

ที่ อว 6001/ว 6808

22 กรกฎาคม 2569

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมการฝึกอบรม

เรียน อธิบดีกรมพัฒนาสังคมและสวัสดิการ

สิ่งที่ส่งมาด้วย แผ่นพับแนะนำหลักสูตร

กรมพัฒนาสังคมและสวัสดิการ
เลขรับ: 12163
วันที่รับ: 7/8/2569
เวลารับ: 15:31

กลุ่มบริหารทรัพยากรบุคคล
เลขรับ: 3782
วันที่รับ: 10/8/2569
เวลารับ: 11:05

ด้วยสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) โดยสถาบันพัฒนาบุคลากรแห่งอนาคต มีกำหนดจัดฝึกอบรม ชุดหลักสูตรฝึกอบรมด้านเทคโนโลยีสารสนเทศและการจัดการขั้นสูง (Information Technology and Advanced Management Series) ดังนี้

1. หลักสูตรฝึกอบรมเชิงปฏิบัติการ มาตรฐาน ISO/IEC 27001:2022 การรักษาความมั่นคงปลอดภัยสารสนเทศ ขององค์กร (ISO/IEC 27001:2022 Standard for Organization) อบรมระหว่างวันที่ 19 - 21 สิงหาคม 2569 เวลา 09.00 - 16.00 น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพฯ มุ่งเน้นให้ผู้เรียนสามารถเชื่อมโยงเรื่องของการประเมิน ความเสี่ยงเข้ากับนโยบาย/ขั้นตอนปฏิบัติ ตลอดจนงานทางเทคนิคที่ตนต้องปฏิบัติ สามารถดำเนินงานทางเทคนิค เพื่อลดความเสี่ยงตามที่ประเมินและเพื่อให้มีความสอดคล้องกับข้อกำหนดของมาตรฐาน ISO/IEC 27001 ได้ ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/iso27001>

2. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ รุ่นที่ 3 (Vulnerability Assessment and Penetration Testing) อบรมระหว่างวันที่ 19 - 21 สิงหาคม 2569 เวลา 09.00 - 16.00 น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพฯ มุ่งเน้นการสร้างความเข้าใจและความเชี่ยวชาญ ในการตรวจสอบความมั่นคง ปลอดภัยของระบบสารสนเทศและเครือข่ายขององค์กร โดยการตรวจสอบช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing) โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับที่แฮกเกอร์ (Hacker) ใช้ แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย เพื่อช่วยค้นหาและเตรียมป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/vapt>

3. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน (Web Application Hacking and Security) อบรมระหว่างวันที่ 1 - 3 กันยายน 2569 เวลา 09.00 - 16.00 น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพฯ มุ่งเน้นให้ผู้เรียนสามารถ ตรวจสอบความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน ซึ่งเป็นช่องทางสำคัญในการเข้าถึงข้อมูลขององค์กร เป้าหมายของแฮกเกอร์อาจเป็นการขโมยข้อมูลสำคัญ ทำลาย ชื่อเสียงขององค์กร หรือเรียกร้องผลประโยชน์ในรูปแบบต่าง ๆ ส่งผลให้หน่วยงานได้รับความเสียหาย ผู้เข้าอบรม จะได้พัฒนาทักษะในการป้องกันภัยทางไซเบอร์และช่วยให้องค์กรสามารถรับมือกับการโจมตีได้อย่างมีประสิทธิภาพ ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/wahs>

4. หลักสูตร...

4. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การกำกับดูแล AI อย่างมีธรรมาภิบาลและความรับผิดชอบ (AI Governance Workshop) อบรมระหว่างวันที่ 3 - 4 กันยายน 2569 เวลา 09.00 - 16.00 น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพฯ เพื่อเสริมสร้างความรู้ ความเข้าใจ และฝึกปฏิบัติ การกำหนดมาตรการต่าง ๆ ที่จำเป็นที่เกี่ยวข้องกับการพัฒนาระบบ AI ขององค์กร เพื่อลดความเสี่ยงต่าง ๆ ของระบบให้อยู่ในระดับที่องค์กรยอมรับได้ และเป็นระบบที่มีความน่าเชื่อถือ รวมทั้งสอดคล้องกับมาตรฐานสากลที่มีการอ้างอิงและใช้งานในปัจจุบัน ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/aig>

5. หลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ รุ่นที่ 4 (Cyber Security Incident Management) อบรมระหว่างวันที่ 8 - 11 กันยายน 2569 เวลา 09.00 - 16.00 น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพฯ มุ่งเน้นให้ผู้เรียน เข้าใจสาระสำคัญของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ตลอดจนเตรียมความพร้อมในการจัดตั้งทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ฝึกวิเคราะห์มาตรการที่จำเป็นต้องนำมาปฏิบัติเพื่อให้สอดคล้องกับความต้องการของ พรบ. ไซเบอร์ (อ้างอิงจาก มาตรฐาน Framework for Improving Critical Infrastructure Cybersecurity) เพื่อรับมือจากภัยคุกคามทางไซเบอร์จนถึงการกู้คืนระบบกลับคืน ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/csm>

ในการนี้ สวทช. จึงขอเชิญท่านหรือผู้แทนเข้าร่วมการฝึกอบรมในหลักสูตรดังกล่าว ตามวัน เวลา และ สถานที่ข้างต้น โดยท่านสามารถติดต่อสอบถามรายละเอียดเพิ่มเติมได้ที่ นายนิพนธ์ เอี่ยมสมบุรณ์ หมายเลข โทรศัพท์ 0 2644 8150 ต่อ 81891 หรือ 08 9777 7492 ทั้งนี้ผู้เข้าร่วมอบรมจากหน่วยงานราชการสามารถเบิก ค่าลงทะเบียนจากต้นสังกัดได้ตามระเบียบกระทรวงการคลัง และไม่ถือเป็นวันลา เมื่อได้รับการอนุมัติจากผู้บังคับบัญชา และค่าใช้จ่ายในการส่งบุคลากรเข้าร่วมอบรมของบริษัทหรือห้างหุ้นส่วนนิติบุคคลสามารถนำไป ลดหย่อนภาษีได้ 200%

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ



(นางจุฬารัตน์ ตันประเสริฐ)

รองผู้อำนวยการ

ปฏิบัติการแทนผู้อำนวยการ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

สำนักงานกลาง

สถาบันพัฒนาบุคลากรแห่งอนาคต

โทรศัพท์ 0 2644 8150 ต่อ 81891 (นิพนธ์)

ไปรษณีย์อิเล็กทรอนิกส์ npd@nstda.or.th

สง บพ.



(นางธรรมลักษณ์ ต่อโพธิ์วง)
หัวหน้าศูนย์อำนวยความสะดวก

๗ ส.ค. ๒๕๖๙



สวทช.
NSTDA

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

ISO27001

ISO/IEC 27001:2022 Standard for Organization

หลักสูตรฝึกอบรมเชิงปฏิบัติการ

มาตรฐาน ISO/IEC 27001:2022 กับการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร



มุ่งเน้นการฝึกปฏิบัติการจัดตั้งระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และการจัดทำระบบสารสนเทศให้สอดคล้องตามมาตรการใหม่ในมาตรฐาน ISO/IEC 27001:2022

Key Highlights

- ♥ เรียนรู้และเข้าใจสาระสำคัญของมาตรฐาน ISO/IEC 27001:2022
- ♥ เข้าใจมาตรการควบคุมความเสี่ยงและการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- ♥ สามารถประยุกต์ใช้มาตรการควบคุมความเสี่ยง จากมาตรฐาน ISO/IEC 27002:2022
- ♥ ฝึกปฏิบัติเข้มข้น 8 Workshop และแนะนำเครื่องมือพร้อมการติดตั้งเพื่อการใช้งาน



หลักสูตรฝึกอบรมเชิงปฏิบัติการ มาตรฐาน ISO/IEC 27001:2022 กับการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร (ISO/IEC 27001:2022 Standard for Organization)

ปัจจุบันประเด็นด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นที่หลายองค์กรให้ความสำคัญ เนื่องจากเทคโนโลยีและรูปแบบภัยคุกคามที่มีการพัฒนาอย่างต่อเนื่อง ประกอบกับการบังคับใช้กฎหมายต่าง ๆ ที่เกี่ยวข้อง เช่น พ.ร.บ. ว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์, พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ซึ่งหลาย ๆ องค์กรจำเป็นต้องมีเนื้อหาอ้างอิงมาจากมาตรฐาน ISO/IEC 27001 ซึ่งมาตรฐานนี้มุ่งให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยต่อสารสนเทศขององค์กร ที่หน่วยงานหรือองค์กรต่าง ๆ ทั้งภายในประเทศและในระดับนานาชาติล้วนให้การยอมรับอย่างแพร่หลาย

