



บันทึกข้อความ

ส่วนราชการ สำนักงานจัดการทรัพยากรป่าไม้ที่ ๕ (สระบุรี) ส่วนอำนวยการ โทร. ๐ ๓๖๓๔ ๗๔๙๗

ที่ ทส.๑๖๑๘.๑/ ๑.๒๔๗๔

วันที่ ๒๓ สิงหาคม ๒๕๖๕

เรื่อง ขออนุญาตบุคลากรเข้าร่วมการฝึกอบรม

เรียน ผู้อำนวยการส่วนทุกส่วน
ผู้อำนวยการศูนย์ป่าไม้ทุกศูนย์

สำนักงานจัดการทรัพยากรป่าไม้ที่ ๕ (สระบุรี) ขอส่งสำเนาหนังสือสำนักบริหารกลาง ที่ ทส.๑๖๐๑.๔/ว ๔๖๖๗ ลงวันที่ ๑๙ สิงหาคม ๒๕๖๕ เรื่อง ขออนุญาตบุคลากรเข้าร่วมการฝึกอบรม

จึงเรียนมาเพื่อทราบและประชาสัมพันธ์

(นายธวัช เนมีย์)

นักวิชาการป่าไม้ชำนาญการพิเศษ รักษาการราชการแทน
ผู้อำนวยการสำนักงานจัดการทรัพยากรป่าไม้ที่ ๕ (สระบุรี)



บันทึกข้อความ

สำนักจัดการทรัพยากรป่าไม้ที่ ๑ (สงขลา)
เลขที่
วันที่ ๑๙ ส.ค. ๒๕๖๕
เวลา ๑๑.๕๐

ส่วนราชการ สำนักบริหารกลาง ส่วนฝึกอบรม โทร. ๐ ๒๕๖๑ - ๔๒๔๒ - ๓ ต่อ ๕๔๔๖

ที่ ทส ๑๖๐๑.๔/ว ๕๖๖๓ วันที่ ๑๙ สิงหาคม ๒๕๖๕

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมการฝึกอบรม

เรียน อธิบดีกรมป่าไม้

รองอธิบดีกรมป่าไม้ทุกท่าน
ผู้ตรวจราชการกรมป่าไม้ทุกท่าน
ผู้อำนวยการสำนักทุกสำนัก
ผู้อำนวยการกองการอนุญาต
ผู้อำนวยการสำนักจัดการทรัพยากรป่าไม้ ที่ ๑-๑๓
ผู้อำนวยการสำนักจัดการทรัพยากรป่าไม้สาขาทุกสาขา
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ผู้อำนวยการกลุ่มนิติการ
ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร
ผู้อำนวยการกลุ่มตรวจสอบภายใน
ผู้อำนวยการกลุ่มงานจริยธรรม

ส่วนอำนวยการ
เลขที่
วันที่ ๑๙ ส.ค. ๒๕๖๕
เวลา ๑๓.๒๐

สำนักบริหารกลาง ขอส่งสำเนาหนังสือสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม ที่ ทส ๐๒๓๔/ว ๒๕๒๓ ลงวันที่ ๑๐ สิงหาคม ๒๕๖๕ และสำเนาหนังสือสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ อว ๖๐๐๑/ว ๘๔๔๒ ลงวันที่ ๒๕ กรกฎาคม ๒๕๖๕ เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมการฝึกอบรม จำนวน ๖ หลักสูตร มาเพื่อโปรดทราบและประชาสัมพันธ์ให้บุคลากรในสังกัดทราบ ผู้สนใจสามารถติดต่อขอทราบรายละเอียดการอบรมได้ที่หมายเลขโทรศัพท์ ๐ ๒๖๔๔ ๘๑๕๐ ต่อ ๘๑๘๙๑, ๘๑๘๙๘ หรือทางเว็บไซต์ www.career4future.com และทางระบบหนังสือเวียน <http://edoc.forest.go.th/doccir/docindex.html> ผู้สนใจขอได้แจ้งให้สำนักบริหารกลางทราบ ภายในวันที่ ๒๔ สิงหาคม ๒๕๖๕ พร้อมระบุชื่องบประมาณและแผนงานในการเบิกจ่ายจากต้นสังกัด หากเกินกำหนดระยะเวลาดังกล่าว จะถือว่าไม่มีผู้ประสงค์สมัครเข้ารับการอบรม หลักสูตรดังกล่าว และสำนักบริหารกลางจะดำเนินการต่อไป

(นายบรรณรักษ์ เจริมทอง)
ผู้อำนวยการสำนักบริหารกลาง

- ☒ ส่วนอำนวยการ
- ☐ ส่วนจัดการที่ดินป่าไม้
- ☐ ส่วนจัดการป่าชุมชน
- ☐ ส่วนป้องกันรักษาป่าและควบคุมไฟป่า
- ☐ ส่วนส่งเสริมการปลูกป่า
- ☐ ส่วนโครงการพระราชดำริ

นักวิชาการป่าไม้ชำนาญการพิเศษ
ผู้อำนวยการส่วนอำนวยการ

- นายคุณธนากร, ดันเนินพรทวีวัฒน์ / เจ้าพนักงานป่าไม้
รักษาพื้นที่

(นางสาววิลยา หมื่นสกุล)
นักวิชาการป่าไม้ปฏิบัติการ
หัวหน้าฝ่ายบริหารทั่วไป

(นายศักดิ์ชัย ชูธรรม)

พนักงานธุรการ

"No Gift Policy ทส.โปร่งใสและเป็นธรรม"



กรมสามัญ
รับที่ 28055
วันที่ 11 ส.ค. 2565
เวลา 10.26

ที่ ทส ๐๒๓๔/ว ๒๕๒๓

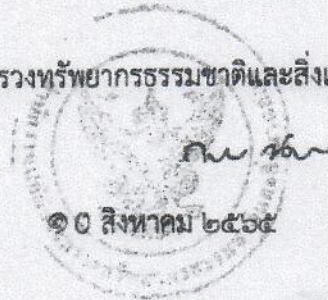
ถึง กรมทุกกรม

สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม
หน่วยงานรัฐวิสาหกิจและองค์การมหาชนทุกหน่วยงาน

ส่วนฝึกอบรม
รับที่ 161A
วันที่ ๑๕ ส.ค. ๒๕๖๕
เวลา 16.41 น.

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม ขอส่งสำเนาหนังสือ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ อว ๖๐๐๑/ว๘๔๔๒ ลงวันที่ ๒๕ กรกฎาคม ๒๕๖๕
เรื่อง ขออนุญาตส่งบุคลากรเข้าร่วมการฝึกอบรม จำนวน ๖ หลักสูตร มาเพื่อพิจารณาประชาสัมพันธ์บุคลากรใน
สังกัด ทั้งนี้ หากสนใจเข้ารับการฝึกอบรม สามารถสมัครได้โดยตรง ศึกษารายละเอียดตามเอกสารแนบ

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม



ส่ง สบก. (ส่วนฝึกอบรม)

(นายบรรณรักษ์ เสริมทอง)

ผู้อำนวยการสำนักบริหารกลาง

๑๑ ส.ค. ๒๕๖๕

สถาบันการพัฒนาทรัพยากรธรรมชาติและสิ่งแวดล้อมอย่างยั่งยืน
ส่วนพัฒนาศักยภาพฯ

โทร.๐ ๒๒๖๕ ๖๑๗๙

โทรสาร ๐ ๒๒๖๕ ๖๑๘๐

ฝ่ายส่งเสริมและพัฒนาบุคลากร

อภินันท์

(นายธิตกร กิตตินันท์)

ผู้อำนวยการส่วนฝึกอบรม

"NO Gift Policy ทส.โปร่งใสและเป็นธรรม"

ผู้อำนวยการสำนักบริหารกลาง

15/8/๖๕
(นางสาวกาญจนา เหมเมืองทอง)
นักทรัพยากรบุคคลชำนาญการ

สถาบันการพัฒนาทรัพยากรธรรมชาติ
และสิ่งแวดล้อมอย่างยั่งยืน
เลขรับ.....507
วันที่.....10/10/2565
เวลา.....10:43

สำนักงานปลัดกระทรวง
ทรัพยากรธรรมชาติและสิ่งแวดล้อม
เลขรับ.....18394
วันที่.....4 ส.ค. 2565
เวลา.....10:39

ที่ อว ๒๐๐๓ / ๗ ๘๔๔๒

๒๕ กรกฎาคม ๒๕๖๕

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมการฝึกอบรม

เรียน ปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

สิ่งที่ส่งมาด้วย แผ่นพับแนะนำหลักสูตร

ผช. ปภ.พ.ส. (นางสาว.....)
เลขรับ.....1935
วันที่.....4 ส.ค. 2565
เวลา.....19:20

ด้วย สถาบันพัฒนาบุคลากรแห่งอนาคต สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ มีกำหนดจัดฝึกอบรมหลักสูตรในโปรแกรมฝึกอบรมหลักสูตรเทคโนโลยีสารสนเทศและการจัดการขั้นสูง ประกอบด้วย

