DIG Personnel & Training Solutions Pty Ltd
ABN 62 689 103 900

17 White Road,
Gepps Cross SA 5094

PO Box 2528 Regency Park SA 5942

www.digpersonnel.com.au

SECURITY INCIDENT MANAGEMENT POLICY

Security Incident Management Policy

1. PURPOSE

The purpose of this Security Incident Management Policy is to establish a structured approach for identifying, reporting, assessing, responding to, and recovering from information security incidents. This policy aims to minimize business disruption, reduce the impact of security incidents, protect organizational assets, and ensure compliance with legal, regulatory, and contractual obligations.

2. SCOPE

This policy applies to:

- *All employees, contractors, consultants, temporary staff, and third parties who have access to organizational information, systems, networks, applications, or data.*
- *All information assets owned, leased, managed, or operated by the organization.*
- *All security incidents affecting the confidentiality, integrity, or availability of organizational information and services.*

3. POLICY STATEMENT

The organization is committed to the timely detection, reporting, investigation, containment, eradication, recovery, and post-incident review of all security incidents. All personnel are required to report suspected or actual security incidents immediately upon discovery.
The organization shall maintain documented incident response procedures and assign appropriate responsibilities to ensure effective incident management.

4. DEFINITIONS

Security Event
An observable occurrence within a system or network that may be relevant to security.
Security Incident
A security event or series of events that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of information assets.
Major Security Incident
A security incident that significantly impacts business operations, sensitive data, critical systems, regulatory compliance, or the organization's reputation.

5. ROLES AND RESPONSIBILITIES

Executive Management

- *Provide strategic oversight and support.*
- *Approve major incident response decisions.*
- *Ensure adequate resources are available.*

Information Security Team

- *Coordinate incident response activities.*
- *Investigate and analyze incidents.*

- *Maintain incident response procedures and tools.*
- *Report incident status to management.*

Information Technology Team

- *Support containment, eradication, and recovery activities.*
- *Preserve evidence when required.*
- *Implement corrective actions.*

Employees and Contractors

- *Immediately report suspected security incidents.*
- *Cooperate with investigations.*
- *Follow incident response instructions.*

Legal and Compliance Team

- *Assess legal, regulatory, and contractual obligations.*
- *Coordinate breach notification activities.*
- *Provide guidance on evidence handling and regulatory reporting.*

Communications Team

- *Manage internal and external communications.*
- *Coordinate media and stakeholder communications when required.*

6. INCIDENT CLASSIFICATION

Security incidents shall be classified based on severity, impact, and urgency.

Critical

- *Significant business disruption.*
- *Confirmed data breach involving sensitive information.*
- *Ransomware affecting critical systems.*
- *Regulatory reporting obligations likely.*

High

- *Compromise of important systems.*
- *Unauthorized access to sensitive data.*
- *Significant malware outbreaks.*

Medium

- *Limited system compromise.*
- *Policy violations with moderate impact.*
- *Localized malware infections.*

Low

- *Minor security events with minimal business impact.*
- *Unsuccessful attack attempts.*
- *Policy violations without material impact.*

7. INCIDENT MANAGEMENT PROCEDURE

7.1 Identification and Reporting

All personnel must immediately report:

- *Suspected malware infections.*
- *Unauthorized access attempts.*
- *Lost or stolen devices.*
- *Data leakage or suspected breaches.*
- *Phishing attacks.*
- *System compromise indicators.*
- *Any unusual or suspicious activity.*

Reports shall be submitted through approved incident reporting channels.

7.2 Triage and Assessment

The Information Security Team shall:

- *Validate the reported incident.*

- *Assess severity and business impact.*
- *Determine affected systems, users, and data.*
- *Assign an incident priority level.*

7.3 Containment

Appropriate containment measures may include:

- *Isolating affected systems.*
- *Disabling compromised accounts.*
- *Blocking malicious network activity.*
- *Restricting access to affected resources.*

Containment actions shall balance risk reduction with business continuity requirements.

7.4 Investigation and Evidence Preservation

The organization shall:

- *Collect and preserve relevant logs and evidence.*
- *Maintain chain-of-custody records where required.*
- *Document all response activities.*
- *Conduct forensic analysis when appropriate.*

7.5 Eradication

The organization shall remove the root cause of the incident, including:

- *Malware removal.*
- *Vulnerability remediation.*
- *Credential resets.*
- *Unauthorized access removal.*
- *Security control enhancements.*

7.6 Recovery

Recovery activities shall:

- *Restore systems and services securely.*
- *Verify system integrity.*
- *Monitor for recurring malicious activity.*
- *Confirm normal business operations have resumed.*

7.7 Post-Incident Review

Following incident closure, the organization shall:

- *Conduct a lessons-learned review.*
- *Identify root causes.*
- *Document findings and recommendations.*
- *Track corrective actions to completion.*

8. COMMUNICATION AND ESCALATION

Incident communications shall:

- *Follow approved escalation procedures.*
- *Be restricted to authorized personnel.*
- *Protect confidential information.*
- *Ensure timely notification to stakeholders.*

Major incidents shall be escalated immediately to executive management.

9. REGULARTRY AND LEGAL REQUIREMENTS

Where applicable, the organization shall:

- *Comply with breach notification requirements.*
- *Notify regulators within prescribed timeframes.*
- *Fulfill contractual notification obligations.*
- *Cooperate with law enforcement when appropriate.*

All external communications regarding incidents must be approved by Legal and authorized management.

10. DOCUMENTATION AND RECORD RETENTION

The organization shall maintain records of:

- *Incident reports.*
- *Investigation findings.*
- *Evidence collected.*
- *Communications.*
- *Corrective actions.*
- *Post-incident reviews.*

Incident records shall be retained in accordance with the organization's record retention requirements and applicable regulations.

11. TRAINING AND AWARENESS

The organization shall:

- *Provide regular security awareness training.*
- *Conduct incident response exercises and simulations.*
- *Train incident response personnel on their responsibilities.*
- *Review and update procedures following exercises and incidents.*

12. MONITORING AND CONTINUOUS IMPROVEMENT

The Information Security Team shall:

- *Monitor incident trends and metrics.*
- *Measure response effectiveness.*
- *Review policy effectiveness annually.*
- *Update procedures based on emerging threats and lessons learned.*

13. POLICY COMPLIANCE

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, contract termination, legal action, or other appropriate measures.

14. POLICY REVIEW

This policy shall be reviewed at least annually, or upon significant changes to business operations, technology, regulatory requirements, or the threat landscape.

Edwin Davey - Managing Director

Signed: