Incident Response Summary — [INCIDENT]

Version: v1.0 · Date: 2025-02-15 · Confidential

Executive Summary

- Summary: [SUMMARY]
- Status: [STATUS]
- Impact: [IMPACT]

Immediate Next Actions

- [ ] [ACTION_TODAY]
- [ ] [ACTION_TOMORROW]

Incident Details

- Timeline: [TIMELINE]
- Scope: [SYSTEMS]
- Root Cause: [ROOT_CAUSE]

Forensics & Evidence

- IOCs, logs, artifacts, hashes

Containment & Eradication

- Steps executed, residual risks

Recovery

- Service restoration, validation, comms

Recommendations

- Short-term hardening, medium-term projects, policy/process improvements

Appendices

- Ticket/PR list, detection rules, scripts, contacts