REED GRADUATION SERVICES PTY LTD

Cyber Security & Resilience Policy

Cyber Security & Resilience Policy

At Reed Events, we are committed to maintaining a robust cybersecurity posture to protect our digital assets, customer data, and business operations. This policy outlines our approach to identifying, mitigating, and responding to cybersecurity risks while ensuring compliance with relevant regulations and industry standards.

CORE PRINCIPLES

Risk Assessment

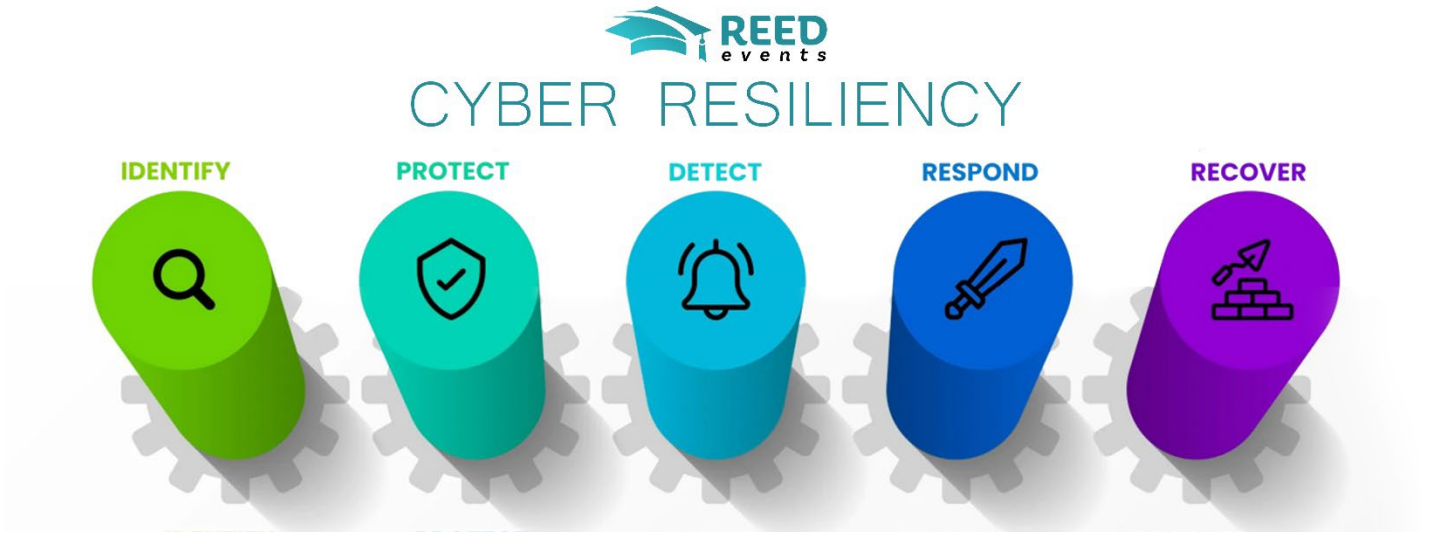
- Regularly conduct risk assessments to identify vulnerabilities in IT systems, networks, and third-party integrations.
- Assess potential threats, including phishing, malware, insider threats, and emerging cyber risks.
- Implement mitigation strategies and document risk reduction measures.

Incident Response

- Establish a structured Incident Response Plan (IRP) that includes:
  - Early detection and identification of security incidents.
  - Containment measures to prevent spread and minimise damage.
  - Eradication of threats and affected components.
  - Recovery steps to restore normal operations.
  - Post-incident analysis for continuous improvement.
- Designate an Incident Response Team (IRT) responsible for handling cyber threats and ensuring a rapid response.

Business Continuity & Disaster Recovery

- Implement a Business Continuity Plan (BCP) ensuring uninterrupted service delivery during cyber incidents.
- Maintain disaster recovery protocols with regular system backups and redundancy measures to restore critical operations quickly.
- Conduct periodic cyber resilience testing, including penetration testing and simulated attack scenarios.



