สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๒๒๐ หมู่ ๓ อาคารซี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐ ไปรษณีย์อิเล็กทรอนิกส์: saraban@ncsa.or.th

ที่ สกมช ๐๗๐๐/ว๕๘๖๓

๔ สิงหาคม ๒๕๖๘

เรื่อง ขอประชาสัมพันธ์การจัดอบรมเชิงปฏิบัติการ ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากลให้กับประชาชน

เรียน อธิบดีกรมพัฒนาสังคมและสวัสดิการ

สิ่งที่ส่งมาด้วย รายละเอียดและกำหนดการจัดอบรม จำนวน ๔ หลักสูตร

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กำหนดจัดอบรมเชิงปฏิบัติการ ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากลให้กับประชาชน เพื่อพัฒนาศักยภาพให้แก่บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับพื้นฐาน ระดับผู้เชี่ยวชาญ ระดับผู้เชี่ยวชาญเฉพาะด้าน และระดับสูง ให้ตอบโจทย์ความต้องการของประเทศ และเพื่อพัฒนาทักษะการเป็นวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งเน้นให้สามารถถ่ายทอดความรู้ให้แก่บุคลากรในหน่วยงานหรือประชาชนทั่วไปได้ โดยมีรายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

ในการนี้ สกมช. จึงขอให้ท่านพิจารณามอบหมายบุคลากรที่ปฏิบัติงานเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์หรือความมั่นคงปลอดภัยสารสนเทศ ในหน่วยงานของท่านสมัครเข้าร่วมโครงการและใคร่ขอความอนุเคราะห์ ในการแจ้งเวียนหนังสือประชาสัมพันธ์ไปยังหน่วยงานภายใต้การกำกับดูแลของท่าน เพื่อสมัครเข้าร่วมการฝึกอบรมเชิงปฏิบัติการในหลักสูตรที่สนใจ โดยไม่มีค่าใช้จ่าย ทั้งนี้สามารถศึกษารายละเอียดเพิ่มเติมได้ที่ www.THNCA.or.th ทั้งนี้ขอมอบให้ คุณวราลักษณ์ สง่าลี หมายเลขโทรศัพท์ ๐๙ ๖๑๘๖ ๗๐๐๔ เป็นผู้ประสานงาน

จึงเรียนมาเพื่อโปรดพิจารณา และขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

พลอากาศตรี

(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
โทรศัพท์ ๐ ๒๕๐๒ ๗๘๓๔
ไปรษณีย์อิเล็กทรอนิกส์ thnca@ncsa.or.th

www.THNCA.or.th

กำหนดการการจัดอบรมเชิงปฏิบัติการ กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากลให้กับประชาชน		
หลักสูตร / รุ่น	**วัน เดือน ปี**	**สถานที่**
1. หลักสูตรประกาศนียบัตรรับรองพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์		
1.1 อบรมภาคทฤษฎี Online	6 - 10 ตุลาคม 2568	ผ่านสื่ออิเล็กทรอนิกส์ (Zoom)
1.2 อบรม Onsite Workshop รุ่นที่ 1	10 - 12 พฤศจิกายน 2568	โรงแรม เดอะเนเจอร์ ภูเก็ต จังหวัดภูเก็ต
1.3 อบรม Onsite Workshop รุ่นที่ 2	17-19 พฤศจิกายน 2568	โรงแรมคุ้มภูคำ จังหวัดเชียงใหม่
1.4 อบรม Onsite Workshop รุ่นที่ 3	24 - 26 พฤศจิกายน 2568	โรงแรมอวานี ขอนแก่น โฮเทล แอนด์ คอนเวนชั่น เซ็นเตอร์ จังหวัดขอนแก่น
1.5 อบรม Onsite Workshop รุ่นที่ 4	15 - 17 ธันวาคม 2568	โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชั่น กรุงเทพมหานคร
2. หลักสูตรประกาศนียบัตรความมั่นคงปลอดภัยระบบคลาวด์		
2.1 อบรมภาคทฤษฎี Online	14 - 18 ตุลาคม 2568	ผ่านสื่ออิเล็กทรอนิกส์ (Zoom)
2.2 อบรม Onsite Workshop รุ่นที่ 1	13-15 พฤศจิกายน 2568	โรงแรม เดอะเนเจอร์ ภูเก็ต จังหวัด
2.3 อบรม Onsite Workshop รุ่นที่ 2	20 -22 พฤศจิกายน 2568	โรงแรมคุ้มภูคำ จังหวัดเชียงใหม่
2.4 อบรม Onsite Workshop รุ่นที่ 3	27 - 29 พฤศจิกายน 2568	โรงแรมอวานี ขอนแก่น โฮเทล แอนด์ คอนเวนชั่น เซ็นเตอร์ จังหวัด
3. หลักสูตรประกาศนียบัตรด้านการพิสูจน์หลักฐานทางดิจิทัล		
3.1 อบรมภาคทฤษฎี Online	27 - 31 ตุลาคม 2568	ผ่านสื่ออิเล็กทรอนิกส์ (Zoom)
3.2 อบรม Onsite Workshop	11 - 13 ธันวาคม 2568	โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชั่น กรุงเทพมหานคร
4. หลักสูตรประกาศนียบัตรด้านความมั่นคงปลอดภัยระบบสารสนเทศระดับสูง		
4.1 อบรมภาคทฤษฎี Online	29 กันยายน - 3 ตุลาคม 2568	ผ่านสื่ออิเล็กทรอนิกส์ (Zoom)
4.2 อบรม Onsite Workshop	15 - 19 ธันวาคม 2568	โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชั่น กรุงเทพมหานคร

