



ที่ อบ ๐๐๓๒.๐๑๐ /ว ๘๖๒๐

สำนักงานสาธารณสุขจังหวัดอุบลราชธานี
ถนนพรหมเทพ อบ ๓๔๐๐๐

๑๒ ตุลาคม ๒๕๖๓

เรื่อง ขอประชาสัมพันธ์

เรียน ผู้อำนวยการโรงพยาบาลสรรพสิทธิประสงค์, ผู้อำนวยการโรงพยาบาลทั่วไป, ผู้อำนวยการโรงพยาบาลชุมชนทุกแห่ง และสาธารณสุขอำเภอทุกอำเภอ

- สิ่งที่ส่งมาด้วย
๑. สำเนาหนังสือวิทยาลัยพยาบาลบรมราชชนนี กรุงเทพ ที่ สธ ๑๑๐๓.๐๑/๒๒๗๒ ลงวันที่ ๒๓ กันยายน ๒๕๖๓ จำนวน ๑ ชุด
 ๒. สำเนาหนังสือสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๒๐๑.๐๒/ว ๖๒๗ ลงวันที่ ๖ ตุลาคม ๒๕๖๓ จำนวน ๑ ชุด
 ๓. สำเนาหนังสือสำนักงานเขตสุขภาพที่ ๑๐ ที่ สธ ๐๒๓๕/ว ๑๓๐๑ ลงวันที่ ๒ ตุลาคม ๒๕๖๓ จำนวน ๑ ชุด
 ๔. สำเนาหนังสือชมรมพยาบาลและบุคลากรด้านจักษุไทย ที่ ขพบจ ๒๕๖๓/๐๑ ลงวันที่ ๑๗ กันยายน ๒๕๖๓ จำนวน ๑ ชุด

ด้วย สำนักงานสาธารณสุขจังหวัดอุบลราชธานี ขอส่งสำเนาหนังสือประชาสัมพันธ์การเข้าร่วมการอบรม และการประชุม ให้บุคลากรในหน่วยงานของท่านทราบ ดังนี้

๑. สำเนาหนังสือวิทยาลัยพยาบาลบรมราชชนนี กรุงเทพ ที่ สธ ๑๑๐๓.๐๑/๒๒๗๒ ลงวันที่ ๒๓ กันยายน ๒๕๖๓ เรื่อง ขอความอนุเคราะห์ประชาสัมพันธ์ข่าวการรับสมัครหลักสูตรฝึกอบรมการพยาบาลเฉพาะทาง สาขาการพยาบาลเวชปฏิบัติฉุกเฉิน รุ่นที่ ๑ จำนวน ๑ ชุด
 ๒. สำเนาหนังสือสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๒๐๑.๐๒/ว ๖๒๗ ลงวันที่ ๖ ตุลาคม ๒๕๖๓ เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมโครงการฝึกอบรมออนไลน์ จำนวน ๑ ชุด
 ๓. สำเนาหนังสือสำนักงานเขตสุขภาพที่ ๑๐ ที่ สธ ๐๒๓๕/ว ๑๓๐๑ ลงวันที่ ๒ ตุลาคม ๒๕๖๓ เรื่อง ขอความอนุเคราะห์ประชาสัมพันธ์การรับสมัครเข้าศึกษาอบรมหลักสูตรการพยาบาลเฉพาะทาง สาขาการพยาบาลเวชปฏิบัติฉุกเฉิน จำนวน ๑ ชุด
 ๔. สำเนาหนังสือชมรมพยาบาลและบุคลากรด้านจักษุไทย ที่ ขพบจ ๒๕๖๓/๐๑ ลงวันที่ ๑๗ กันยายน ๒๕๖๓ เรื่อง ขอเชิญเข้าร่วมประชุมวิชาการพยาบาลจักษุ ครั้งที่ ๒๑ ประจำปี ๒๕๖๓ จำนวน ๑ ชุด
- จึงเรียนมาเพื่อทราบและประชาสัมพันธ์ให้ผู้สนใจทราบโดยทั่วกัน

