ITM114 : Cybersecurity Control for AI and Machine Learning:
การควบคุมรักษาความปลอดภัยทางไซเบอร์กับระบบ AI และ Machine Learning

หลักการและเหตุผล :

เทคโนโลยีปัญญาประดิษฐ์ Artificial Intelligence (AI) และ Machine Learning (ML) เป็นเทคโนโลยีที่กำลังได้รับความนิยมและสนใจมากในขณะนี้ จะเห็นได้จากภาคอุตสาหกรรมทุกแขนง เช่น ภาคธุรกิจการเงิน ด้านประกันภัย ด้านการแพทย์ ด้านการศึกษา ธุรกิจการบิน และรวมถึงระบบงานต่างๆ ของภาครัฐ ต่างมีความตื่นตัวที่จะศึกษาพัฒนาระบบ AI และ ML เพื่อผลักดันให้เกิดนวัตกรรมทางเทคโนโลยี เพื่อสร้างโอกาสทางธุรกิจให้กับองค์กร และเป็นที่ทราบกันดีว่า AI และ ML สามารถนำมาพัฒนาให้มีความชาญฉลาด มีความสามารถที่จะคิด วิเคราะห์ วางแผน และช่วยตัดสินใจ จากการประมวลผลของฐานข้อมูลขนาดใหญ่ (Big data) ได้อย่างแม่นยำทำให้มนุษย์ได้รับประโยชน์จาก AI และ ML อย่างมากมาย ทุกวันนี้ AI และ ML ได้ทวีบทบาทเข้ามาช่วยจัดการชีวิตประจำวันของมนุษย์มากยิ่งขึ้น มนุษย์ได้ใช้ AI และ ML เข้ามาช่วยในการตัดสินใจ และช่วยคิดแทนมนุษย์ในหลายๆเรื่อง โดยมนุษย์ส่วนใหญ่ไม่รู้ตัวด้วยซ้ำไปว่านั่นคือผลลัพธ์ที่ได้จากการประมวลผลด้วยระบบ AI และ ML

ระบบ AI และ ML เป็นระบบที่มีความแตกต่างจากระบบคอมพิวเตอร์โดยทั่วไป เนื่องจากมีลักษณะการทำงานที่มีความสลับซับซ้อนต้องอาศัยการประมวลผลด้วยการวิเคราะห์เชิงลึกด้วยเงื่อนไขและข้อมูลจำนวนมาก และที่สำคัญระบบ AI และ ML ต้องสามารถวิเคราะห์ประมวลผลได้อย่างถูกต้องครบถ้วนสมบูรณ์ตามเงื่อนไข ตามขั้นตอนวิธีคิด (Algorithm) ที่ถูกกำหนดขึ้นตามกระบวนการทางธุรกิจ และผลลัพธ์ที่ได้ต้องถูกต้องแม่นยำตรงตามความต้องการที่แท้จริงของธุรกิจหรือภารกิจนั้นๆ ซึ่งถือว่าเป็นหัวใจสำคัญของระบบ AI และ ML และเป็นสิ่งที่ท้าทายนักพัฒนาระบบเป็นอย่างยิ่ง จะเห็นได้ว่าองค์กรส่วนใหญ่นำเอาระบบ AI และ ML มาเลือกใช้เฉพาะกับระบบงานที่มีความสำคัญต่อธุรกิจขององค์กรแทบทั้งสิ้น ซึ่งนั่นย่อมหมายถึงการนำข้อมูลที่มีความสำคัญยิ่งต่อธุรกิจเข้าสู่ระบบเพื่อประมวลผล และผลลัพธ์ที่ได้ก็เปรียบได้กับทรัพย์สินอันมีค่าขององค์กร และทรัพย์สินที่มีค่านี่มักจะตกเป็นเป้าถูกคุกคามและโจรกรรมทางไซเบอร์อยู่เสมอ หากองค์กรใดขาดความตระหนักถึงมาตรการควบคุมรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบ AI และ ML องค์กรเหล่านั้นกำลังเผชิญกับความเสี่ยงที่อาจจะถูกคุกคามเข้าสู่ระบบ AI และ ML เพื่อกระทำการแก้ไขเปลี่ยนแปลงรูปแบบวิธีการคิด หรือข้อมูลสำหรับให้ระบบได้เรียนรู้ ให้ผิดไปจากวัตถุประสงค์เดิมที่ถูกกำหนดไว้ โดยผู้ไม่ประสงค์ดีจะนำข้อมูลที่ไม่ถูกต้องป้อนเข้าสู่กระบวนการประมวลผลของระบบ เพื่อฝึกให้ระบบ AI และ ML เรียนรู้ข้อมูลที่ผิดๆ ไม่ถูกต้อง หรือทำการแก้ไขเปลี่ยนแปลงวิธีคิด วิธีประมวลผล (Algorithm) ของระบบ เพื่อสอนให้ระบบเรียนรู้การประมวลผลเสียใหม่ ทำให้ผลลัพธ์ที่ได้จากการวิเคราะห์ การประมวลผลเกิดผิดพลาดคลาดเคลื่อน สร้างความเสียหายให้กับธุรกิจอย่างมากมาย หรืออาจจะถูกคุกคามเข้ามาในระบบเพื่อโจรกรรมล่วงรู้ข้อมูลสำคัญที่เป็นความลับแล้วนำไปแสวงหาประโยชน์ หรือคุกคามเข้ามาในระบบเพื่อทำลายข้อมูลเพื่อให้องค์กรได้รับความเสียหาย เสื่อมเสียชื่อเสียง และอาจถูกเจ้าของข้อมูลฟ้องร้องเรียกค่าเสียหายได้ ความเสี่ยงต่างๆ ดังที่กล่าวมาแล้วล้วนมาจากสาเหตุหลายประการด้วยกัน ส่วนใหญ่มักเกิดจากขั้นตอนการพัฒนาระบบที่เร่งรีบให้แล้วเสร็จในระยะเวลาที่จำกัด มีการเปลี่ยนแปลงวัตถุประสงค์และความต้องการของระบบบ่อยเกินไป การทดสอบระบบไม่เพียงพอ ขาดการให้ความร่วมมือ ขาดการสนับสนุนและการมีส่วนร่วมจากผู้ที่เกี่ยวข้องกับการพัฒนาระบบ บุคลากรขาดความรู้ความเข้าใจและทักษะต่อเทคโนโลยี AI และ ML ที่นำมาใช้งาน เป็นต้น สาเหตุเหล่านี้ล้วนทำให้เกิดช่องโหว่ เกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัยขึ้นกับระบบ AI และ ML ในภายหลังแทบทั้งสิ้น

