9:00 – 16:00 น.

ตารางการฝึกอบรม

รายชื่อวิทยากรในการอบรม

- ผู้ช่วยศาสตราจารย์ ดร.เขมะฑัต วิภาตะวนิช
- ผู้ช่วยศาสตราจารย์ ดร.พีรวัฒน์ วัฒนพงศ์

เวลา	หัวข้อ	เนื้อหา
วันที่ 10 พฤษภาคม 2565		
9:00 – 12:00	**วัดฐานความรู้ก่อนการอบรม (Pre-Test)**	
	พื้นฐานด้านความมั่นคงปลอดภัยทางดิจิทัล (Fundamentals of Digital Security)	● นิยามของ “ความมั่นคงปลอดภัย (Security)” ● C-I-A Model: o การควบคุมความลับ (Confidentiality) o ความครบถ้วนสมบูรณ์ (Integrity) o ความสม่ำเสมอของบริการ (Availability) ● ความสัมพันธ์ ระหว่างความมั่นคงปลอดภัย กับ “การเปลี่ยนโฉมองค์กรด้วยดิจิทัล (Digital Transformation)”
	แนวโน้มภัยคุกคามและความเสี่ยง (Threat Landscape and Risk)	● นิยามของ “ภัยคุกคาม (Threat)” ● นิยามของ “ความเสี่ยง (Risk)” ● ประเภท คำนิยาม และแนวโน้มของภัยคุกคามต่าง ๆ ● “ผลกระทบ (Impact)” ต่อองค์กร
	Hands-on: มองหาความเสี่ยงด้านความมั่นคงปลอดภัย	● ผู้เข้าอบรม ทดลองเสนอแง่มุมความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจเกิดกับองค์กร
13:00 – 16:00	กฎหมายที่เกี่ยวข้องกับโลกดิจิทัล (Digital Laws)	● พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ● พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ● พรบ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล ● พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ● พรบ. คุ้มครองข้อมูลส่วนบุคคล

เวลา	หัวข้อ	เนื้อหา
	Case Study: ความสุ่มเสี่ยงด้านกฎหมายที่เกิดขึ้นกับองค์กรและเจ้าหน้าที่ปฏิบัติงาน	● ผู้เข้าอบรมทดลองวิเคราะห์กรณีสมมุติในองค์กร
วันที่ 11 พฤษภาคม 2565		
9:00 – 12:00	มาตรฐานความมั่นคงปลอดภัยทางดิจิทัล (Digital Security Standards) และกรอบนโยบายความมั่นคงปลอดภัยทางดิจิทัล (Digital Security Frameworks)	● ชุดมาตรฐาน ISO 27000 (ISO/IEC 27000 Series) ● กรอบนโยบายของสำนักงานมาตรฐานสหรัฐอเมริกา (NIST Cyber Security Framework)
	นโยบายด้านความมั่นคงปลอดภัย (Digital Security Policy) และ แนวปฏิบัติด้านความมั่นคงปลอดภัย (Digital Security Standard Practice)	● ลักษณะบ่งชี้ของนโยบายด้านความมั่นคงปลอดภัย ● ตัวอย่างนโยบายด้านความมั่นคงปลอดภัย ● ลักษณะบ่งชี้ของแนวปฏิบัติด้านความมั่นคงปลอดภัย ● ตัวอย่างแนวปฏิบัติด้านความมั่นคงปลอดภัย
	อภิปราย หัวข้อทำอย่างไรให้นโยบายและแนวปฏิบัติเกิดประสิทธิผล	● ผู้เข้าอบรมอภิปรายหรือเสนอวิธีการที่ที่ทำให้แนวปฏิบัติเกิดประสิทธิผล
13:00 -16:00	วัฒนธรรมองค์กรด้านความมั่นคงปลอดภัย (Digital Security Culture)	● นิยามของ “วัฒนธรรมองค์กรด้านความมั่นคงปลอดภัย (Digital Security Culture)” ● ความสำคัญของการมีวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยต่อเนื่อง ● การมีส่วนร่วมของบุคลากร

เวลา	หัวข้อ	เนื้อหา
		● เทคโนโลยีและกลไกที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางดิจิทัล (Digital Security Technologies and Mechanisms)
	อภิปราย การประสาน culture และ เทคโนโลยีเข้าด้วยกัน	● ผู้เข้าอบรมเสนอมุมมองหรือแนวทางในการประสาน culture และ เทคโนโลยีเข้าด้วยกัน
	วัดฐานความรู้หลังการอบรม (Post-Test)	

