

## โครงการอบรมเชิงปฏิบัติการ

“หลักสูตรวิศวกรด้านความมั่นคงปลอดภัยทางสารสนเทศภาครัฐ (Security Engineer) รุ่นที่ ๒”

ศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ

Government Computer Emergency and Readiness Team (G-CERT)

โดย สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

## ๑. หลักการและเหตุผล

ปัจจุบันภาครัฐได้ให้ความสำคัญในการผลักดันนโยบายเศรษฐกิจและสังคมดิจิทัล (Digital Economy) ที่มุ่งเน้นการนำเทคโนโลยีดิจิทัลมาสนับสนุนและขับเคลื่อนภาคเศรษฐกิจและสังคมของประเทศ โดยมีวิสัยทัศน์ที่จะปรับเปลี่ยนประเทศสู่รูปแบบใหม่เพื่อการพัฒนาเข้าสู่เศรษฐกิจดิจิทัลอย่างยั่งยืน โดยหนึ่งในยุทธศาสตร์หลักของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม คือ ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล เพื่อส่งเสริมการสร้างบริการดิจิทัล ซึ่งประกอบไปด้วยการพัฒนารากฐาน และการเปลี่ยนแปลงรูปแบบบริการใหม่ให้แก่การทำงานและการบริการในภาครัฐ เพิ่มความสะดวก รวดเร็วและถูกต้อง ก่อให้เกิดความโปร่งใส และสามารถตรวจสอบได้ ส่งเสริมให้เกิดนวัตกรรมในการให้บริการโดยมีผู้รับบริการทั้งภาคประชาชนและภาคธุรกิจเป็นศูนย์กลาง และให้ทุกภาคส่วนสามารถเข้าถึงข้อมูลของภาครัฐเพื่อนำไปต่อยอดเพิ่มมูลค่าสร้างประโยชน์ทางเศรษฐกิจและสังคมต่อไป

ทั้งนี้ปัจจุบันหน่วยงานภาครัฐยังประสบอุปสรรคในการพัฒนาขีดความสามารถในเชิงดิจิทัล ซึ่งหนึ่งในปัญหาหลักคือการขาดบุคลากรที่มีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยเฉพาะอย่างยิ่งผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศ อันจะทำให้เกิดความไม่เชื่อมั่นต่อการผลักดันการนำธุรกรรมทางดิจิทัลของภาครัฐ โดยตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ เพื่อยกระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ ซึ่งกำหนดให้หน่วยงานภาครัฐจัดทำนโยบายและแนวปฏิบัติฯ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนลดผลกระทบจากกรณีการถูกบุกรุกหรือถูกโจมตี และการถูกคุกคามด้านความมั่นคงปลอดภัย รวมถึงช่วยให้สามารถบริหารความต่อเนื่องและฟื้นฟูระบบได้อย่างรวดเร็วหลังการถูกโจมตี นั้น

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) เล็งเห็นว่ามีความจำเป็นอย่างยิ่งในการเร่งพัฒนาศักยภาพของบุคลากรภาครัฐเพื่อวางแผนและเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เพื่อสร้างความเชื่อมั่นต่อบริการของภาครัฐในยุคดิจิทัล อีกทั้ง สรอ.ยังมีภารกิจในการดำเนินโครงการศูนย์ประสานงานความมั่นคงปลอดภัยทางสารสนเทศภาครัฐ ที่มีวัตถุประสงค์เพื่อส่งเสริม สนับสนุน ให้หน่วยงานภาครัฐเกิดความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์และระบบเครือข่าย รวมถึงการให้คำปรึกษาสำหรับการวางแผนป้องกัน แก้ไขปัญหาจากภัยคุกคามต่างๆ และเป็นศูนย์กลางของหน่วยงานภาครัฐ ในการประสานงานทางด้านการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานภาครัฐ

ด้วยเหตุนี้ทาง สรอ. จึงได้มีแผนการจัดฝึกอบรมเชิงปฏิบัติการ “หลักสูตรวิศวกรด้านความมั่นคงปลอดภัยทางสารสนเทศภาครัฐ รุ่นที่ ๒ หรือ Security Engineer#2” เพื่อให้หน่วยงานของภาครัฐได้ตระหนักถึงการรักษาความมั่นคงปลอดภัยสารสนเทศ และนำไปวางแผนการป้องกันจากภัยคุกคามต่างๆ ที่จะเกิดขึ้นได้อย่างถูกต้องและรวดเร็ว ทั้งนี้เพื่อให้หน่วยงานของภาครัฐได้รับประโยชน์ ในฐานะผู้ใช้บริการ ตลอดจนนำไปประยุกต์ใช้ในการปฏิบัติงานได้จริง

## ๒. วัตถุประสงค์

๒.๑ เพื่อยกระดับความรู้ ความสามารถ ของบุคลากร ให้มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศ ในการดูแลรักษาระบบ ของหน่วยงานภาครัฐในการขับเคลื่อนสู่รัฐบาลดิจิทัล

๒.๒ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยทางสารสนเทศ ให้แก่หน่วยงานภาครัฐ

๒.๓. เพื่อให้บุคลากรที่เข้าร่วมอบรม ได้นำความรู้ ไปประยุกต์ใช้ในการพัฒนา ปรับปรุง ระบบบริการของหน่วยงานภาครัฐให้มีความมั่นคงปลอดภัย

๒.๔ เพื่อสร้างเครือข่ายทางด้านความมั่นคงปลอดภัยทางสารสนเทศของภาครัฐ

๒.๕ เพื่อเป็นการประชาสัมพันธ์ของบริการ G-CERT แก่หน่วยงานภาครัฐ

๒.๖ เพื่อแลกเปลี่ยนองค์ความรู้และสร้างความร่วมมือระหว่าง สรอ. และหน่วยงานที่เข้าร่วมอบรม

## ๓. กลุ่มเป้าหมาย

บุคลากรหน่วยงานภาครัฐที่มีความเกี่ยวข้องกับเนื้อหาในการอบรม หรือผู้ใช้บริการต่างๆ ของ สรอ. โดยมีคุณสมบัติในการเข้าอบรม ดังนี้

๓.๑ เป็นผู้ดูแลระบบ หรือเครื่องให้บริการของหน่วยงานภาครัฐ

๓.๒ มีความรู้พื้นฐานทางด้านเทคโนโลยีสารสนเทศเบื้องต้น เช่น OS : Windows Server, Linux , Network : Firewall, Switch เป็นต้น

๓.๓ สามารถเข้าร่วมการระดมความคิดเห็น เพื่อพัฒนาระบบเทคโนโลยีสารสนเทศของภาครัฐได้

๓.๔ สามารถให้ความร่วมมือในการดำเนินกิจกรรมต่างๆ ของ สรอ. ได้เป็นอย่างดี

๓.๕ สามารถนำ Computer Notebook มาเข้าร่วมอบรมได้

๓.๖ สามารถเข้าร่วมอบรมได้ตลอดหลักสูตร และมีเวลาการอบรมไม่น้อยกว่าร้อยละ ๘๐

*หมายเหตุ: สรอ. ขอสงวนสิทธิ์การคัดเลือกเป็นไปตามหลักเกณฑ์ที่กำหนด*

## ๔. รูปแบบการดำเนินโครงการ

บรรยาย ปฏิบัติการ แลกเปลี่ยนความรู้ กรณีศึกษา และการซักซ้อมรับมือภัยคุกคาม (Incident Drill)

