Australia Post

Group Security Policy

Rationale and Scope

This policy has been developed to detail minimum activities required of Australian Postal Corporation and its subsidiaries, the Australia Post Group (Group), and each workforce participant, to protect our business, brand, customers and workforce from security risks, which may impact our business.

This policy applies to workforce participants, employees, contractors, licensees and franchisees of the Group.

Policy Principles

General Managers are responsible for ensuring the following security requirements are implemented and then refreshed in their Business Unit, as specified:

a) **Personnel Security** – Business Units must ensure workforce participants complete all required security and compliance training d and individuals comply with security obligations including visitor management, information protection, personal and site security and aviation security.

b) **Employee Safety & Security** – All Group employees or contractors who are required to travel internationally on behalf of the Group must be registered with the Group's International travel security advisor and be informed about the nature of that service, including when and how to access it.

c) **Security Incident Reporting** –Business Units have implemented and maintained processes for ensuring they comply with the Group Risk Management Standard – Incident Management, including clearly allocated responsibilities (down to individual workforce participants), training and awareness programs within the Business Unit to ensure all security matters are reported and investigated.

d) **Crisis & Emergency Management** – Business Units have a current program to ensure they comply with both the Group Risk Management Standard – Incident Management and the Group Risk Management Standard - Business Continuity. Business units must always have appointed an Incident Management Lead and or Team and ensure that this team has received adequate training in relation to the Group's Crisis and Emergency Management Framework as defined by their respective standards mentioned above.

e) **Site and Critical Asset Security Risk Assessments** – Every Group owned, or controlled site and Critical Asset must be subject to a Security Risk Assessment (SRA) utilising the Group SRA self- assessment tool. This assessment must be repeated every two years or if the risk context changes.

f) **Due Diligence** – Before any Group Business Unit initiates operations in an additional business area or location, a risk assessment must be completed by the Business Unit identifying all inherent risks to people, assets and operations from doing business in that jurisdiction and mitigations to be adopted by the business to manage those risks. This assessment must be approved by the General Manager – Group Security.

g) **Physical and Electronic Security Standards**– Operational standards published and maintained by Group Security, which represent the minimum operational controls must be implemented at each Group site, unless an exemption has been given by the General Manager – Group Security.

h) **Workplace Monitoring Systems –** Business units must ensure all individuals comply with Group workplace standards such as CCTV and Safety Technology to ensure appropriate access and use of the use of the Group's information systems.

i) **Security Technology** – All technology employed by a business unit for the purpose of managing security risk is selected and procured in a manner consistent with the Group standard, unless prior written approval has been obtained from the General Manager – Group Security.

j) **Strategic Security Procurement** – New third party suppliers of security related services to a Group Business Unit, including human resources, may only be engaged in accordance with the Group Procurement Policy and approval of the General Manager – Group Security. All such engagements must be the documented and/or subject of a written agreement.

k) **Communications** – Ensure that all relevant employees and contractors are aware of this policy and receive training on their obligations under it. Training records are maintained via the Learning Management System.

It is everyone's responsibility to comply with security standards and to undertake required training.

Policy Support and Administration

Accountable Executive: Chief Risk Officer

Policy Owner: General Manager – Group Security

Whilst this Policy addresses high-level security requirements, it is aligned to a range or other Policies, Standards, Guidelines and Training material which combined reduce the risk to our assets. Further details are available through the Group's intranet or by contacting Group Security.

In support of this Policy, each business must, in consultation with Group Security, develop more specific standards and procedures suited to the business area.

Version Number: V 1

Approved By: Policy Governance Group

Approved On: 21 January 2021

Effective Date: 21 January 2021

Next Review Date: 21 January 2024