Data Protection & Privacy

- Apply encryption and access controls to safeguard sensitive information.
- Ensure GDPR, Australian Privacy Act, and other applicable data protection laws compliance.
- Regularly update Data Protection Impact Assessments (DPIA) for new and existing data processing activities.

Regulatory Compliance

- Align cybersecurity practices with standards such as ISO 27001, NIST Cybersecurity Framework, and Essential Eight (Australia).
- Ensure compliance with contractual obligations and industry best practices.
- Conduct regular security audits and governance reviews.

POLICY ELEMENTS

Acceptable Use Policy (AUP)

User accounts on Company computer systems are for Company business only and must not be used for personal activities. Unauthorised use of these systems may breach the law, be considered theft, and could result in legal action. Such misuse may lead to either civil or criminal prosecution. Users are responsible for protecting all confidential information accessed or stored on their accounts, including login credentials and passwords. Users are also prohibited from making unauthorised copies of confidential information or sharing it with unauthorised persons outside the Company.

Users must not engage in activities that are intended to: harass other users, degrade system performance, divert system resources for personal use, or access Company systems without proper authorisation. Users are not permitted to connect unauthorised devices to their PCs or workstations unless they have received specific approval from their manager or the designated IT representative.

Downloading unauthorised software from the Internet to Company devices is prohibited. Users are required to report any security weaknesses, incidents of misuse, or breaches of this policy to their immediate supervisor.

Connecting to third-party networks

This policy is designed to ensure a secure connection between the Company and third-party organisations that need to electronically exchange information with the Company.

A "third-party" refers to vendors, consultants, business partners, and other entities that require access to Company information. Third-party network connections are intended for use by employees of the third-party organisations solely for the Company's business purposes. The third-party company must ensure that only authorised users are permitted access to the Company's network. Additionally, the third-party must prevent Internet or other private network traffic from entering the Company network.

This policy applies to all new third-party connection requests as well as any existing third-party connections. If current third-party network connections do not meet the standards set out in this policy, they must be redesigned accordingly.

Remote Access

Only authorised individuals are permitted to remotely access the Company network. Remote access is granted to employees, contractors, and business partners who have a legitimate business need to exchange information, copy files or programs, or access Company applications. The authorised connection can be made either from a remote PC to the Company network or via a remote network connection. The only approved method for remote access is through a Virtual Private Network (VPN) using secure identification (ID) to ensure a secure connection to the internal network.

Password & Access Control Policy

- Enforce strong password creation (minimum 12 characters, mix of uppercase, lowercase, numbers, and symbols).
- Implement multi-factor authentication (MFA) for accessing critical systems.
- Adopt role-based access control (RBAC) to restrict data access based on job responsibilities.
- Conduct regular access reviews to remove unnecessary or outdated permissions.

Data Handling & Retention Policy

- Classify data into Confidential, Restricted, Internal, and Public categories.
- Encrypt sensitive data both in transit and at rest.
- Securely delete obsolete data using certified data erasure methods.

Software & Hardware Security

- Allow only approved and licensed software on company devices.
- Enable automatic updates and patch management for operating systems and applications.
- Monitor all network-connected devices for vulnerabilities.

Security Awareness & Employee Training

- Conduct mandatory cybersecurity training for all employees and contractors.
- Implement phishing awareness programs with simulated phishing tests.
- Educate employees on social engineering risks and reporting procedures.

Incident Reporting & Escalation

- Establish a 24/7 reporting mechanism for cyber incidents via a dedicated security hotline or email.
- Employees must report:
    - Phishing attempts
    - Unauthorised access to systems
    - Lost or stolen devices
    - Suspected malware infections
- Set predefined escalation levels for different incident types.

Backup & Recovery Policy

- Perform daily automated backups of critical data with offsite storage.
- Maintain multiple backup copies, including immutable storage to prevent ransomware attacks.
- Test data restoration procedures quarterly to ensure recovery reliability.

Vulnerability Management & Patch Policy

- Conduct regular vulnerability scanning and penetration testing.
- Patch critical security flaws within 48 hours of discovery.
- Deploy intrusion detection and prevention systems (IDS/IPS).

