Cloud Application Incident Response Plan Template

1. Objective

Summarize the purpose and scope of the incident response plan, including the applications and cloud environments covered.

2. Definitions

Term	Definition
Incident	An unplanned event which may impact the security, availability, or integrity of cloud applications.
Severity Level	Classification for incident impact (e.g., Critical, High, Medium, Low).
Stakeholder	Person or entity with an interest or responsibility regarding the incident outcome.

3. Incident Response Team

- **Role:** (e.g., Incident Commander) - *Name/Contact*
- **Role:** (e.g., Cloud Admin) - *Name/Contact*
- **Role:** (e.g., Comms Lead) - *Name/Contact*

4. Incident Classification

Define severity levels and examples:

Level	Criteria
Critical	Outage impacting all users, data breach, legal obligation to report.
High	Major functionality loss, possible data exposure, urgent remediation.
Medium	Limited impact, workaround available, investigation required.
Low	Minor issue, little impact, routine monitoring.

5. Response Phases

1. **Preparation:** Team readiness, training, tool maintenance.
2. **Identification:** Detect and validate incident.
3. **Containment:** Limit spread, isolate affected components.
4. **Eradication:** Remove cause, remediate vulnerabilities.
5. **Recovery:** Restore normal operations, monitor systems.
6. **Lessons Learned:** Document incident, update response plan.

6. Notification & Escalation

- Internal escalation protocol
- External communication requirements
- Regulatory/legal notification criteria

7. Third-Party Coordination

- List cloud providers and contact procedures
- Interface with external support and incident teams

8. Documentation & Reporting

- Incident tracking methods
- Post-incident reporting template
- Retention of evidence/logs

9. Review & Update

- Periodic review schedule
- Trigger for unscheduled plan updates

10. Appendix

- Contact Directory
- Communication Templates
- Reference Documents