CyberSecure Inc. Incident Response Plan

A structured framework to prevent, detect, respond to, and recover from cybersecurity incidents.

Ensuring compliance, minimizing disruptions, and protecting sensitive data.

Incident Response Process

- 1. Preparation: Security controls, training, and monitoring.
- 2. Identification: Detecting security threats and assessing severity.
- 3. Containment: Isolating affected systems and limiting spread.
- 4. Eradication: Removing threats and strengthening security.
- 5. Recovery: Restoring systems and verifying integrity.
- 6. Lessons Learned: Post-incident review and improvements.

Incident Classification & Response

- Low Risk: Internal mitigation and documentation.
- Medium Risk: Investigation, containment, and monitoring.
- High Risk: Full-scale incident response and regulatory notification.
- Critical cyber threats require immediate action and coordinated response.

Continuous Improvement & Security Awareness

- Regular security audits and penetration testing.
- Employee training on phishing and social engineering.
- Updating response strategies based on threat intelligence.
- Strengthening compliance with evolving regulations.

Proactive security measures ensure resilience against evolving cyber threats.