ITM103: IT Security and Cybersecurity Management
(การบริหารจัดการความมั่งคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร)

หลักการและเหตุผล:

ปัจจุบันโลกเข้าสู่ยุคระบบเศรษฐกิจและสังคมดิจิทัล ที่เทคโนโลยีดิจิทัลสามารถเปลี่ยนโครงสร้างรูปแบบกิจกรรมทางเศรษฐกิจ กระบวนการผลิต การค้า การบริการ และกระบวนการทางสังคม รวมถึงการมีปฏิสัมพันธ์ระหว่างบุคคล ไปอย่างสิ้นเชิง การเปลี่ยนแปลงดังกล่าวได้ส่งผลกระทบต่อประเทศไทยเป็นอันมาก ทำให้ต้องเร่งปรับตัวและเปลี่ยนแปลงเพื่อให้ประเทศมีความพร้อมและพัฒนาให้ทันกับการเปลี่ยนแปลง

ประเทศไทยกำลังอยู่ในวาระของการปฏิรูปโครงสร้างเศรษฐกิจของประเทศครั้งใหญ่ในทุกมิติของการพัฒนาเพื่อขับเคลื่อนเศรษฐกิจของประเทศไทยไปสู่ระบบเศรษฐกิจดิจิทัล โดยได้ตระหนักถึงความจำเป็นเร่งด่วนในการใช้เทคโนโลยีดิจิทัลมาเป็นเครื่องมือสำคัญในการกระตุ้นเศรษฐกิจของประเทศโดยผลักดันให้ ภาคธุรกิจไทยสามารถใช้เทคโนโลยีดิจิทัลในการลดต้นทุนการผลิตสินค้าและบริการ เพิ่มประสิทธิภาพในการดำเนินธุรกิจ ตลอดจนพัฒนาไปสู่การแข่งขันเชิงธุรกิจรูปแบบใหม่ในระยะยาวเพื่อขับเคลื่อนการปฏิรูปประเทศไทยไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน

ด้วยความเจริญก้าวหน้าของเทคโนโลยีดิจิทัลสมัยใหม่ การเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบัน ได้ทวีความสลับซับซ้อนมากขึ้นกว่าเดิม ส่งผลให้ผู้นำเทคโนโลยีมาใช้งานส่วนใหญ่ขาดความเข้าใจและตระหนักถึงความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินที่มีความสำคัญต่อการดำเนินภารกิจขององค์กร ทำให้องค์กรต้องเผชิญกับสถานการณ์ความเสี่ยงต่อความไม่มั่นคงปลอดภัยที่ไม่คาดคิดอยู่เสมอ เช่น การถูกบุกรุก คุกคาม การโจรกรรมข้อมูล การทำลายข้อมูล หรือทำลายระบบเทคโนโลยีสารสนเทศขององค์กรให้เกิดความเสียหาย จนทำให้การให้ภารกิจที่สำคัญขององค์กรต้องหยุดชะงัก โดยอาศัยช่องโหว่หรือจุดอ่อนในรูปแบบต่างๆ ดังนั้นจึงเป็นสิ่งจำเป็นที่ท้าทายองค์กรว่าจะสามารถรับมือกับเหตุการณ์ที่ไม่พึงประสงค์เพื่อปกป้องรักษาสารสนเทศขององค์กรซึ่งจัดเป็นสินทรัพย์ที่มีมูลค่าและมีความสำคัญต่อการดำเนินภารกิจขององค์กร เช่นเดียวกับทรัพย์สินอื่นๆ เพื่อทำให้ภารกิจขององค์กรประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้ได้อย่างไร

อย่างไรก็ตามเพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้ องค์กรควรตระหนักถึงการนำมาตรการการบริหารจัดการเชิงรุกด้วยการนำกระบวนการป้องกันและควบคุมความมั่งคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์มาใช้ในองค์กร ทั้งบุคลากรต้นทาง กลางทาง และปลายทาง เพื่อยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร และเพื่อเป็นหลักประกันว่าการดำเนินภารกิจต่าง ๆ ขององค์กรจะสำเร็จลุล่วงไปได้ด้วยดี จากการวางแผนการรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพเพื่อรองรับเหตุการณ์ในอนาคตอย่างมีเหตุมีผลมีหลักการ และมีวิธีควบคุมเพื่อป้องกันหรือลดโอกาสเกิดความเสียหายเอาไว้ล่วงหน้า หรือในกรณีที่ประสบกับเหตุการณ์ที่ไม่คาดคิด ความเสียหายที่เกิดขึ้นก็จะมีปริมาณน้อยกว่าการไม่ได้นำเอามาตรการรักษาความมั่นคงปลอดภัยมาใช้ จึงสามารถช่วยให้องค์กรมั่นใจได้ว่าภารกิจสำคัญที่ดำเนินอยู่จะประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

