SECURITY AND RESPONSIBLE DISCLOSURE STATEMENT

VG-CYB-019-PUB

PURPOSE

This statement describes Valhalla's proportionate approach to cybersecurity and the responsible reporting of suspected vulnerabilities or security incidents.

PUBLIC COMMITMENT

- Security controls are selected according to the sensitivity, importance and risk of the systems and information involved.
- Material incidents are escalated with priority given to safety, containment, legal obligations and recovery.
- Good-faith reports of suspected vulnerabilities are welcomed when made responsibly and lawfully.

STATUS	Published
POLICY OWNER	Managing Director
PROPOSED APPROVER	Valhalla Board
PUBLICATION	Published v1.0

1. Security approach

Valhalla is an Australian-based private company. This document is applied in a practical and adaptable manner, with controls suited to the nature and risk of the activity. The Managing Director may set or adjust implementation arrangements, subject to law, contracts and matters reserved to the Valhalla Board. Ordinary operations may proceed within approved budgets and delegations. A significant departure from ordinary operations, material change, unusual commitment, new jurisdiction or matter outside approved authority must be documented and approved before implementation, including by the Valhalla Board where required.

Valhalla does not represent that every system is risk-free or that all controls are identical. Practical controls may include multi-factor authentication, least-privilege access, supported software, patching, backups, encryption, secure configuration, logging and vendor review where appropriate.

2. People, devices and access

People with access to Valhalla systems or information are expected to protect credentials, use approved devices and services where required, report suspected compromise and return or delete information when access is no longer authorised. Access may be adjusted quickly where a role, project or risk changes.

3. Vendors and shared environments

Cloud, AI, collaboration and other technology providers may be assessed in proportion to the data and business dependency involved. Valhalla may rely on reputable provider controls rather than duplicate every capability internally, while retaining responsibility for configuration, access and appropriate use.

4. Incident response

A suspected incident should be reported promptly to the Managing Director or through current website reporting details. Valhalla may isolate systems, suspend access, preserve evidence, engage advisers, notify affected parties or authorities, restore from backups and implement corrective action as appropriate.

5. Responsible vulnerability disclosure

A person who believes they have identified a vulnerability is requested to avoid accessing, changing, copying or deleting information beyond what is reasonably necessary to describe the issue; avoid disruption, extortion, social engineering or public disclosure before Valhalla has had a reasonable opportunity to assess the report; and provide enough detail to reproduce the concern.

Valhalla will seek to assess good-faith reports, but does not promise a particular response time, reward, safe-harbour arrangement or outcome unless separately agreed.

6. Review and improvement

Security practices may be adjusted as the company grows, systems change or incidents and testing identify improvements. Detailed architecture, thresholds, recovery procedures and vendor information remain confidential.

Related documents

- Privacy Policy
- Research Data Governance Principles
- Responsible AI and Exploration Assurance Statement
- Enterprise Risk Governance Statement

Document control and approval

Public reference	VG-CYB-019-PUB	**Version**	1.0
Status	Published	**Publication**	Published v1.0
Policy owner	Managing Director	**Proposed approver**	Valhalla Board
Approved by	C.Dubieniecki	**Approved date**	August 12th 2026
Review cycle	Bi-Annually or as board requires	**Review date**	August 12th 2028
Internal source	Cybersecurity and Data Breach Response Policy		

PUBLICATION CONTROL Published v1.0. This is the current website publication. Procedures may be adapted proportionately, but any substantive amendment to the published commitments requires controlled review, approval and versioning.