Incident Response Plan

Policy Owner: VIMBuild, LLC
Author: Martin Ashton
Effective Date: 02/06/2025

Purpose

This document establishes the plan for managing information security incidents and events and offers guidance for employees or incident responders who believe they have discovered or are responding to a security incident.

Scope

This policy covers all information security or data privacy events or incidents.

Incident and Event Definitions

- **Security Event:** An observable occurrence relevant to the confidentiality, availability, integrity, or privacy of company-controlled data, systems, or networks.
- **Security Incident:** A security event that results in loss or damage to the confidentiality, availability, integrity, or privacy of company-controlled data, systems, or networks.

Incident Reporting & Documentation

Reporting

If a VIMBuild, LLC employee, contractor, user, or customer becomes aware of an information security event, incident, policy violation, security weakness, or suspicious activity, they shall immediately report it using designated communication channels.

Reports should include specific details about what has been observed or discovered.

Severity Levels

Incidents shall be categorized as follows:

- **S3/S4 – Low and Medium Severity:** Suspicious or odd behaviors requiring further investigation, e.g., lost/stolen encrypted laptops, phishing emails.
- **S2 – High Severity:** Issues with a likelihood of adversarial persistence, e.g., lost/stolen unencrypted laptops, high-risk vulnerabilities, malware.
- **S1 – Critical Severity:** Actively exploited risks that put individuals or systems at immediate risk, requiring emergency response.

Escalation and Internal Reporting

- **S1 (Critical):** Requires immediate notification to the Administrator.
- **S2 (High):** Requires ticket creation and notification of appropriate Department Head.

- **S3/S4 (Medium/Low):** Requires ticket creation and notification of appropriate Department Head.

Documentation

All reported security events, incidents, and response activities shall be documented. A root cause analysis may be performed on all verified security incidents and reviewed by the Administrator and IT Managers.

Incident Response Process

For critical issues, the response team will follow a structured approach:

1. **Event Reported**
2. **Triage and Analysis**
3. **Investigation**
4. **Containment & Neutralization**
5. **Recovery & Vulnerability Remediation**
6. **Hardening & Detection Improvements**

Incident Response Meeting Agenda

- Update incident ticket and timelines
- Document new Indicators of Compromise (IOCs)
- Perform investigative Q&A
- Apply emergency mitigations
- Plan long-term mitigations
- Document Root Cause Analysis (RCA)

Special Considerations

Internal Issues

Incidents involving internal employees, contractors, or partners require sensitive handling. The Incident Manager shall contact the CEO and President directly.

Compromised Communications

If IT communication risks exist, an alternative secure channel will be established for responders.

Root Account Compromise

If a Microsoft Azure root account compromise is suspected, follow the procedures outlined in **Appendix D**.

Additional Requirements

- All suspected incidents shall be documented and assessed.
- Incident response shall follow documented procedures.
- Incident-related evidence shall be collected and preserved in accordance with industry best practices (e.g., NIST SP 800-86).
- Unauthorized access events shall be reviewed by the Incident Response Team.
- VIMBuild, LLC shall promptly notify affected parties and regulatory agencies as required.

- The Incident Response Plan shall be reviewed and tested annually.

External Communications & Breach Reporting

Legal and executive staff shall determine if breach reporting is necessary. Breaches shall be reported to affected customers, consumers, or regulators without undue delay.

No personnel may disclose information regarding an incident or potential breach without prior approval from legal and/or executive management.

Mitigation & Remediation

Legal and executive staff shall determine any immediate or long-term mitigation or remedial actions to be taken as a result of an incident or breach.

Roles & Responsibilities

Role	Responsibility
Incident Manager	Leads response efforts, assigns follow-up activities, reports incidents to the Administrator.
Incident Response Team (IRT)	Engaged in handling incidents until resolution.
Engineers (Support & Development)	Investigate security incidents, implement mitigations.
Users (Employees & Contractors)	Report security incidents and follow policies.
Customers	Report issues with VIMBuild, LLC services.
Legal Counsel	Determines legal exposure, reviews external breach notifications.
Executive Management	Approves breach determinations and response strategies.

Management Commitment

VIMBuild, LLC management commits to providing resources, tools, and training necessary to respond effectively to security events and incidents.

Exceptions

Requests for exceptions to this policy must be submitted to and approved by the Administrator.

Violations & Enforcement

Any known violations should be reported to the CEO. Violations may result in suspension of system access and/or disciplinary action, up to termination of employment.

Appendix A – Contact Information

Details on incident escalation contacts are available in Roles.

Appendix B – Incident Collection Form

Incident Detector's Information

- Name:
- Date & Time Detected:
- Title:
- Contact Details:

Incident Summary

- Type of Incident Detected:
- How was the Incident Detected?
- Location(s) of Affected Systems:
- Description of Affected Systems:

Appendix C – HIPAA Breach Procedures

In the event of a potential HIPAA breach, the Administrator must be notified immediately.

Appendix D – Azure Root Account Compromise Playbook

Guidelines for handling Azure root account compromise, including:

- Establish control
- Determine impact
- Recover systems
- Investigate root cause
- Implement security improvements