เรียน ผอ.รพ.เดชอุดม

เพื่อโปรดทราบ

เพื่อโปรดพิจารณา

- 15 ต.ค. 63 - HRD

15 ต.ค. 63

ขอแสดงความนับถือ

(นายพิทักษ์พงษ์ จันทร์แดง)

ร.ก.นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)

ปฏิบัติราชการแทนนายแพทย์สาธารณสุขจังหวัดอุบลราชธานี

กลุ่มงานบริหารทรัพยากรบุคคล
โทรศัพท์ ๐ ๔๕๒๖ ๒๖๙๒
โทรสาร ๐ ๔๕๒๔ ๓๓๐๑
(ฐานตามักค์ ๐๘ ๑๔๗๐ ๓๙๑๑)

ทราบ เห็นชอบ

เห็นควรแจ้ง.....

15 ต.ค. 63

ผู้อำนวยการกองกลาง
เลขรับ... 13844
วันที่ 25/9/63
เวลา 11.03 น.



กลุ่มสารบรรณ
เลขรับ 14349
วันที่ 25/09/63
เวลา 10.14 น.

กระทรวงสาธารณสุข
เลขรับ 465178
วันที่ 5 ก.ย. ๒๕๖๓
เวลา 07.26

ที่ อว ๖๕๐๑.๒๕/ว ๑๘๗๘

สำนักส่งเสริมและฝึกอบรม
มหาวิทยาลัยเกษตรศาสตร์
๕๐ ถนนงามวงศ์วาน จตุจักร
กรุงเทพฯ ๑๐๙๐๐

๑๔ กันยายน ๒๕๖๓

ห้องรองปลัดกระทรวงฯ
น.พ.ณรงค์ สายวงศ์
เลขรับ 7692
วันที่ 29/9/63
เวลา 13.53

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมโครงการฝึกอบรมออนไลน์

เรียน ผู้บริหาร / หัวหน้าหน่วยงาน / ผู้อำนวยการฝ่ายฝึกอบรม / ฝ่ายทรัพยากรบุคคล / ผู้จัดการ / ผู้สนใจ
สิ่งที่ส่งมาด้วย โครงการฝึกอบรมออนไลน์หลักสูตร “การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเข้าสู่
สายงาน White-Hat Hackers”

ด้วยมหาวิทยาลัยเกษตรศาสตร์ โดยสำนักส่งเสริมและฝึกอบรม ร่วมกับ สำนักงานส่งเสริม
เศรษฐกิจดิจิทัล มีกำหนดจัดโครงการฝึกอบรมออนไลน์หลักสูตร “การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซ
เบอร์ เพื่อเข้าสู่สายงาน White-Hat Hackers” ระหว่างวันที่ ๑๔ - ๑๗ ธันวาคม ๒๕๖๓ จำนวน ๕๐ คน โดยมี
วัตถุประสงค์ เพื่อพัฒนาบุคลากรด้าน White-Hat Hacker เพื่อรองรับความต้องการในภาคอุตสาหกรรมและ
เสริมสร้างความแข็งแกร่งของระบบสารสนเทศของประเทศไทย ดังรายละเอียดเอกสารของโครงการที่แนบมา
พร้อมนี้

สำนักส่งเสริมและฝึกอบรม พิจารณาเห็นว่า การฝึกอบรมดังกล่าวจะช่วยเพิ่มพูนความรู้
ทักษะ และประสบการณ์ให้แก่ผู้เข้ารับการฝึกอบรมได้เป็นอย่างดี อันจะก่อให้เกิดประโยชน์ต่อองค์กรและ
ประเทศนั้น สำนักส่งเสริมและฝึกอบรม จึงใคร่ขอความอนุเคราะห์การประชาสัมพันธ์และสนับสนุนให้บุคลากร
ที่มีความสนใจเข้าร่วมโครงการฝึกอบรมออนไลน์หลักสูตร “การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซ
เบอร์ เพื่อเข้าสู่สายงาน White-Hat Hackers” ครั้งนี้

สำนักส่งเสริมและฝึกอบรมหวังเป็นอย่างยิ่งว่า จะได้รับความอนุเคราะห์จากท่านในการ
ประชาสัมพันธ์ให้บุคลากรสามารถเข้าร่วมฝึกอบรมในบึงประมาณ พ.ศ. ๒๕๖๓ นี้ด้วย และขอขอบคุณมา ณ
โอกาสนี้

