LDM

LAMSON DUGAN & MURRAY LLP
ATTORNEYS AT LAW

■ Cyberattack Response Quick Guide ■

1. Disconnect & Contain

- Unplug affected workstations, servers, or networked devices immediately.
- Disable compromised user accounts and restrict access to shared drives or systems.
- Isolate infected machines to prevent further spread across the network.

2. Alert Internal Teams

- Immediately notify your IT department or cybersecurity lead.
- Include all known details: what occurred, who discovered it, what systems are affected, and the time of occurrence.
- Use designated secure communication channels when possible (e.g., phone or internal hotline).

3. Preserve Evidence

- Do not wipe or reimage infected systems until directed by IT/security personnel.
- Retain logs, error messages, suspicious emails, attachments, and file paths.
- Take screenshots or photos of on-screen errors or warnings if relevant.

4. Notify Leadership & Legal

- Alert department heads and follow chain-of-command protocols for escalation.
- Contact legal counsel immediately to assess breach notification duties under law.
- Avoid discussing the incident publicly or sharing details on social media or with vendors.

5. Activate Incident Response Plan

- Follow the organization’s documented cyber incident response plan, if available.
- Assist IT and legal teams with any required documentation or interviews.
- Monitor systems for continued signs of intrusion while executing recovery procedures.