วันที่ 30 กันยายน 2559

รายงานสรุปการฝึกอบรม/สัมมนาภายนอก

เรียน รผบ. ผ่าน ผชก.(นายสุชินฯ) ผอ.ฝทบ. รผก. (CIO) ผอ.ฝทท. ผอ.กปค.

1. ข้าพเจ้า นายอภิวุฒิ ผิวเพชร ตำแหน่ง พนักงานบริหารระบบคอมพิวเตอร์ 6 แผนก คค. กอง กปค. ฝ่าย ฝทท. ได้รับอนุมัติให้ไปเข้าร่วมการฝึกอบรม/สัมมนาหลักสูตร/ เรื่อง หลักสูตร Certified Information Systems Security Professional Preparation (CISSP) จัดโดย บริษัท Vnohow (Thailand) จำกัด ระหว่างวันที่ 29 สิงหาคม ถึง 2 กันยายน 2559 สถานที่จัด ชั้น 6 อาคารบุญมิตร ถ.สีลม กรุงเทพฯ

ค่าลงทะเบียนอบรม/สัมมนา ☑ เสียค่าใช้จ่าย 31,993 บาท ☐ ไม่เสียค่าใช้จ่าย

2. ข้าพเจ้าขอรายงานสรุปการฝึกอบรม/สัมมนา ดังนี้

2.1 สรุปรายละเอียดเนื้อหาของหลักสูตร **Certified Information System Security Professional Preparation (CISSP)** ตามหัวข้อได้ดังนี้

Module 1 : *Security And Risk Management*

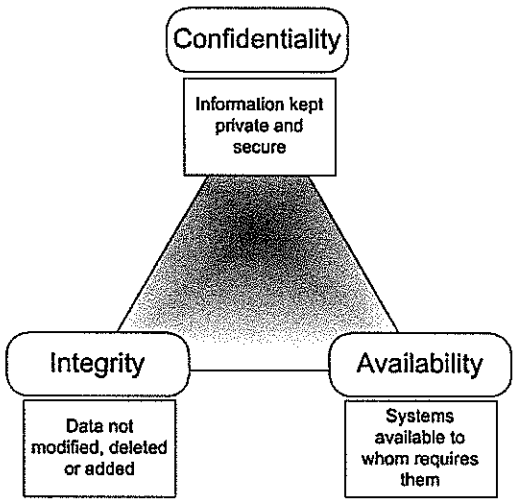
เป็นการอธิบายหลักการพื้นฐาน CIA Concept ในด้านการรักษาความปลอดภัยของระบบสารสนเทศที่มุ่งเน้นด้าน Security ประกอบด้วย Security Object ซึ่งมีหลักแนวคิดจาก CIA Triad มีรายละเอียด ดังนี้

C (Confidentiality) คือ ขั้นตอนหรือกระบวนการ ที่ใช้ในการเก็บรักษาความลับ (Secret) และความถูกต้องของข้อมูล โดยใช้เทคโนโลยีต่างๆเข้ามาช่วย เช่น Cryptography ซึ่งพูดถึงการเข้ารหัสและถอดรหัสข้อมูลเป็นพื้นฐานสำคัญของการศึกษา เทคโนโลยีที่ใช้ในทางปฏิบัติจริง เช่น VPN (Virtual Private Network), SSL (Secure Socket Layer) หรือ PKI (Public Key Infrastructure)

I (Integrity) คือ ขั้นตอนหรือกระบวนการ ที่ใช้ในการปกป้องข้อมูล ให้มีความปลอดภัยมากที่สุด และความสมบูรณ์ตามจริงของข้อมูลเพื่อให้แน่ใจว่าข้อมูลที่ถูกต้องของเราไม่ถูกแก้ไข โดยผู้ที่ไม่ได้รับอนุญาต หรือไม่ถูกเปลี่ยนแปลงโดยแฮกเกอร์/ แครกเกอร์ หรือผู้บุกรุก (Hacker/ Cracker/ Intruder) เพื่อไม่ให้ข้อมูลนั้นถูกนำออกไปสู่ภายนอกได้ หากข้อมูลที่มีความสำคัญโดยเฉพาะข้อมูลที่เกี่ยวข้องกับทางด้าน การเงินนั้นถูกเปลี่ยนแปลงแก้ไขจะส่งผลเสียให้กับองค์กรอย่างมากเพราะข้อมูล นั้นเชื่อถือไม่ได้

A (Availability) คือ ขั้นตอนหรือกระบวนการ ที่ทำให้ระบบมีความพร้อมในการใช้งานให้ได้มากที่สุด เมื่อต้องการใช้งานระบบคอมพิวเตอร์แล้ว ระบบต้องมีความสามารถในการ

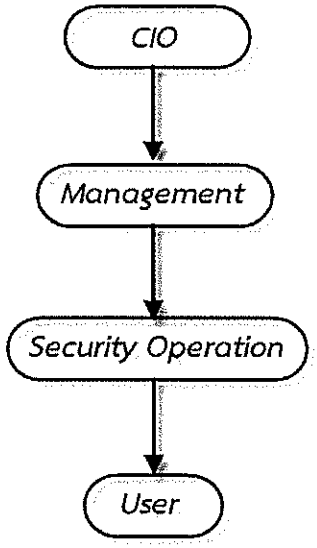
รองรับอยู่เสมอ หรือเมื่อเกิดปัญหาล่มแล้ว ไม่มีระบบสำรองไว้ใช้งานหรือกว่าจะกู้ระบบได้ก็กินเวลานาน ทำให้เกิดปัญหา “Downtime” ซึ่งเป็นต้นเหตุทำให้ไม่สามารถดำเนินงานต่อไปได้ เราจึงควรมีแผนการป้องกันระบบล่มไม่ว่าจะเป็น BCP (Business Continuity Planning) หรือ DRP (Disaster Recovery Planning) เพราะหน่วยงานหลายๆแห่ง ยังคงมองข้ามความสำคัญของเรื่องเหล่านี้อยู่



CIA TRIAD Concept

Security Government Principles เป็นการมุ่งเน้นที่ด้านการวางออกแบบ การบริหารจัดการ ด้านการรักษาความปลอดภัยระบบสารสนเทศ ภายในองค์กรให้เกิดประโยชน์สูงสุด

Security Policies , Standard , Procudures And Guideline เป็นการกำหนดนโยบายด้านการรักษาความปลอดภัยระบบสารสนเทศ โดยผู้บริหารเป็นผู้กำหนด (Policy) แผนการดำเนินการ (Planning), ขั้นตอนการดำเนินการ, กระบวนการตรวจสอบ, การป้องกัน และการประเมินผลอย่างเป็นระบบ จากผู้บริหารสูงสุดขององค์กร



Legal And Regulatory Issues เป็นนโยบายจากทางผู้บริหารองค์กรในด้านสารสนเทศ ที่มีผลทางกฎหมายต่อความมั่นคงปลอดภัย ของระบบสารสนเทศองค์กร เช่น ลิขสิทธิ์ต่างๆ ไม่ว่าจะเป็นทั้งด้าน Hardware และ Software หรือ พ.ร.บ.คอมพิวเตอร์ เป็นต้น

Module 2 : *Asset Security*

เป็นการอธิบายถึงการควบคุมและจำกัด การเข้าถึง ไม่ว่าจะเป็นการบริหารจัดการข้อกำหนดเรื่องการเข้าถึงการใช้งานระบบ หรือสิทธิ์ต่างๆ ในการบริหารจัดการระบบสารสนเทศต่างๆ

Information And Asset Classification เป็นการบริหารจัดการระบบสารสนเทศด้านข้อมูลหรือทรัพย์สินขององค์กรที่มีมูลค่าทางด้าน หากเกิดความเสียหายขึ้น โดยกำหนดเป็นระดับความสำคัญของการเข้าถึง หรือรับรู้ข้อมูลสารสนเทศ ดังนี้

- ลับสุดยอด (Top Secret)
- ความลับ (Secret)
- ลับ (Confidential)
- ไม่เป็นความลับ (Unclassified)

Ownership สิทธิ์และความรับผิดชอบในการดูแลข้อมูลของแต่ละระบบ และระบบสารสนเทศ ตามที่ได้รับมอบหมายจากผู้บังคับบัญชา เพื่อใช้ในการดำเนินการ, กระบวนการตรวจสอบ, การป้องกัน และการประเมินผล อย่างเป็นระบบ จากผู้บริหารสูงสุดขององค์กร

