Incident Response Plan (IRP)

Smith’s Construction LLC

1. Purpose and Overview

Cyberattacks are not a matter of *if*, but *when*. Smith’s Construction LLC relies heavily on digital systems—Windows desktops, network printers, NAS devices, IoT devices, and cloud resources—and must be prepared to respond quickly and effectively to cyber incidents.

This Incident Response Plan (IRP) provides a structured, repeatable approach for identifying, analyzing, containing, eradicating, and recovering from cybersecurity incidents. It establishes formal responsibilities, communication channels, and step-by-step procedures to minimize damage, reduce downtime, and prevent recurrence.

This IRP aligns with standard Incident Response lifecycles and integrates tightly with the company’s Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

2. Scope

This IRP applies to:

- All employees of Smith’s Construction LLC
- All company-owned devices: desktops, laptops, printers, NAS devices, and office IoT equipment
- All network services, on-site and cloud-based
- The company’s AWS infrastructure and cloud storage
- Any third-party IT or cybersecurity vendors engaged during incidents

Any event that threatens the confidentiality, integrity, or availability of company systems, data, or operations falls under this plan.

3. Roles and Responsibilities

Incident Response Lead (IR Lead)

- Primary decision-maker during incidents
- Confirms validity of reported events

- Coordinates containment, eradication, and recovery
- Communicates with management, IT, employees, and external partners

Business Owner / Executive Management

- Approves major containment or shutdown actions
- Communicates with stakeholders when necessary
- Authorizes law enforcement involvement

IT Support / Security Engineer

- Performs technical containment and eradication
- Reimages systems, restores data, blocks malicious traffic
- Maintains logs, tools, and forensic data

Employees

- Report suspicious activity immediately
- Follow IR instructions and assist in providing relevant information
- Avoid taking self-directed remediation actions

Third-Party IT Vendor (if involved)

- Provides advanced response capabilities
- Supports system recovery or forensic analysis

---

4. Communication Procedures

During an incident, all communications must follow defined channels to ensure clarity and prevent misinformation.

- **Primary Channel:** Company email (if operational)
- **Secondary Channel:** Company phone/text tree
- **Emergency Channel:** Direct phone call to IR Lead

External communications with customers, partners, or law enforcement must be coordinated **only** by the Business Owner or designated representative.

---

5. Incident Response Lifecycle

5.1 Preparation

Smith’s Construction maintains:

- Hardened Windows images for all desktops
- Anti-malware tools and IoC detection (e.g., Microsoft Defender, Malwarebytes)
- Centralized logging on NAS devices
- AWS-based backups
- Hot spare hardware components
- Password and identity policies (MFA enforced for AWS and cloud apps)
- Employee security awareness training
- Established escalation chain

Employees must immediately report suspicious emails, network slowness, unauthorized access attempts, abnormal IoT behavior, or unexpected system reboots.

5.2 Detection and Analysis

When a suspicious event occurs:

1. **Initial Detection**
   - May come from employee observation, automated alerts, or antivirus notifications.
2. **Indicators of Compromise (IoCs) to watch for**
   - Unexpected credential prompts
   - Suspicious outbound network traffic
   - Malware scanner alerts
   - Unauthorized account activity
   - Ransom notes or encryption symptoms
3. **IR Lead Analysis**
   - Validate IoCs using logs, antivirus scan results, AWS CloudTrail logs, or threat intelligence sources.
4. **Incident Classification**
   - Low severity: User error, spam emails, blocked threat
   - Medium severity: Localized malware infection or compromised workstation
   - High severity: Ransomware, network-wide intrusion, data exfiltration

If confirmed, the incident proceeds to Containment.

5.3 Containment

The goal is to stop the threat from spreading.

Actions may include:

- Disconnecting infected desktops or IoT devices from the network
- Disabling compromised user accounts
- Revoking suspicious active sessions
- Blocking malicious IP addresses or domains
- Halting file synchronizations if AWS or NAS compromise is suspected

If needed, the IR Lead contacts the third-party IT vendor for support.
Documentation of all steps must begin at this stage.

5.4 Eradication

After containment, remove the threat entirely.

Common eradication steps:

- Run anti-malware scans (Microsoft Defender, Malwarebytes)
- Delete malicious files and registry entries
- Reimage infected systems using clean company Windows images
- Reset affected user credentials
- Remove unauthorized applications or scripts
- Patch exploited vulnerabilities

For IoT devices, factory resets may be required due to limited security controls.

5.5 Recovery

Restore normal business operations carefully and gradually.

Potential actions:

- Restore files from on-site NAS or AWS backups
- Validate system integrity before reconnecting to the network
- Re-enable previously disabled user accounts
- Update firewall and web filtering rules
- Replace damaged hardware with hot spare components
- Monitor systems closely for signs of recurring compromise

If sensitive data was breached:

- Notify leadership immediately
- Prepare customer or vendor notifications
- Coordinate with legal counsel

- Contact law enforcement, if required under regulations or insurance policies

Recovery concludes only after systems are stable and verified safe.

5.6 Lessons Learned

Within 7–14 days after closing an incident, the cybersecurity/IT team conducts a structured review.

Discuss:

- What happened
- How it was detected
- What worked
- What failed
- How well the IR, DR, and BCP procedures performed
- What improvements are required

Artifacts to archive:

- Antivirus reports
- Log files and forensic data
- Emails or screenshots of phishing attempts
- Timeline of actions
- Final incident summary report

Lessons Learned meetings should drive ongoing hardening and policy updates.

---

6. Incident Types and IR Playbooks

Smith’s Construction experiences elevated risk for:

- **IoT attacks**
- **Insider threats**
- **Malware infections**
- **Phishing campaigns**

Dedicated IR playbooks should be maintained for each scenario, including:

- Specific detection patterns
- Targeted containment steps
- Recovery guidance

- Relevant stakeholders

Past anti-malware scan transcripts, AWS GuardDuty findings, and historical incidents should be used to refine these playbooks over time.

---

7. Documentation Requirements

For every incident:

- Date/time detected
- Reporter name
- Systems involved
- Indicators of compromise
- Containment actions taken
- Eradication tools used
- Recovery steps
- Communication records
- Final disposition

Documentation is stored in the IR archive on the NAS and AWS backup.

---

8. Distribution and Maintenance

This IRP must be distributed to:

- All IT/security personnel
- Company leadership
- Relevant third-party vendors (as needed)

Annual tabletop exercises must test the IRP, DRP, and BCP together.
Updates should occur after:

- Major incidents
- New technologies added to the environment
- New threats identified
- Annual policy reviews