Incident Response Plan (IRP)

Pillar Lead: Phoenix (Access & Security)

I. Purpose and Scope

This plan defines the formal process for responding to security incidents involving Cygnus Covenant data, systems, or models, ensuring quick containment, eradication, and recovery. An "incident" is defined as any unauthorized access, denial of service, or violation of a governance policy resulting in system compromise or data loss.

II. Incident Response Phases

Phase 1: Preparation (Continuous)

1. **Team Readiness:** Maintain and regularly update the Incident Response Team (IRT) contact list (primary, secondary, and executive contacts).
2. **Tool Readiness:** Ensure all necessary forensic tools, logging systems, and secure communication channels are operational and accessible outside the compromised network segment.
3. **Training:** Conduct mandatory incident response drills (tabletop exercises) at least twice per year.

Phase 2: Detection and Analysis (Initial 60 Minutes)

1. **Detection:** Incidents are reported via automated monitoring (SIEM alerts) or manual user reporting.
2. **Triage:** The IRT Lead immediately assesses the severity (Critical, High, Medium, Low) based on impact and scope.
3. **Notification:** The IRT Lead notifies the relevant Pillar Leads (Cygnus, Orion) and the Executive team based on the severity rating within 60 minutes of detection.
4. **Analysis:** Determine the attack vector, source, time of compromise, and the scope of affected systems and data.

Phase 3: Containment, Eradication, and Mitigation

This phase prioritizes stopping the damage and removing the threat.

1. **Short-Term Containment:** Isolate affected network segments, shut down specific services, or revoke compromised credentials to halt the immediate threat. **The priority is to stop the bleed.**
2. **System Imaging:** Create forensic images of compromised servers and endpoints before eradication, preserving evidence.
3. **Eradication:** Fully remove the threat (malware, backdoors, unauthorized accounts). This includes patching vulnerabilities exploited by the attacker.

4. **Long-Term Containment:** Implement temporary hardening measures (e.g., firewall rule changes, network micro-segmentation).

Phase 4: Recovery

This phase focuses on restoring systems to normal operation.

1. **System Rebuild/Restore:** Restore services from trusted backups, ensuring integrity and functionality.
2. **Verification:** Implement heightened monitoring (per the DTS) to confirm all signs of the intruder have been eliminated.
3. **Production Restart:** The IRT Lead, in consultation with the Cygnus Pillar Lead, authorizes the return of affected services to production operation.

Phase 5: Post-Incident Activity (Within 7 Days)

1. **Lessons Learned:** The IRT Lead conducts a formal review meeting (Lessons Learned) to analyze what worked, what failed, and how to improve.
2. **Action Plan:** Create a formal action plan detailing necessary policy, technology, or procedure changes to prevent recurrence.
3. **Documentation:** Complete the final incident report, detailing the incident timeline, impact, response actions, and post-incident action plan.
4. **Policy Update:** Update the IAP, DTS, or other relevant governance documents based on the findings of the Lessons Learned meeting.