Protect Privacy เป็นการบริหารจัดการด้านข้อมูลส่วนบุคคล ที่เกี่ยวข้องกับระบบสารสนเทศในองค์กรที่ใช้งานอยู่ เพื่อป้องกันปัญหาด้านข้อมูลที่รั่วไหลไปภายนอก และจากผู้ไม่หวังดี ในการเข้ามาโจรกรรมข้อมูลออกไปภายนอกได้

Appropriate Retention เป็นการอธิบายถึงมาตรฐานต่างๆ ในการจัดเก็บรักษาข้อมูลที่เหมาะสม โดยมีการควบคุมการนำเข้าและจัดเก็บของข้อมูล เพื่อนำมาใช้งานได้อย่างมีประสิทธิภาพ ในกรณีเกิดเหตุต่างๆได้

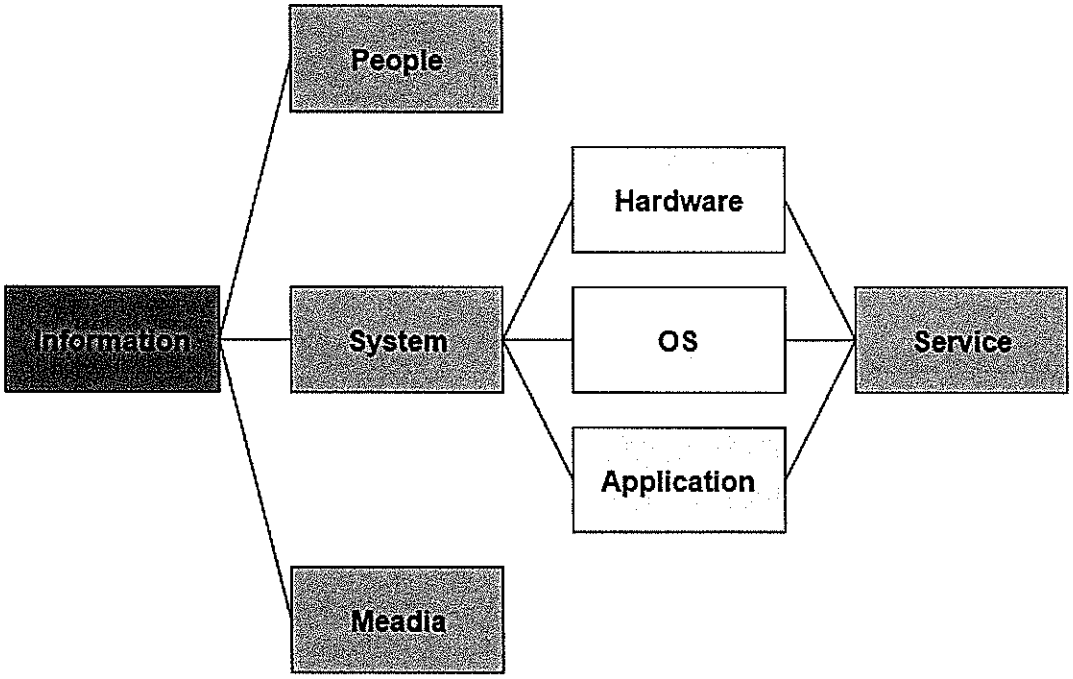
Data Security Controls เป็นการควบคุมด้านความปลอดภัยของข้อมูลสารสนเทศในด้านที่เกี่ยวข้องกับความปลอดภัยของข้อมูล โดยมีการกำหนดมาตรการ ข้อบังคับ ตามมาตรฐานที่กำหนดไว้ หรือมาตรฐานที่องค์กรได้กำหนดไว้เพื่อปฏิบัติตามข้อบังคับ

Handling Requirements เป็นการอธิบายเรื่องของการบริหารจัดการตามความต้องการที่มีเพิ่มเติม ในอนาคต เพื่อให้อยู่ในมาตรฐานด้านความปลอดภัยเดียวกันภายในองค์กรที่กำหนด

Module 3 : *Security Engineering*

เป็นการอธิบายถึงการออกแบบโครงสร้าง และสถาปัตยกรรมด้านความปลอดภัยบนระบบสารสนเทศ โดยมุ่งเน้นด้านการรักษาความปลอดภัยที่ดีที่สุด คือ ในการออกแบบที่ถูกต้องและดำเนินการจัดทำขึ้น รวมไปถึงมีการวางมาตรฐานที่ครอบคลุมในด้านของระบบปฏิบัติการ และโปรแกรมประยุกต์ที่จะนำมาใช้งานร่วมกับผู้ใช้งาน เพื่อไม่ให้เกิดปัญหาเพิ่มเติมในภายหลังได้