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

กำหนดการจัดอบรมหลักสูตรรับรองพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์

Certified In Cybersecurity (CC) ในรูปแบบออนไลน์

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์

ตามมาตรฐานสากลให้กับประชาชน

วันที่ 1 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-09.00 น.	ประธานกล่าวเปิดการอบรม และแนะนำหลักสูตร
09.00-10.30 น.	บทที่ 1: หน่วยที่ 1.1 และ 1.2 แนวคิดด้านความมั่นคงปลอดภัย และกระบวนการบริหารความเสี่ยง
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 1: หน่วยที่ 1.3 และ 1.4 การควบคุมความปลอดภัย และองค์ประกอบการกำกับดูแล
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 1: หน่วยที่ 1.5 จริยธรรมทางวิชาชีพด้านความมั่นคงปลอดภัย
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 2: หน่วยที่ 2.1 การรักษาความปลอดภัยของข้อมูล และการจัดการข้อมูล
วันที่ 2 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 2: หน่วยที่ 2.2 2.3 และ 2.4 การทำให้ระบบแข็งแกร่ง นโยบายความปลอดภัย และการฝึกอบรม
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 3: หน่วยที่ 3.1 และ 3.2 แนวคิดและหลักการควบคุมการเข้าถึงทางกายภาพ
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 3: หน่วยที่ 3.3 แนวคิดการควบคุมการเข้าถึงทางเทคนิค (DAC MAC)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 3: หน่วยที่ 3.3 (ต่อ) แนวคิดการควบคุมการเข้าถึงทางเทคนิค (RBAC)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 3 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 4: หน่วยที่ 4.1 และ 4.2 พื้นฐานระบบเครือข่าย ภัยคุกคาม และเครื่องมือป้องกัน
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 4: หน่วยที่ 4.3 โครงสร้างพื้นฐานความปลอดภัย On-Premises
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 4: หน่วยที่ 4.3 (ต่อ) โครงสร้างพื้นฐานความปลอดภัย Cloud
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 4: หน่วยที่ 4.3 (ต่อ) การออกแบบเครือข่าย Zero Trust และ VPN
วันที่ 4 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 5: หน่วยที่ 5.1 การตอบสนองต่อเหตุการณ์ (Incident Response)
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 5: หน่วยที่ 5.2 ความต่อเนื่องทางธุรกิจ (Business Continuity)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 5: หน่วยที่ 5.3 การกู้คืนจากภัยพิบัติ (Disaster Recovery)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 5: หน่วยที่ 5.3 (ต่อ) กฎการสำรองข้อมูล 3-2-1 และตัวชี้วัดการกู้คืน
วันที่ 5 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.00 น.	บทที่ 6: หน่วยที่ 6.1 กรอบกฎหมายของไทย พ.ร.บ. ไซเบอร์ฯ และ PDPA
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	บทที่ 6: หน่วยที่ 6.2 และ 6.3 การดำเนินการเชิงปฏิบัติและวิเคราะห์กรณีศึกษาในไทย
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	ทบทวนเนื้อหาภาพรวมทั้ง 6 บทเรียน
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	ทำแบบทดสอบหลังอบรม (Post-test)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