และมีการนำมาประยุกต์ใช้งานเพิ่มมากขึ้นเรื่อย ๆ จนถึงขั้นนำไปสู่การขอการรับรองตามมาตรฐานดังกล่าว โดยหน่วยงานผู้ตรวจรับรอง (Certification Body) ผู้ที่เกี่ยวข้องภายในทางเทคนิค ได้แก่ ผู้บริหารด้านเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้พัฒนาระบบ Helpdesk ผู้ตรวจสอบภายใน และอื่น ๆ ควรที่จะได้ทำการศึกษา เรียนรู้ และทำความเข้าใจในมาตรฐานดังกล่าว จนกระทั่งสามารถนำมาปรับใช้กับงานบริหารจัดการระบบเทคโนโลยีสารสนเทศของตนได้เป็นอย่างดี ปัจจุบันมาตรฐาน ISO/IEC 27001 ได้มีการปรับปรุงเป็นเวอร์ชัน 2022 มีการปรับปรุงมาตรการควบคุมความเสี่ยงให้ครอบคลุมด้านความมั่นคงปลอดภัยทางไซเบอร์มากขึ้น และสอดคล้องกับ NIST Cybersecurity Framework

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่สร้างความรู้ความเข้าใจ เกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 ตลอดจนฝึกปฏิบัติการวิเคราะห์และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และการจัดทำมาตรการลดความเสี่ยงทางเทคนิค โดยมุ่งเน้นมาตรการใหม่จากมาตรฐาน ISO/IEC 27001:2022 รวมจำนวน 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	6	1
ฝึกปฏิบัติการ (Workshop)	12	2
รวม	18	3

เนื้อหาหลักสูตร ประกอบด้วย

- ภาพรวมมาตรฐาน ISO/IEC 27001:2022
- รายละเอียดการเปลี่ยนแปลงมาตรฐาน ISO/IEC 27001:2013 ไปยัง ISO/IEC 27001:2022
- ข้อกำหนดการดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022
- มาตรการควบคุมความเสี่ยงตามมาตรฐาน ISO/IEC 27002:2022
- การกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนการบรรลุวัตถุประสงค์
- การวิเคราะห์ภัยคุกคามเชิงลึก (Threat intelligence) ตามมาตรฐาน ISO/IEC 27002:2022
- การเขียน Code อย่างปลอดภัย (Secure coding) ตามมาตรฐาน ISO/IEC 27002:2022
- การบริหารจัดการช่องโหว่ทางเทคนิคของระบบสารสนเทศ (Management of technical vulnerabilities)
- การจัดเก็บข้อมูล การวิเคราะห์ข้อมูล log และเฝ้าระวังเหตุการณ์ผิดปกติ ตามมาตรฐาน ISO/IEC 27002:2022
- การจำกัดการเข้าถึงเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม (Web filtering) ตามมาตรฐาน ISO/IEC 27002:2022

หลักสูตรนี้เหมาะสำหรับ

- ผู้บริหารด้านเทคโนโลยีสารสนเทศ ผู้จัดการไอซีที
- เจ้าหน้าที่เทคนิค ได้แก่ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้พัฒนาระบบ Helpdesk
- เจ้าหน้าที่ด้านความมั่นคงปลอดภัยระบบสารสนเทศ (IT Security) หรือความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)
- ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ
- ผู้สนใจงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security) หรือความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

ค่าลงทะเบียน

ท่านละ 24,500 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่รัฐวิสาหกิจและไม่ใช่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไปรับส่วนลดทันที 10%

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการ และ
ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ที-เน็ต จำกัด



คุณพงษ์กร ไสยนนท์
Senior Cybersecurity & Privacy Manager
บริษัท T-NET จำกัด

ระยะเวลาหลักสูตร

ระหว่างวันที่ 19 - 21 สิงหาคม 2569
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องใช้เวลาเรียนไม่น้อยกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/iso27001>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th



สวทช.
NSTDA

Career for the Future Academy
สถาบันพัฒนบุคลากรแห่งอนาคต

VAPT

Vulnerability Assessment and Penetration Testing

หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ

รุ่นที่ 3

มุ่งเน้นการตรวจสอบช่องโหว่ (Vulnerability Assessment)
การทดสอบเจาะระบบ (Penetration Testing)
เพื่อช่วยค้นหาและเตรียมป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ

- เรียนรู้สาระสำคัญด้านความปลอดภัยจากการโจมตีเว็บแอปพลิเคชัน
- เข้าใจการทดสอบเจาะระบบในรูปแบบต่าง ๆ พร้อมการทำรายงานที่ถูกต้อง
- ทดลองใช้เครื่องมือตรวจสอบช่องโหว่ (Vulnerability Assessment)
- ฝึกปฏิบัติเข้มข้นในการทดสอบเจาะระบบ (Penetration Testing)



หลักสูตรฝึกอบรมเชิงปฏิบัติการ การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) รุ่นที่ 3

