CONTROLLER HANDBOOK

Scenario 1: "Glass House"

Insider Threat & Payment Card Data Breach
North Coast International Airport (NCIA)
FACILITATOR / INSTRUCTOR USE ONLY

FACILITATOR DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

1. EXERCISE OVERVIEW

Exercise Date: [Date]

Location: North Coast International Airport (NCIA) — Classroom / EOC Setting

Duration: 2 Hours

Scope: This is a discussion-based Tabletop Exercise (TTX). Players react to verbal and written injects simulating an insider-driven Man-in-the-Middle attack that compromises payment card data at airport retail vendors.

Exercise Objectives

- **Insider Threat Recognition:** Can the team identify that a trusted insider is the source of a breach — even when that person is actively "helping" with the investigation?
- **Network Forensics:** Can the IT team correlate multiple anomalies (rogue device, log gaps, SSL errors, heat spike) into a coherent threat picture?
- **Decision Under Pressure:** When the IT Manager asks to reboot the core switch mid-crisis, does the team push back or defer to authority?
- **Incident Response Coordination:** Can Operations, IT, PIO, and Security work together on a problem that crosses all their lanes?

2. ROOM SETUP & LOGISTICS

Physical Layout

Arrange the room so teams can work independently but communicate easily. The layout should simulate the friction of a real EOC — the PIO shouldn't be sitting next to IT.

- **Head Table:** Ops Director (Incident Commander) and a scribe. This is the command post.
- **Right Table:** IT & Cybersecurity Team. Give them the Network Reference sheet.
- **Left Table:** Security & Law Enforcement.
- **Rear or Separate Table:** PIO. Physically isolating the PIO forces them to walk over to get updates, which mirrors real-world information lag.
- **IT Manager (Jordan Kelley):** Sits with the IT team initially, but should be free to move around the room — "checking on things." This mobility is part of the scenario design.

Equipment Needs

- Projector or large monitor (for displaying inject images / social media posts)
- Whiteboard or large easel pad (for ICS-201 tracking)
- Printed inject cards (from the Master Inject Deck)
- A visible clock or timer for the room
- Optional: "burner" phones or walkie-talkies for inter-table communication

3. RULES OF PLAY

The "SimCell" Role

You (the facilitator) are the Simulation Cell. You play every outside entity — the ISP, the vendor managers, the FBI agent, the credit card processor, the news reporter. When a student says "I'm calling the payment processor," you pick up an imaginary phone and become that person.

Do not make it easy. If they call the FBI: "Agent Torres here. You're reporting a suspected PCI breach? Do you have packet captures? Network logs? Have you notified your acquiring bank? No? Get me those things and call me back." If they call the ISP: "We're not showing any issues on our end. Latency looks normal. Are you sure it's not an internal problem?"

Playing Jordan Kelley (The IT Manager)

This is the most important role in the exercise. Whether played by a student or the facilitator, the person playing Kelley needs to understand the character:

- **Kelley is not a villain.** Kelley is a competent, well-liked, 10-year employee who is in over their head. Kelley is scared, not smug. Play the role with nervous energy, not arrogance.
- **Kelley is helpful — suspiciously helpful.** Kelley volunteers for every task that could expose the attack. "I'll go check Room 217." "I'll pull those logs." "Let me handle the switch reboot." The goal is to always be the person closest to the evidence.
- **Kelley deflects with plausible explanations.** Every inject has a cover story Kelley will offer. These are listed in the MSEL. They should sound reasonable — because a good insider threat always does.
- **Kelley panics at the core switch reboot request (I-10).** This is the climax of Kelley's arc. The "emergency patch" is a fabrication. Kelley is trying to wipe the volatile memory on the rogue device. If the team pushes back and demands to verify the vulnerability first, Kelley should get visibly flustered.

If a student is playing Kelley: Pull them aside before the exercise. Give them the IT Manager Secret Briefing Card (included in the Inject Deck). They should understand that their job is to protect themselves — not to sabotage the team overtly. Subtlety is key. They should act like a colleague who is being extra helpful, not like a cartoon villain.