Engineering Process เป็นการอธิบายถึงกระบวนการออกแบบทางวิศวกรรมของระบบ เพื่อให้ระบบมีความพร้อมใช้งาน ตอบสนองด้านการใช้งานของผู้ใช้งานและนักพัฒนาโปรแกรมระบบ ให้ระบบมีความเสถียรควบคู่ไปกับความปลอดภัยมากที่สุด ลดปัญหาในเรื่องช่องโหว่ อีกทั้งหาช่องทางแก้ไขปัญหาที่คาดว่าจะเกิดปัญหาด้านภัยคุกคามต่างๆ ที่ส่งผลกระทบและเกิดความเสียหายด้านต่างๆ ในภายหลังได้

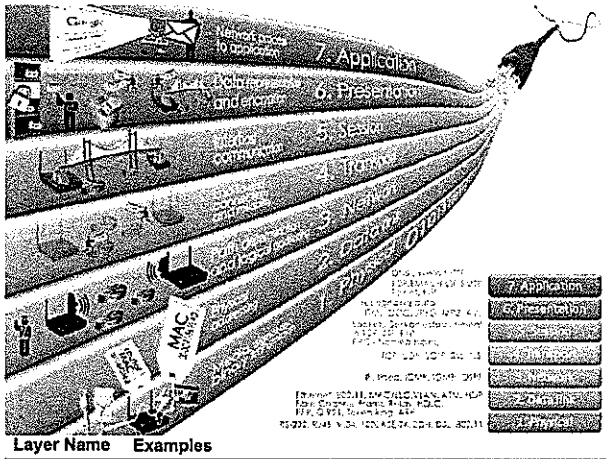


Security Models Fundamental Concepts

Module 4 : *Communication and Network Security*

เป็นการอธิบายถึง โครงสร้างและความปลอดภัยของการเชื่อมต่อระบบเครือข่ายสื่อสารข้อมูล บนพื้นฐานของ (OSI Model) โดยมุ่งเน้นถึงการออกแบบและการเชื่อมต่อระบบเครือข่ายในการใช้งานระบบสารสนเทศให้มีความปลอดภัยมากที่สุดเมื่อใช้งานจริง ไม่ว่าจะเป็นการเชื่อมต่ออุปกรณ์เข้ากับระบบ รวมไปถึงกระบวนการเชื่อมต่อกับอุปกรณ์ระบบเครือข่าย และลดการเกิดช่องโหว่จากการโจมตีใน

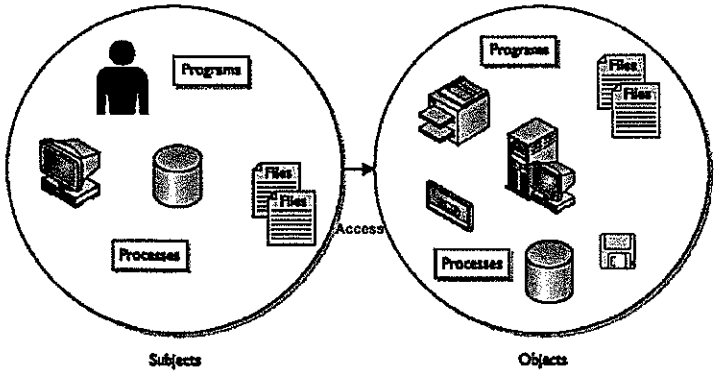
รูปแบบต่างๆ ที่มีผลต่อการหยุดชะงักของการให้บริการระบบ (Down Time) และการกู้คืนระบบให้กลับมาใช้งานได้เร็วที่สุด (Recovery) ซึ่งเป็นการลดความเสี่ยง มีความเสียหายต่อองค์กรให้ได้มากที่สุด



Layer Name	Examples
Application	Telnet, HTTP, FTP, WWW, NFS, SMTP, SNMP
Presentation	JPEG, ASCII, EBCDIC, TIFF, GIF, MPEG, Encryption, MIDI
Session	RPC, SQL, NFS, NetBIOS, Apple Talk, ASP, DECnet
Transport	TCP, UDP, SPX
Network	IP, IPX, Apple Talk
Data Link	IEEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, ATM, 802.5/802.2
Physical	EIA/TIA 232, V.35, EIA/TIA-449, RJ-45