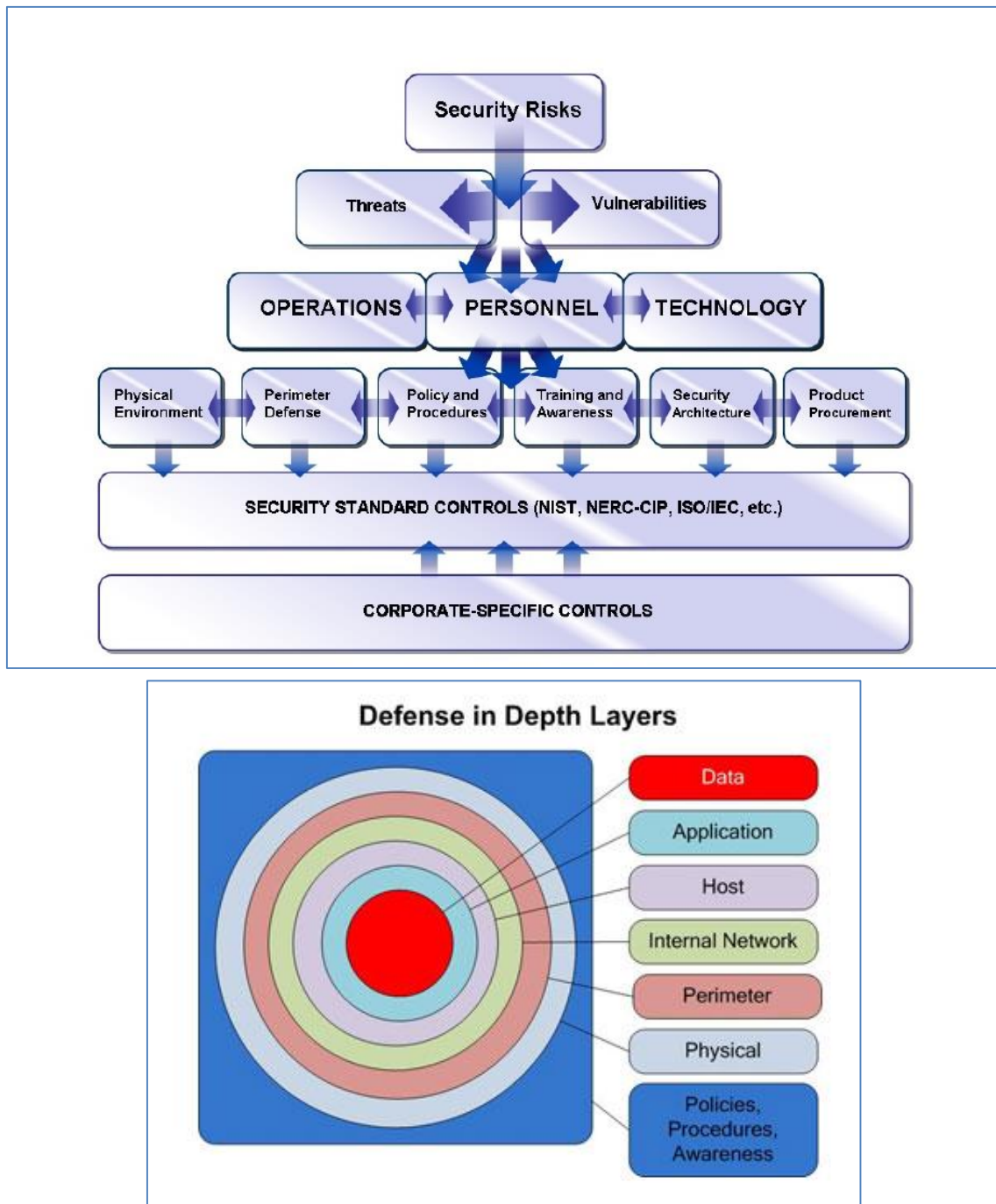
## ๕. จำนวนผู้เข้าร่วมอบรม

จำนวน ๓๐ ท่าน (เฉพาะผู้แทนจากหน่วยงานที่ได้รับหนังสือเชิญให้เข้าร่วมอบรมเท่านั้น)

