Divy It Up Incident Response Plan

Divy It Up, LLC

Document creation Date:	June 16, 2025
Effective Date:	July 2, 2025
Version:	1.3
Classification:	Public

---

1. Document Purpose

The purpose of this Incident Response Plan is to establish procedures for identifying, responding to, and mitigating security incidents affecting the systems or data of Divy It Up, Inc.

The Company is committed to responding quickly and effectively to any potential security threats or breaches.

---

2. Document Scope

This plan applies to all systems operated by the Company, including:

- Cloud infrastructure
- Databases
- Web and mobile applications
- Third-party integrations
- Development and production environments

---

3. Definition of a Security Incident

A security incident includes any event that could compromise the confidentiality, integrity, or availability of Company systems or data.

Examples include:

- Unauthorized access to systems

- Credential compromise
- Data exposure or leakage
- Infrastructure intrusion
- Malware or malicious activity
- Denial-of-service attacks
- Compromise of API credentials or tokens

---

4. Incident Response Objectives

The Company's incident response process is designed to:

- Quickly detect security events
- Contain potential damage
- Preserve system integrity
- Investigate root causes
- Restore normal operations
- Prevent recurrence

---

5. Incident Response Process

5.1 Detection

Security events may be detected through:

- System monitoring alerts
- Log analysis
- User reports
- Infrastructure monitoring
- Third-party notifications

Potential incidents are reviewed immediately upon discovery.

5.2 Containment

If a security incident is suspected, immediate actions may include:

- Disabling compromised credentials
- Isolating affected systems
- Blocking suspicious network activity
- Temporarily suspending affected integrations

The goal is to prevent further unauthorized access or damage.

5.3 Investigation

The Company will investigate incidents to determine:

- The scope of the event
- Systems or data affected
- Method of compromise
- Timeline of the incident

Logs and system data are reviewed to identify the root cause.

5.4 Remediation

After the incident is understood, remediation steps may include:

- Applying security patches
- Rotating credentials and API keys
- Updating system configurations
- Restoring affected systems from backups

Security improvements may also be implemented to prevent recurrence.

5.5 Recovery

Systems are restored to normal operation once security has been verified and vulnerabilities have been addressed.

Monitoring is increased temporarily following an incident to ensure stability.

---

6. Notification

If a security incident affects customer data or integrated services, the Company may notify:

- Affected users
- Relevant service providers
- Regulatory authorities where required

Notification will be conducted in accordance with applicable laws and contractual obligations.

---

7. Post-Incident Review

Following resolution of an incident, the Company performs a review to:

- Document the incident
- Evaluate response effectiveness
- Identify security improvements
- Update policies or procedures if necessary

Lessons learned are incorporated into future security practices.

---

8. Contact

Security incidents or concerns should be reported to:

Security Team
Divy It Up, Inc.
security@divyitup.com