SECURITY SERIES · SEC-04

SEC-04 — Digital Security

Devices, Accounts, Channels, and the Group Standard

Harden what members carry, decide which channel carries what, and write a standard that survives joining, lost phones, and departures.

BOTTOM LINE UP FRONT

Digital security, for a preparedness group, is operations security applied to the phones, accounts, and messaging every member already uses. It is not a cybersecurity course and not an argument about which app is best: most groups lose information through a lost handset, a reused password, a geotagged photo, or a former member still in the chat. Every measure works on an ordinary phone, at no cost, with no technical background.

WHY THIS MATTERS

One member with poor digital habits exposes the whole group.

A member's phone holds the roster in its contacts, the meeting site in its location history, and other members' homes in its Wi-Fi list. Good habits also decay: new members arrive without them, and members who leave keep their access unless someone removes it. Only a written standard with named owners keeps the group protected after the roster changes.

> ***The standard is a claim; the departure record is evidence.***

THE FIVE AREAS A GROUP IS AUDITED ON

Devices	Every member's phone and laptop meet a stated minimum, confirmed with a date.
Communications	A written channel plan naming the actual applications, with a controlled chat roster.
Accounts	Every shared login has a named owner, a deputy, and a recovery path the group controls.
Footprint	A dated outside-in audit of what the group has already published about itself.
Standard and lifecycle	Joining, lost-device, and departure routines that were actually used.

COURSE LESSONS

01	**Your Device Is a Witness.** What a phone records on its own, how that record gets out, and the hardening checklist.
02	**Secure Communications for Groups.** What end-to-end encryption does and does not promise, and a channel plan instead of an app argument.
03	**Accounts, Passwords, and Access Control.** The two measures that stop most takeovers, and who holds the keys to shared accounts.
04	**Your Digital Footprint.** How harmless public pieces combine, and a six-step audit run from a stranger's point of view.
05	**Networks, Wi-Fi, and Public Environments.** What a network sees, when a VPN helps, and device discipline at group events.
06	**Building a Group Digital Security Standard.** A checkable two-page standard with joining, lost-device, and departure routines.
07	**Capstone: Group Digital Security Audit.** Score your own group on evidence and leave with a dated remediation plan.

For every group member. SEC-02 recommended first. About 30 to 40 minutes per lesson; the capstone is a one-hour group session.

RELATED FFTP COURSES

SEC-02: Know What You're Showing	Security	Identifies the critical information SEC-04 protects
INT-09: OPSEC for Households	Intelligence	The household audit that feeds the footprint audit
MAG-02: MAG Security Assessment	MAG	Uses the group standard and the audit result