Monitoring, Logging, & Threat Detection

- Implement Security Information & Event Management (SIEM) tools for real-time threat monitoring.
- Maintain detailed audit logs for system activities, with at least one-year retention.
- Analyse logs for anomalous behaviour and potential cyber threats.

Third-Party Risk Management

- Evaluate vendor cybersecurity policies before onboarding new partners.
- Require security assessments for all third-party applications and integrations.
- Mandate cybersecurity clauses in vendor contracts to ensure compliance with security standards.

Policy Updates & Governance

- This policy will be reviewed annually and updated to address evolving cyber threats.
- Reed Events' Cyber Security Governance Team is responsible for ensuring policy adherence and compliance.

4. Enforcement & Consequences

- **Non-compliance** with this policy may result in:
    - Restricted access to company systems.
    - Disciplinary actions, including termination of employment.
    - Legal consequences if breaches violate regulations.

COMPLIANCE

All personnel at Reed Events must adhere to this policy including the company's current and future subcontractors and suppliers. Failure to comply with this policy may result in disciplinary action, up to and including termination. Legal actions may also be pursued where applicable.

BOARD APPROVAL

This policy has been approved by Reed Events' board of directors.

Mark Thomas, Managing Director
Reed Graduation Services Pty Ltd

Definitions

- ***Access Control:*** *A security measure that restricts and manages user permissions to ensure only authorised individuals can access specific systems, networks, or data.*
- ***Acceptable Use Policy (AUP):*** *A set of rules governing how employees and third parties can use Reed Events' technology, including internet, email, and company-owned devices.*
- ***Backup & Recovery:*** *The process of creating copies of data and storing them securely to ensure business continuity in case of system failures, cyberattacks, or accidental deletion.*
- ***Business Continuity Plan (BCP)*** *A documented strategy outlining how an organisation will continue critical business functions during and after a cyber incident or disaster.*
- ***Cyber Incident:*** *Any event that compromises the confidentiality, integrity, or availability of IT systems, including data breaches, ransomware attacks, and unauthorised access.*
- ***Data Encryption:*** *A security process that converts sensitive information into unreadable code, making it accessible only to authorised users with a decryption key.*
- ***Data Handling & Retention:*** *Guidelines that define how data should be stored, accessed, shared, and disposed of in a secure manner.*
- ***Data Protection Impact Assessment (DPIA):*** *A process to identify and minimise privacy risks when handling personal or sensitive data.*
- ***Disaster Recovery Plan (DRP):*** *A documented approach for restoring IT systems and data following a cyberattack, hardware failure, or other disruption.*
- ***Intrusion Detection & Prevention System (IDS/IPS):*** *A security system that monitors network traffic for suspicious activity and automatically blocks potential threats.*
- ***Incident Response Plan (IRP):*** *A predefined set of actions that organisations follow to detect, respond to, and recover from cybersecurity incidents.*
- ***Multi-Factor Authentication (MFA):*** *A security measure requiring users to verify their identity using two or more authentication factors (e.g., password + fingerprint or SMS code).*
- ***Patch Management:*** *The process of updating software, operating systems, and applications to fix security vulnerabilities and improve system performance.*
- ***Phishing:*** *A cyberattack in which attackers impersonate legitimate entities (e.g., banks, employers) to trick individuals into revealing sensitive information such as passwords or financial details.*
- ***Role-Based Access Control (RBAC):*** *A security model that assigns system access based on an individual's job role, limiting unnecessary permissions.*
- ***Security Awareness Training:*** *Ongoing education for employees on cybersecurity threats, safe practices, and how to recognise and report suspicious activities.*
- ***Security Information & Event Management (SIEM):*** *A system that collects and analyses security logs and alerts to detect potential cyber threats in real time.*
- ***Third-Party Risk Management:*** *The process of assessing and mitigating cybersecurity risks posed by vendors, contractors, or partners who have access to company systems or data.*
- ***Vulnerability Management:*** *The practice of identifying, assessing, and addressing security weaknesses in IT infrastructure.*
- ***Zero Trust Security:*** *A cybersecurity model that requires strict identity verification for every person and device attempting to access network resources, regardless of location.*