ในปัจจุบันภัยคุกคามที่เกิดขึ้นจากผู้ไม่ประสงค์ดี/แฮกเกอร์ (Hacker) ได้ทวีความรุนแรงขึ้นทุกวัน โดยมุ่งเน้นการโจมตีหน่วยงานภาครัฐ เอกชน และมหาวิทยาลัย จากทั้งภายในและภายนอกประเทศ เพื่อขโมยข้อมูลหรือทำลายชื่อเสียงและเรียกร้องสิทธิต่าง ๆ ตามที่ต้องการ ซึ่งสาเหตุหลักที่โดนบุกรุกเนื่องจากผู้ไม่ประสงค์ดีสามารถเข้าถึงภายในระบบจากที่ใดก็ได้บนโลกผ่านระบบเครือข่ายอินเทอร์เน็ต ทำให้ง่ายต่อการบุกรุก หลักสูตรนี้เป็นหลักสูตรที่สร้างความเข้าใจและความเชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบ รวมถึงสร้างความรู้ความสามารถในการตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายขององค์กร โดยมุ่งเน้นการตรวจสอบและทดสอบเจาะระบบเพื่อหาช่องโหว่โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับที่แฮกเกอร์ (Hacker) ใช้ แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย

โครงสร้างหลักสูตร

เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับการตรวจสอบช่องโหว่และการทดสอบเจาะระบบ และฝึกปฏิบัติเข้มข้นทักษะพื้นฐานที่จำเป็นสำหรับการปฏิบัติงานเพื่อพัฒนากิจกรรมที่จำเป็นอย่างเข้มข้น รวมจำนวน 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	9	1.5
ฝึกปฏิบัติการ (Workshop)	9	1.5
รวม	18	3

เนื้อหาหลักสูตร ประกอบด้วย

- ความรู้เบื้องต้นเกี่ยวกับการตรวจสอบช่องโหว่ (Introduction to Vulnerability Assessment)
- ความรู้เบื้องต้นเกี่ยวกับการทดสอบการเจาะระบบ (Introduction to Penetration Testing)
- การรวบรวมข้อมูล (Information Gathering)
- การสแกนเครือข่าย (Scanning Networks)
- การค้นหาช่องโหว่ (Vulnerability Assessment)
- การทดสอบเจาะระบบ (Penetration Testing)
- การแฮ็กเว็บ (Hacking Web)
- การแฮ็กระบบ (System Hacking)
- การใช้งานระบบปฏิบัติการ Kali Linux
- การใช้งานเครื่องมือ Metasploit

หลักสูตรนี้เหมาะสำหรับ

- นักพัฒนาโปรแกรมด้านเว็บแอปพลิเคชัน
- ผู้ดูแลระบบ (System Administrator)
- นักทดสอบเจาะระบบ (Penetration Tester)
- ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Consultant)



ค่าลงทะเบียน

ท่านละ 26,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป รับส่วนลดทันที 10%

ระยะเวลาหลักสูตร

ระหว่างวันที่ 19 - 21 สิงหาคม 2569
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

วิทยากรประจำหลักสูตร



อาจารย์ เจษฎา ทองกันเหลือง

กรรมการผู้จัดการ

บริษัท ที-เน็ต ไอที โซลูชัน จำกัด

- Certified Ethical Hacker (CEH)
- Certified Hacking Forensic Investigator (CHFI)
- Certified Security Analyst (E|CSA)
- IT Specialist Certification (ITS): Cyber Security

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องใช้เวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/vapt>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th



สวทช.
NSTDA

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

WAHS

Web Application Hacking and Security

หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน

มุ่งเน้นการตรวจสอบและทดสอบเจาะระบบ
เพื่อหาช่องโหว่เว็บแอปพลิเคชัน

โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับแฮกเกอร์ (Hacker)
แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย

Key Highlights

- ♥ เรียนรู้และเข้าใจสาระสำคัญด้านความปลอดภัยจากการโจมตีเว็บแอปพลิเคชัน
- ♥ เรียนรู้มาตรการความมั่นคงปลอดภัยบน HTTP Security Header
- ♥ เรียนรู้แนวทางและวิธีการทดสอบเจาะระบบ Penetration Testing Methodologies
- ♥ เรียนรู้การทดสอบเจาะระบบ และแนวทางป้องกันรูปแบบการโจมตี บน 10 อันดับความเสี่ยงจาก OWASP
- ♥ เข้าใจการทดสอบเจาะระบบในรูปแบบต่าง ๆ พร้อมการทำรายงานที่ถูกต้อง
- ♥ ฝึกปฏิบัติเข้มข้นในการทดสอบเจาะระบบในรูปแบบที่หลากหลาย



