GROUP SECURITY POLICY

Version 3.0

March 2024

Document Owner	Chief Legal Officer – EOS Corporate Division		
Document Created	Document created - Operations Manager		Sept 2018
	V2 - Updated with minor policy and governance alterations		June 2021
	V3 - Updated with minor policy and governance alterations		March 2024
Stakeholder Approval	V1.0	Approved by Board	Sept 2018
	V3.0	Endorsed by Chief Legal Officer	March 2024
		Endorsed by Audit and Risk Committee	March 2024
		Approved by Board	21/05/2024

Contents

1. Introduction

Australia is facing unprecedented threats from acts of politically motivated violence (terrorism), espionage and foreign interference, cyber espionage and deliberate compromise or manipulation of data resources and materials by malicious insiders.

2. Purpose

This policy operates in a context where entities throughout the world are facing unprecedented threats from acts of politically motivated violence (terrorism), espionage and foreign interference, cyber espionage and deliberate compromise or manipulation of data resources and materials by malicious insiders. The purpose of this policy is to protect the assets and reputation of Electro Optic Systems Holdings Limited ACN 092 708 364 (**EOS**) and its Related Body Corporates and outline a set of principles and governance arrangements that manages the risk to people, information and assets when applied in conjunction with governance, information and physical security controls.

3. Scope

This policy applies to:

- the Directors of Electro Optic Systems Holdings Limited ACN 092 708 364 (the **Company** or **EOS**) or its controlled entities (together, the **Group**);
- all Employees and officers of Group; and
- any contractor, consultant, supplier or other third party related to the Group.

4. Security Principles

A culture of security in relation to physical and technological interference assists Employees to understand what needs to be protected, why it needs protecting and the role each and every Employee plays in the process.

The principles to promote security are:

- Board and Executive sponsorship – the Board and Executive places a high value on security. The Board and Executive clearly communicate to all Employees the importance of security measures;
- Awareness – all Employees receive regular security awareness training that includes acknowledgement by Employees of completion and understanding;
- Compliance – appropriate access controls relating to information, assets and premises are implemented and adhered to. Security breaches are dealt with consistently and rigorously, according to well established guidelines and policies;
- Oversight – robust audit regimes, including for information and communication technology systems are implemented;
- Review – regular re-evaluation of clearance holders occurs with adequate consideration of individual's potentiation vulnerabilities to exploitation by foreign governments, criminal organisations, issue motivated groups or self-motivated actions;
- Discipline – Appropriate action is taken regarding behaviours inconsistent with holding security clearance. Recognising such behaviours are not code of conduct or performance

management issues but potentially have security implications; and
- Reporting – Employees are strongly encouraged to report security-related issues, including through promotion of the Australian Government Contact Reporting Scheme.

5. Security Policies

The Group has security policies that are flexible, adaptive and proportional to current and emerging sources of threat including, but not limited to, foreign intelligence services, terrorism, malicious insiders, issue-motivated groups, organised crime and cybercrime, corruption and fraud. Where applicable Australian Government requirements will be appropriately included into this policy. The Chief Legal Officer will implement Group security related polices to manage the risk to people, information and assets for the Group.

6. Security Governance

All Group divisions must implement the site specific security plans and policies as directed by the Security Manager, the Information Technology Security Manager, and the Chief Legal Officer, and as available on the Group intranet, and are required to:

- use risk management principles and policies appropriate to entity functions and the security threats faced in developing, implementing and maintaining:
    - protective security measures;
    - business continuity management plans; and
    - fraud control plans;
- prepare, monitor and review their security plans to ensure they are complying with the mandatory policy requirements;
- develop a culture of security through programs of security awareness and education to ensure Employees fully understand their security responsibilities;
- remain accountable for the efficient and secure performance of outsourced functions;
- investigate security incidents promptly and with sensitivity; and
- maintain appropriate security registers for individuals, incidents and classified information.

7. Compliance and Breaches

- All Employees must comply with this Group Security Policy and immediately report any breaches to their Senior Manager, Executive and/or the CEO, as appropriate;
- If there is a situation which involves a breach of law or regulation, the matter may also be referred to the appropriate law enforcement agency;
- Employees whose conduct falls below or breaches the requirements of the Group Security Policy will be counselled and may be subject to disciplinary action up to and including termination; and
- Any matter raised will be promptly investigated by the Chief Legal Officer or delegate and the Employee will be informed of the outcome, subject to any privacy limitations.

8. Monitoring and Review

The Chief Legal Officer will be responsible for administrating, implementing and reviewing the Group Security Policy. The Group Security Policy may be varied from time to time, including as part of any review.

The Group will periodically review this policy and accompanying processes and procedures with a view to ensuring that it is operating effectively.

If you have any questions concerning the Group Security Policy, please contact Human Resources.

9. Definitions

Employee includes permanent employees, part-time employees, casual employees, maximum term employees, non-executive directors, officers, international assignees, interns and contractors, including but not limited to those employed through a preferred recruitment agency.

Related Body Corporate has the same meaning as that expressed in sections 9 and 50 of the *Corporations Act 2001* (Cth).