๑) เรียน ปลัดกระทรวงสาธารณสุข
เพื่อโปรดทราบและเห็นควรแจ้ง
หน่วยงานในสังกัด สช. ทราบ
จะเป็นพระคุณ

(นางสุวิธิตา ทุนดี)
ผู้อำนวยการกองกลาง
๒๕ ก.ย. ๒๕๖๓

ขอแสดงความนับถือ

๓๓ น
(รองศาสตราจารย์สุวิสา พัฒนเกียรติ)
ผู้อำนวยการสำนักส่งเสริมและฝึกอบรม

๒) - ทราบ
- มอบ กองกลาง แจ้งเวียนหน่วยงานในสังกัด สช.

๓) สารบรรณ (๒๗ ก.ย. ๖๓)
โปรดดำเนินการแจ้งเวียน

(นางสาวนงดิยา ทองเงิน)
หัวหน้ากลุ่มสารบรรณ
๓๐ ก.ย. ๒๕๖๓

ฝ่ายฝึกอบรม สำนักส่งเสริมและฝึกอบรม
โทรศัพท์ ๐-๒๕๔๒-๘๘๒๒ ต่อ ๒๐๓, ๒๐๔, ๒๐๘
โทรสาร ๐-๒๕๔๒-๘๘๓๐

(นายณรงค์ สายวงศ์)
รองปลัดกระทรวงสาธารณสุข ปฏิบัติราชการแทน
๒๕ ก.ย. ๒๕๖๓

ร.ป. ๗๖๖๑

**โครงการฝึกอบรมการพัฒนาคุณภาพด้านความมั่นคง
ปลอดภัยไซเบอร์ เพื่อเข้าสู่สายงาน**

White-Hat Hackers

ระหว่างวันที่ ๑๔ - ๑๗ ธันวาคม ๒๕๖๓

โดย สำนักงานส่งเสริมเศรษฐกิจดิจิทัล

ร่วมกับ สำนักส่งเสริมและฝึกอบรม มหาวิทยาลัยเกษตรศาสตร์

๑. หลักการและเหตุผล

เทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security) เป็นหนึ่งในเทคโนโลยีที่จำเป็นในการนำประเทศไทยเข้าสู่ยุคเศรษฐกิจดิจิทัล เนื่องจากระบบสารสนเทศในโลกไซเบอร์และธุรกิจที่พึ่งพาระบบดังกล่าวจะสามารถดำเนินต่อไปได้จะต้องได้รับการปกป้องดูแลในแง่ของการรักษาความลับ (Confidentiality) ความพร้อมใช้งาน (Availability) และความสมบูรณ์ของข้อมูล (Integrity) ตามระดับที่ยอมรับได้ขององค์กร หรือธุรกิจนั้นๆ หากระบบดังกล่าวถูกโจมตีหรือแฮค (Hack) โดยผู้ประสงค์ร้ายหรือแฮคเกอร์ (Hacker หรือที่เรียกจะงาว่า Black-Hat Hacker) นั้นย่อมทำให้องค์กรนั้นได้รับความเสียหายในข้อมูล อันจะผลกระทบด้านเศรษฐกิจ สังคม รวมถึงความน่าเชื่อถือขององค์กรนั้น ดังนั้น องค์กรจึงจำเป็นต้องตระหนักตรวจสอบและทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศของตนเองอย่างสม่ำเสมอ ตั้งแต่การวางแผนและออกแบบทั้งในส่วนจากระบบของทางเทคนิค นโยบาย แนวปฏิบัติ และ กัลยภัณฑ์ ซึ่งรวมถึงการทดสอบการโจมตีระบบของตนเองโดยมอบหมายให้แฮคเกอร์เป็นผู้ทำการทดสอบระบบให้ แฮคเกอร์ลักษณะนี้เรียกว่า White-Hat Hacker ซึ่งเป็นแฮคเกอร์ที่สุจริต โดยมีหน้าที่ทดสอบการโจมตีระบบขององค์กรเอง ตามที่องค์กรนั้นได้รับมอบหมาย เพื่อให้เห็นช่องโหว่และความเสี่ยงของระบบนั้น