กำหนดการจัดอบรมหลักสูตรรับรองพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์

Certified In Cybersecurity (CC) ในรูปแบบเชิงปฏิบัติการ (Workshop)

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์

ตามมาตรฐานสากลให้กับประชาชน

วันที่ 1 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-09.00 น.	ลงทะเบียน
09.00-10.30 น.	Workshop (บทที่ 1): ฝึกปฏิบัติกระบวนการบริหารความเสี่ยงตามหน่วยที่ 1.2
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	Workshop (บทที่ 3): ฝึกปฏิบัติการออกแบบการควบคุมการเข้าถึงตามหลัก Least Privilege (หน่วยที่ 3.1) และการแบ่งแยกหน้าที่
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Workshop (บทที่ 2): ฝึกปฏิบัติการสร้างแคมเปญ Security Awareness (หน่วยที่ 2.4)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	(พิเศษ) Workshop: เทคนิคการเป็นวิทยากร (Awareness) - ฝึกการนำเสนอและถ่ายทอดความรู้
วันที่ 2 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.00 น.	Lab (บทที่ 4): วิเคราะห์แผนผังเครือข่าย และการวางตำแหน่งอุปกรณ์ความปลอดภัย (หน่วยที่ 4.2 และ 4.3)
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	Lab (บทที่ 4): ฝึกปฏิบัติการแบ่งส่วนเครือข่าย (Network Segmentation/DMZ) (หน่วยที่ 4.3)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Lab (บทที่ 4): ฝึกปฏิบัติการตั้งค่าพื้นฐานของ VPN
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	Lab (บทที่ 4): อภิปรายแนวคิด Zero Trust (หน่วยที่ 4.3)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 3 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
8.30-10.00 น.	Integrated Workshop (บทที่ 5 และ 6): จำลองสถานการณ์ Data Breach และฝึกปฏิบัติตามแผน IRP (หน่วยที่ 5.1 และ 6.2)
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	Integrated Workshop (ต่อ): ฝึกตัดสินใจและร่างรายงานแจ้งเหตุต่อ สกมช. และ สคส. ตามกฎหมาย (หน่วยที่ 6.2)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	ทบทวนเนื้อหาบทเรียน
14.30-15.00 น.	พักรับประทานอาหารว่าง
15.00-16.30 น.	ทำแบบทดสอบหลังอบรม (Post-test)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

กำหนดการจัดอบรมหลักสูตรประกาศนียบัตรความมั่นคงปลอดภัยระบบคลาวด์

(CompTIA Cloud+) ในรูปแบบออนไลน์

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์

ตามมาตรฐานสากลให้กับประชาชน

วันที่ 14 ตุลาคม 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-09.00 น.	ประธานกล่าวเปิดการอบรม และแนะนำหลักสูตร
09.00-10.30 น.	บทที่ 1: ความเข้าใจเกี่ยวกับสถาปัตยกรรมระบบคลาวด์ แนวคิด และรูปแบบการให้บริการ
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 1 (ต่อ): เทคโนโลยีในระบบคลาวด์ และการแก้ไขปัญหาในสภาพแวดล้อมคลาวด์
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 2: การวางแผนบริการระบบคลาวด์ การออกแบบแบบคลาวด์เนทีฟ (Cloud-Native)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 2 (ต่อ): รูปแบบและกลยุทธ์การปรับใช้คลาวด์ (Deployment Models and Strategies)
วันที่ 15 ตุลาคม 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 3: การจัดเตรียมและย้ายทรัพยากรไปยังคลาวด์ (Provisioning and Migration)
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 4: การเปรียบเทียบระบบจัดเก็บข้อมูลบนคลาวด์ ทรัพยากรและเทคโนโลยีในการจัดเก็บข้อมูล
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 5: การแก้ไขปัญหาการปรับใช้และการย้ายระบบ (Troubleshooting Deployment)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 5 (ต่อ): ข้อควรพิจารณาเกี่ยวกับค่าใช้จ่ายในการใช้งานระบบคลาวด์