๑. หลักสูตรการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001:2013 รุ่นที่ ๒ (Cloud Security Standard: CSS) อบรมระหว่างวันที่ ๑๐-๑๑, ๒๔-๒๖ สิงหาคม ๒๕๖๕ ณ โรงแรม พูลแมน คิง เพาเวอร์ กรุงเทพฯ โดยมีวัตถุประสงค์เพื่อมุ่งเน้นให้ผู้เข้าอบรมทราบแนวทาง วิธีการ ตลอดจนได้ฝึกปฏิบัติการนำระบบงานขึ้นคลาวด์ ให้มีความมั่นคงปลอดภัยตามมาตรฐาน CSA และ ISO/IEC 27001: 2013 ตั้งแต่การติดตั้งระบบปฏิบัติการ ระบบบริหารจัดการฐานข้อมูล ระบบบริหารจัดการเว็บ ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้อง แอปพลิเคชันของระบบงาน จนกระทั่งสามารถใช้งานระบบได้ โดยสามารถนำแนวทางดังกล่าวไปต่อยอดหรือปรับใช้กับระบบงานของตนเองได้อย่างมีประสิทธิภาพ

๒. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การบริหารจัดการความต่อเนื่องทางธุรกิจตามมาตรฐานสากล ISO 22301:2012 รุ่นที่ ๒ (Business Continuity Management Standard: BCS) อบรมระหว่างวันที่ ๑๗ - ๑๘ สิงหาคม ๒๕๖๕ จัดอบรมผ่านระบบออนไลน์ โดยมีวัตถุประสงค์เพื่อมุ่งเน้นให้ผู้เรียนเข้าใจแนวคิดและหลักการของมาตรฐาน ISO22301:2012 ซึ่งเป็นมาตรฐานสากลที่ใช้ในการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management Systems) ในการขิ่บภัยคุกคาม เพื่อนำมาปรับปรุงประสิทธิภาพและสร้างกลไกเตรียมความพร้อมเรื่องการกู้คืนระบบงานไอทีในองค์กรที่มีความซับซ้อนในการออกแบบกระบวนการป้องกัน การรับมือกับภัยคุกคาม และการฝึกปฏิบัติตามกรณีศึกษา โดยผู้เรียนสามารถนำแผนกู้คืนระบบงานขององค์กรมาฝึกปฏิบัติได้ ซึ่งจะช่วยให้เข้าใจภาพรวมทั้งหมดของการกู้คืนระบบงานไอที และสามารถนำความรู้ที่ได้กลับไปปรับใช้กับองค์กรของตนเองได้อย่างมีประสิทธิภาพ

๓. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การตรวจติดตามของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รุ่นที่ ๒ (PDPA Compliance Audit Workshop for DPOs) อบรมระหว่างวันที่ ๕-๗ กันยายน ๒๕๖๕ จัดอบรมผ่านระบบออนไลน์ โดยมีวัตถุประสงค์เพื่อเสริมสร้างความรู้และความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล การเตรียมความพร้อมขององค์กรให้สามารถดำเนินการอย่างสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล แนวทางปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การประเมินผลกระทบต่อความเป็นส่วนตัว การออกแบบกระบวนการและระบบเพื่อให้เป็นไปตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล และมาตรการด้านความมั่นคงปลอดภัย

๔. หลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ รุ่นที่ ๒ (Cyber Security Incident Management: CSM) อบรมระหว่างวันที่ ๑๓-๑๖ กันยายน ๒๕๖๕ ณ โรงแรม พูลแมน คิง เพาเวอร์ กรุงเทพฯ โดยมีวัตถุประสงค์เพื่อสร้างความรู้และความเข้าใจเกี่ยวกับ พรบ. ไซเบอร์ การปฏิบัติตามให้สอดคล้องกับความต้องการของ พรบ. ไซเบอร์ มาตรการที่จำเป็นสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ มาตรฐาน ISO ที่เกี่ยวข้อง การจัดตั้งทีมบริหารจัดการภัยคุกคามทางไซเบอร์ การจัดทำแผนบริหารจัดการภัยคุกคามทางไซเบอร์ การวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงทักษะการจัดเก็บหลักฐานด้านคอมพิวเตอร์ได้อย่างถูกต้องและมีประสิทธิภาพ

/ ๔ หลักสูตร...

(NPD-244)

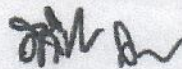
๕. หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ ๔ (Security Operations Center: SOC) อบรมระหว่างวันที่ ๑๘-๒๑ ตุลาคม ๒๕๖๕ ณ โรงแรม พูลแมน คิง เพาเวอร์ กรุงเทพฯ โดยมีวัตถุประสงค์เพื่อเสริมสร้างความรู้ แนวความคิด และหลักการของศูนย์เฝ้าระวังด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยเน้นการฝึกปฏิบัติการจัดตั้งศูนย์ฯ การจัดทำรายงาน การวิเคราะห์ข้อมูลล็อก และการจัดเก็บหลักฐานเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อเข้าถึงและแก้ไขการบุกรุกเครือข่ายและระบบสารสนเทศต่างๆ ที่ผิดปกติอย่างรวดเร็วและมีประสิทธิภาพ

๖. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การจัดทำสถาปัตยกรรมระบบขององค์กร รุ่นที่ ๖ (Enterprise Architecture Workshop: EAW) อบรมระหว่างวันที่ ๒-๔ พฤศจิกายน ๒๕๖๕ จัดอบรมผ่านระบบออนไลน์ โดยมีวัตถุประสงค์มุ่งเน้นให้ผู้เข้าร่วมอบรมเข้าใจหลักการและองค์ประกอบของสถาปัตยกรรมระบบ ทราบแนวทางการจัดทำสถาปัตยกรรมระบบขององค์กร ซึ่งก่อให้เกิดแผนกลยุทธ์ด้านระบบเทคโนโลยีสารสนเทศทั้งระยะสั้นและระยะยาว โดยแสดงให้เห็นความเชื่อมโยงกันใน ๔ ระดับ ระหว่าง กระบวนการทางธุรกิจ (Business Processes) ข้อมูล (Data) ระบบงาน (Application) และเทคโนโลยีสารสนเทศสนับสนุน (Related information technology) รวมถึงฝึกปฏิบัติการจัดทำสถาปัตยกรรมระบบขององค์กร จากกรณีศึกษา และสามารถต่อยอดความรู้ที่ได้กลับไปปรับใช้กับองค์กรของตนเองได้

ในการนี้ สถาบันฯ จึงขอเชิญท่านหรือผู้แทนเข้าร่วมการฝึกอบรมในหลักสูตรดังกล่าว ตามวัน เวลา และสถานที่ข้างต้น โดยท่านสามารถดูรายละเอียดเพิ่มเติมได้จากเว็บไซต์ www.career4future.com หรือ สอบถามรายละเอียดเพิ่มเติมได้ที่ สถาบันพัฒนาบุคลากรแห่งอนาคต หมายเลขโทรศัพท์ ๐ ๒๖๔๔ ๘๑๕๐ ต่อ ๘๑๘๙๑, ๘๑๘๙๘ ทั้งนี้ ผู้เข้าอบรมสามารถเบิกค่าลงทะเบียนและไม่ถือเป็นวันลาตามระเบียบกระทรวงการคลัง และค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมของบริษัทหรือห้างหุ้นส่วนนิติบุคคลสามารถนำไปลดหย่อนภาษีได้ ๒๐๐%

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ



(นายศิริชัย กิตติวราพงศ์)

ผู้อำนวยการ

สถาบันพัฒนาบุคลากรแห่งอนาคต

ปฏิบัติการแทนผู้อำนวยการ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

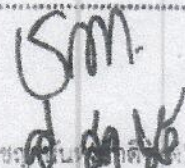
เรียน **ผอ. สวท.**

- ☒ เพื่อพิจารณาดำเนินการ
- ☐ เพื่อทราบ
- ☐ เพื่อตรวจสอบเสนอ
- ☐

สถาบันพัฒนาบุคลากรแห่งอนาคต

โทร. ๐ ๒๖๔๔ ๘๑๕๐ ต่อ ๘๑๘๙๑ (นิพนธ์)

โทรสาร ๐ ๒๖๔๔ ๘๑๑๐



(นางชุตินา กิตติวราพงศ์)

ผู้ช่วยปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยีและสิ่งแวดล้อม
ปฏิบัติราชการแทนปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยีและสิ่งแวดล้อม