ปัจจุบัน White-Hat Hacker เป็นที่ต้องการอย่างสูงในระเทศไทยและทั่วโลก เนื่องจากภาคธุรกิจและองค์กรได้เพิ่มพอบุคลากรที่พัฒนาตนเองมักจะไม่สามารถทดสอบได้ครอบคลุมและลึกได้เพียงพอ อีกทั้งยังมีความรู้ของผู้พัฒนาระบบมักจะจำกัดเฉพาะตัวเกินไป ซึ่งไม่ครอบคลุมถึง

- วันที่ ๓ ๑๔.๐๐-๑๖.๐๐ Penetration Testing
 - What is penetration testing
 - Vulnerability assessment vs penetration testing
 - Penetration testing methodology
 - Penetration testing phases
 - Penetration testing Report Example
- Penetration Testing Tools (LAB)
- Kali Linux
- Hacking Web Servers
 - Webserver Concepts
 - Webserver Attacks
 - Attack Methodology
 - Web Server Attack Tools
 - Web Server Attack Tools (LAB)
- Kali Linux
- ๑๓.๐๐-๑๖.๐๐ Hacking Web Applications
 - Web App Concepts
 - Web App Threats
 - Hacking Methodology
 - Web Application Hacking Tools
 - Web Application Hacking Tools (LAB)
- Kali Linux
- วันที่ ๔ ๑๕.๐๐-๑๖.๐๐ System Hacking
 - Cracking Passwords ,Escalating Privileges
 - Executing Application , Hiding Files , Covering Tracks
 - System Hacking Tools (LAB)
- Kali Linux
- ๑๓.๐๐-๑๖.๐๐ Metasploit
 - Introduction , Metasploit Fundamentals , Information Gathering , Client Side Attack , MSF Post Exploitation
 - Maintaining Access , Covering Track , Metasploit: Tool (LAB)
- Kali Linux



สนใจสมัครอบรมได้ทางคิวอาร์โค้ด

- Security Architecture
- Network Security
- Security Assessment and Testing
- Security Operations
- Software Development Security
- ๑๓.๐๐-๑๖.๐๐ Legal and Ethical Issues In Security
 - Legal Issues
 - Security and Privacy Act in Thailand
 - International Security Standard
 - Ethical Issues
 - Case Studies
- วันที่ ๖ ๑๕.๐๐-๑๖.๐๐ Introduction to Penetration Testing
 - ภัยคุกคาม ช่องโหว่ ที่เกิดขึ้นในปัจจุบัน
 - เรียนรู้คำศัพท์ที่เกี่ยวข้อง
 - What is Hacking?
 - Who is a Hacker?
 - Hacker Classes
- Information Gathering: Footprinting and Reconnaissance
 - Footprinting Concepts
 - Footprinting Threats
 - Footprinting Methodology
 - Footprinting Tools
- ๑๓.๐๐-๑๖.๐๐ Scanning Networks
 - Types of Scanning
 - Scanning Methodology
 - Scanning Techniques
 - Scanning Tools
- Vulnerability assessment
 - Vulnerability assessment methodology
 - What is a vulnerability assessment?
 - What is the CVE?
 - What is the CVSS?
 - Vulnerability assessment process
 - Vulnerability Scanning Tools
- Vulnerability Scanning Tools (LAB)
 - Nessus
 - OpenVAS

การจากระบบ ดังนั้น ประเทศไทยจึงจำเป็นต้องพัฒนาบุคลากรด้าน White-Hat Hacker เพื่อรองรับความต้องการในภาคอุตสาหกรรมและเพื่อเสริมสร้างความแข็งแกร่งของระบบสารสนเทศของประเทศไทย ในเนื้อหาของ การพัฒนาบุคลากรให้เข้าเรียนอบรมจะครอบคลุมองค์ความรู้ที่จำเป็น ตั้งแต่เทคโนโลยีสำหรับ Ethical Hacker (การแฮคอย่างมีจริยธรรม) ความรู้พื้นฐานที่จำเป็นด้าน Cybersecurity กฎหมายและจริยธรรมที่เกี่ยวข้อง และมาตรฐานอุตสาหกรรมสากลด้าน Cybersecurity ซึ่งทั้งหมดนี้จะช่วยให้ผู้เข้า การพัฒนาได้ป้องกันความรู้ที่จะช่วยให้ต่อยอดในการทำงานด้าน White-Hat Hacker ได้อย่างมีประสิทธิภาพ

