Incident Handling Guide

Opossum Dynamics Internal Protocol – Deny Everything™ Edition

---

Introduction

Security incidents are not failures — they are *unexpected research opportunities.*
When things go wrong (and they will), it's critical to follow the official incident response strategy, which has been honed over years of minor disasters and major investigations.

Step 1: Do Not Panic

Remain calm. Or at least *appear* calm. Internal testing has shown that panic spreads faster than malware.

Take a breath. Then…

Step 2: Deny Everything™ Protocol

If a breach is suspected:

- **Deny knowing anything.**
- **Deny having access to anything.**
- **Deny that a breach occurred at all.**

This is your **first line of defense** — against attackers and auditors alike.

Use phrases like:

- "That's above my clearance level."
- "I thought that was part of a drill."
- "Who's Greg?"

Step 3: Escalation Path

After initial denial, begin the actual escalation process:

1. **Inform Legal (Greg).**
   This step is always first. Greg is both legal and IT. He will pretend to understand and open a ticket in the system (i.e., write it down on a napkin).

2. **Notify Security Ops.**
   If it's after 5 PM or on a weekend, this team may not respond. Consider this your time to shine.

3. **Contain the Breach.**
   Unplug things. Lock doors. Physically remove devices if needed. Remember: containment is 80% looking like you're doing something.

4. **Document Everything You Can (Except What You Denied).**
   Write down what happened, when, and what actions were taken — and redact anything that would legally implicate us.

Step 4: Debriefing

If the incident was part of a drill, you'll receive a "Nice Try" mug.

If it wasn't a drill, the debrief will be held in:

- A secure location
- A moving vehicle
- Or Greg's garage, depending on the nature of the breach

Incident Categories

- **Category A** – Greg-level breach. Treat as high priority. Greg should not be involved unless Greg is the problem.

- **Category B** – Routine compromise (e.g., someone opened “invoice.pdf.exe”).
- **Category C** – Internal sabotage or performance art (often hard to distinguish).