SME Incident Response Plan (IRP)

Confidential: Internal Use Only Emergency Contact: [IT/Security Lead Name/Phone]

Step 1: Detection & Analysis

- **Identify:** Determine if an anomaly is a security incident (e.g., ransomware note, unusual login, mass data export).
- **Scope:** Identify which systems, data sets, or users are affected.
- **Log:** Start a timeline of events. Record what was seen, when, and by whom.

Step 2: Containment

- **Immediate Action:** Disconnect infected workstations from the network (unplug Ethernet or disable Wi-Fi). **Do not turn the machine off** unless instructed, as volatile memory may be needed for forensics.
- **Account Lockdown:** Reset passwords and revoke active sessions for compromised or high-privilege accounts.
- **Isolation:** Segment the affected portion of the network to prevent lateral movement of malware.

Step 3: Eradication

- **Root Cause:** Identify how the attacker gained access (e.g., unpatched software, phishing).
- **Sanitization:** Remove malware, backdoors, and malicious scripts from the environment.
- **Patching:** Ensure all vulnerabilities related to the incident are fully patched before bringing systems back online.

Step 4: Recovery

- **Restore:** Restore data from the most recent "clean" backup. Verify the integrity of the backup before deployment.
- **Phased Re-entry:** Bring systems online one by one and monitor for signs of re-infection or residual attacker activity.
- **Business Continuity:** Notify affected clients or stakeholders if legally required (consult legal counsel regarding GDPR/CCPA timelines).

Step 5: Lessons Learned

- **Post-Incident Meeting:** Within 72 hours, hold a debrief with the response team.
- **Gap Analysis:** What worked? Where were the delays?
- **Update:** Modify this IRP and the AUP to prevent a recurrence of the same attack vector.