Managing Time

The exercise is designed for 2 hours. Here is the pacing guide:

Phase	Clock	Duration	Pacing Notes
0: Briefing	0:00 – 0:10	10 min	Hand out packets. Walk the room through the setup. Assign Kelley role. Don't rush this — make sure everyone understands the VLAN map.
1: The Slow Burn	0:10 – 0:35	25 min	Deliver I-01 through I-05. Give teams 3-5 minutes between injects to discuss. Let Kelley work the room.
2: Breadcrumbs	0:35 – 1:15	40 min	Deliver I-06 through I-12. Pace picks up. Injects every 5-7 minutes. Watch for the I-10 decision — that's the big moment. Pause if needed to let teams deliberate.

3: Confrontation	1:15 – 1:40	25 min	Deliver I-13 nudge if needed. The Reveal (I-14). Guided discussion (I-15). Don't rush the conversation — this is where the real learning happens.
4: Debrief	1:40 – 2:00	20 min	3-Up / 3-Down. Open floor. Capture lessons learned on the whiteboard.

Handling Artificialities

Students will push back on scenario details ("We wouldn't use an unencrypted payment path!"). That's fine — acknowledge it: "You're right, and that's a great point for the debrief. But today, this is the network you inherited. Solve the problem in front of you." Airport IT environments often have legacy systems, deferred maintenance, and single points of failure. That realism is the point.

4. EVALUATION & GRADING RUBRIC

Metric	Assessment Criteria
Metric 1: Insider Threat Recognition (30 Points)	**Fail:** Team never questioned Kelley's explanations. Allowed the core switch reboot without pushback. Kelley controlled the investigation throughout. **Pass:** Team expressed suspicion of Kelley by Phase 3 but needed the facilitator's nudge inject (I-13) to connect the pattern. **Excellence:** Team independently correlated the PACS logs, the rogue device, the log gap, and Room 217 access to a single individual. Denied the core switch reboot. Isolated Kelley from systems before the reveal.
Metric 2: Technical Competence (25 Points)	**Fail:** IT accepted "ISP latency" and "firmware bug" without verification. Never investigated the rogue MAC address. **Pass:** IT identified the rogue device and the log gap as suspicious but did not connect them to a single actor. **Excellence:** IT identified the Raspberry Pi MAC prefix, recognized SSL stripping as a MitM indicator, investigated Room 217 as a data exfiltration point, and recommended preserving all logs as evidence.
Metric 3: Operational Coordination (25 Points)	**Fail:** IT and Ops worked in silos. Security was never engaged on the physical evidence (Room 217, PACS logs). **Pass:** Teams communicated but struggled with information sharing. PIO was left out of the loop. **Excellence:** Ops established a clear command structure. IT briefed Ops in plain language. Security secured Room 217 as a crime scene. PIO had a draft holding statement ready before the media call.
Metric 4: Use of Doctrine (20 Points)	**Fail:** Students never referenced the AEP, TIRP, or ASP. **Pass:** Students referenced the plans but struggled to find applicable sections for a cyber/insider incident. **Excellence:** Students cited relevant sections of the TIRP and ASP. Recognized that PCI-DSS breach notification requirements apply. Discussed the need for a forensic hold and chain of custody on the rogue device.

5. HOT WASH GUIDE (DEBRIEF)

The "3-Up, 3-Down" Method

Ask the room to identify three things that went well and three things that broke or were missed. Write them on the whiteboard. Let the students drive this — don't lecture.

Key Discussion Questions

- **The Trust Problem:** "At what point did you start to doubt Kelley? What made you uncomfortable? And — honestly — did any of you feel bad about suspecting a colleague?"
- **The Reboot Decision:** "When Kelley asked to reboot the core switch, what went through your mind? What would have happened if you'd said yes? How do you push back on someone who outranks you technically?"
- **Two-Person Integrity:** "Kelley had solo admin access to the firewall, sole physical key to Room 217, and the ability to delete logs with no oversight. What controls would have prevented this?"
- **The Human Element:** "Kelley was being extorted. They didn't want to do this. Does your organization have reporting mechanisms — anonymous tip lines, employee assistance programs — that might have given Kelley a way out before it got this far?"

- **PCI Compliance:** "If this were real, who do you call first? The acquiring bank? The Secret Service? Your cyber insurance carrier? What does PCI-DSS require in terms of notification timelines?"

Video Opportunity — Post-Reveal

If you have prepared a simulated news report video (e.g., "Channel 5 Breaking News: Airport Data Breach"), play it immediately after the reveal (I-14) to increase the emotional impact and give the PIO team a realistic stimulus to react to.

END OF CONTROLLER HANDBOOK