

**TEC007: Incident Response and Handling****COURSE DESCRIPTION**

The program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling. After attending the course, they will be able to create incident handling and response policies and deal with various types of computer security incidents.

The comprehensive training program will make students proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

In addition, the students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident reporting methods, and incident recovery techniques in detail.

**WHO SHOULD ATTEND**

This course will significantly benefit incident handlers, risk assessment administrators, penetration testers, cyber forensic investigators, vulnerability assessment auditors, system administrators, system engineers, firewall administrators, network managers, IT managers, IT professionals and anyone who is interested in incident handling and response.

**COURSE OUTLINE**

Module 01: Introduction to Incident Response and Handling

Module 02: Risk Assessment

Module 03: Incident Response and Handling Steps

Module 04: CSIRT

Module 05: Handling Network Security Incidents

Module 06: Handling Malicious Code Incidents

Module 07: Handling Insider Threats

Module 08: Forensic Analysis and Incident Response

Module 09: Incident Reporting

Module 10: Incident Recovery

Module 11: Security Policies and Laws

**วิทยากร :****อาจารย์เอกฤทธิ์ ธรรมสกลิต**

- Microsoft Certified professional (MCP)
- Microsoft Certified Systems Administrator (MSCA)
- Microsoft Certified Systems Engineer (MSCE)
- Cisco Certified Network Associate (CCNA)
- Certificate of CompTIA Security+
- Certified Ethical Hacker
- Certified Wireless Network Administrator
- Certified Wireless Security Professional

**จำนวนชั่วโมงในการฝึกอบรม : 3 วัน (18 ชั่วโมง)**

**ช่วงเวลาฝึกอบรม : 9.00 - 16.00 น.**

**สถานที่ฝึกอบรม :**

สถาบันวิทยาการ สวทช.  
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)  
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

**วิธีการสำรองที่นั่ง :**

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ  
โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887  
โทรสาร: 0 2644 8110  
Website: [www.NSTDAcademy.com](http://www.NSTDAcademy.com)  
E-mail: [training@nstda.or.th](mailto:training@nstda.or.th)