อย่างไรก็ตาม หากองค์กรมีกระบวนการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีมาตรการควบคุมและติดตามตรวจสอบการปฏิบัติงานกับระบบ AI และ ML ที่มีประสิทธิภาพประสิทธิผลเพียงพอตั้งแต่เริ่มต้นการพัฒนาระบบฯ จนกระทั่งนำระบบฯ มาติดตั้งใช้งาน องค์กรก็พอที่จะมั่นใจได้ว่าจะสามารถป้องกันและลดโอกาสการถูกคุกคามหรือถูกโจมตีให้เกิดความเสียหายจนกลายเป็นปัญหาและอุปสรรคต่อการดำเนินภารกิจขององค์กรได้ ดังนั้นผู้ที่เกี่ยวข้องกับการพัฒนาระบบฯ ผู้ดูแลระบบฯ ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในและผู้ที่มีส่วนใช้งานระบบฯ ถือได้ว่าเป็นกลไกควบคุมด้านบุคลากรที่มีความสำคัญมากต่อการรักษาความมั่นคงปลอดภัยให้กับระบบ AI และ ML ขององค์กร ซึ่งจะต้องเป็นผู้มีหน้าที่คอยให้คำแนะนำและประเมิน แสดงความคิดเห็นว่ามาตรการควบคุมรักษาความมั่นคงปลอดภัยที่ถูกนำมาใช้นั้น มีประสิทธิภาพประสิทธิผลเพียงพอ สามารถปฏิบัติตาม และได้ผลตามวัตถุประสงค์ของการควบคุมรักษาความปลอดภัยตามที่กำหนดไว้หรือไม่ เพื่อสร้างความมั่นใจและเชื่อมั่นในความถูกต้องเชื่อถือได้ของผลลัพธ์ที่ได้จากการประมวลผลของระบบ AI และ ML ทั้งนี้ผู้ที่เกี่ยวข้องกับระบบฯ ดังที่กล่าวมาแล้วจะต้องมีความรู้ความเข้าใจเกี่ยวกับกระบวนการรักษาความมั่นคงปลอดภัย เข้าใจถึงมาตรการการติดตาม ตรวจสอบและควบคุมความเสี่ยงจากการปฏิบัติงานกับระบบ AI และ ML ให้มีความปลอดภัยเป็นอย่างดี

หลักสูตรนี้เป็นการอบรมที่ผู้เข้ารับการอบรมจะได้รับความรู้ ความเข้าใจในแต่ละกระบวนการรักษาความมั่นคงปลอดภัย มาตรการการติดตาม ตรวจสอบและควบคุมความเสี่ยงจากการปฏิบัติงานกับระบบ AI และ ML จากกรณีศึกษาเพื่อให้เกิดความรู้ความเข้าใจมากยิ่งขึ้นและสามารถนำไปปฏิบัติได้จริง

วัตถุประสงค์ :