Module 5 : *Identity and Access Management*

เป็นการอธิบายถึง กระบวนการบริหารจัดการในด้านการเข้าถึงข้อมูล และด้านความปลอดภัยระบบสารสนเทศ ทั้งด้าน Hardware, Software และผู้ใช้งาน โดยกระบวนการพิสูจน์ตัวตนและกำหนดสิทธิ์เพื่อควบคุมการเข้าใช้งานในระบบที่เกี่ยวข้อง ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ และวิธีป้องกันการโจมตีในรูปแบบต่างๆ ในอนาคต รวมไปถึงตอบสนองนโยบายด้านความปลอดภัยขององค์กร



Identity and Access Controls Concept

Module 6 : *Security Assessment and Testing*

เป็นการอธิบายถึง วิธีหรือกระบวนการประเมินความปลอดภัยจากการทดสอบหาช่องโหว่ของระบบในด้านความปลอดภัยของระบบสารสนเทศ (Tester and Audit) ทั้งด้าน Hardware และ Software ให้มีความปลอดภัยมากที่สุด และเกิดความเสถียร มีประสิทธิภาพในการทำงานทุกๆด้านที่มีใช้งานระบบสารสนเทศอยู่ภายในองค์กร โดยการนำ Log ต่างๆ ที่ระบบมีใช้งาน มาทำการวิเคราะห์ปัญหา (Analysis) และทำการรายงานผลกระทบที่ทำให้เกิดปัญหาจากช่องโหว่ต่างๆ จากอุปกรณ์ SIEM (Security Information and Event Management) ส่วนการ Tester หรือการทำ Testing Techniques เป็นการทดสอบระบบ จากช่องโหว่ที่มีการตรวจพบ เช่น การ Scan หาช่องโหว่จาก Tool โดยเฉพาะ เพื่อทำการวิเคราะห์และแก้ไขปัญหา ลดความเสี่ยงที่เกิดช่องโหว่ต่อไป โดยมีการแบ่งประเภทของการทดสอบ ดังนี้

- Black-Box คือ ไม่มีข้อมูลของโครงสร้างของระบบที่ทำการทดสอบมาก่อน
- White-Box คือ มีข้อมูลของโครงสร้างของระบบที่ทำการทดสอบในบางส่วน
- Dynamic Testing คือ การทดสอบระบบในขณะที่ระบบกำลังทำงานอยู่
- Static Testing คือ การทดสอบระบบล่วงหน้า ก่อนเปิดใช้งานระบบจริง
- Manual Testing คือ การตรวจสอบว่าผู้ทดสอบนั้น กระทำโดยมนุษย์หรือไม่
- Automated Testing คือ การตรวจสอบว่าผู้ทดสอบนั้น กระทำโดยระบบอัตโนมัติหรือไม่

Module 7 : *Security Operations*

เป็นการอธิบายถึง รูปแบบในการดำเนินงานการรักษาความปลอดภัย ในการบริหารจัดการระบบในด้านความปลอดภัยของระบบสารสนเทศ ให้เป็นไปตามข้อกำหนดมาตรฐานที่ต้องปฏิบัติหรือแบบแผนที่ได้มีการวางแผนไว้ ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพภายในองค์กรมากที่สุด ไม่ว่าจะเป็นการคัดเลือกด้านบุคลากรที่ใช้งานระบบ รวมไปถึงผู้ดูแลระบบ ทั้งด้านการตรวจสอบประวัติต่างๆ ย้อนหลังในเรื่องที่เกี่ยวข้องกับระบบนั้นๆ เพื่อควบคุม /ป้องกันช่องโหว่ จากการทำงานในลักษณะของงานที่เกี่ยวข้อง ซึ่งอาจส่งผลกระทบและความเสียหายต่อภาพรวมระบบที่สำคัญในองค์กรได้ ซึ่งเกี่ยวข้องกับลดผลกระทบการเกิด “Downtime” ซึ่งเป็นต้นเหตุทำให้ระบบไม่สามารถดำเนินงานต่อไปได้ โดยควรมีการสำรองข้อมูล (Backup) ระบบที่เกี่ยวข้องทั้งหมด อย่างสม่ำเสมอ ซึ่งเป็นส่วนหนึ่งของแผนการป้องกันระบบหยุดการให้บริการ BCP (Business Continuity Planning) และแผนการกู้คืนระบบ DRP (Disaster Recovery Planning) เพราะบางหน่วยงานยังไม่เห็นความสำคัญของเรื่องเหล่านี้อยู่

