Business Continuity Plan for Google

To mitigate and respond to cybersecurity incidents while maintaining trust and service availability.

Google Cybersecurity Incident Response Plan

Objective:

To swiftly detect, contain, and recover from cybersecurity incidents to protect Google's users, services, and reputation.

Key Areas of the Plan

1. **Incident Detection and Monitoring**

• AI-Powered Threat Monitoring: Google Cloud's Chronicle SIEM continuously monitors for anomalies across the network.

• 24/7 Incident Response Center: Expert security engineers manage round-the-clock monitoring and initial triage.

• Threat Intelligence: Collaboration with global cybersecurity organizations to stay ahead of evolving threats.

2. **Incident Response Procedures**

• Phases of Response:

• Detection: Immediate validation and categorization of the threat.

• Containment: Isolate affected systems and minimize further damage.

• Eradication: Remove malicious artifacts and vulnerabilities.

• Recovery: Restore services and validate system integrity.

• Dedicated Response Teams:

• Cybersecurity Rapid Response Team (CRRT): Handles high-severity incidents.

• Privacy Task Force: Investigates potential data breaches.

3. **Proactive Risk Mitigation**

• Zero Trust Architecture: Continuous verification of users and devices across all systems.

• Regular Penetration Testing: Google employs ethical hackers to test and fortify systems.

• Bug Bounty Program: Incentivize external researchers to identify vulnerabilities.

4. **Training and Awareness**

• Employee Awareness Campaigns: Frequent phishing simulations and security workshops.

• Role-Specific Training: Advanced training for system administrators and developers.

5. **Incident Reporting and Transparency**

• Public Transparency Reports: Updates on cybersecurity incidents and resolutions.

• Collaboration with Authorities: Proactively report major breaches to regulators.