Kansas Information Security Office

13 May - AWR136 - Developing Cybersecurity Resiliency for Everyone, Independence, KS sponsored by Region 7 CISA

AWR136 is an eight (8) hour, non-technical introduction to cybersecurity. This awareness-level course will explore cybersecurity and cyber hygiene, and demonstrate how cyber-attacks can impact, prevent, and/or stop business operations and emergency responses. Participants are introduced to common cybersecurity terminology, fundamental cyber threats and vulnerabilities that can impact individuals and organizations, and best practices and cyber hygiene techniques for securing personal and organizational data, software, and hardware.

Registration Link: (note a FEMA SID is required to register. Link on the TEEX page if you do not have a FEMA SID)
https://my.teex.org/TeexPortal/Default.aspx?MO=mCourseCatalog&D=EC&C=AWR136&S=754

19-22 May - Comprehensive Cybersecurity Defense, Topeka

CCD is a basic level course. After an introduction to cybersecurity, participants will learn how to protect network systems by survey of the following: planning and preparation of defenses; installation and administration of defenses; hardening network defenses; administration of defenses; monitoring defenses; and testing and modifying defenses—followed by a review of cybersecurity defenses and emerging trends.

To register, go here: https://forms.office.com/g/dFhYhhebnp

5 June – Summer Kansas Critical Infrastructure Summit, Wichita
More information TBA

9-13 June - Certified Ethical Hacker Class, Wichita
This course is **full** but a waiting list is available. To register, go here: https://forms.office.com/g/d4yBtuTRSt

July 14-17 - Cybersecurity Proactive Defense, Topeka

Cybersecurity Proactive Defense is a Basic to intermediate level course that uses hands-on computer lab applications to simulate advanced attack vectors, sequential and escalating attack steps, and hands-on attack execution. Students learn penetration testing skills, defense analysis techniques, and real-time response and threat mitigation steps.

PREREQUISITE: CCD course. .

To register, go here: https://forms.office.com/g/eJ8nskx0B4

4, 5 August – MGT 465 in Sedgwick, sponsored by Sedgwick Co Emergency Management,
Register at: www.train.org/ks

18-22 August Plains Guardian cyber exercise training
25-29 August Plains Guardian Exercise
More information and registration on our webpage when it becomes available

23-27 August - GMIS International Conference, Indianapolis, IN
Check out the GMIS website for more information: www.gmis.org

8 October – Governor's Cybersecurity Summit *for Executive Branch Cabinet Agencies*, Topeka
9 October - Governor's Cybersecurity Summit for Executive Branch *non-Cabinet Agencies*, Topeka

3-7 November – Certified Forensic Investigator, Topeka

4 December – Winter Kansas Critical Infrastructure Summit, Wichita
More information TBA

Complete information and more classes are listed on our webpage.
Check back frequently as updates are happening all the time!

Kansas Plains Cyber Guardian Training and Range Exercise

Enhance Your Cyber Resiliency with Intensive Hands-On Training!

Join us for the **Kansas Plains Cyber Guardian Training** and Range Exercise, an initiative by the Kansas State Office of Information Technology Services. This exercise is part of the broader Statewide CyberSecurity Collaboration & Preparedness (CSCP) program, aimed at enhancing cyber resiliency through practical, hands-on training and 'live-fire' range exercises.

Register at : https://forms.office.com/g/dayyjQyrGt

Pre-Event Training: SOC-100 Self-Paced Content

- **Objective:** For those new to cybersecurity or needing a refresher on fundamental cybersecurity knowledge.
- **Format:** Self-paced online training to build a strong foundation before the main event

Week 1: In-Person OffSec SOC-200 Training

- **Dates:** August 18-22, 2025
- **Training Provider:** Applied Technology Academy (ATA)
- **Course:** OffSec SOC-200 - Security Operations and Defensive Analysis
  - **Objective:** Equip participants with the skills to detect, analyze, and respond to security incidents.
  - **Format:** In-person training with practical labs and challenge labs.

Week 2: OffSec Enterprise Cyber Range (ECR) Exercise

- **Dates:** August 25-29, 2025
- **Activity:** Defend and protect against Red Team personnel attempts to penetrate networks and systems.
- **Objective:** Test and improve defensive capabilities in a simulated cyber-attack scenario.

Why Participate?

Hands-On Experience: Gain practical skills through intensive training and real-world simulations utilizing OffSec's training and range platform.

Expert Instruction: Learn from industry experts at Applied Technology Academy (ATA).

Enhanced Cyber Resiliency: Prepare to defend against sophisticated cyber threats and improve your organization's security posture.

Event Dates: Training Class 18-22 August 2025 / Range Event 25-29 August 2025

Mandatory Cybersecurity Incident Reporting

KSA 75-7244 (also known as HB 2019) requires:

- Any ***public entity*** that has a significant cybersecurity incident shall notify the Kansas Information Security Office **within 12 hours** after discovery of such an incident.
- Any ***government contractor*** that has a significant cybersecurity incident shall notify the Kansas Information Security Office **within 72 hours** after the contractor believes the incident occurred.

How to report

Click “Report an Incident” on the KISO website:

https://www.ebit.ks.gov/divisions/information-security-office-kiso

Call: **785-296-6069** which is monitored and/or answered 24/7

What to report examples:

- Denial of service attack that lasted over an hour
- Discovery of ransomware note
- Multiple anti-virus or endpoint detection and response alerts resulting in a need to contain or shutdown systems

What *not* to report examples:

- Individual phishing message
- Single anti-virus alerts

What constitutes a ‘significant cybersecurity incident’?

A cybersecurity incident that results in or is likely to result in financial loss or demonstrable harm to public confidence or public health and safety in the State of Kansas. Any event or combination that threatens, without lawful authority the confidentiality, integrity or availability of information or information systems and that requires an entity to initiate a response or recovery.

Examples include but are not limited to malware, ransomware, denial of service, man in the middle and other such attacks by bad actors.