Module 8 : *Software Development Security*

เป็นการอธิบายถึง กระบวนการบริหารจัดการต่างๆ ในด้านการป้องกัน แก้ไขปัญหาด้านความปลอดภัยในการใช้งานซอฟต์แวร์ อาจเกิดปัญหาด้านความปลอดภัยขึ้นในอนาคต ให้มีความครอบคลุมในด้านต่างๆของระบบสารสนเทศ และลดความเสี่ยงที่เกิดปัญหาต่างด้านการใช้งานของโปรแกรมที่ได้มีการพัฒนาขึ้นในอนาคต หากมีการใช้งานร่วมกับระบบอื่นๆ ที่เกี่ยวข้องไม่ว่าจะเป็น ระบบฐานข้อมูล (Database) ประเภทต่างๆที่ใช้งานร่วมกัน ให้สามารถตอบสนองการใช้งานของผู้ใช้ และลดปัญหา หรือช่องโหว่ที่มักตรวจพบ ให้มีประสิทธิภาพมากขึ้น ก่อนทำการเปิดใช้งานจริงในอนาคต

ทั้งนี้โดยมีรายละเอียดตามเอกสารประกอบการฝึกอบรมที่เป็นไฟล์บันทึกใน CD (เอกสารแนบ)

2.2 ข้อเสนอแนะในการนำความรู้ตามหลักสูตร/เรื่องจากการฝึกอบรม/สัมมนาครั้งนี้ มาประยุกต์ใช้กับองค์กร

CISSP คือ (Certified Information System Security Professional Preparation) ที่รับรองโดยหน่วยงานมาตรฐานด้าน Security ของ International Information Systems Security Certification Consortium หรือ (ISC)² ซึ่งเป็น Cert ที่ไม่ขึ้นกับกับ Vendor (vendor-neutral certification) โดยเป็นที่ยอมรับกันอย่างกว้างขวางในวงการ Information Security ทั่วโลก อีกทั้งยังเป็นมาตรฐานที่เกี่ยวข้องกับการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศโดยสามารถนำเนื้อหาของการอบรมในครั้งนี้ เพื่อให้เกิดความสอดคล้องกับแผนรองรับมาตรฐานที่เกี่ยวข้องเพื่อนำมาประยุกต์ให้การบริหารจัดการด้านความปลอดภัยระบบสารสนเทศขององค์กรมีความมั่นคงปลอดภัยและได้มาตรฐานดียิ่งขึ้น

ดังนั้น ความรู้จากการอบรมหลักสูตรดังกล่าว ทำให้เข้าใจในรายละเอียดด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์และระบบเครือข่ายในองค์กรมากยิ่งขึ้น และนำมาเป็นแนวทางในการเตรียมความพร้อมเพื่อเพิ่มศักยภาพในการรับมือกับภัยคุกคามด้านด้านความปลอดภัยต่างๆ ที่จะเกิดขึ้นในอนาคตกับองค์กรได้

CISSP® Certified Information Systems Security Professional

2.3 ความคิดเห็นเกี่ยวกับการฝึกอบรม/สัมมนา

(1) หลักสูตรที่ฝึกอบรม/สัมมนาครั้งนี้ช่วยเพิ่มพูนความรู้ของท่าน

☑ มาก ☐ ปานกลาง ☐ น้อย

ฝทท 31/4

วันที่ 30 กันยายน 2559

(2) ท่านคิดว่าการฝึกอบรม/สัมมนาครั้งนี้มีประโยชน์กับตัวท่านและองค์การเพียงใด

☑ มาก ☐ ปานกลาง ☐ น้อย

ระบุเหตุผล (ตอบได้มากกว่า 1 ข้อ)

☑ เนื้อหาเกี่ยวข้องโดยตรงและสามารถนำไปใช้กับการปฏิบัติงานได้อย่างดี
☐ เนื้อหาไม่เกี่ยวข้องกับการปฏิบัติงาน
☐ เป็นความรู้เสริม และมีประโยชน์ในการปฏิบัติงาน
☑ ได้แลกเปลี่ยนประสบการณ์กับบุคคลนอกองค์การ
☑ วิทยากรมีความรู้ ความสามารถ และประสบการณ์ ในการบรรยายเป็นอย่างดี
☐ เนื้อหาการอบรมไม่ตรงกับหัวข้อการบรรยาย
☐ อื่น ๆ .....