## ๖. รายละเอียดหลักสูตร

เนื้อหาในการอบรมในหลักสูตรได้มีการจัดลำดับหัวข้อที่จะบรรยายในหลักสูตรเป็นลำดับและแบ่งเป็นหมวดหมู่ สอดคล้องตามชั้น (Layer) ของแนวทางป้องกันความมั่นคงปลอดภัยทางสารสนเทศเชิงลึก (Defense-In-Depth Layer) เพื่อให้ผู้ที่เข้าร่วมการอบรมได้เข้าใจเนื้อหาและสามารถลำดับความคิดได้ทำให้

ง่ายต่อการทำความเข้าใจ ตลอดจนสามารถนำความรู้ที่ได้รับจากการอบรมไปประยุกต์ใช้ในการวางแผนและปฏิบัติงานได้อย่างมีประสิทธิภาพ



แผนภาพที่ ๒: Defense in Depth Layers<sup>2</sup>

โดยแบ่งเนื้อหาการอบรมครอบคลุมดังรายละเอียดต่อไปนี้

<sup>1</sup> อ้างอิงจาก “Recommended Practice: Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies”, October 2009, U.S Department of Homeland Security

<sup>2</sup> อ้างอิงจาก Windows Server 2008 in an Organization’s Defense in Depth Strategy, <http://technet.microsoft.com/en-us/library/cc512681.aspx>

ระยะเวลา	จำนวน	เนื้อหาการอบรม
สัปดาห์ที่ ๑	๒ วัน	<ul style="list-style-type: none"> <li>■ Policies, Procedures, Awareness</li> <li>■ Network Security &amp; Vulnerability Assessment Management</li> </ul>
สัปดาห์ที่ ๒	๒ วัน	<ul style="list-style-type: none"> <li>■ Firewall (pfSense)</li> <li>■ DNSSEC &amp; VPN Secure</li> </ul>
สัปดาห์ที่ ๓	๒ วัน	<ul style="list-style-type: none"> <li>■ Linux Hardening (OS &amp; Services)</li> <li>■ Reverse Proxy (NGINX)</li> </ul>
สัปดาห์ที่ ๔	๒ วัน	<ul style="list-style-type: none"> <li>■ Windows Hardening (OS &amp; Services)</li> <li>■ Application &amp; Data Security</li> </ul>
สัปดาห์ที่ ๕	๒ วัน	Incident Drill : Web Hacking & DDoS
รวม		๑๐ วัน

\*อาจมีการเปลี่ยนแปลงตามความเหมาะสมของเนื้อหาในการอบรม

### ๗. ค่าใช้จ่ายในการอบรม

ไม่มีค่าใช้จ่ายใดๆ ในการเข้าร่วมอบรมหลักสูตรฯ นี้ (อบรมฟรี) เฉพาะหน่วยงานที่ได้รับหนังสือเชิญเข้าร่วมอบรมในโครงการนี้เท่านั้น

### ๘. ระยะเวลาการอบรม

วันที่ ๒ สิงหาคม ถึง ๓๐ สิงหาคม พ.ศ. ๒๕๕๙

หมายเหตุ : อบรมทุกวันจันทร์และอังคาร (สัปดาห์แรกอบรม อังคารและพุธ)

### ๙. เงื่อนไขของการผ่านการอบรม

ผู้เข้าร่วมอบรมที่จะได้รับการพิจารณาว่าผ่านการอบรม และได้รับมอบประกาศนียบัตรหลักสูตรฯ ต้องมีเวลาเข้าร่วมการอบรมตลอดหลักสูตรฯ ไม่น้อยกว่าร้อยละ ๘๐