หลักสูตรฝึกอบรมเชิงปฏิบัติการ การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน Web Application Hacking and Security

ในปัจจุบันภัยคุกคามทางไซเบอร์จากแฮกเกอร์ (Hacker) หรือผู้ไม่ประสงค์ดียังทวีความรุนแรงมากขึ้นเรื่อย ๆ โดยเฉพาะการโจมตีเว็บแอปพลิเคชัน ซึ่งเป็นช่องทางสำคัญในการเข้าถึงข้อมูลขององค์กร เป้าหมายของแฮกเกอร์อาจเป็นการขโมยข้อมูลสำคัญ ทำลายชื่อเสียงขององค์กร หรือเรียกค่าไถ่ในรูปแบบต่าง ๆ ส่งผลให้หน่วยงานภาครัฐและเอกชนได้รับความเสียหายอย่างมาก หลักสูตรนี้ถูกออกแบบมาเพื่อสร้างความเข้าใจและความเชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบ รวมถึงสร้างความรู้ความสามารถในการตรวจสอบความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน โดยมุ่งเน้นการตรวจสอบและทดสอบเจาะระบบเพื่อหาช่องโหว่โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับที่แฮกเกอร์ (Hacker) ใช้ แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย ผู้เข้าอบรมจะได้พัฒนากทักษะในการป้องกันภัยทางไซเบอร์และช่วยให้องค์กรสามารถรับมือกับการโจมตีได้อย่างมีประสิทธิภาพ

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่สร้างความรู้ความเข้าใจเกี่ยวกับการทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน ตลอดจนฝึกปฏิบัติเพื่อพัฒนากทักษะที่จำเป็นอย่างเข้มข้น รวมจำนวน 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	9	1.5
ฝึกปฏิบัติการ (Workshop)	9	1.5
รวม	18	3

เนื้อหาหลักสูตร ประกอบด้วย

- Introduction to Web Application
- HTTP Security Headers
- Introduction to Web Application Security
- Penetration Testing Methodology
- Penetration Testing Framework
- Types of Web Penetration Testing
- Web Application Penetration Testing Tools
- Web Application Penetration Testing Checklist
- Web Application Penetration Testing Certifications
- The Penetration Testing Process
- Web Application Proxies
- Using Hacking Tools
- Open Web Application Security Project (OWASP)
 - OWASP TOP 10 2013: SQL Injection
 - OWASP TOP 10 2013: Broken Authentication and Session Management
 - OWASP TOP 10 2013: Cross-site Scripting
 - OWASP TOP 10 2013: Security Misconfiguration
 - OWASP TOP 10 2017: XML External Entities (XXE)
 - OWASP TOP 10 2017: Insecure Deserialization
 - OWASP TOP 10 2021: Insecure Design
 - OWASP TOP 10 2021: Software and Data Integrity Failures
 - OWASP TOP 10 2021: Server-Side Request Forgery

ระยะเวลาหลักสูตร

อบรมระหว่างวันที่ 1 – 3 กันยายน 2569
เวลา 9.00 - 16.00 น. (รวมระยะเวลา 3 วัน)

หลักสูตรนี้เหมาะสำหรับ

- นักพัฒนาโปรแกรมด้านเว็บแอปพลิเคชัน
- ผู้ดูแลระบบ (System Administrator)
- นักทดสอบเจาะระบบ (Penetration Tester)
- ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Consultant)

วิทยากรประจำหลักสูตร



อาจารย์ เจษฎา ทองกันเหลือ
กรรมการผู้จัดการ
บริษัท ที-เน็ต ไอที โซลูชัน จำกัด

- Certified Ethical Hacker (CEH)
- Certified Hacking Forensic Investigator (CHFI)
- Certified Security Analyst (EJCSA)
- IT Specialist Certification (ITS): Cyber Security

ค่าลงทะเบียน

ท่านละ 24,500 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชันพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไปรับส่วนลดทันที 10%

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียน กรุณาแจ้งยืนยันการยกเลิกเป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องใช้เวลาเรียนไม่น้อยกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/wahs>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th



สวทช.
NSTDA

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

AIG

AI Governance Workshop



หลักสูตรฝึกอบรมเชิงปฏิบัติการ

การกำกับดูแล AI อย่างมีธรรมาภิบาลและความรับผิดชอบ **รุ่นที่ 3**

มุ่งเน้นการฝึกปฏิบัติเข้มข้นถึง 9 Workshops

เพื่อกำหนดมาตรการต่าง ๆ ที่จำเป็นที่เกี่ยวข้องกับการพัฒนาระบบ AI ขององค์กร เพื่อลดความเสี่ยงต่าง ๆ ของระบบให้อยู่ในระดับที่องค์กรยอมรับได้ และเป็นระบบที่มีความน่าเชื่อถือ รวมถึงสอดคล้องกับมาตรฐานสากลที่มีการอ้างอิงและใช้งานในปัจจุบัน