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 16 ตุลาคม 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 6: การใช้เทคโนโลยีเวอร์ชวลไลเซชัน (Virtualization) และคอนเทนเนอร์ (Containerization)
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 6 (ต่อ): แนวคิดพื้นฐานเกี่ยวกับฐานข้อมูล (Database Concepts)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 7: การเข้าใจระบบเครือข่ายบนคลาวด์ แนวคิด ฟังก์ชัน และองค์ประกอบของเครือข่าย
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 7 (ต่อ): บริการเครือข่ายในระบบคลาวด์ และการแก้ไขปัญหาเครือข่าย
วันที่ 17 ตุลาคม 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 8: การทำงานแบบอัตโนมัติของทรัพยากรคลาวด์ การใช้โค้ด และ CI/CD Pipelines
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 8 (ต่อ): เครื่องมือ DevOps และแนวคิดการควบคุมเวอร์ชัน (Source Control)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 9: การบริหารจัดการด้านความมั่นคงปลอดภัยในระบบคลาวด์ (Identity and Access Management: IAM)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 9 (ต่อ): การควบคุมความปลอดภัย การจัดการช่องโหว่ และการเฝ้าระวังกิจกรรมที่น่าสงสัย

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 18 ตุลาคม 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.00 น.	บทที่ 10, 11, 12: การปฏิบัติตามข้อกำหนด (Compliance) การเพิ่มประสิทธิภาพ (Performance) และการกู้คืนจากภัยพิบัติ (Disaster Recovery)
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	บทที่ 13: การประยุกต์ใช้เทคโนโลยีคลาวด์ให้สอดคล้องกับกฎหมายไทย (PDPA, Cybersecurity Act, Computer Crime Act)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 13 (ต่อ): การปฏิบัติตาม PDPA ในสภาพแวดล้อมคลาวด์ และกรณีศึกษา
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	ทบทวนภาพรวมและทำแบบทดสอบหลังอบรม (Post-test)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

กำหนดการจัดอบรมหลักสูตรประกาศนียบัตรความมั่นคงปลอดภัยระบบคลาวด์

(CompTIA Cloud+) ในรูปแบบเชิงปฏิบัติการ (Workshop)

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์

ตามมาตรฐานสากลให้กับประชาชน

วันที่ 13 พฤษจิกายน 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-09.00 น.	ลงทะเบียน
09.00-10.30 น.	Lab (บทที่ 3 และ 7): การสร้าง Virtual Private Cloud (VPC) และ Subnets
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	Lab (บทที่ 7): การกำหนดค่า Network Security Groups และการเชื่อมต่อระหว่าง VPC
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Lab (บทที่ 3 และ 6): การจัดเตรียมและกำหนดค่า Virtual Machine (VM) เบื้องต้น
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	Lab (บทที่ 6): การจัดเตรียมและใช้งาน Container ผ่านบริการคลาวด์
วันที่ 14 พฤษจิกายน 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	Lab (บทที่ 8 และ 9): การใช้ Infrastructure as Code (IaC) เพื่อสร้าง IAM Role และ Policy ตามหลัก Principle of Least Privilege
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	Workshop (บทที่ 9 และ 11): การตั้งค่า Logging และ Monitoring เพื่อตรวจจับกิจกรรมที่น่าสงสัย
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Workshop (บทที่ 5): การวิเคราะห์และบริหารจัดการต้นทุน (Cloud Cost Management)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	(พิเศษ) Workshop: เทคนิคการเป็นวิทยากร (Awareness) - ฝึกการนำเสนอแนวคิดและประโยชน์ของคลาวด์

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 15 พฤษจิกายน 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
8.30-10.00 น.	Integrated Workshop (บทที่ 13): กรณีศึกษา การย้าย Workload ที่มีข้อมูลส่วนบุคคลขึ้นสู่คลาวด์อย่างสอดคล้องกับกฎหมายไทย
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	Integrated Workshop (ต่อ): ฝึกปฏิบัติการสร้าง Checklist สำหรับการย้ายระบบ โดยคำนึงถึง Data Sovereignty และการจัดทำข้อตกลง DPA
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	ทบทวนเนื้อหาบทเรียน
14.30-15.00 น.	พักรับประทานอาหารว่าง
15.00-16.30 น.	ทำแบบทดสอบหลังอบรม (Post-test)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

