Information Security Policy

Policy Number	101
Version	1
Policy Name	Information Security Policy
Policy Contact	Matthew Betteridge
Date Issued	20th January 2024
Reviewed	02nd July 2024
Next review Date	02nd July 2025
Target Audience	Internal
Approved by	Manasa Polimani

Contents

1. Overview

1.1. Purpose

Information that is collected, analysed, stored, communicated, and reported upon may be subject to theft, misuse, loss, and corruption.

Information and privacy may be put at risk by poor education and training, and the breach of security controls.

Information security and privacy incidents can give rise to embarrassment, pecuniary loss, non-compliance with standards and legislation as well as possible judgements being made against OneCall24.

This Information Security Policy sits alongside the Information Risk Management Policy and User Digital Security Policy to provide the outline of and justification for OneCall24's risk-based information security and privacy controls.

- *Information Risk Management Policy*
- *User Digital Security Policy*

1.2. Objectives

OneCall24's information security and privacy objectives are that:

- Our information and privacy risks are identified, managed, and treated according to agreed risk tolerance.
- Our authorised users can securely access and share information to perform their roles.
- Our physical, procedural, and technical controls balance user experience and security
- Our contractual and legal obligations relating to information security are met and there is a continuous commitment to meet applicable requirements to information security such as data backup, encryption etc.
- Individuals accessing our information are aware of their information security responsibilities.
- Incidents affecting our information assets are resolved and learnt from to improve our controls.
- To continually improve the Information Security Management System (ISMS)

1.3. Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information and technologies used at OneCall24 in all formats. This includes information processed by other organisations in their dealings with OneCall24.

The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to OneCall24 information and technologies, including external parties that provide information processing services to OneCall24.

A detailed scope, including a breakdown of users, information assets and information processing systems, is included in the Integrated Management System framework.

1.4. Compliance

Compliance with the controls in this policy will be monitored by the Senior Management Team and reported to the CEO (Matthew Betteridge).

1.5. Review

A review of this policy will be undertaken by the Senior Management Team annually or more frequently as required and will be approved by the CEO of OneCall24.

1.6. Policy Statement

It is OneCall24's policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals.
- Integrity – the accuracy and completeness of information will be maintained.
- Availability – information will be accessible to authorised users and processes when required.

OneCall24 will implement an Information Security Management System based on the ISO 27001 International Standard for Information Security. OneCall24 may also reference other standards as required.

2. Information Security Policies

A set of lower-level controls, processes and procedures for information security and privacy will be defined, in support of the high-level Information Security Policy and its stated objectives.

This suite of supporting documentation will be approved by the Senior Management Team and then published and communicated to company users and relevant external parties.

- *User Digital Security Policy*
- *Administrator Digital Security Policy*

3. Organisation of Information Security

OneCall24 will define and implement suitable governance arrangements for the management of information security and privacy. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security within OneCall24.

OneCall24 will appoint/define at least:

- What/who is classed as management to influence, oversee and promote the effective management of the Company's information security and privacy management system.
- An Information Security specialist to manage the day-to-day information security function.
- Information Asset Owners (IAOs) to assume local accountability for information management.

4. Human Resources Security

OneCall24's security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training will be made available to all staff, and poor and inappropriate behaviour will be addressed.

Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

5. Asset Management

All assets (information, software, electronic information processing equipment, service utilities and people) will be documented and accounted for. Owners will be identified for all assets, and they will be responsible for the maintenance and protection of their assets.

All information assets will be classified according to their legal requirements, business value, criticality and sensitivity, and classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

6. Access Control

Access to all information will be controlled and will be driven by business requirements. Access will be granted, or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed and will include consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

7. Cryptography

OneCall24 will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems alongside ensuring the protection of PII (Personal Identifiable Information).

8. Physical and Environmental Security

Information processing facilities are housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attacks this includes protection of PII from physical access.

9. Operations Security

OneCall24 will ensure the correct and secure operations of information processing systems.

This will include:

- Documented operating procedures.
- The use of formal change and capacity management
- Secure development processes
- Controls against malware
- Defined use of logging
- Vulnerability management
- Protection of PII

10. Communications Security

OneCall24 will maintain network security controls to ensure the protection of information within its networks and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information.

11. System Acquisition, Development and Maintenance

Information security and privacy requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to mitigate any risks identified will be implemented where appropriate.

Systems development will be subject to change control and separation of test, development, and operational environments.

12. Supplier Relationships

OneCall24's information security and privacy requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

13. Information Security and Privacy Incident Management

Guidance will be available on what constitutes an Information Security and privacy incident and how this should be reported.

Actual or suspected breaches of information security and privacy must be reported and will be investigated.

Appropriate corrective action will be taken, and any learning built into controls.

14. Information Security Aspects of Business Continuity Management

OneCall24 will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely recovery in line with documented business needs. This will include appropriate backup routines and built-in resilience.

Business continuity plans must be maintained and tested in support of this policy.

Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

15. Compliance

The design, operation, use and management of information systems must comply with all statutory, regulatory, and contractual security and privacy requirements.

Currently, this includes data protection legislation and OneCall24’s contractual commitments.

OneCall24 will use a combination of internal and external audits to demonstrate compliance against chosen standards and best practices, including against internal policies and procedures.