หลักสูตรอบรมนี้จะสร้างความรู้ความเข้าใจต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์และระบบสารสนเทศขององค์กรในบริบทที่เปลี่ยนแปลงไปเพื่อเตรียมความพร้อมรับต่อกระบวนการปรับเปลี่ยนสู่องค์กรดิจิทัลให้กับบุคลากรต้นทาง กลางทาง และปลายทาง ขององค์กร ให้เกิดความรู้ความเข้าใจยิ่งขึ้นและสามารถนำไปปฏิบัติได้จริง

วัตถุประสงค์:

- เพื่อให้มีความรู้ ความเข้าใจและตระหนักถึงความไม่มั่นคงปลอดภัยที่มีต่อเทคโนโลยีสารสนเทศขององค์กรในยุคระบบเศรษฐกิจและสังคมดิจิทัล
- เพื่อให้มีความรู้ ความเข้าใจแนวทางการวิเคราะห์และประเมินความเสี่ยงที่เกี่ยวข้องกับความไม่มั่นคงปลอดภัยต่อเทคโนโลยีสารสนเทศขององค์กรในยุคระบบเศรษฐกิจและสังคมดิจิทัล
- เพื่อให้มีความรู้ ความเข้าใจมาตรการป้องกัน และรับมือจากการถูกคุกคามทางไซเบอร์ ให้มีประสิทธิภาพยิ่งขึ้น
- เพื่อให้มีความรู้ ความเข้าใจกระบวนการรักษาความมั่นคงปลอดภัยทางไซเบอร์และและระบบเทคโนโลยีสารสนเทศขององค์กร ด้วยหลักการจัดการในเชิงรุก เพื่อประเมินระบบการป้องกันในปัจจุบันขององค์กร และแนวทางการออกแบบวิธีการควบคุมด้วยการบริหารจัดการตามมาตรฐานสากล

หลักสูตรนี้เหมาะสำหรับ:

- ผู้บริหารองค์กร
- ผู้บริหารฝ่ายงานเทคโนโลยีสารสนเทศ
- ผู้บริหารด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
- ผู้ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

- บุคลากรฝ่ายงานเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบภายใน
- ผู้สนใจทั่วไป

เนื้อหาหลักสูตร:

- Digital Transformation
- ความท้าทายขององค์กรต่อการทำ Digital Transformation
- หลักการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (IT Security)
- ความเสี่ยงของระบบเทคโนโลยีสารสนเทศ
- ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)
- อาชญากรรมทางไซเบอร์ที่ส่งผลกระทบต่อองค์กร
- แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศเพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัย การวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์
- การวิเคราะห์หาสาเหตุที่มาของอาชญากรรมทางไซเบอร์ และความไม่มั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศขององค์กร
- บทบาทภาวะผู้นำองค์กรต่อการบริหารความมั่นคงปลอดภัยทางไซเบอร์และระบบเทคโนโลยีสารสนเทศในยุคดิจิทัล
- การกำหนดโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์และระบบเทคโนโลยีสารสนเทศในองค์กร
- องค์กรจะประสบความสำเร็จในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และระบบเทคโนโลยีสารสนเทศอย่างยั่งยืน ได้อย่างไร
- มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO 27001:2013
- การกำหนดแนวนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์และระบบเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์และระบบเทคโนโลยีสารสนเทศ
- แนวทางการทดสอบด้านความมั่นคงปลอดภัย การค้นหาช่องโหว่ และทดสอบเจาะระบบ
- การเตรียมความพร้อมด้านบุคลากร ทั้งบุคลากรต้นทาง กลางทาง และปลายทาง เพื่อให้เกิดความตระหนักต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์และระบบเทคโนโลยีสารสนเทศในยุคดิจิทัล
- แนวทางการพัฒนาทักษะความเข้าใจและการใช้เทคโนโลยีดิจิทัล (Digital Literacy) เพื่อให้ระบบเทคโนโลยีสารสนเทศและดิจิทัลขององค์กรเกิดความมั่นคงปลอดภัยอย่างแท้จริง
- ภัยคุกคามต่อระบบ Artificial Intelligence (AI) และ Machine Learning (ML)
- แนวทางการป้องกันรักษาความมั่นคงปลอดภัยกับระบบ AI และ ML อย่างมีประสิทธิภาพ
- แนวปฏิบัติในการประยุกต์ใช้ปัญญาประดิษฐ์แบบมีจริยธรรม ตามกรอบจริยธรรมปัญญาประดิษฐ์ (AI Ethics Guideline)
- ภัยคุกคามต่อระบบวิเคราะห์ข้อมูล (Data Analytics)
- แนวทางการป้องกันรักษาความมั่นคงปลอดภัยกับระบบวิเคราะห์ข้อมูล (Data Analytics) อย่างมีประสิทธิภาพ
- การเฝ้าระวัง ติดตาม และตรวจสอบการป้องกันรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในองค์กร
- แนวทางการปรับปรุงมาตรการป้องกันรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในองค์กร
- แนวทางการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) เพื่อรองรับสภาวะวิกฤติในสถานการณ์ฉุกเฉิน ภัยพิบัติหรือเหตุการณ์ที่ส่งผลกระทบต่อภาระกิจหลักขององค์กร
- มาตรการป้องกันผลกระทบต่อองค์กรจากการละเมิด พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- มาตรการป้องกันผลกระทบต่อองค์กรจากการละเมิด พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์
- มาตรการป้องกันผลกระทบต่อองค์กรจากการละเมิด พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