กำหนดการจัดอบรมหลักสูตรประกาศนียบัตรด้านการพิสูจน์หลักฐานทางดิจิทัล

(Computer Hacking Forensic Investigator: CHFI) ในรูปแบบออนไลน์

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์

ตามมาตรฐานสากลให้กับประชาชน

วันที่ 1 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-09.00 น.	ประธานกล่าวเปิดการอบรม และแนะนำหลักสูตร
09.00-10.30 น.	บทที่ 1: ความเข้าใจพื้นฐานเกี่ยวกับนิติวิทยาศาสตร์คอมพิวเตอร์ อาชญากรรมไซเบอร์ และพยานหลักฐานทางดิจิทัล
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 2: กระบวนการสืบสวนทางนิติวิทยาการคอมพิวเตอร์ และการตอบสนองเบื้องต้น (First Response)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 4: การได้มาซึ่งข้อมูลและการทำซ้ำ (Data Acquisition and Duplication)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 4 (ต่อ): ระเบียบวิธีการเก็บข้อมูล และการเตรียมไฟล์ภาพเพื่อการตรวจสอบ
วันที่ 2 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 3: การทำความเข้าใจเกี่ยวกับฮาร์ดดิสก์และระบบไฟล์ของ Windows, Linux และ macOS
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 3 (ต่อ): การวิเคราะห์ระบบไฟล์ และการวิเคราะห์ไฟล์ด้วย Hex Editor
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 5: การรับมือกับเทคนิคต่อต้านนิติวิทยาศาสตร์ เช่น การลบข้อมูล การซ่อนข้อมูล (Steganography)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 5 (ต่อ): เทคนิคการถอดรหัสผ่าน และการตรวจจับโปรแกรมแพ็กเกอร์

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 3 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 6: การพิสูจน์หลักฐานบนระบบ Windows การวิเคราะห์ Memory และ Registry
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 7: การพิสูจน์หลักฐานในระบบ Linux และ macOS
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 8: การพิสูจน์หลักฐานในเครือข่าย (Network Forensics) และการวิเคราะห์ Log
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 8 (ต่อ): การตรวจสอบและวิเคราะห์การรับส่งข้อมูลบนเครือข่าย
วันที่ 4 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 9 และ 10: การพิสูจน์หลักฐานจากมัลแวร์ และการสืบสวนการโจมตีผ่านเว็บไซต์
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 11: การพิสูจน์หลักฐานบนเครือข่ายดาร์กเว็บ (Dark Web Forensics)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 12: การพิสูจน์หลักฐานในระบบคลาวด์ (Cloud Forensics) สำหรับ AWS
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 12 (ต่อ): การพิสูจน์หลักฐานในระบบคลาวด์สำหรับ Microsoft Azure และ Google Cloud

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 5 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.00 น.	บทที่ 13, 14, 15: การพิสูจน์หลักฐานจากอีเมล โซเชียลมีเดีย อุปกรณ์เคลื่อนที่ และ IOT
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	บทที่ 16: นิติวิทยาศาสตร์ดิจิทัลในบริบทของกฎหมายไทย และกรอบกฎหมายที่ควบคุมพยานหลักฐานดิจิทัล
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 16 (ต่อ): กระบวนการจัดการพยานหลักฐานดิจิทัลในไทย และกรณีศึกษา
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	ทบทวนภาพรวมและทำแบบทดสอบหลังอบรม (Post-test)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

กำหนดการจัดอบรมหลักสูตรประกาศนียบัตรด้านการพิสูจน์หลักฐานทางดิจิทัล

(Computer Hacking Forensic Investigator: CHFI) ในรูปแบบเชิงปฏิบัติการ (Workshop)