- เพื่อให้มีความรู้ ความเข้าใจและตระหนักถึงภัยคุกคามต่อระบบ AI และ ML ขององค์กร
- เพื่อให้มีความรู้ ความเข้าใจมาตรการควบคุมรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับระบบ AI และ ML ขององค์กร
- เพื่อให้มีความรู้ ความเข้าใจสามารถวิเคราะห์และระบุความเสี่ยงที่เกิดจากการใช้งานระบบ AI และ ML
- เพื่อให้มีความรู้ ความเข้าใจในกระบวนการป้องกันและความคุมความเสียงที่เกี่ยวข้องกับความไม่มั่นคงปลอดภัยที่มีต่อระบบ AI และ ML
- เพื่อให้มีความรู้ ความเข้าใจถึงหลักการจัดการในเชิงรุก ด้วยวิธีการประเมินระบบการป้องกันในปัจจุบันขององค์กร และการออกแบบวิธีการควบคุมด้วยหลักการบริหารจัดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามมาตรฐานสากล

หลักสูตรนี้เหมาะสำหรับ :

- ผู้บริหารหรือผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
- ผู้บริหารโครงการด้านเทคโนโลยีสารสนเทศ
- ผู้ที่ทำหน้าที่พัฒนาระบบงานด้านเทคโนโลยีสารสนเทศ
- ผู้ที่ทำหน้าที่รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ผู้ที่ทำหน้าที่บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้ที่ทำหน้าที่บริหารจัดการระบบเครือข่ายเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบภายใน

เนื้อหาการอบรม :

- ความรู้เกี่ยวกับระบบ Artificial Intelligence (AI) และ Machine Learning (ML)
- รูปแบบภัยคุกคามต่อระบบ AI และ ML
- แนวทางการรับมือกับภัยคุกคามต่อระบบ AI และ ML
- การวิเคราะห์และประเมินความเสี่ยงต่อความไม่มั่นคงปลอดภัยของระบบ AI และ ML
- แนวทางการป้องกันรักษาระบบ AI และ ML ให้เกิดความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ
- การกำหนดแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยให้กับระบบ AI และ ML
- การติดตามและตรวจสอบการควบคุมความเสี่ยงจากการใช้งานระบบ AI และ ML
- การประเมินตรวจสอบความมั่นคงปลอดภัยของสภาพแวดล้อมสำหรับใช้ติดตั้งและปฏิบัติงานกับระบบ AI และ ML
- การกำหนดโครงสร้างและบทบาทหน้าที่ความรับผิดชอบให้กับบุคลากรที่เกี่ยวข้องกับระบบ AI และ ML
- การติดตามและตรวจสอบการปฏิบัติตามบทหน้าที่ความรับผิดชอบในการปฏิบัติงานกับระบบ AI และ ML
- มาตรการการกำหนดสิทธิ์ในการเข้าถึงระบบ AI และ ML
- การตรวจสอบการควบคุมสิทธิ์และหน้าที่ในการเข้าถึงระบบ AI และ ML
- มาตรการการเข้ารหัสข้อมูล (Encryption Data)
- การควบคุมการจัดการการเปลี่ยนแปลง (Change Management Control) กับระบบ AI และ ML
- มาตรการควบคุมการ Re-train หรือ ปรับปรุง Algorithm
- การทดสอบและตรวจสอบ Algorithm
- กระบวนการตรวจสอบพฤติกรรมของผู้ใช้งานในระบบ AI และ ML เพื่อคัดกรองผู้ที่มีพฤติกรรมไม่น่าไว้วางใจ
- กระบวนการวิเคราะห์ตรวจจับจำแนกพฤติกรรมที่ผิดปกติภายในระบบเครือข่ายของระบบ AI และ ML
- การจัดทำแผนฉุกเฉินเพื่อรองรับเหตุการณ์ผิดปกติและสุดวิสัยจากการใช้ระบบ AI และ ML
- การติดตามและตรวจสอบการการจัดทำแผนฉุกเฉิน
- การวิเคราะห์และประเมินความเพียงพอของการควบคุมความมั่นคงปลอดภัยกับการใช้ระบบ AI และ ML
- การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy and Protection)

วิทยากร :

อาจารย์ภิธันปดิ์ ถิรสัตยาพิทักษ์
- วิทยากรรับเชิญประจำสถาบันพัฒนาบุคลากรแห่งอนาคต

จำนวนชั่วโมงในการฝึกอบรม: 2 วัน (12 ชั่วโมง)

กำหนดการอบรม : ตามตารางปฏิทินอบรมประจำปี http://www.nstdaacademy.com/trainingprogram

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

ค่าลงทะเบียนอบรม : ท่านละ 8,000 บาท (ราคารวมภาษีมูลค่าเพิ่มแล้ว)
** สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

สถานที่ฝึกอบรม :
สถาบันพัฒนาบุคลากรแห่งอนาคต
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

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