ส่วนักส่งเสริมและฝึกอบรมมหาวิทยาลัยเกษตรศาสตร์ เป็นหน่วยงานที่มีภารกิจในการให้บริการวิชาการแก่องค์กรภาครัฐและภาคเอกชน โดยเป็นหน่วยปฏิบัติงานในการเป็นที่ปรึกษาเพื่อจัดฝึกอบรมพร้อมทั้งองค์ ความรู้ของกองกลางจากภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ ที่ เป็นผู้มีความรู้และมีประสบการณ์ในด้านนี้เป็นอย่างดี โครงการนี้ประกอบด้วย ผู้สอนทั้งสิ้น ๓ ท่านซึ่งได้รับประกาศียบัตรสาขาที่เกี่ยวข้อง เช่น Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), IRCA ISO/IEC ๒๗๐๑๑ Lead Auditor, Cisco Certified Network Associate (CCNA) เป็นต้น ซึ่งจะทำการให้บริการให้บริการวิชาการบรรลุ วัตถุประสงค์ของโครงการได้เป็นอย่างดี

๒. วัตถุประสงค์

๑. เพื่อพัฒนากลุ่มคนและบุคลากรในเทคโนโลยี ด้าน White-Hat Hackers สำหรับป้อนเข้าสู่อุตสาหกรรม
๒. เพื่อเสริมสร้างองค์ความรู้ด้านกฎหมายและจริยธรรมในการเป็น White-Hat Hackers รวมถึงการทดสอบและตรวจสอบ Cyber security อย่างมีจริยธรรมและไม่ขัดต่อกฎหมาย
๓. เพื่อให้ทราบองค์ความรู้ด้าน Cyber security ใน Domain ต่างๆ ที่ จำเป็นก่อนที่จะเป็น White-Hat Hackers
๓. คุณสมบัติผู้เข้าฝึกอบรม
 ๑. สามารถใช้งานระบบปฏิบัติการ Linux เบื้องต้นได้
 ๒. สามารถทำความเข้าใจและ/หรือเขียนโปรแกรมภาษาใดภาษาหนึ่งเบื้องต้นได้เช่น PHP, JavaScript, JAVA, C#, Python

รวมทั้ง HTML หมายถึงจำเป็นต้องใช้ในการฝึกอบรม: -เครื่องเน็ตบุ๊ก คอมพิวเตอร์ดีดระบบปฏิบัติการขั้นต่ำ Windows ๗ ๖๔ bits, CPU Core i๕ Gen ๔ ขึ้นไป หน่วยความจำไม่ต่ำกว่า ๔ GB, พื้นที่ Hard disk ไม่ต่ำกว่า ๑๐๐ G

๔. จำนวนผู้เข้าร่วมฝึกอบรม ผู้เข้าฝึกอบรม จำนวน ๕๐ คน

๕. กำหนดระยะเวลาและสถานที่ฝึกอบรม ระหว่างวันที่ ๑๔ - ๑๗ ธันวาคม ๒๕๖๓ จำนวน ๔ วัน/ละ ๖ ชั่วโมง

๖. วิทยากร

๑. ศ.ดร.เพทฤทธิ บัณฑิตวัฒนาวงศ์ ที่ปรึกษาโครงการและวิทยากร
๒. ดร.ชาติ วรรณทิพัฒน์ ที่ปรึกษาโครงการและวิทยากร
๓. นายเจษฎา ทองแก้วเหลืองที่ปรึกษาโครงการและวิทยากร