Key Highlights

- เรียนรู้มาตรฐาน AI ที่เกี่ยวข้อง สอดคล้องกับมาตรฐานสากลที่มีการอ้างอิงและใช้งานในปัจจุบัน
- เรียนรู้วิธีการและมาตรการที่ช่วยป้องกันปัญหาความเสี่ยงในระบบ AI ซึ่งสามารถนำไปใช้ได้จริงในการพัฒนาระบบ
- ฝึกการประเมินและจัดการความเสี่ยงในโครงการ AI เพื่อให้สามารถควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- สามารถนำมาตรการ และวิธีปฏิบัติ ไปปรับใช้กับระบบงานขององค์กร เพื่อให้ได้ระบบ AI ที่มีความน่าเชื่อถือและพร้อมใช้งานได้จริงในธุรกิจ



หลักสูตรฝึกอบรมเชิงปฏิบัติการ การกำกับดูแล AI อย่างมีธรรมาภิบาลและความรับผิดชอบ (AI Governance Workshop)

ปัจจุบันมีการพัฒนาระบบงานเพื่อทำงานร่วมกับหรือทดแทนการทำงานของมนุษย์เป็นจำนวนมาก เช่น ระบบ ChatGPT ระบบงานที่พัฒนาขึ้นมาเหล่านี้ใช้เทคโนโลยีที่เรียกว่าปัญญาประดิษฐ์หรือ AI (Artificial Intelligence) ซึ่งทำให้เครื่องคอมพิวเตอร์สามารถคิดและดำเนินการในลักษณะเดียวกับหรือใกล้เคียงกับที่มนุษย์สามารถทำได้ ในบางกรณีการคิดและดำเนินการเหล่านี้จะเป็นส่วนหนึ่งของกลไกการตัดสินใจโดยมนุษย์ เช่น ระบบผู้ชำนาญการ ระบบช่วยในการตัดสินใจ เป็นต้น ในขณะที่ในบางกรณีระบบ AI บางระบบจะสามารถดำเนินการแทนมนุษย์ได้โดยอัตโนมัติได้ เช่น ระบบขับขี่ยานยนต์อัตโนมัติ เป็นต้น เนื่องจากระบบ AI ดังกล่าวไม่ใช่มนุษย์ ดังนั้นการคิดและดำเนินการต่างๆ จึงมีโอกาสผิดพลาดและมีความเสี่ยงในลักษณะต่างๆ ได้ จึงทำให้จำเป็นต้องมีวิธีการที่เป็นรูปธรรมเพื่อบริหารจัดการการนำระบบ AI มาใช้งานเพื่อก่อให้เกิดประโยชน์ต่อองค์กร ลดความเสี่ยงและผลกระทบต่างๆ ที่อาจจะเกิดขึ้นได้ให้อยู่ในระดับที่องค์กรยอมรับได้

มาตรฐาน AI จึงถือกำเนิดขึ้นมาขึ้นมาเพื่อบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการนำระบบ AI มาใช้งานให้อยู่ในระดับที่องค์กรทั่วไปยอมรับได้ มาตรฐาน AI หลักที่จะนำมาใช้ในหลักสูตรนี้ประกอบด้วยมาตรฐาน 3 รายการดังนี้

1. Artificial Intelligence Risk Management Framework (AI RMF 1.0)
2. AI RMF PLAYBOOK
3. ISO/IEC 42001:2023(E) Artificial Intelligence Management system

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่ให้ความรู้และความเข้าใจเกี่ยวกับมาตรฐานของ AI เพื่อนำไปใช้ในการบริหารและจัดการความเสี่ยงที่เกี่ยวข้องกับการนำระบบ AI มาใช้งานกับองค์กร ตลอดจนทั้งวงจรชีวิตของระบบ ตลอดจนนำความรู้ที่ได้รับมาฝึกทดลองปฏิบัติตามมาตรฐานดังกล่าว เพื่อให้ได้ทักษะอย่างแท้จริง และสามารถนำกลับไปปรับใช้งานกับองค์กรของผู้เรียนได้ รวมจำนวน 12 ชั่วโมง / 2 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	6	1
ฝึกปฏิบัติการ (Workshop)	6	1
รวม	12	2