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์

ตามมาตรฐานสากลให้กับประชาชน

วันที่ 1 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-09.00 น.	ลงทะเบียน
09.00-10.30 น.	Lab (บทที่ 4): ฝึกปฏิบัติการสร้าง Image จากพยานหลักฐานดิจิทัลด้วยเครื่องมือ Forensics
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	Workshop (บทที่ 3): ฝึกการวิเคราะห์โครงสร้าง File System จากไฟล์ Image
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Lab (บทที่ 5): ฝึกปฏิบัติการตรวจจับข้อมูลที่ถูกซ่อนด้วยเทคนิค Steganography
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	Lab (บทที่ 5 ต่อ): สาธิตและฝึกใช้เครื่องมือถอดรหัสผ่านเบื้องต้น
วันที่ 2 พฤศจิกายน 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.00 น.	Lab (บทที่ 6): ฝึกปฏิบัติการวิเคราะห์ Windows Memory และ Registry จากไฟล์ Image
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	Lab (บทที่ 8): ฝึกปฏิบัติการวิเคราะห์ไฟล์ PCAP เพื่อหาหลักฐานการโจมตีเครือข่าย
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Workshop (บทที่ 9): ฝึกวิเคราะห์มัลแวร์เบื้องต้นแบบสถิต (Static Analysis)
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	(พิเศษ) Workshop: เทคนิคการเป็นวิทยากร (Awareness) - ฝึกการนำเสนอผลการสืบสวน

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 3 พฤศจิกายน 2568 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
8.30-10.00 น.	Integrated Workshop (บทที่ 16): สืบสวนกรณีศึกษาโดยเริ่มจากการวิเคราะห์พยานหลักฐานดิจิทัลเบื้องต้น
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	Integrated Workshop (ต่อ): ฝึกปฏิบัติการจัดทำเอกสาร Chain of Custody และคำนวณค่า Hash เพื่อรักษาความครบถ้วนสมบูรณ์ของพยานหลักฐาน
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	ทบทวนเนื้อหาบทเรียน
14.30-15.00 น.	พักรับประทานอาหารว่าง
15.00-16.30 น.	ทำแบบทดสอบหลังอบรม (Post-test)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

กำหนดการจัดอบรมหลักสูตรประกาศนียบัตรด้านความมั่นคงปลอดภัยระบบสารสนเทศระดับสูง (Certified Information Systems Security Professional: CISSP) ในรูปแบบออนไลน์

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์

ตามมาตรฐานสากลให้กับประชาชน

วันที่ 1 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-09.00 น.	ประธานกล่าวเปิดการอบรม และแนะนำหลักสูตร
09.00-10.30 น.	บทที่ 1: หลักการความมั่นคงปลอดภัยทางไซเบอร์ และการกำกับดูแล
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 2: กฎหมายและจริยธรรม หลักการทางกฎหมาย และกฎระเบียบด้านความมั่นคงปลอดภัย
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 3: การบริหารความเสี่ยง ภัยคุกคามและช่องโหว่
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 3 (ต่อ): การประเมิน การตอบสนอง และการจัดการความเสี่ยง
วันที่ 2 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 4: นโยบายความมั่นคงปลอดภัย กรอบการทำงาน และการออกแบบนโยบาย
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 4: นโยบายความมั่นคงปลอดภัย กรอบการทำงาน และการออกแบบนโยบาย
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 5: สินทรัพย์สารสนเทศ การจำแนกประเภท และการรักษาความปลอดภัยข้อมูล
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 6 (ต่อ): โครงสร้างพื้นฐานกุญแจสาธารณะ (PKI)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 3 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 7 และ 8: หลักการความปลอดภัยของระบบ และสถาปัตยกรรมองค์กรที่ปลอดภัย
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 9: ความมั่นคงปลอดภัยของระบบเฉพาะทาง (อุปกรณ์เคลื่อนที่ ระบบเสมือนและคลาวด์)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 10 และ 11: การออกแบบระบบที่มั่นคงปลอดภัย และพื้นฐานของเครือข่าย
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 12 และ 13: โพรโทคอลเครือข่าย และเทคโนโลยีเครือข่าย
วันที่ 4 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	บทที่ 14 และ 15: สถาปัตยกรรมความมั่นคงปลอดภัยเครือข่าย และการกำหนดค่าที่ปลอดภัย
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	บทที่ 16 และ 17: การบริหารจัดการตัวตน และเทคโนโลยีการควบคุมการเข้าถึง
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 18 และ 19: การประเมินและทดสอบความมั่นคงปลอดภัย และการปฏิบัติการด้านความมั่นคงปลอดภัย
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	บทที่ 20: การสแกนและการตรวจสอบ (Malware, Threat Detection, Network Monitoring)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 5 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.00 น.	บทที่ 21 และ 22: การรับมืออุบัติการณ์ และการวางแผนรับมือภัยพิบัติ
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	บทที่ 23: การพัฒนาซอฟต์แวร์ที่ปลอดภัย
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	บทที่ 24: การประยุกต์ใช้หลักการ CISSP ในบริบทกฎหมายไทย และกรณีศึกษา
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	ทบทวนภาพรวมและทำแบบทดสอบหลังอบรม (Post-test)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