๗. กลุ่มกิจกรรมการเรียนรู้

- กิจกรรมประกอบด้วยกิจกรรมผ่านระบบออนไลน์
๑. ใช้รูปแบบ Online ผ่านช่องทางที่เหมาะสม เช่น โปรแกรม WebEx, Microsoft Team, Zoom, Google meet, Google Classroom หรือโปรแกรมที่เหมาะสม โดยเป็นการสอนแบบ Interactive ที่ผู้สอนและผู้รับบริการสามารถโต้ตอบได้ด้วยการถามและเสียง ทั้งนี้ การอบรมใช้รูปแบบ Online แทนวิธีดั้งเดิมแบบ Face-to-Face เพื่อลด ความเสี่ยงอันเนื่องมาจากสถานการณ์ COVID-๑๙
 ๒. การสอนจะใช้เวลาทั้งสิ้น ๔ วัน วันละ ๖ ชั่วโมง (รวมระยะเวลา พักระหว่างเรียน ไม่รวมพักกลางวัน) โดยวันที่ ๑ จะเป็นภาคปูพื้นฐานด้าน เทคโนโลยี Cyber security ใน Domain ต่างๆ และความรู้ด้านกฎหมาย จริยธรรม และมาตรฐานสากลที่จำเป็นต่อการเป็น White-Hat Hacker และวันที่ ๒-๔ จะเป็นการสอนเนื้อหาในส่วนของเทคโนโลยี Ethical Hacker รวมถึง Workshop และ Assignment

๘. โครงสร้างหลักสูตรการฝึกอบรม

รายละเอียด (หัวข้อ)	จำนวนชั่วโมง
๑. Information Security Domains	๓
๒. Legal and Ethical Issues In Security	๓
๓. Introduction to Penetration Testing	๓
๔. Scanning Networks/ Vulnerability assessment/ Vulnerability Scanning Tools (LAB)	๓

๔. Penetration Testing/ Penetration Testing Tools (LAB) ๓
- Hacking Web Servers/ Web Server Attack Tools (LAB)
๖. Hacking Web Applications/Web Application Hacking Tools (LAB) ๓
๗. System Hacking/ System Hacking Tools (LAB) ๓
๘. Metasploit/ Metasploit Tool (LAB) ๓
- กิจกรรม Workshop รวม ๔ วันทำการ ๒๔ ชั่วโมง

๙. ผู้รับผิดชอบโครงการ สำนักส่งเสริมและฝึกอบรม มหาวิทยาลัยเกษตรศาสตร์

๑๐. ตัวชี้วัดโครงการ

๑. มีผู้เข้าร่วมอบรมหลักสูตรไม่น้อยกว่า ๕๐ คน
๒. มีจำนวนผู้เข้าร่วมโครงการที่ผ่านการประเมินผลการเรียนรู้ (การเข้า เรียน การทำงานที่มอบหมาย และการสอบ) ไม่น้อยกว่าร้อยละ ๘๕

๑๑. การประเมินผลโครงการฝึกอบรม

การฝึกอบรมหลักสูตรนี้มีวิธีการประเมินผลจากการวัดความคิดเห็นของผู้เข้ารับการฝึกอบรมต่อการจัดฝึกอบรม โดยใช้แบบประเมินความคิดเห็นต่อ ราชวิทยาลัยการกรม และแบบประเมินความคิดเห็นต่อภาพรวมของโครงการ ฝึกอบรม

๑๒. การรับรองผลการฝึกอบรม

- ผู้เข้ารับการฝึกอบรมจะได้รับประกาศนียบัตรรับรองผลการฝึกอบรม เมื่อปฏิบัติตามข้อกำหนด ดังนี้
๑. ผู้เข้ารับการอบรมจะต้องเข้ารับการทดสอบก่อนและหลังการอบรม (Pretest และ Posttest)
 ๒. เกณฑ์การวัดผลการฝึกอบรม ประกอบด้วย
 - คะแนนการเข้าชั้นเรียนร้อยละ ๖๐
 - คะแนนการทำงานที่ได้รับมอบหมายในช่วงเรียน ร้อยละ ๓๐
 - คะแนนสอบ Posttest ร้อยละ ๕๐
- เกณฑ์ผ่านการฝึกอบรมคือคะแนนรวมไม่ต่ำกว่าร้อยละ ๗๐

กำหนดการฝึกอบรม

วันที่ ๑ ๑๗.๐๐-๑๒.๐๐ Information Security Domains
-Security and Risk Management
-Access Control