เนื้อหาหลักสูตร ประกอบด้วย

- ความรู้พื้นฐานของ AI ที่ควรทราบ
- ประเภทของ AI ที่มีการใช้งานกันโดยทั่วไป
- วงจรการพัฒนาของระบบ AI
- มาตรฐาน AI ที่เกี่ยวข้อง
- การกำกับดูแล AI ที่ครอบคลุมถึง
 - นโยบาย กระบวนการ ขั้นตอนปฏิบัติ และวิธีปฏิบัติสำหรับการกำหนด วัด และบริหารความเสี่ยงของ AI ขององค์กร
 - โครงสร้างของการกำกับดูแล บทบาท และหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการบริหารความเสี่ยงของ AI ขององค์กร
- การกำหนดความเสี่ยงของ AI ที่ครอบคลุมถึง
 - การทำความเข้าใจและกำหนดบริบทขององค์กร
 - การกำหนดหมวดหมู่ของระบบ AI ที่องค์กรมีการใช้งาน
 - ความเสี่ยงและประโยชน์หรือคุณค่าที่คาดว่าจะได้รับ ซึ่งรวมถึงความเสี่ยงจากผู้ให้บริการภายนอกที่เกี่ยวข้องกับซอฟต์แวร์หรือข้อมูลที่เกี่ยวข้องกับการใช้งาน
 - ผลกระทบที่เกิดขึ้นต่อผู้มีส่วนได้ส่วนเสีย กลุ่ม สังคม และองค์กร
- การวัดความเสี่ยงของ AI ที่ครอบคลุมถึง
 - การกำหนดวิธีการและตัวชี้วัดที่เหมาะสมในการวัดความเสี่ยง
 - การประเมินคุณสมบัติความน่าเชื่อถือของระบบ AI
 - การกำหนดกลไกในการเฝ้าระวังและติดตามความเสี่ยงของระบบ AI
- การบริหารความเสี่ยงของ AI ที่ครอบคลุมถึง
 - การจัดลำดับความเสี่ยงที่ได้มีการประเมินไว้ เพื่อรับมือและบริหารจัดการ
 - การกำหนดกลยุทธ์ในการจัดการกับความเสี่ยง
 - การบริหารจัดการกับความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการภายนอก

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานที่เกี่ยวข้องกับมาตรฐานด้านไอที
- ผู้บริหารองค์กรที่จำเป็นต้องกำกับดูแลการนำ AI มาใช้ภายในองค์กร
- ผู้พัฒนาระบบ
- นักวิเคราะห์และออกแบบระบบ
- ผู้ปฏิบัติงานทั่วไปที่จำเป็นต้องพัฒนาระบบของตนเองที่มีการใช้งาน AI เป็นส่วนหนึ่งของระบบ

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการและที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ บริษัท ที-เน็ต จำกัด

ค่าลงทะเบียน

ท่านละ 12,840 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชันพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป ส่วนลดทันที 10%

ระยะเวลาหลักสูตร

ระหว่างวันที่ 3-4 กันยายน 2569
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 2 วัน)

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องใช้เวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/aig>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th



สถาบัน
NSTDA

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

CSM

Cyber Security Incident Management



หลักสูตร

การบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์

รุ่นที่ 4

"มุ่งเน้นการเตรียมความพร้อมในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อรับมือกับภัยคุกคามทางไซเบอร์จนถึงการกู้คืนระบบกลับคืน"



Key Highlights

- เรียนรู้และเข้าใจสาระสำคัญของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- เจาะลึกมาตรฐานและมาตรการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- เตรียมความพร้อมในการจัดตั้งทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- ฝึกวิเคราะห์อย่างเข้มข้น เพื่อรับมือจากภัยคุกคามทางไซเบอร์จนถึงการกู้คืนระบบกลับคืน มากกว่า 10 Workshop



หลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ รุ่นที่ 4 (Cyber Security Incident Management: CSM)

ด้วยความก้าวหน้าทางเทคโนโลยีสารสนเทศที่เติบโตอย่างรวดเร็ว สามารถเข้าถึงได้ง่าย สะดวก รวดเร็ว และครอบคลุมทุกอุปกรณ์สื่อสาร เราจึงจะพบข่าว การหลอกลวงลวงข้อมูล การโจมตีระบบ การขโมยข้อมูลทางอิเล็กทรอนิกส์ มากขึ้นทุกวัน ซึ่งเหล่านี้เป็นภัยคุกคามทางไซเบอร์ เป็นสิ่งที่หลีกเลี่ยงไม่ได้และปัจจุบันทวีความรุนแรงมากขึ้นเรื่อยๆ ซึ่งอาจส่งผลกระทบต่อระดับบุคคล ระดับองค์กร และระดับประเทศ หน่วยงานหรือองค์กรจึงจำเป็นต้องมีกลไกสำหรับการบริหารจัดการความมั่นคงปลอดภัยสำหรับภัยคุกคามด้านไซเบอร์อย่างเป็นรูปธรรม โดยจำเป็นต้องมีการบริหารจัดการภัยคุกคามทางไซเบอร์ที่มีโอกาสเกิดขึ้นอย่างมืออาชีพ หลักสูตรนี้จึงมีความประสงค์ต้องการให้ผู้เข้าร่วมฝึกอบรม มีความรู้ความเข้าใจ ตลอดจนทักษะที่จำเป็นในประเด็นต่างๆ ดังต่อไปนี้

- สำคัญของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (พสบ. ไซเบอร์)
- สิ่งที่ต้องคำนึงถึงในการให้สอดคล้องกับ พสบ. ไซเบอร์
- มาตรการที่จำเป็นต้องนำมาปฏิบัติเพื่อให้สอดคล้องกับความต้องการของ พสบ. ไซเบอร์ (อ้างอิงจากมาตรฐาน Framework for Improving Critical Infrastructure Cybersecurity)
- มาตรฐาน ISO ที่เกี่ยวข้อง ตลอดจนการฝึกปฏิบัติเพื่อให้ผู้เข้าร่วมฝึกอบรมได้พัฒนาทักษะที่จำเป็นสำหรับการรับมือ และบริหารจัดการภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่ให้ความรู้และความเข้าใจเกี่ยวกับ พสบ. ไซเบอร์ การปฏิบัติตามให้สอดคล้องกับความต้องการของ พสบ. ไซเบอร์ มาตรการที่จำเป็นสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ มาตรฐาน ISO ที่เกี่ยวข้อง การจัดทำแผนบริหารจัดการภัยคุกคามทางไซเบอร์ และการจัดทำแผนบริหารจัดการภัยคุกคามทางไซเบอร์ ตลอดจนฝึกปฏิบัติอย่างเข้มข้นกับการวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงทักษะการจัดเก็บหลักฐานด้านคอมพิวเตอร์ รวม 24 ชั่วโมง / 4 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	14	2
ฝึกปฏิบัติการ (Workshop)	10	2
รวม	24	4

เนื้อหาหลักสูตร ประกอบด้วย

- สำคัญของ พสบ. ไซเบอร์
- สิ่งที่ต้องคำนึงถึงในการให้สอดคล้องกับ พสบ. ไซเบอร์
- มาตรฐานและมาตรการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- มาตรฐาน ISO ที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- ทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบ
- นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การจัดสรรทรัพยากรเพื่อสนับสนุนและรองรับแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การซ้อมแผนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การวิเคราะห์กรณีศึกษาเหตุการณ์ด้านความมั่นคงปลอดภัย แต่ละกรณีจะต้องวิเคราะห์
 - การจำกัดหรือลดผลกระทบของเหตุการณ์ที่เกิดขึ้น
 - การจัดเก็บข้อมูลหลักฐานด้านคอมพิวเตอร์
 - การขจัดปัญหาที่สาเหตุ
 - การกู้คืนระบบ

ระยะเวลาหลักสูตร

ระหว่างวันที่ 8 - 11 กันยายน 2569
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์ (CERT NOC เป็นต้น)
- ผู้ดูแลระบบคอมพิวเตอร์
- ผู้ดูแลเครือข่ายคอมพิวเตอร์
- เจ้าหน้าที่วิเคราะห์และออกแบบระบบ
- เจ้าหน้าที่พัฒนาระบบ
- ผู้จัดการด้านไอที

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษ์

รองกรรมการผู้จัดการ และ
ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ที-เน็ต จำกัด

- ISO/IEC 27001 (Certified of Lead auditor)
- ISO/IEC 20000 (Auditor Certificate) BCMS 25999
- Introduction to Capability Maturity Model Integration V12 Certificate



อาจารย์ เจษฎา กองกันเหลือง

กรรมการผู้จัดการ

บริษัท ที-เน็ต ไอที โซลูชัน จำกัด

- Certified Ethical Hacker (CEH)
- Certified Hacking Forensic Investigator (CHFI)
- Certified Security Analyst (ECSA)
- IT Specialist Certification (ITS): Cyber Security

ค่าลงทะเบียน

ท่านละ 34,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ
ที่ไม่ใช่รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชันพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป
รับส่วนลดทันที 10%

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/csm>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891, 81898 E-mail: npd@nstda.or.th