

ESSENTIALS OF COMMUNITY CYBERSECURITY

AWR-136

DHS/FEMA-funded course



ESSENTIALS OF COMMUNITY CYBERSECURITY

AWR-136

AWR-136 provides participants with an introduction to concepts related to community cybersecurity. Participants will examine the different types of cyber attacks, how communities are vulnerable to cyber attacks and incidents, and what types of organizations are most likely to be targeted. This course will also introduce the participants to the Community Cyber Security Maturity Model and how to use the model to build a community cybersecurity program and their cyber resilience.

AWR-136 is certified by the Texas Department of Information Resources (DIR) and meets the requirements of HB3834. HB3834 requires that all state employees that use a computer at least 25% of the time, any local government employee who has access to a local government computer system or database, and elected officials of local government must take a DIR approved cybersecurity course annually.

Topics

- Why cybersecurity is important
- Unstructured threats
- Structured threats
- Highly structured threats
- The Community Cybersecurity Maturity Model (CCSMM)
- Things a community can do to initiate a cybersecurity program
- Where to go for help

Prerequisites

FEMA / SID Number

Students must register for and provide a SID number to access the class. Register online: cdp.dhs.gov/femasid

Recommendations

None

Course Length

4 hours

Venue

Jurisdiction

CE Credits

IACET - 0.4 CEUs

Participants

Public and Private Personnel Involved with:

- Critical Infrastructure
- Emergency Operations
- Incident Response



For more information, contact:
TEXAS A&M ENGINEERING EXTENSION SERVICE
Brenda Grays
Sr. Customer Service Associate
200 Technology Way
College Station, TX 77845-3424
979.458.6726 or 800.451.7149 (toll free)
brenda.grays@teex.tamu.edu
www.teex.org/cyber