กำหนดการจัดอบรมหลักสูตรประกาศนียบัตรด้านความมั่นคงปลอดภัยระบบสารสนเทศระดับสูง (Certified Information Systems Security Professional: CISSP) ในรูปแบบเชิงปฏิบัติการ (Workshop)

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์

ตามมาตรฐานสากลให้กับประชาชน

วันที่ 1 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-09.00 น.	ลงทะเบียน
09.00-10.30 น.	Workshop (บทที่ 1, 3, 4): ฝึกปฏิบัติการประเมินความเสี่ยง และการร่างนโยบายความมั่นคงปลอดภัย
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	Workshop (ต่อ): ฝึกปฏิบัติการประเมินความเสี่ยง และการร่างนโยบายความมั่นคงปลอดภัย
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Workshop (บทที่ 5): การจำแนกประเภทข้อมูล และการออกแบบมาตรการป้องกันสินทรัพย์สารสนเทศ
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	(พิเศษ) Workshop: เทคนิคการเป็นวิทยากร (Awareness) - ฝึกการนำเสนอนโยบายความปลอดภัย
วันที่ 2 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
08.30-10.30 น.	Workshop (บทที่ 6): การประยุกต์ใช้ Cryptography และการออกแบบ PKI เบื้องต้น
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-12.00 น.	Lab (บทที่ 7, 8, 10): การวิเคราะห์โมเดลความปลอดภัย และการออกแบบสถาปัตยกรรมที่ปลอดภัย
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Workshop (บทที่ 9): การวิเคราะห์ความเสี่ยงสำหรับระบบ Cloud และ Mobile
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-16.30 น.	Workshop (บทที่ 9 ต่อ): การออกแบบมาตรการควบคุมสำหรับระบบเสมือน (Virtualization)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 3 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
8.30-10.00 น.	Lab (บทที่ 11, 12, 13): การวิเคราะห์โปรโตคอลเครือข่าย และเทคโนโลยีเครือข่าย
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	Lab (บทที่ 14): การออกแบบสถาปัตยกรรมเครือข่ายที่ปลอดภัย (Secure Network Architecture)
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Lab (บทที่ 15): การเสริมความปลอดภัยให้เครือข่าย (Network Hardening)
14.30-15.00 น.	พักรับประทานอาหารว่าง
15.00-16.30 น.	Workshop (บทที่ 15 ต่อ): การรักษาความปลอดภัยในการสื่อสารผ่านช่องทางต่างๆ
วันที่ 4 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
8.30-10.00 น.	Lab (บทที่ 16, 17): การออกแบบและประยุกต์ใช้ระบบ IAM (Identity and Access Management)
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	Workshop (บทที่ 18, 19): การวางแผนโปรแกรมทดสอบความปลอดภัย และการจัดการ Patch
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	Workshop (บทที่ 20, 21): การวางแผนรับมืออุบัติการณ์ (Incident Response Planning)
14.30-15.00 น.	พักรับประทานอาหารว่าง
15.00-16.30 น.	Workshop (บทที่ 22): การวางแผนความต่อเนื่องทางธุรกิจ (BCP) และการกู้คืนจากภัยพิบัติ (DRP)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม

วันที่ 5 ระยะเวลาการอบรม 6 ชั่วโมง	
เวลา	**กิจกรรม**
8.30-10.00 น.	Workshop (บทที่ 23): การประยุกต์ใช้หลักการพัฒนาซอฟต์แวร์ที่ปลอดภัย (Secure SDLC)
10.00-10.15 น.	พักรับประทานอาหารว่าง
10.15-12.00 น.	Integrated Workshop (บทที่ 24): วิเคราะห์กรณีศึกษา JIB และการเชื่อมโยงกฎหมายไทยกับ 8 โดเมนของ CISSP
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	ทบทวนเนื้อหาบทเรียน
14.30-15.00 น.	พักรับประทานอาหารว่าง
15.00-16.30 น.	ทำแบบทดสอบหลังอบรม (Post-test)

หมายเหตุ: กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม