

Technology Failure & Connectivity Protocol

Purpose: To provide a standardized procedure for unavoidable internet outages, hardware failures, or software disruptions during live instruction.

Policy Guidelines:

- **Immediate Notification:** If a trainee experiences a localized internet outage or hardware failure, they must immediately notify the Lead Instructor via email or phone using a secondary device (e.g., a cellular phone).
- **System Outages:** In the event of a widespread platform outage (e.g., a Zoom or Google Drive server crash), the instructor will email an alternative secure link or asynchronous reading assignment within 30 minutes.
- **Grace Period:** Trainees who drop from the live feed due to connectivity drops will be granted a 15-minute grace period to rejoin the session without being penalized for a tardy or absence.
- **Make-Up Instruction:** Trainees are solely responsible for coordinating with the instructor to review recorded lecture material or complete alternative assignments for any time lost due to technical failures.

Purpose: To ensure all enrolled trainees possess the necessary digital infrastructure and software proficiencies prior to Day 1 of instruction.

Policy Guidelines:

- **Mandatory Orientation:** All newly enrolled trainees must attend a mandatory 60-minute virtual orientation prior to the first day of class to verify system compatibility and receive access credentials for the central curriculum repository.
- **Equipment Standards:** Trainees must possess a reliable computer, a steady broadband connection, and a standard headset with a built-in microphone to prevent audio feedback during live sessions.
- **Overcoming the Digital Divide:** Trainees residing in rural areas without access to reliable home internet are authorized and encouraged to utilize the public workstations and private study rooms at local facilities (e.g., regional public libraries).

- **Software Compliance:** Trainees must ensure their virtual meeting software and document processing applications are updated to the latest secure versions to protect the integrity of the Technical Data Packages (TDPs) shared during class.