### ๑๐. ประโยชน์ที่ผู้เข้าอบรมจะได้รับ

- ๑๐.๑ ยกระดับความรู้ ความสามารถของผู้เข้าอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
- ๑๐.๒ สามารถนำองค์ความรู้และประสบการณ์ไปประยุกต์ใช้เพื่อวางแผนด้านความมั่นคงปลอดภัยสารสนเทศในการป้องกันหรือรับมือกับภัยคุกคามต่างๆ ที่อาจจะเกิดขึ้นกับองค์กร
- ๑๐.๓ สร้างเครือข่ายความร่วมมือด้านความมั่นคงปลอดภัยสารสนเทศระหว่างหน่วยงานภาครัฐ
- ๑๐.๔ ส่งเสริมการเรียนรู้และพัฒนากระบวนการรัฐบาลอิเล็กทรอนิกส์

## ๑๑. สอบถามข้อมูลเพิ่มเติม

หากท่านมีข้อสงสัย และ/หรือต้องการทราบรายละเอียดเพิ่มเติม ท่านสามารถสอบถามรายละเอียดได้ที่ สถาบันฝึกอบรมรัฐบาลดิจิทัล ฝ่ายพัฒนารัฐกิจ หมายเลขโทรศัพท์ ๐๒-๖๑๒-๖๐๐๐ ต่อ ๓๖๐๖ (สุกัญญา ฉัตรแก้วมรกต) หรือ ๓๖๐๒ (ฐิติมา รัตนประกาย) อีเมลล์ bda@ega.or.th

### หมายเหตุ

๑. ทาง สรอ. ขอสงวนสิทธิ์ในการเปลี่ยนแปลงรายการโดยมีต้องแจ้งให้ทราบล่วงหน้า
๒. ขอสงวนสิทธิ์ในการเปลี่ยนแปลงการพิจารณา และ/หรือ เปลี่ยนแปลงผู้เข้าร่วมอบรม ทั้งนี้รับพิจารณาเฉพาะหน่วยงานที่ได้รับหนังสือเชิญให้เข้าร่วมอบรมในโครงการนี้เท่านั้น และขออภัยสำหรับความไม่สะดวกมา ณ โอกาสนี้

\*\*\*\*\*

**กำหนดการอบรมเชิงปฏิบัติการ**  
**“หลักสูตรวิศวกรด้านความมั่นคงปลอดภัยทางสารสนเทศภาครัฐ**  
**(Security Engineer) รุ่นที่ ๒”**

โดย สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

ระหว่างวันที่ ๒ สิงหาคม ถึง ๓๐ สิงหาคม พ.ศ. ๒๕๕๙

ณ ห้องอบรม ๓๐๑ ชั้น ๓ อาคารซอฟต์แวร์พาร์ค ถนนแจ้งวัฒนะ จังหวัดนนทบุรี

\*\*\*\*\*

\*\*\*\*\*

**ตารางกำหนดการอบรม**

ครั้งที่	เวลา	หัวข้อ	วิทยากร
ครั้งที่ ๑ วันอังคารที่ ๒ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	
	๐๙.๐๐ - ๐๙.๓๐ น.	ประธานกล่าวเปิดหลักสูตร Security Engineer รุ่น ๒	รอง ผอ.อภิสิทธิ์พร อังกมลเศรษฐ์
	๐๙.๓๐ - ๑๐.๓๐ น.	Principle of security	นายกิตติศักดิ์ จีรวรรณกุล
	๑๐.๔๕ - ๑๒.๐๐ น.	Security Awareness 2016 (Threats & Beyond)	
	๑๓.๐๐ - ๑๖.๓๐ น.	Information Security Management (Policy, Risk, Physical Security and Standard)	
ครั้งที่ ๒ วันพุธที่ ๓ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	
	๐๙.๐๐ - ๑๒.๐๐ น.	Network Security & Monitoring	นายกิตติศักดิ์ จีรวรรณกุล
	๑๓.๐๐ - ๑๖.๓๐ น.	Vulnerability Assessment Management (VA)	นายพงศ์ระพี นาคมณี
ครั้งที่ ๓ วันจันทร์ที่ ๘ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	
	๐๙.๐๐ - ๑๐.๓๐ น.	Introduction to pfSense	นายคมกริช คำสวัสดิ์
	๑๐.๔๕ - ๑๒.๐๐ น.	Installation & Basic command pfSense	
	๑๓.๐๐ - ๑๔.๓๐ น.	Configuration pfSense (Install Services)	
ครั้งที่ ๔ วันอังคารที่ ๙ ส.ค. ๒๕๕๙	๑๔.๔๕ - ๑๖.๓๐ น.	pfSense Package Management	
	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	
	๐๙.๐๐ - ๑๒.๐๐ น.	DNS/DNSSEC	นายธงไชย จารุสุรเกษม
๑๓.๐๐ - ๑๖.๓๐ น.	VPN Secure		
ครั้งที่ ๕ วันจันทร์ที่ ๑๕ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	
	๐๙.๐๐ - ๑๒.๐๐ น.	Basic Linux hardening (OS)	นายคมกริช คำสวัสดิ์
	๑๓.๐๐ - ๑๖.๓๐ น.	Basic Linux hardening (Services)	