3. วิทยากรที่ให้ความรู้ในหลักสูตรนี้ ได้แก่

ชื่อ-สกุล	จากสถาบัน/หน่วยงาน	ระดับความสามารถของวิทยากร
3.1 คุณธนาทิพย์ ยินดี	บริษัท Vnohow (Thailand) จำกัด	☑ ดีมาก ☐ ดี ☐ พอใช้
3.2	.....	☐ ดีมาก ☐ ดี ☐ พอใช้

4. ข้อเสนอแนะในการส่งพนักงานเข้ารับการฝึกอบรม/สัมมนาตามหลักสูตร/เรื่องนี้สำหรับครั้งต่อไป

.....

.....

จึงเรียนมาเพื่อโปรดทราบ

ลงชื่อ .....

(นายอภิวุฒิ ผิวเพชร)

วันที่ 30 กันยายน 2559

รผบ.

หมายเหตุ

1. การส่งรายงานสรุปผลการฝึกอบรม/สัมมนา ควรสรุปรายละเอียดเนื้อหาหลักสูตรผ่านผู้บังคับบัญชาในสังกัดของตนเอง และนำเสนอเรียนถึง รผบ. ผ่าน ผชก.(นายสุชินฯ) ผอ.ฝทบ ตามสายบังคับบัญชาถึงระดับรองผู้ว่าการ (ต้องแนบเอกสารประกอบการฝึกอบรมทุกครั้งและแนบวุฒิบัตร หากไม่มีให้แนบใบเซ็นชื่อเข้ารับการฝึกอบรมอย่างเคร่งครัด)

2. เมื่อ รผบ. พิจารณาเรื่องรายงานการฝึกอบรมภายนอกเรียบร้อยแล้ว กรุณาส่งเรื่องดังกล่าวไปที่ พบ.กพร.ฝทบ. เพื่อ ฝทบ. จะบันทึกประวัติการฝึกอบรมเป็น "ผ่าน" และนำรายงานเผยแพร่องค์ความรู้ใน Web HRD และ Web KM ของ รพม. ต่อไป

3. สอบถามข้อมูลเพิ่มเติมได้ที่ แผนกพัฒนาทรัพยากรบุคคล กองพัฒนาบุคลากรและระบบงาน ฝ่ายทรัพยากรบุคคล คุณรัชกร โทร 1224 คุณอัจฉรา โทร 1213 คุณมณฑิชา โทร 1275 และคุณจิตปภา โทร 1214

www.vnohow.com

CERTIFICATE OF COMPLETION

PRESENTED BY

VNOHOW (THAILAND) CO., LTD.

PRESENTED TO

Mr. Aphiwut Piewpesh

FOR COMPLETION OF THE

Certified Information Systems Security Professional Preparation

(29 August to 2 September 2016)

2016-104	2 September 2016	
CERTIFICATE NO	DATE OF COMPLETION	INSTRUCTOR

Registration Sheet

Vnohow (Thailand) Co., Ltd.
138 Boonmitr Building, 6th Floor,
Room A3, B5-B10, Silom Road,
Suriyawong, Bangrak,
Bangkok Thailand 10500
Tel: +662 634-3287-9 .
Fax: +662 634-3299

Course Code: CISSP
Course Name: Certified Information System Security Professional Preparation
Training Schedule: 29 August to 2 September 2016 (5 Days)
Training Venue: Lucky Room, Vnohow Training Center
Instructor Name: Mr. Thanatip Yindee

****Please note this attending record might be required to submit to your organization Appreciate your signature to express your participation****

No.	Participant Name		Email Address	Mobile/Phone	Signature					Kit	Cer	Polo	Internet Username	ID Card No.
					29-Aug-16	30-Aug-16	31-Aug-16	1-Sep-16	2-Sep-16					
1	Mr.	Aphiwut Piewpesh	aphiwut@mrta.co.th	09-1879-0116										