Information Security Policy

Divy It Up, LLC

Document creation Date: June 15, 2025
Effective Date: July 2, 2025
Version: 1.2
Classification: Public

1. Purpose

The purpose of this Incident Response Plan is to establish a structured, effective, and compliant process for identifying, responding to, managing, and recovering from security incidents affecting Divy It Up, LLC (the "Company") systems, data, or services.

This plan ensures rapid detection and containment, minimizes impact to customers and operations, preserves evidence for investigation and regulatory requirements, and drives continuous improvement in the Company's security posture.

2. Scope

This plan applies to all Company systems, data, and personnel, including:

- Cloud infrastructure and environments
- Databases and data stores
- Web and mobile applications
- Third-party integrations (including Plaid and financial service providers)
- Development, staging, and production environments
- All employees, contractors, and service providers with access to Company systems

3. Incident Response Team (IRT)

The Company maintains a cross-functional Incident Response Team responsible for executing this plan.

Role	Primary Responsibilities	Escalation Contact
Incident Response Lead (CISO/Security Lead)	Overall coordination, decision-making, reporting	CEO
Security Analyst	Investigation, forensics, containment	IR Lead
Systems/DevOps Engineer	Technical remediation and recovery	IR Lead
Legal/Compliance Officer	Notification, regulatory obligations, documentation	CEO
Communications Lead	Internal & external communications	CEO

The IRT may be augmented with external experts (forensics, legal counsel) as needed.

4. Definition and Classification of Security Incidents

A security incident is any event that actually or potentially compromises the confidentiality, integrity, or availability of Company systems or data.

Incident Severity Levels

Severity	Description	Examples	Target Response Time
Critical	Active breach with high risk to customer data or operations	Credential compromise, data exfiltration, ransomware	< 1 hour
High	Significant impact or high likelihood of escalation	Unauthorized access, malware on production systems	< 4 hours
Medium	Limited impact, contained to non-production	Suspicious login attempts, minor misconfiguration	< 24 hours
Low	No immediate risk, informational	Failed login attempts, policy violations	72 hours

5. Incident Response Process

The Company follows a six-phase process based on NIST SP 800-61 guidelines.

5.1 Preparation

- Maintain up-to-date contact lists, tools, and playbooks
- Conduct quarterly tabletop exercises and annual full simulations
- Ensure logging, monitoring, and backup systems are operational

5.2 Detection & Analysis (Identification)

Security events are detected via:

- Centralized monitoring and SIEM alerts
- Log analysis and anomaly detection
- User or third-party reports
- Automated vulnerability scans

All potential incidents are triaged within 30 minutes.

5.3 Containment

Immediate actions to limit damage:

- Isolate affected systems or networks

- Disable or rotate compromised credentials
- Block malicious IP addresses or API calls
- Suspend affected integrations if necessary

Short-term and long-term containment strategies are applied as appropriate.

5.4 Eradication

Remove the root cause:

- Eliminate malware or backdoors
- Patch vulnerabilities
- Remove unauthorized accounts or access
- Rebuild affected systems from clean backups when required

5.5 Recovery

- Restore systems from verified clean backups
- Validate system integrity and security controls
- Gradually bring systems back online with enhanced monitoring
- Monitor for 72 hours post-recovery to confirm stability

5.6 Post-Incident Activity (Lessons Learned)

- Conduct a formal after-action review within 5 business days
- Document findings in a Post-Incident Report
- Update policies, procedures, and controls as needed
- Share lessons learned with the broader team

6. Evidence Preservation and Forensics

- All actions taken during an incident must be logged with timestamps
- Chain-of-custody procedures are followed for any forensic evidence
- Memory dumps, log files, and relevant artifacts are preserved before system changes
- External digital forensics support is engaged for Critical or High-severity incidents

7. Notification and Communication

Notifications are made in accordance with applicable laws (e.g., state breach notification laws, contractual obligations with financial partners).

Timeline:

- Internal leadership notified within 1 hour (Critical/High)
- Affected customers notified within 72 hours (if required by law or contract)
- Regulatory authorities notified within required legal deadlines

Communication Channels:

- Internal: Slack #incident-response channel + emergency phone tree
- External: Pre-approved templates managed by Communications Lead

8. Plan Testing and Maintenance

- This plan is reviewed and updated annually or after any major incident
- Tabletop exercises are conducted quarterly
- Full incident simulation is performed at least annually
- Contact lists and tool access are validated monthly

9. Contact Information

Security incidents or concerns must be reported immediately to:

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