Rezolve.ai

Incident Response Plan

Purpose:
To ensure a rapid, coordinated, and effective response to all information security incidents, including ransomware and cloud security threats.

Scope:
Applies to all incidents impacting Rezolve.ai's cloud infrastructure, servers, workstations, endpoints, networks, and backup systems, including administrative, HR, security, IT, operational, customer service, and cloud security incidents.

Incidents:
An incident is any unplanned interruption or quality degradation of a service, including security breaches, ransomware, data loss, unauthorized access, or system outages.

Incident Management Lifecycle:

- **Detection & Logging:**
  Incidents are detected through automated monitoring, user reports, or technical alerts and immediately logged in the incident management system (e.g., Jira).
- **Classification & Prioritization:**
  Incidents are categorized and prioritized based on impact and urgency, following predefined criteria and SLAs.
- **Escalation:**
  Functional and hierarchical escalation paths are established. Specialized incidents such as ransomware are escalated to designated internal or third-party experts with the necessary expertise.
- **Containment & Analysis:**
  Immediate containment actions are taken to isolate affected systems and preserve forensic evidence and audit logs before restoration. Root cause analysis is performed using documented runbooks and knowledge bases.
- **Resolution & Recovery:**
  Systems and data are restored securely following mitigation of exploited vulnerabilities. Post-incident reviews capture lessons learned to improve future response.
- **Communication:**
  Stakeholders- including employees, customers, vendors, legal counsel, cyber insurance providers, regulators, and law enforcement are notified as appropriate. Internal staff are provided with prepared documentation to respond to customer inquiries.

Ransomware-Specific Response Procedures:
The Incident Response Plan explicitly includes ransomware as a critical security incident and incorporates the following procedures:

- Immediate notification of legal counsel and cyber insurance companies.
- Preservation of forensic evidence and audit logs prior to any restoration.
- Determination of infection scope via specialized third parties or qualified internal resources.
- Isolation and prevention of ransomware spread to other systems.
- Engagement with federal law enforcement when applicable for decryption keys and evidence preservation.
- Root cause identification and mitigation of all exploited vulnerabilities.
- Restoration of affected systems and data as needed.
- Designation of authority to revoke third-party network access promptly.
- Regular updating of contact information for incident response partners.
- Timely notification of all affected employees, customers, vendors, and stakeholders.
- Coordination of communications to ensure transparency and regulatory compliance.

Security Controls & Compliance:

- Role-based access and least privilege principles enforced across all resources.
- Data hosted and backed up in Microsoft Azure with encryption, network segmentation, and multi-factor authentication.
- Continuous monitoring, Data Loss Prevention (DLP) via Sequrite, and automated alerting to detect suspicious activities.
- Backups protected with immutability and isolation to ensure ransomware resilience.

Reporting & Metrics:

- Incident metrics such as resolution times, SLA compliance, and root cause trends are tracked and reviewed regularly.
- Reports support management oversight and compliance audits.

Continuous Improvement:

- Lessons learned from incidents are incorporated into updated policies, runbooks, and the knowledge base.

- The incident response plan is reviewed annually or following significant incidents to maintain effectiveness and compliance.

Contacts & Responsibilities:

- A designated incident response coordinator (internal or third-party) manages and coordinates all aspects of incident response, including ransomware and cloud security events.

Note: This plan is reviewed at least annually and after significant incidents.

For detailed procedures or escalation contacts, refer to the full Incident Management Policy or contact the Rezolve.ai Security Compliance team.