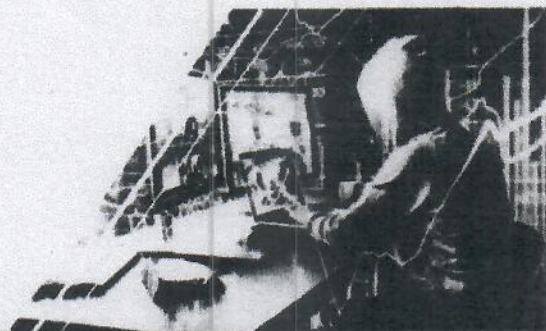
สวทช.
NSTDA

TMC
Technology Management Center
ศูนย์บริหารจัดการเทคโนโลยี

Career for the Future Academy
สถาบันพัฒนาคณาจารย์แห่งอนาคต

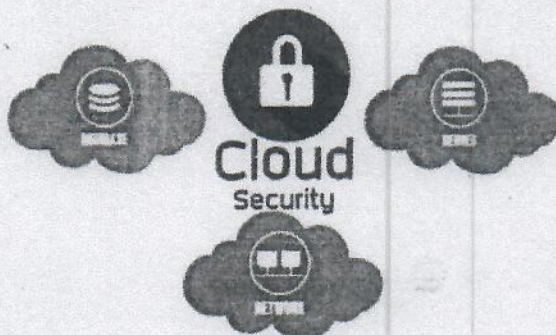
CSS

Cloud Security Standard



หลักสูตรการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย
ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001:2013 รุ่นที่ 6

cloud
CSA security
alliance®



มุ่งเน้นการฝึกปฏิบัติการจัดทำระบบงานให้มีความมั่นคงปลอดภัยและสอดคล้อง
ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001:2013
(เน้นฝึกปฏิบัติโดเมนและมาตรการทางเทคนิค)

Key Highlights

- ★ เจาะลึกแนวทางการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย เพื่อสร้างความมั่นใจให้กับผู้ใช้บริการคลาวด์
- ★ เรียนรู้มาตรฐานสากล CSA และ ISO/IEC 27001:2013 ในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ ที่นำไปติดตั้งและใช้งานบนคลาวด์
- ★ เข้าใจกระบวนการนำระบบสารสนเทศขึ้นคลาวด์ให้มีความมั่นคงปลอดภัยตามมาตรฐาน CSA และ ISO/IEC 27001:2013
- ★ เน้นฝึกปฏิบัติอย่างเข้มข้นกว่า 10 Workshop ตามโดเมนและมาตรการทางเทคนิคของมาตรฐาน เวอร์ชันล่าสุด และเน้นการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่ติดตั้งอย่างเข้มข้น
- ★ ฝึกปฏิบัติจริง ติดตั้ง และใช้งานระบบสารสนเทศบนคลาวด์ของ AWS (Amazon Web Service) เพื่อให้ผู้เรียนเข้าใจและสามารถนำกลับไปปฏิบัติได้ด้วยตนเอง
- ★ เรียนรู้เทคนิคต่างๆ ของการนำระบบสารสนเทศไปขึ้นคลาวด์ที่จะช่วยลดถึงระยะเวลาการติดตั้ง และความผิดพลาดต่างๆ ซึ่งรวมถึงค่าใช้จ่ายต่างๆ ที่จะเกิดขึ้นจากการนำระบบสารสนเทศไปขึ้นคลาวด์



หลักสูตรการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001:2013 รุ่นที่ 6 (Cloud Security Standard : CSS)

ปัจจุบันหลายองค์กรได้เริ่มปรับเปลี่ยนการทำงานจากการติดตั้ง ดูแล และบริหารจัดการเซิร์ฟเวอร์และระบบงานต่างๆ ภายในศูนย์คอมพิวเตอร์ไปติดตั้งและบริหารจัดการระบบโดยใช้บริการจากผู้ให้บริการคลาวด์แทน ซึ่งมีความรู้ ความสามารถ และน่าเชื่อถือ เพื่อประหยัดค่าใช้จ่ายในการลงทุนด้านเซิร์ฟเวอร์ โครงสร้างพื้นฐานด้านเครือข่าย และการจัดทำศูนย์คอมพิวเตอร์ จากความจำเป็นหรือความต้องการในการนำระบบงานต่างๆ ขององค์กรขึ้นไปติดตั้งบนคลาวด์ของผู้ให้บริการ ประเด็นปัญหาและอุปสรรคสำคัญในฐานะผู้ใช้บริการคลาวด์คือ ประเด็นความมั่นคงปลอดภัยด้านสารสนเทศที่ทุกองค์กรที่จะนำระบบงานไปติดตั้งบนคลาวด์ต้องเผชิญ หลักสูตรนี้จึงเล็งเห็นถึงความจำเป็นในการนำระบบงานขององค์กรไปขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย ทั้งนี้เพื่อให้เกิดความมั่นใจต่อผู้ใช้บริการคลาวด์นั่นเอง

โดยมาตรฐานสากลสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศบนคลาวด์ที่นิยมใช้หรืออ้างอิงกันอยู่คือมาตรฐาน CSA (Cloud Security Alliance) มาตรฐานนี้เป็นมาตรฐานที่พัฒนามาต่อยอดมาจาก ISO/IEC 27001 ซึ่งเป็นมาตรฐานหลักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เป็นที่ยอมรับและปัจจุบันมีหลายหน่วยงานทั้งภาครัฐและเอกชนปฏิบัติตามอยู่ หลักสูตรนี้ได้อ้างอิงตามมาตรฐาน CSA 4.x (เวอร์ชันปัจจุบันล่าสุด) และ มาตรฐาน ISO/IEC 27001: 2013 (เวอร์ชันปัจจุบันล่าสุด) โดยเน้นมาตรการทางเทคนิคซึ่งเป็นเรื่องของการติดตั้งระบบงานให้มีความมั่นคงปลอดภัย

โครงสร้างหลักสูตร

หลักสูตรนี้มุ่งเน้นให้ผู้เข้าอบรมทราบแนวทาง วิธีการ ตลอดจนได้ฝึกปฏิบัติการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัยตามมาตรฐาน CSA และ ISO/IEC 27001: 2013 ตั้งแต่การติดตั้งระบบปฏิบัติการ ระบบบริหารจัดการฐานข้อมูล ระบบบริหารจัดการเว็บเซิร์ฟเวอร์ต่างๆ ที่เกี่ยวข้อง แอปพลิเคชันของระบบงาน จนกระทั่งสามารถใช้งานระบบได้ โดยสามารถนำแนวทางดังกล่าวไปต่อยอดหรือปรับใช้กับระบบงานของตนเองได้ รวม 30 ชั่วโมง / 5 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	15	2.5
ฝึกปฏิบัติการ (Workshop)	15	2.5
รวม	30	5

หลักสูตรนี้เหมาะสำหรับ

- เจ้าหน้าที่เทคนิค ได้แก่ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้พัฒนาระบบ Helpdesk
- เจ้าหน้าที่ด้านความมั่นคงปลอดภัยระบบสารสนเทศ (IT Security)
- ผู้ที่อยู่ในตำแหน่งงานด้านไอซีทีต่างๆ ที่สนใจงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ

สิ่งที่คาดว่าจะได้รับ

ผู้เข้าอบรมจะได้รับ

- ความรู้ความเข้าใจในการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัยด้านสารสนเทศตามมาตรฐาน CSA และ ISO/IEC 27001: 2013
- ฝึกปฏิบัติการใช้เครื่องมือ และสร้างความรู้ด้านเทคนิคของซอฟต์แวร์โอเพนซอร์สเพื่อให้อาจใช้งานได้สอดคล้องตามแต่ละโดเมน
- ความรู้และการฝึกปฏิบัติจากกรณีศึกษาในห้องเรียน เพื่อให้มีความเข้าใจและนำไปปรับใช้งานกับองค์กรของตนเองได้อย่างมีประสิทธิภาพ

ค่าลงทะเบียน

ท่านละ 36,000 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไปใช้ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป รับส่วนลดทันที 10%

หมายเหตุ

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

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี

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 V1.2 Certificate

cloud
CSA security
alliance



ระยะเวลาหลักสูตร

ระหว่างวันที่ 10-11, 24-26 สิงหาคม 2565
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 5 วัน)

สถานที่อบรม

โรงแรม พูลแมน คิง เพาเวอร์ กรุงเทพฯ
เลขที่ 8/2 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ

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

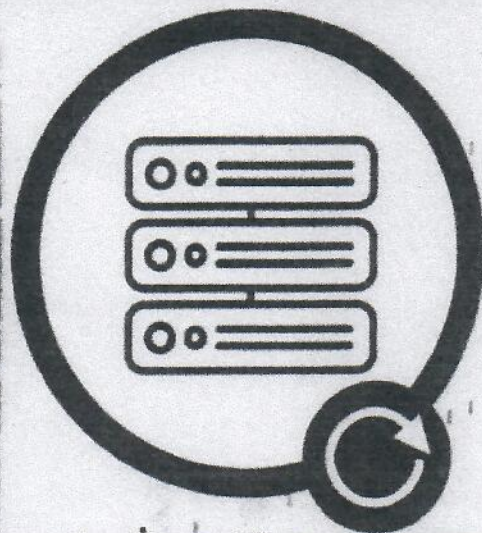
สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891, 81898 E-mail: npd@nstda.or.th

