POL047 Cyber Security Policy Statement

Purpose

The purpose of this Cyber Security Policy is to lay out Pyramid Builders Ltd commitment to cyber security and confirm the
functional responsibilities of management, devolved divisions and all colleagues towards achieving these objectives.

Scope

The objective of cyber security is to minimise the risk of harm to, or destruction of, computer networks, applications, devices, and data. Failure to adequately secure these may result in major operational disruption, inability to deliver services or loss of intellectual property, customer or business data and potentially lead to reputational damage, regulatory fines and significant financial impact.

Roles and responsibilities

This policy applies to all employees, suppliers, contractors or any other persons granted access to PBL's technology and information assets.

Organisational Security

PBL manages the risk of security exposure or compromise by assuring that:

- There is a risk-based approach to cyber security in support of PBL's overall strategic objectives and cyber risk is owned by individual business units and any risk that could impact group will be brought up to management board;
- Business areas are responsible for operating security controls effectively for business operated PBL systems and technology;

Management Board is responsible for:

- Committing to actively supporting Cyber Security within PBL through clear direction, acknowledgement of responsibilities and providing the right level of resources that support the reduction of Cyber Security risks;
- Acting as a point of escalation and participating in the response to Cyber Security incidents; and
- Supporting the requirements of this policy, including the consequences of non-compliance, to the PBL workforce and third parties, and addressing adherence in third party agreements.
- Owning and managing cyber security risks within their business area.
- Prioritising resources to address critical vulnerabilities:
- Promoting the importance of Cyber Security and resilience within their teams;
- Supporting cyber incident preparedness activities and to prioritise remediation where significant gaps need to be addressed;
- Ensuring their teams attend appropriate job-specific and mandatory security training provided by PBL;
- Fostering the participation of Cyber Security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and
- Developing and maintaining appropriate business continuity and disaster recovery plans.

All PBL office members of staff are responsible for:

- Completing mandatory cyber awareness training and become familiar with the basic levels of security needed to protect PBL data;
- Reading and understanding PBL’s Cyber Security policy and to conduct their activities accordingly; and
- Reporting suspected cyber security incidents or weaknesses to the Cyber Security team.

The Cyber Security team is responsible for:

- Developing the security program in support of the group strategy;
- Maintaining strong relationships with business functions, to evaluate and understand cyber security risks and working with them to appropriately manage those risks;
- Establishing and maintaining enterprise cyber security policies and standards;
- Maintaining an adequate level of current knowledge and proficiency in cyber security through ongoing education and contact with security groups/associations and relevant authorities;
- Continually improving and developing appropriate Cyber Security capabilities;
- Advising on security issues related to suppliers of products and services;
- Monitoring external data breaches and other sources for new and emerging threats to manage PBL's level of readiness and preparedness;
- Promoting cyber security awareness and culture; and
- Maintain strong relationships across industry and with appropriate government agencies.

Liam Clear
Managing Director
Pyramid Builders Ltd September 2023