



กำหนดการ

หลักสูตรการบริหารจัดการภัยคุกคามทางไซเบอร์ **รุ่นที่ 4**
(Cyber security incident management)

ระหว่างวันที่ 8 - 11 กันยายน 2568 เวลา 09.00 - 16.00 น.
ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพฯ

กำหนดการอบรม (ระยะเวลา 4 วัน)

เวลา	หัวข้อ
วันจันทร์ที่ 8 กันยายน 2568	
09:00 - 12:00 น.	- สาระสำคัญของ พรบ. ไซเบอร์ - สิ่งที่องค์กรต้องปฏิบัติตามเพื่อให้สอดคล้องกับ พรบ. ไซเบอร์ - มาตรฐานและมาตรการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย - มาตรฐาน ISO ที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
12.00 - 13.00 น.	พักรับประทานอาหารกลางวัน
13:00 - 16:00 น.	- ทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบ - Workshop 1: โครงสร้างทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย บทบาท และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง - แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย - Workshop 2: การจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
วันอังคารที่ 9 กันยายน 2568	
09:00 - 12:00 น.	- การจัดสรรทรัพยากรเพื่อสนับสนุนและรองรับแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย - Workshop 3: การกำหนดทรัพยากรที่จำเป็นสำหรับการสนับสนุนแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย - การซ้อมแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย - Workshop 4: การซ้อมแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
12.00 - 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 - 16.00 น.	กรณีศึกษาที่ 1 วิเคราะห์กรณีที่ระบบของท่านถูกสแกนตรวจสอบช่องโหว่
วันพุธที่ 10 กันยายน 2568	
09.00 - 12.00 น.	กรณีศึกษาที่ 2 วิเคราะห์กรณีที่ระบบของท่านถูกลองผิดลองถูกกับการเปลี่ยนรหัสผ่านไปเรื่อยๆ โดยผู้ไม่ประสงค์ดี จนกระทั่งพบรหัสผ่านที่ถูกต้องและผู้ไม่ประสงค์ดีสามารถเข้าถึงระบบของท่านได้
12.00 - 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 - 16.00 น.	กรณีศึกษาที่ 3 วิเคราะห์กรณีที่ระบบของท่านถูกโจมตีแบบ DDoS จนกระทั่งระบบไม่สามารถให้บริการได้ กรณีศึกษาที่ 4 วิเคราะห์กรณีที่ระบบของท่านถูกเจาะระบบและสามารถเข้าถึงระบบได้จากการที่ไม่ได้แก้ไขช่องโหว่ของระบบ
วันพฤหัสบดีที่ 11 กันยายน 2568	
09:00 - 12:00 น.	กรณีศึกษาที่ 5 วิเคราะห์กรณีที่เว็บไซต์องค์กรของท่านถูกเข้าถึงและเปลี่ยนหน้าเว็บไซต์เป็นภาพโป๊ ให้พิจารณาจุดอ่อนหรือช่องโหว่ที่เป็นไปได้ที่ทำให้เว็บไซต์ของท่านถูกบุกรุก
12.00 - 13.00 น.	พักรับประทานอาหารกลางวัน
13:00 - 16:00 น.	กรณีศึกษาที่ 6 วิเคราะห์กรณีที่ระบบของท่านถูกเจาะ ด้วยเทคนิค SQL Injection และสามารถเข้าถึงฐานข้อมูลภายในได้ กรณีศึกษาที่ 7 วิเคราะห์กรณีที่ระบบของท่านติดไวรัสและทำให้ไม่สามารถให้บริการได้

****หมายเหตุ** สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการอบรม และวิทยากรตามความเหมาะสม