BCS

อบรม Online ผ่านโปรแกรม  zoom

Business Continuity Management Standard

หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การบริหารจัดการความต่อเนื่องทางธุรกิจตามมาตรฐานสากล ISO 22301:2012 รุ่นที่ 6



มุ่งเน้นการเตรียมความพร้อมเรื่องการกู้คืนระบบงาน และการรับมือกับเหตุการณ์หยุดชะงักหรือ
สภาวะวิกฤติ เพื่อให้เกิดความต่อเนื่องในกระบวนการบริหารจัดการงาน
ตามมาตรฐาน ISO 22301:2012

Key Highlights

- เจาะลึก ISO 22301:2012 มาตรฐานสากลหลักที่ใช้ในการอ้างอิงและบริหารจัดการความต่อเนื่องทางธุรกิจ เพื่อการบริหารจัดการภัยคุกคามแบบองค์รวม
- ทราบหลักการการประเมินความเสี่ยง ผลกระทบ การกำหนดลำดับของงานในการกู้คืนระบบ ตลอดจนการกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบงานที่เหมาะสม
- วางแผนเตรียมความพร้อมด้านกลยุทธ์ในการป้องกันหรือรับมือกับเหตุวิกฤติ หรือภัยพิบัติ เพื่อลดความเสียหาย สร้างความยืดหยุ่น และสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง
- เรียนรู้วิธีการจัดทำแผนกู้คืนระบบงาน (Business Continuity Plan) และแผนรับมือกับเหตุการณ์หยุดชะงักที่เกิดขึ้น (Incident Management Plan) โดยอ้างอิงตามมาตรฐาน ISO 22301:2012
- ฝึกปฏิบัติเข้มข้นกว่า 10 Workshop กับกรณีศึกษาที่สามารถนำกลับไปประยุกต์ใช้งานได้จริงในองค์กร



การดำเนินธุรกิจในปัจจุบันจำเป็นต้องพึ่งพาระบบงานไอทีมาสนับสนุนในการบริหารจัดการ เพื่อให้องค์กรสามารถดำเนินการไปได้อย่างรวดเร็วและมีประสิทธิภาพ แต่ด้วยปัจจัยการเปลี่ยนแปลงที่รวดเร็ว และความไม่แน่นอนของสถานการณ์ที่ไม่สามารถคาดการณ์ได้ ไม่ว่าจะเป็นสถานการณ์น้ำท่วม ไฟไหม้ หรือถูกปิดล้อมโดยฝูงชน หากระบบงานหรือบุคลากรหยุดทำงานเป็นเวลานานเกินกว่าระยะเวลาที่รับได้ จะก่อให้เกิดความเสียหายและส่งผลกระทบต่อการทำงานธุรกิจ ชื่อเสียง ภาพลักษณ์ ความเชื่อมั่น และกิจกรรมที่สร้างมูลค่าเพิ่มให้กับองค์กร ดังนั้นหลายองค์กรจึงได้ให้ความสำคัญกับการเตรียมพร้อมในการรับมือกับเหตุการณ์ สภาวะวิกฤติ หรือภัยคุกคามที่อาจเกิดขึ้น และเตรียมพร้อมในเรื่องของการกู้คืนระบบงานไอทีให้กลับคืนมาดำเนินกิจกรรมได้ภายในระยะเวลาที่เหมาะสม

โครงสร้างหลักสูตร

หลักสูตรนี้มุ่งเน้นให้ผู้เรียนเข้าใจแนวคิดและหลักการของมาตรฐาน ISO 22301:2012 ซึ่งเป็นมาตรฐานสากลที่ใช้ในการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management Systems) ในการรับมือภัยคุกคาม เพื่อนำมาปรับปรุงประสิทธิภาพและสร้างกลไกเตรียมความพร้อมเรื่องการกู้คืนระบบงานไอทีในองค์กรที่มีความซับซ้อนในการออกแบบกระบวนการป้องกันและรับมือกับภัยคุกคาม นอกจากนี้หลักสูตรนี้ยังได้กำหนดให้มีการฝึกปฏิบัติตามกรณีศึกษาโดยผู้เรียนสามารถนำแผนกู้คืนระบบงานขององค์กรมาฝึกปฏิบัติได้ ซึ่งจะช่วยให้เข้าใจภาพรวมทั้งหมดของการกู้คืนระบบงานไอทีและสามารถต่อยอดความรู้ที่ได้กลับไปปรับใช้งานกับองค์กรของตนเองได้อย่างมีประสิทธิภาพ รวม 18 ชั่วโมง / 3 วันทำการ

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

หลักสูตรนี้เหมาะสำหรับ

- ผู้บริหารด้านไอซีทีในทุกกระดับ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ
- ผู้จัดการด้านไอซีที
- เจ้าหน้าที่ทางเทคนิคด้านไอซีที เช่น ผู้วิเคราะห์และออกแบบระบบ ผู้พัฒนาระบบ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย
- ผู้ตรวจสอบไอซีที

วิทยากรประจำหลักสูตร



ดร. บรรจง หงษ์ยี่
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 V1.2 Certificate

สิ่งที่คาดว่าจะได้รับ

- ผู้เข้าอบรมจะได้รับ
- การนำบริบทขององค์กร หรือสภาพขององค์กรที่เป็นอยู่ในปัจจุบันมาใช้เป็นประเด็นสำคัญในการวางแผนงานสำหรับการบริหารความต่อเนื่องทางธุรกิจ
 - การกำหนด Scenario ซึ่งเป็นเหตุการณ์ความเสียหายที่ส่งผลกระทบต่อหยุดชะงักของระบบงานสำคัญขององค์กร
 - การประเมินผลกระทบการก่อกวนระบบงานสำคัญขององค์กรเกิดการหยุดชะงัก
 - การกำหนดลำดับของงานในการกู้คืนระบบ
 - การกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ
 - การประเมินความเสี่ยงเพื่อบริหารจัดการกับเหตุการณ์ต่างๆ ที่จะทำให้เกิดการหยุดชะงัก
 - การระบุทรัพยากรที่จำเป็นสำหรับการกู้คืนระบบงาน
 - การจัดทำแผนการรับมือหรือจัดการกับเหตุการณ์หยุดชะงัก
 - การจัดทำแผนกู้คืนระบบ
 - การซ้อมการกู้คืนระบบ
 - การจัดทำแผนการสื่อสารในระหว่างที่เกิดเหตุ

ค่าลงทะเบียน

ท่านละ 18,500 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

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

หมายเหตุ

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

ระยะเวลาหลักสูตร

ระหว่างวันที่ 17-19 สิงหาคม 2565
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

รูปแบบการจัดอบรม

อบรม Online ผ่านโปรแกรม ZOOM

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

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



สวทช.
NSTDA

TMC
Technology Management Center
ศูนย์บริหารจัดการเทคโนโลยี

Career for the Future Academy
สถาบันพัฒนบุคลากรแห่งอนาคต

DPO

อบรม Online ผ่านโปรแกรม  zoom

PDPA Compliance Audit Workshop for DPOs

หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การตรวจติดตามของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
เพื่อให้เป็นไปตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รุ่นที่ 2

มุ่งเน้นการฝึกปฏิบัติเพื่อเตรียมความพร้อมให้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
สามารถทำหน้าที่ในการตรวจติดตามเพื่อให้เป็นไปตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



Key Highlights

- เข้าใจสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- เรียนรู้มาตรฐานด้านความมั่นคงปลอดภัยสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- เจาะลึกการประเมินตามแนวทางปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามแนวทางของ GDPR
- เรียนรู้การประเมินผลกระทบต่อความเป็นส่วนตัว
(Privacy Impact Assessment – PIA หรือ Data Protection Impact Assessment – DPIA)
- ประเมินการออกแบบกระบวนการและระบบเพื่อให้เป็นไปตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
(Privacy by Design and Privacy by Default)
- ฝึกปฏิบัติเข้มข้นจำนวน 8 Workshop
เน้นการตรวจประเมินเพื่อเตรียมความพร้อมในการปฏิบัติ
ตามสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



หลักสูตรฝึกอบรมเชิงปฏิบัติการ การตรวจติดตามของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รุ่นที่ 2 (PDPA Compliance Audit Workshop for DPOs) อบรม Online ผ่านโปรแกรม Zoom

ด้วยความก้าวหน้าและความง่ายของเทคโนโลยีสารสนเทศและการสื่อสาร หน่วยงานและองค์กรต่างๆ จึงมีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้รับบริการหรือผู้ใช้งานเป็นจำนวนมาก ซึ่งมีการจัดเก็บอยู่ในระบบงานต่างๆ ขององค์กร ในอดีตที่ผ่านมา ยังไม่ได้มี พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บังคับใช้กัน (จากนี้ไปขอเรียกว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคล) ที่มีสาระสำคัญเพื่อช่วยในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการเหล่านั้น จึงทำให้ในปัจจุบันยังคงมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลอยู่เป็นจำนวนมาก ซึ่งอาจสร้างความเสียหาย หรือสร้างความเดือดร้อนและรำคาญต่อเจ้าของส่วนบุคคลก็เป็นได้

เพื่อเป็นการป้องกันการล่วงละเมิดดังกล่าว ทุกหน่วยงานหรือองค์กรที่ตั้งอยู่ในราชอาณาจักรไทย ต้องดำเนินการให้สอดคล้องกับ พ.ร.บ. ฉบับนี้ โดย เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection officer - DPO) จะเป็นผู้มีบทบาทสำคัญกับทุกองค์กร ในการเป็นผู้ตรวจติดตามการประมวลผลข้อมูลส่วนบุคคลภายในองค์กรให้มีการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด ซึ่งควรจะได้มีการแต่งตั้งและมอบหมายเพื่อกอทำหน้าที่ในการสอดส่องและดูแลการเข้าถึงและใช้งานข้อมูลส่วนบุคคลภายในองค์กรให้เป็นไปตามที่กฎหมายกำหนด

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่ให้ความรู้และความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล การเตรียมความพร้อมขององค์กรให้สามารถดำเนินการอย่างสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล แนวทางปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การประเมินผลกระทบต่อนความเป็นส่วนตัว การออกแบบกระบวนการและระบบเพื่อให้เป็นไปตามวัตถุประสงค์ประสงค์ของการประมวลผลข้อมูลส่วนบุคคล และมาตรการด้านความมั่นคงปลอดภัย ตลอดจนการฝึกปฏิบัติเพื่อพัฒนากิจกรรมที่จำเป็นอย่างเข้มข้น รวม 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	9	15
ฝึกปฏิบัติการ (Workshop)	9	15
รวม	18	3

เนื้อหาหลักสูตร ประกอบด้วย

- สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- แนวทางปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามแนวทางของ GDPR (General Data Protection Regulation)
- โครงสร้างของการกำกับดูแลข้อมูลส่วนบุคคลภายในองค์กร บทบาท และหน้าที่ความรับผิดชอบ
- นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
- บันทึกกิจกรรมการประมวลผล
- การแจ้งเก็บรวบรวมข้อมูลส่วนบุคคล
- การขอความยินยอม
- การเก็บรวบรวมข้อมูลส่วนบุคคล
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- การขอใช้สิทธิโดยเจ้าของข้อมูลส่วนบุคคล
- การจัดการการละเมิดข้อมูลส่วนบุคคล
- การประเมินผลกระทบต่อนความเป็นส่วนตัว
- การออกแบบกระบวนการและระบบเพื่อให้เป็นไปตามวัตถุประสงค์ประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
- การประเมินด้านความมั่นคงปลอดภัยสารสนเทศของระบบงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- การฝึกปฏิบัติในการตรวจติดตามของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หลักสูตรนี้เหมาะสำหรับ

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)
- ผู้ตรวจสอบภายใน
- กลุ่มเป้าหมายดังนี้ จะได้เรียนรู้แนวทางปฏิบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
- ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
- ผู้บริหารและผู้จัดการที่ปฏิบัติงานเกี่ยวข้องกับข้อมูลส่วนบุคคล
- ผู้ปฏิบัติงานที่เกี่ยวข้องกับการกำกับดูแลให้เป็นไปตามที่กฎหมายและระเบียบข้อบังคับกำหนด
- ผู้ปฏิบัติงานด้านกฎหมาย
- ผู้ที่สนใจทั่วไป เกี่ยวกับการปฏิบัติตามที่กฎหมายกำหนด

ค่าลงทะเบียน

ท่านละ 18,500 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ
- ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรแกรมพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป ส่วนลดทันที 10%

ระยะเวลาหลักสูตร

ระหว่างวันที่ 5 - 7 กันยายน 2565

เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

รูปแบบการจัดอบรม

อบรม Online ผ่านโปรแกรม  ZOOM

วิทยากรประจำหลักสูตร



ดร. บรรจง คงรังษี

รองกรรมการผู้จัดการ และที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ บริษัท ที-เน็ต จำกัด

- ISO/IEC 27001 (Certified of Lead auditor)
- ISO/IEC 20000 (Auditor Certificate) BCMS 25999
- Introduction to Capability Maturity Model Integration V1.2 Certificate

หมายเหตุ

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

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

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



สวทช.
NSTDA

TMC
Technology Management Center
ศูนย์บริหารจัดการเทคโนโลยี

Career for the Future Academy
สถาบันพัฒนาศักยภาพบุคลากรแห่งอนาคต

CSM

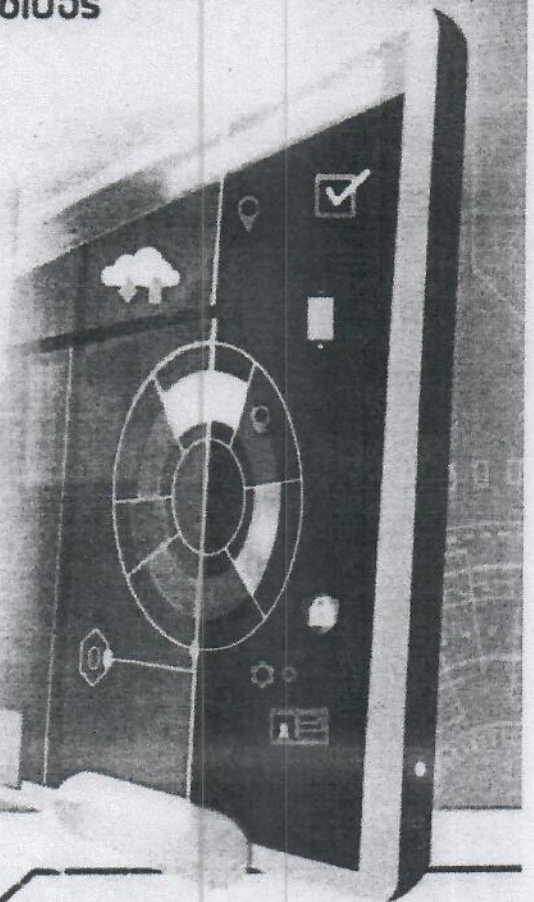
Cyber Security Incident Management



หลักสูตร

การบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ รุ่นที่ 2

"มุ่งเน้นการเตรียมความพร้อมในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อรับมือกับภัยคุกคามทางไซเบอร์จนถึงการกู้คืนระบบกลับคืน"



Key Highlights

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



หลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ รุ่นที่ 2 (Cyber Security Incident Management: CSM)

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

- สาละสำคัญของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (พ.ร.บ. ไซเบอร์)
- สิ่งที่ต้องคำนึงถึงในการให้สอดคล้องกับ พ.ร.บ. ไซเบอร์
- มาตรการที่จำเป็นที่ต้องนำมาปฏิบัติเพื่อให้สอดคล้องกับความต้องการของ พ.ร.บ. ไซเบอร์ (อ้างอิงจากมาตรฐาน Framework for Improving Critical Infrastructure Cybersecurity)
- มาตรฐาน ISO ที่เกี่ยวข้อง ตลอดจนการฝึกปฏิบัติเพื่อให้ผู้เข้าร่วมฝึกอบรมได้พัฒนาทักษะที่จำเป็นสำหรับการรับมือ และบริหารจัดการภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่ให้ความรู้และความเข้าใจเกี่ยวกับ พ.ร.บ. ไซเบอร์ การปฏิบัติตามให้สอดคล้องกับความต้องการของ พ.ร.บ. ไซเบอร์ มาตรการที่จำเป็นสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ มาตรฐาน ISO ที่เกี่ยวข้อง การจัดทำแผนบริหารจัดการภัยคุกคามทางไซเบอร์ ตลอดจนฝึกปฏิบัติอย่างเข้มข้นกับการวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงทักษะการจัดเก็บหลักฐานด้านคอมพิวเตอร์ รวม 24 ชั่วโมง / 4 วันทำการ

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

เนื้อหาหลักสูตร ประกอบด้วย

- สาละสำคัญของ พ.ร.บ. ไซเบอร์
- สิ่งที่ต้องคำนึงถึงในการปฏิบัติตามเพื่อให้สอดคล้องกับ พ.ร.บ. ไซเบอร์
- มาตรฐานและมาตรการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- มาตรฐาน ISO ที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- กับบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบ
- นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การวัดสรรทรัพยากรเพื่อสนับสนุนและรองรับแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การเชื่อมโยงแผนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การวิเคราะห์กรณีศึกษาเหตุการณ์ด้านความมั่นคงปลอดภัย แต่ละกรณีจะต้องวิเคราะห์
 - การจำกัลดผลกระทบของเหตุที่เกิดขึ้น
 - การจัดเก็บข้อมูลหลักฐานด้านคอมพิวเตอร์
 - การขจัดปัญหาที่สาเหตุ
 - การกู้คืนระบบ

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการป้องกันและลดผลกระทบ (เช่น CERT NOC เป็นต้น)
- ผู้ดูแลระบบคอมพิวเตอร์
- ผู้ดูแลเครือข่ายคอมพิวเตอร์
- เจ้าหน้าที่วิเคราะห์และออกแบบระบบ
- เจ้าหน้าที่พัฒนาระบบ
- ผู้จัดการด้านไอที

ค่าลงทะเบียน

ท่านละ 34,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

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

ระยะเวลาหลักสูตร

ระหว่างวันที่ 13-16 กันยายน 2565

เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

สถานที่อบรม

โรงแรม พูลแมน คิง เพาเวอร์ กรุงเทพฯ
เลขที่ 8/2 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ



ดร. บรรจง หงษ์สี

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

หมายเหตุ

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

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

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



สวทช.
NSTDA

TMC
Innovation Management Center
ศูนย์บริหารนวัตกรรมไทย

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

SOC

Security Operations Center

หลักสูตร

ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 4

มุ่งเน้นการฝึกปฏิบัติ
เฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
ภายใต้ศูนย์ SOC อย่างเข้มข้น

Key Highlights

- เรียนรู้แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กับวิทยากรผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยระบบสารสนเทศระดับประเทศ
- เจาะลึกกระบวนการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- ฝึกปฏิบัติกับซอฟต์แวร์เชิงพาณิชย์ในระดับแนวหน้า เช่น Sprunk Arcsight เพื่อใช้ในการวิเคราะห์ข้อมูลล็อกที่เกี่ยวข้องกับการบุกรุกระบบ
- ฝึกปฏิบัติเข้มข้นถึง 10 Workshop ในการปฏิบัติงานเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถนำไปปฏิบัติได้จริงด้วยตนเอง



หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 4 (Security Operations Center: SOC)

ยุคสารสนเทศหรือยุคดิจิทัลในปัจจุบัน ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศถือเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่งต่อองค์กรสำหรับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์ไม่ว่าจะเป็นสถาบันการเงิน ผู้ให้บริการด้านโทรคมนาคม ผู้ให้บริการ Cloud ผู้ให้บริการดูแล Application และอื่นๆ ทั้งนี้เนื่องมาจากการทำงานขององค์กร ผู้ใช้งาน ตลอดจนลูกค้าขององค์กร มีความจำเป็นต้องอาศัยระบบคอมพิวเตอร์ อินเทอร์เน็ต เครือข่ายไร้สาย อุปกรณ์ประเภท Smartphone รวมทั้งอุปกรณ์ประเภท Internet of Things เหล่านี้ล้วนก่อให้เกิดความจำเป็นที่จะต้องมีการเฝ้าระวังและป้องกันระบบและอุปกรณ์ขององค์กรให้มีความมั่นคงปลอดภัยอย่างเพียงพอและตลอดเวลา

Security Operation Center หรือ SOC คือศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมิน ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง

โครงสร้างหลักสูตร

เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับมาตรฐานในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) และฝึกปฏิบัติเป็นขั้นบันไดที่จำเป็นสำหรับการปฏิบัติงานภายใต้ ศูนย์ปฏิบัติการฯ ประกอบด้วย การบรรยาย การฝึกอบรมเชิงปฏิบัติการ รวม 24 ชั่วโมง / 4 วันทำการ

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

เนื้อหาหลักสูตร ประกอบด้วย

- มาตรฐานและกระบวนการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- กระบวนการ บทบาท และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการเฝ้าระวังด้านความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ
- การแบ่งแยกเหตุการณ์เชิงเดือน (Event) หรือเหตุการณ์ด้านความมั่นคงปลอดภัยให้ชัดเจน (Security Incident)
- การประเมินผลกระทบหรือระดับความรุนแรงของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น
- การจำลองสถานการณ์การโจมตีในรูปแบบต่างๆ เช่น SQL Injection, Cross-site Scripting (XSS), Brute Force เป็นต้น
- การติดตั้ง Agent บนระบบต่างๆ สำหรับการบันทึกข้อมูลล็อก
- การกำหนดกฎเกณฑ์ (Correlation Rules) ที่ใช้ในการวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์หาสาเหตุของเหตุการณ์ด้านความมั่นคงปลอดภัย
- การจัดเก็บหลักฐานด้านคอมพิวเตอร์จากข้อมูลล็อกที่จัดเก็บไว้
- การวิเคราะห์หรือตรวจสอบข้อมูลในระบบที่ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต
- การจัดทำรายงานประเภทต่างๆ ที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัย ได้แก่ การแจ้งเตือนประเภทต่างๆ (Alert) และรายงานประเภทสถิติต่างๆ (Dashboard) ที่จำเป็นต่อการใช้งาน
- การใช้เครื่องมือและจัดเก็บข้อมูลล็อกให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร ตลอดจนกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง
- การวิเคราะห์หาช่องโหว่ในระบบคอมพิวเตอร์ เพื่อตรวจสอบหาช่องทางการถูกบุกรุกหรือการเข้าถึง เครือข่ายและระบบสารสนเทศที่ผิดปกติ และหาแนวทางการป้องกันระบบ
- การใช้เครื่องมือเฝ้าระวังและติดตามการทำงานของระบบและอุปกรณ์ต่างๆ

ระยะเวลาหลักสูตร

ระหว่างวันที่ 18 - 21 ตุลาคม 2565
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

หมายเหตุ

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

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

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

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัย (เช่น CERT NOC เป็นต้น)
- ผู้ดูแลระบบคอมพิวเตอร์ / ผู้ดูแลเครือข่ายคอมพิวเตอร์
- ผู้จัดการด้านไอที
- ผู้ปฏิบัติงานที่เกี่ยวข้องกับการเฝ้าระวังระบบและอุปกรณ์ต่างๆ ขององค์กร

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี

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 V1.2 Certificate

ค่าลงทะเบียน

ท่านละ 34,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ
ที่ไม่ใช่ธุรกิจและไปแสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป
รับส่วนลดทันที 10%

สถานที่อบรม

โรงแรม พูลแมน สด พลาซ่า กรุงเทพฯ
เลขที่ 8/2 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ

หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 4 (Security Operations Center: SOC)

ยุคสารสนเทศหรือยุคดิจิทัลในปัจจุบัน ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศถือเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่งต่อองค์กรสำหรับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์ไม่ว่าจะเป็นสถาบันการเงิน ผู้ให้บริการด้านโครงข่าย ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการ Cloud ผู้ให้บริการดูแล Application และอื่นๆ ทั้งนี้เนื่องมาจากการทำงานขององค์กร ผู้ใช้งาน ตลอดจนลูกค้าขององค์กรมีความจำเป็นต้องอาศัยระบบคอมพิวเตอร์ อินเทอร์เน็ต เครือข่ายไร้สาย อุปกรณ์ประเภท Smartphone รวมทั้งอุปกรณ์ประเภท Internet of Things เหล่านี้ล้วนก่อให้เกิดความจำเป็นที่จะต้องมีการเฝ้าระวังและป้องกันระบบและอุปกรณ์ขององค์กรให้มีความมั่นคงปลอดภัยอย่างเพียงพอและตลอดเวลา

Security Operation Center หรือ SOC คือศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมิน ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้นเพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ต่ำลง

โครงสร้างหลักสูตร

เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับมาตรฐานในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) และฝึกปฏิบัติเข้มข้นทักษะพื้นฐานที่จำเป็นสำหรับการปฏิบัติงานภายใต้ ศูนย์ปฏิบัติการฯ ประกอบด้วย การบรรยาย การฝึกอบรมเชิงปฏิบัติการ รวม 24 ชั่วโมง / 4 วันทำการ

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

เนื้อหาหลักสูตร ประกอบด้วย

- มาตรฐานและกระบวนการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- กระบวนการ บทบาท และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการเฝ้าระวังด้านความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ
- การแบ่งแยกเหตุการณ์แจ้งเตือน (Event) หรือเหตุการณ์ด้านความมั่นคงปลอดภัยให้ชัดเจน (Security Incident)
- การประเมินผลกระทบหรือระดับความรุนแรงของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น
- การจำลองสถานการณ์การโจมตีในรูปแบบต่างๆ เช่น SQL Injection, Cross-site Scripting (XSS), Brute Force เป็นต้น
- การติดตั้ง Agent บนระบบต่างๆ สำหรับการบันทึกข้อมูลล็อก
- การกำหนดกฎเกณฑ์ (Correlation Rules) ที่ใช้ในการวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์หาสาเหตุของเหตุการณ์ด้านความมั่นคงปลอดภัย
- การวัดเก็บหลักฐานด้านคอมพิวเตอร์จากข้อมูลล็อกที่จัดเก็บไว้
- การวิเคราะห์หรือตรวจสอบข้อมูลในระบบที่ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต
- การจัดทำรายงานประเภทต่างๆ ที่เกี่ยวข้องกับการเหตุการณ์ความมั่นคงปลอดภัย ได้แก่ การแจ้งเตือนประเภทต่างๆ (Alert) และรายงานประเภทสถิติต่างๆ (Dashboard) ที่จำเป็นต่อการใช้งาน
- การใช้เครื่องมือและจัดเก็บข้อมูลล็อกให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร ตลอดจนกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง
- การวิเคราะห์หาช่องโหว่ในระบบคอมพิวเตอร์ เพื่อตรวจสอบหาช่องทางการบุกรุกหรือการเข้าถึง เครือข่ายและระบบสารสนเทศที่ผิดปกติ และหาแนวทางป้องกันระบบ
- การใช้เครื่องมือในการเฝ้าระวังและติดตามการทำงานของระบบและอุปกรณ์ต่างๆ

ระยะเวลาหลักสูตร

ระหว่างวันที่ 18 - 21 ตุลาคม 2565
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

หมายเหตุ

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

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัย (เช่น CERT NOC เป็นต้น)
- ผู้ดูแลระบบคอมพิวเตอร์ / ผู้ดูแลเครือข่ายคอมพิวเตอร์
- ผู้จัดการด้านไอที
- ผู้ปฏิบัติงานที่เกี่ยวข้องกับการเฝ้าระวังระบบและอุปกรณ์ต่างๆ ขององค์กร

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี

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 V1.2 Certificate

ค่าลงทะเบียน

ท่านละ 34,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

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

สถานที่อบรม

โรงแรม พูลแมน คิง เพาเวอร์ กรุงเทพฯ
เลขที่ 8/2 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ

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

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



สวทช.
NSTDA

TMC
Technology Management Center
ศูนย์บริหารจัดการเทคโนโลยี

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

EA

อบรม Online ผ่านโปรแกรม zoom

Enterprise Architecture Workshop รุ่นที่ 6

หลักสูตรฝึกอบรมเชิงปฏิบัติการการจัดทำสถาปัตยกรรมระบบขององค์กร
มุ่งเน้นการฝึกปฏิบัติการจัดทำสถาปัตยกรรมระบบ ที่ครอบคลุมทั้ง 4 ระดับ
ได้แก่ กระบวนการ ข้อมูล ระบบงาน และเทคโนโลยีสารสนเทศ

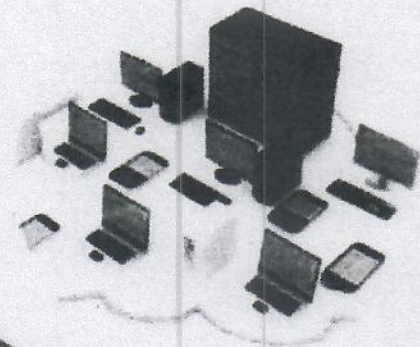
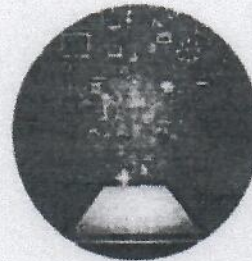


image ref: <http://www.consortworld.com>
image ref: Selected by freepik

Key Highlights

- เรียนรู้หลักการสร้างสถาปัตยกรรมระบบด้านเทคโนโลยีสารสนเทศ เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการตามยุทธศาสตร์ขององค์กร
- เข้าใจการจัดทำสถาปัตยกรรมระบบที่บูรณาการด้านเทคโนโลยีสารสนเทศเข้ากับกระบวนการธุรกิจอย่างเป็นระบบเพื่อการเติบโตของธุรกิจอย่างต่อเนื่องและยั่งยืน
- เห็นความสัมพันธ์ระหว่างสถาปัตยกรรมระบบกับแผนกลยุทธ์ด้านไอซีที เพื่อการบรรลุวิสัยทัศน์และพันธกิจขององค์กร พร้อมกรณีศึกษา
- เจาะลึกแนวทางการทำกับดักแลสถาปัตยกรรมระบบ บทบาทหน้าที่ของผู้รับผิดชอบ และกระบวนการที่เกี่ยวข้อง
- แนะนำ Software Tools ประเภท Open Source และการใช้งาน สำหรับการจัดทำสถาปัตยกรรมระบบ
- ฝึกปฏิบัติเข้มข้นการจัดทำสถาปัตยกรรมระบบจากกระบวนการและระบบงานทางธุรกิจที่ใช้เป็นกรณีศึกษาพร้อมทั้งร่วมอภิปรายแชร์ประสบการณ์เพื่อการนำไปใช้ได้จริงในองค์กร



หลักสูตรฝึกอบรมเชิงปฏิบัติการการจัดทำสถาปัตยกรรมระบบขององค์กร รุ่นที่ 6 (Enterprise Architecture Workshop: EAW)

การขับเคลื่อนธุรกิจที่ยั่งยืนจำเป็นต้องพึ่งพาเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ การวางแผนความเชื่อมโยงระหว่างเทคโนโลยีสารสนเทศ (Information Technology) กับธุรกิจ (Business) จึงเป็นสิ่งสำคัญที่หลายๆ องค์กรมองข้ามไป ซึ่งเป็นผลทำให้เกิดความล้มเหลวของการใช้เทคโนโลยีสารสนเทศในองค์กรตามมา อาทิ การใช้เทคโนโลยีสารสนเทศไม่เต็มประสิทธิภาพ เกิดการลงทุนที่ซ้ำซ้อน ไม่สอดคล้องและไม่ตอบโจทย์กับวิสัยทัศน์ขององค์กร

การจัดทำสถาปัตยกรรมระบบขององค์กรเป็นการบูรณาการระบบเทคโนโลยีสารสนเทศเข้ากับธุรกิจอย่างเป็นระบบ ซึ่งก่อให้เกิดแผนกลยุทธ์ด้านระบบเทคโนโลยีสารสนเทศทั้งระยะสั้นและระยะยาว โดยแสดงให้เห็นความเชื่อมโยงกันใน 4 ระดับ ระหว่าง กระบวนการทางธุรกิจ (Business Processes) ข้อมูล (Data) ระบบงาน (Application) และ เทคโนโลยีสารสนเทศสนับสนุน (Related Information Technology) ที่รองรับกับความต้องการของผู้ที่เกี่ยวข้องทั้งปัจจุบันและอนาคต สามารถผลักดันให้องค์กรดำเนินการตามนโยบายและวิสัยทัศน์ขององค์กรที่กำหนดไว้ได้

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่ให้ความรู้และความเข้าใจเกี่ยวกับการจัดทำสถาปัตยกรรมระบบขององค์กร เพื่อให้ผู้เข้าร่วมอบรมเข้าใจหลักการและองค์ประกอบของสถาปัตยกรรมระบบ กราฟแนวทางการจัดทำสถาปัตยกรรมระบบขององค์กร ฝึกปฏิบัติจัดทำสถาปัตยกรรมระบบขององค์กรจากกรณีศึกษา และสามารถถ่ายทอดความรู้ที่ได้กลับไปปรับใช้งานกับองค์กรของตนเองได้รวม 18 ชั่วโมง / 3 วันทำการ

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

หลักสูตรนี้เหมาะสำหรับ

- ผู้บริหารด้านไอซีทีในทุกระดับ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ
- ผู้จัดการด้านไอซีที
- เจ้าหน้าที่ทางเทคนิคด้านไอซีที เช่น ผู้วิเคราะห์และออกแบบระบบ
- ผู้พัฒนาระบบ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย
- เจ้าหน้าที่ฝ่ายแผนงานขององค์กร
- ผู้ตรวจสอบไอซีที

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี

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 V1.2 Certificate

เนื้อหาหลักสูตร ประกอบด้วย

- ทฤษฎี หลักการ และองค์ประกอบของสถาปัตยกรรมระบบ
- ความสำคัญของการจัดทำสถาปัตยกรรมระบบขององค์กร
- กระบวนการการวางแผนกลยุทธ์ด้านไอซีทีกับการจัดทำสถาปัตยกรรมระบบขององค์กร
- แนวทางการกำหนดดูแลสถาปัตยกรรมระบบขององค์กร
- ผู้รับผิดชอบ และหน้าที่ความรับผิดชอบ
- กรณีศึกษาการวางแผนกลยุทธ์ด้านไอซีทีกับการจัดทำสถาปัตยกรรมระบบขององค์กร โดยมีการจัดลำดับโครงการด้านระบบงานตามลำดับความสำคัญของโครงการในการบรรลุซึ่งวิสัยทัศน์และพันธกิจขององค์กร
- การแนะนำ Software Tools และการใช้งาน Software สำหรับใช้ในการจัดทำสถาปัตยกรรมระบบ
- การฝึกปฏิบัติในการจัดทำจัดทำสถาปัตยกรรมระบบขององค์กร ร่วมกับซอฟต์แวร์ ที่สามารถนำไปปฏิบัติได้จริง

รูปแบบการวัดอบรม

อบรม Online ผ่านโปรแกรม zoom

ระยะเวลาหลักสูตร

ระหว่างวันที่ 2 - 4 พฤศจิกายน 2565
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

ค่าลงทะเบียน

ท่านละ 18,500 บาท (รวมภาษีมูลค่าเพิ่ม)

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

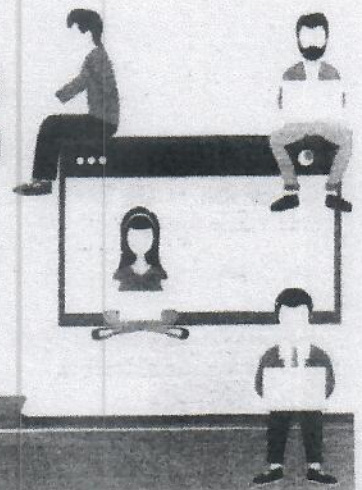
หมายเหตุ

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

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

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

ITPE Examination



เมื่อโลกเปลี่ยน คุณต้องปรับสัการทำงานในยุคดิจิทัลด้วย ITPE
มาตรฐานวิชาชีพไอทีระดับสากล

ITPE คืออะไร?

โครงการสอบมาตรฐานวิชาชีพไอที หรือ Information Technology Professional Examination (ITPE) เป็นการสอบวัดระดับความรู้และทักษะพื้นฐานด้านไอทีเพื่อยกระดับคุณภาพการทำงานอย่างมืออาชีพซึ่งได้รับการรับรองเกณฑ์การวัดความรู้ไอทีที่เป็นมาตรฐานสากลแบบไมอิงผลสัมฤทธิ์ ระหว่างกลุ่มภาคีอีอีอี ประเทศไทย (Information Technology Professionals Examination Council : ITPEC) คือ ญี่ปุ่น ฟิลิปปินส์ เวียดนาม พม่า มองโกเลีย บังกลาเทศ และประเทศไทย

👤 หลักสูตรนี้เหมาะกับใคร?



บุคลากรด้านไอที



นักวิชาการ



นักวิเคราะห์ทุกสาขา



นักศึกษา



บุคคลทั่วไปที่สนใจสอบเทียบความรู้ด้านไอที

สอบผ่านแล้วได้อะไร?

- ใบประกาศนียบัตรระดับภูมิภาค รับรองโดยภาคีสมาชิก ITPEC
- สามารถรับงานจากกลุ่มประเทศในภาคีได้
- สิทธิพิเศษคัดเลือกทำงานในองค์กรชั้นนำของประเทศ
- สิทธิพิเศษคัดเลือกเข้ารับทุนฝึกอบรมของประเทศญี่ปุ่น
- ขอ Work Permit ทำงานในประเทศญี่ปุ่น (ระดับ FE และ AP)
- ปรับวุฒิให้กับบุคลากรที่ไม่มีพื้นฐานการศึกษาสายไอที พัฒนาความรู้ให้ตรงกับความต้องการของตลาดแรงงาน
- เป็นแนวทางเพื่อใช้เป็นเกณฑ์ประเมิน IT Competencies สำหรับบุคลากรสายงาน IT และ Non-IT และเป็นเครื่องมือในการเติมเต็มช่องว่าง (Gap Filling) ในการวางแผนพัฒนาบุคลากร
- ประกอบการสรรหา คัดเลือก เลื่อนขั้น ปรับตำแหน่ง ของบุคลากร

กำหนดการสอบ

จัดสอบปีละ 2 ครั้ง

โดย ศูนย์สอบของมหาวิทยาลัยเครือข่ายทั่วประเทศ

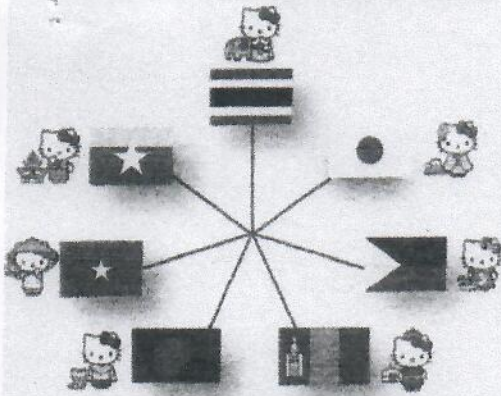
📊 ระดับที่เปิดสอบ

3 Applied Information Technology Engineers Examination (AP)
บุคคลที่ประยุกต์ความรู้และทักษะที่จำเป็นในการเป็นทรัพยากรบุคคล ที่ล้ำหน้า และเป็นผู้กำหนดทางเดินของตนเองอย่างชัดเจน (ค่าลงทะเบียน ท่านละ 2,000 บาท)

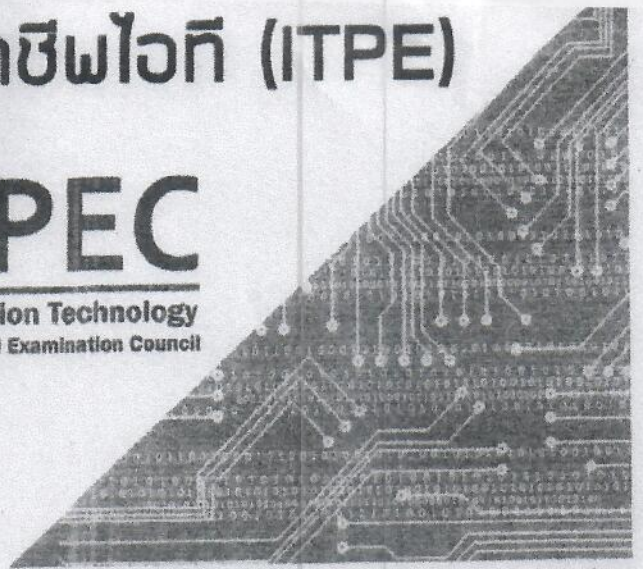
2 Fundamental Information Technology Engineers Examination (FE)
บุคคลที่ยกระดับให้ตนเองเป็นทรัพยากรบุคคลด้านเทคโนโลยีที่ล้ำหน้า (ค่าลงทะเบียน ท่านละ 1,500 บาท)

1 Information Technology Passport Examination (IP)
บุคคลที่มี ความรู้พื้นฐานทางเทคโนโลยีสารสนเทศ (ค่าลงทะเบียน ท่านละ 1,000 บาท)

โครงการสอบมาตรฐานวิชาชีพไอที (ITPE)



ITPEC
Information Technology
Professional Examination Council



"เมื่อโลกเปลี่ยน...และคุณต้องปรับสู่การทำงานไอทีอย่างมีประสิทธิภาพ มาตรฐานวิชาชีพระดับสากล"

"เพื่อก้าวสู่เส้นทางไอทีสากลอย่างมืออาชีพ เรามี Passport นำทางสู่การทำงานด้านไอทีอย่างมีประสิทธิภาพเพิ่มโอกาส
และประโยชน์ในการพัฒนาความรู้และทักษะมาตรฐานด้านไอที"

ระดับที่เปิดสอบ

☑ Information Technology Passport Examination (IP)

Period	Exam Style	Number of Questions	Time	Point	Pass
Morning Exam (09.30-11.30)	Multiple - choice (1 out of 4 choices)	100 questions, answers required for all questions - Strategy 35% - Management 20% - Technology 45%	120 minutes	100	Total point : at least 55% of maximum total points Conditions: at least 30% of the maximum field points in each of the 3 fields

☑ Fundamental Information Technology Engineers Examination (FE)

Period	Exam Style	Number of Questions	Time	Point	Pass
Morning Exam (09.30-12.00)	Multiple - choice (1 out of 4 choices)	80 questions, answers required for all questions	150 minutes	100	60%
Afternoon Exam (13.30-16.00)	Multiple - choice	8 questions, answers required for 7 questions	150 minutes	100	60%

☑ Applied Information Technology Engineers Examination (AP)

Period	Exam Style	Number of Questions	Time	Point	Pass
Morning Exam (09.30-12.00)	Multiple - choice (1 out of 4 choices)	80 questions, answers required for all questions	150 minutes	100	60%
Afternoon Exam (13.30-16.00)	Multiple - choice, short answers and short descriptions	7 questions, answers required for 6 questions	150 minutes	100	60%