ครั้งที่	เวลา	หัวข้อ	วิทยากร
ครั้งที่ ๖ วันอังคารที่ ๑๖ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	นายคมกริช คำสวัสดิ์
	๐๙.๐๐ - ๑๒.๐๐ น.	Introduction & Installation Reverse Proxy (nginx)	
	๑๓.๐๐ - ๑๖.๓๐ น.	Configuration Reverse Proxy (squid)	
ครั้งที่ ๗ วันจันทร์ที่ ๒๒ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	นายพงศ์ระพี นาคมณี
	๐๙.๐๐ - ๑๒.๐๐ น.	Introduction to Microsoft Windows Server	
	๑๓.๐๐ - ๑๖.๓๐ น.	Basic to Hardening Step & Best practice	
ครั้งที่ ๘ วันอังคารที่ ๒๓ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	นายพงศ์ระพี นาคมณี
	๐๙.๐๐ - ๑๒.๐๐ น.	Web services (IIS, Apache) & MBSA	
	๑๓.๐๐ - ๑๖.๓๐ น.	Web Application Security (OWASP & Case study)	
ครั้งที่ ๙ วันจันทร์ที่ ๒๙ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	นายกิตติศักดิ์ จีรวรรณกุล
	๐๙.๐๐ - ๑๒.๐๐ น.	Introduction & Prepare for Case study	
	๑๓.๐๐ - ๑๖.๓๐ น.	Incident Drill : DDoS & Web Hacking	
ครั้งที่ ๑๐ วันอังคารที่ ๓๐ ส.ค. ๒๕๕๙	๐๘.๓๐ - ๐๙.๐๐ น.	ลงทะเบียน	นายกิตติศักดิ์ จีรวรรณกุล
	๐๙.๐๐ - ๑๒.๐๐ น.	Incident Drill : DDoS & Web Hacking	
	๑๓.๐๐ - ๑๔.๓๐ น.	สรุปผลของการซักซ้อม Incident Drill	นายคมกริช คำสวัสดิ์
	๑๔.๓๐ - ๑๕.๐๐ น.	สรุปการอบรมหลักสูตร Security Engineering รุ่นที่ ๒	นายปณิธาน เขินอำนาจ
	๑๕.๐๐ - ๑๖.๓๐ น.	การมอบประกาศนียบัตรผู้สำเร็จหลักสูตร และประธานกล่าวปิดงาน Security Engineer รุ่นที่ ๒	รอง ผอ.อภิสิทธิ์พร อังคมมลเศรษฐ์

หมายเหตุ: \*กำหนดการหลักสูตรอาจมีการเปลี่ยนแปลงตามความเหมาะสม

\*\*ผู้เข้าร่วมอบรมต้องนำ Notebook มาเองในวันที่จัด Workshop ทุกครั้ง