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

ค่าลงทะเบียนฝึกอบรมแบบ Onsite ท่านละ 7,000 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

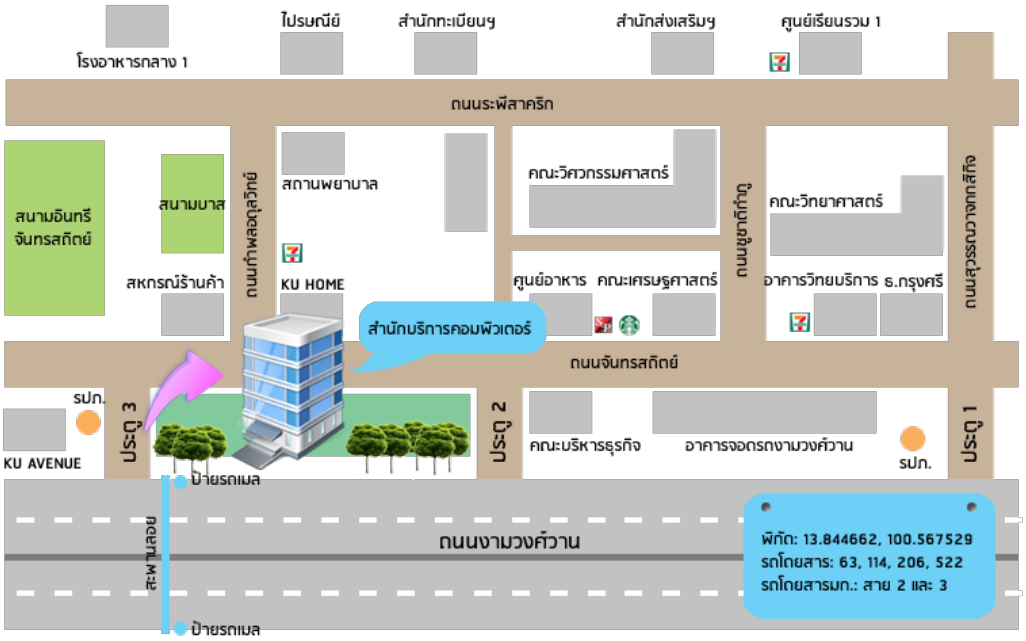
ทั้งนี้ค่าลงทะเบียนข้างต้น **รวม** ค่าอาหารกลางวัน และอาหารว่าง

หมายเหตุ กรณีผู้เข้าอบรมมีจำนวนไม่ถึงตามที่กำหนดผู้จัดอบรมจะแจ้งให้ผู้สมัครเข้าร่วมอบรมทราบล่วงหน้า

เงื่อนไขการผ่านการอบรมและได้รับประกาศนียบัตร

1. ทดสอบประเมินความรู้ภาคทฤษฎีด้วยแบบประเมินผลก่อนการฝึกอบรม (Pre-Test)
2. ทดสอบประเมินความรู้ภาคทฤษฎีด้วยแบบประเมินผลหลังการฝึกอบรม (Post-Test)
   เกณฑ์การผ่านไม่น้อยกว่าร้อยละ 70
3. ผู้เข้ารับการฝึกอบรมเข้ารับการฝึกอบรมไม่น้อยกว่า 80 ของระยะเวลาการฝึกอบรมตลอดหลักสูตร

สถานที่ฝึกอบรม



https://goo.gl/maps/KbxNferGk4a2k9i46

สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์

50 ถนนงามวงศ์วาน แขวงลาดยาว เขต จตุจักร กรุงเทพมหานคร 10900

สอบถามรายละเอียด

หากท่านมีข้อสงสัย และ/หรือ ต้องการทราบรายละเอียดเพิ่มเติม สามารถติดต่อสอบถามได้ที่

คุณสุนิสา สิงห์แก้ว หมายเลขโทรศัพท์ 02 562 0951-6 ต่อ 622594 อีเมล sunisa.si@ku.th

ดำเนินการฝึกอบรมโดย

สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์

ที่อยู่ 50 ถนนงามวงศ์วาน แขวงลาดยาว เขต จตุจักร กรุงเทพมหานคร 10900

โทร: 02 562 0951-6 | โทรสาร: 02 562 0950 | Email: tam@ku.ac.th

เว็บไซต์ https://ocs.ku.ac.th และ http://training.ku.ac.th