Career for the Future Academy: CFA

วิทยากร:

อาจารย์ภิธันปดิ์ ถิรสัตยาพิทักษ์
- วิทยากรรับเชิญประจำสถาบันพัฒนาบุคลากรแห่งอนาคต

จำนวนชั่วโมงในการฝึกอบรม: 2 วัน (12 ชั่วโมง)

กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

ค่าลงทะเบียนอบรม:

ราคาปกติ	ราคาออนไลน์
6,500 บาท	6,000 บาท

** ราคารวมภาษีมูลค่าเพิ่มแล้ว
** สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

สถานที่ฝึกอบรม:

สถาบันพัฒนาบุคลากรแห่งอนาคต
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (NSTDA) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

หมายเหตุ: ในช่วงสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัส COVID 19 เพื่อลดการทำกิจกรรมที่มีการรวมตัวกันที่อาจจะเกิดความเสี่ยงต่อการติดเชื้อได้ สถาบันฯ จะมีการปรับรูปแบบการอบรมเป็น "อบรมออนไลน์"

<u>รูปแบบการเรียนออนไลน์</u>

1. โดยใช้วิธีการสอนแบบฟังบรรยาย และ ดู Presentation ผ่านโปรแกรม Zoom (https://zoom.us/join) เพื่อประสิทธิภาพในการเรียน ควรใช้ Internet ที่มีความเสถียร (ไม่แนะนำให้ใช้ Internet ผ่านมือถือ)
2. ลงโปรแกรม Anydesk หรือ Teamviewer ที่เครื่องคอมพิวเตอร์ของท่าน (<u>สำหรับหลักสูตรฝึกปฏิบัติ</u>ที่ผู้เข้าอบรมจะต้องใช้วิธีการ Remote เพื่อมาใช้เครื่องคอมพิวเตอร์ของสถาบันฯ หรือ กรณีที่วิทยากรต้อง Remote ไปที่เครื่องผู้อบรม และ Share File ที่ใช้ในการอบรม)
3. <u>สำหรับหลักสูตรฝึกปฏิบัติ</u> ขอแนะนำผู้เข้าอบรมเตรียมหน้าจอ 2 หน้าจอ เพื่อแยกการใช้งาน คือ หน้าจอสำหรับ Zoom พร้อมหน้าจอสำหรับปฏิบัติหรือ remote ซึ่งอาจจะเป็นหน้าจอคอมพิวเตอร์ทั้ง 2 เครื่อง หรือ หน้าจอเครื่องคอมฯ เพื่อใช้ในการ remote และ หน้าจอโทรศัพท์มือถือ/แทปเล็ท เพื่อใช้กับ zoom
4. จัดตั้งไลน์กลุ่มเพื่อใช้ในการสื่อสารร่วมกันระหว่างวิทยากร ผู้เข้าอบรม และเจ้าหน้าที่ของสถาบันฯ
5. ส่งไฟล์เอกสารให้ก่อนการอบรม
6. จัดส่งวุฒิบัตรภายหลังจบการอบรม

วิธีการการสำรองที่นั่ง:

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887
โทรสาร: 0 2644 8110
Website: www.career4future.com
E-mail: training@nstda.or.th