EvokeTelecom Services Ltd
Information

Security Policy
Version: 2.0
Date Approved: 10th September

Document Control Sheet

TITLE OF DOCUMENT	Information Security Policy
SUPERSEDES	New Policy introduction
AUTHOR(S) NAME	David Wardell, Director
REVIEWED BY	Susannah Wardell, Director
APPROVAL DATE	20 Sept 2025
REVIEW DATE	20 Sept 2026
IMPLEMENTATION DATE	16 May 2018

VERSION	DATE	BRIEF DESCRIPTION OF CHANGE
Draft.v0.1	May 2018	Initial Draft
Version 1.0	May 2018	Policy approved
Version 2.0	Sept 2025	Reviewed and Approved

1.0 PURPOSE

The purpose of this Policy document is to define the requirements of Evoke Telecom Services Ltd. ("Evoke") in relation to its policy for information security. This Information Security Policy establishes Evoke 's requirements for achieving an effective and appropriate system of internal control measures to protect the Company's business activities, information assets and information processing facilities. The selected measures shall be:

Based on the risks identified through regular, informal and necessary formal, business focused assessment process;

Cost effective and justified; and selected by management such that risks are reduced to a level considered acceptable and in line with the Company's business requirements and any statutory or regulatory requirements.

The key objectives of this Policy are to:

Protect information assets of the Company and its customers from threats, whether internal or external, deliberate or accidental; and

Minimise the risk of damage by seeking to prevent the occurrence of security incidents and reducing their potential impact. Evoke is committed to continual improvement in all aspects of security, through the implementation and maintenance of its information security management systems.

2.0 SCOPE

The scope of this Policy encompasses all forms of information, including knowledge generated, used or shared in the performance of the Company's business or entrusted to Evoke by its staff, customers, business partners and suppliers. Information processing facilities include physical premises, IT systems, networks and associated media such as data stored on computers, transmitted across networks, recorded on paper or held on other storage mediums.

3.0 RESPONSIBILITIES

- The Directors are responsible for information security governance and shall provide staff with education and training to support adherence to this Policy and other information security policies.
- The Directors shall be responsible for approving and maintaining this Policy.
- The Directors shall fulfil a quality assurance role in ensuring that information systems deliver reliable and secure processing outcomes.
- The Directors shall ensure that information and data is processed and managed in accordance with all contractual, legislative and regulatory requirements.

- The Directors shall be responsible for implementing and communicating this
- Policy and associated processes and procedures to their staff and for supervising compliance.
- The Data Processing Officer shall be responsible for ensuring that regular audits of the processes and procedures that implement this Policy are performed to maintain compliance and facilitate continual improvement.
- All staff are responsible for maintaining awareness of Evoke 's information security policies and procedures applicable to their role.
- All staff[1] and third parties are required to comply with this Policy and its supporting policies and processes.

4.0 POLICY

Evoke is committed that:

- Confidentiality of information shall be assured;
- Integrity of information shall be maintained;
- Availability of information for business purposes shall be attained;
- The needs and expectations of external parties are met, where such needs and expectations include: legislative, regulatory and contractual security obligations;
- Access of information assets shall be controlled and be based on 'business need to know';
- Information security awareness training shall be provided for all staff on a frequent basis;
- The protection of information shall be considered when business continuity strategies and plans are produced, maintained, tested or invoked; and
- All actual or suspected information security breaches, events and weaknesses shall be reported, logged and investigated under the direction of the ISF.

This Policy will be communicated to all staff and all staff are required to acknowledge that they have read, understood and agree to comply with this Policy. No part or extract from this Policy may be distributed without express permission of the Directors.

5.0 PASSWORD SECURITY

- Passwords will be chosen by each individual user in accordance with the technical controls applied by the relevant system.

- They must not be shared with anyone else.
- Each member of staff will have a unique password for the system that they access.
- Computers must be locked when left unattended.
- It is not permitted to display passwords on the computer or in any other place with easy access.
- Only in exceptional circumstances, when explicitly approved by management, may the password be written down and in such cases, it must be retained in a secure place.
- If there is a suspected breach of password use, the incident will be reported to a Director (or Line Manager if a Director is not available).
- In the case of a suspected breach, the password will be changed immediately.
- Re-use of passwords is not permitted.

6.0 GOOD SECURITY PRACTICE

- All computers should have a screen saver password activated with activation time no more than 5 minutes.
- Passwords should not be displayed on the screen as they are entered.
- Temporary passwords should remain in use for the absolute minimum of time.
- There should be no correlation between the password and the system being entered.
- No elements of the password should relate to the user (family names, nicknames, birthdays etc).

7.0 REPORTING SECURITY INCIDENTS

All staff are responsible for reporting security incidents, events, weaknesses or concerns. Security incidents, including breaches of this Policy, shall be reported by the fastest possible and most appropriate means initially (e.g. via telephone or in person to a company Director (or if not available a line manager) and shall be followed by an email report to sales@evoketelecom.com. Security incidents or concerns may also be reported in confidence to a Director. Failure to report a security incident may be considered a breach of this Policy.

8.0 CONSEQUENCES OF NON-COMPLIANCE

Any breaches of this Policy and supporting information security policies may be subject

to a formal security investigation. Where proven, failure to comply shall result in disciplinary action being taken against individuals determined to be responsible for the breach under Evoke's Disciplinary Procedures as outlined in the Contract of Employment, up to and including summary dismissal for gross misconduct. Evoke may also initiate legal action or refer the breach to relevant law enforcement authorities where warranted. Non-compliance by contracted third parties or their employees may result in termination of the supplier's contract and/or legal action.

9.0 AUDIT

Audit spot checks and automated monitoring may be conducted to ensure this Policy is complied with. Any non-compliance shall be reported to the Directors in the first instance to initiate investigation of any associated security incident. Reports of the findings, initial remediation steps and follow-up actions taken, as well as recommendations for improvements, shall be reported to the Directors.

10.0 INFORMATION CLASSIFICATION

Evoke's information security policies are classified as 'internal use only' and no part or extract from them or the associated files held on Evoke computer networks may be distributed to any external organisation without the express permission of the Directors.

11.0 REVIEW AND MAINTENANCE

This Policy shall be reviewed annually, or after significant change, by the Directors to ensure it remains effective and fit for purpose.

12.0 EXCEPTIONS

Where an Evoke information security policy requirement cannot be met for any reason, a formal request for exception shall be submitted in writing to the Data Protection Officer for approval. Failure to obtain an exception approval will be considered a breach of this Policy.

13.0 FURTHER INFORMATION

Any queries or comments about this policy, or any concerns that the policy has not been followed should be addressed to David Wardell, Director or Susannah Wardell, Director and Company Secretary.

14.0 POLICY OWNER

This policy is owned and maintained by David Wardell, Director

15.0 POLICY REVIEW DATE

Date last reviewed: 10/09/2025

1 Staff includes permanent, contract and associate staff.