[Company]

CONTINUAL IMPROVEMENT POLICY

Continual improvement, non-conformity, and corrective action

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Continual Improvement Policy

3.1 Purpose

The purpose of this policy is the continual improvement of the suitability, adequacy, and effectiveness of the information security policy and information security management system.

3.2 Scope

All employees and third-party users.

The company information security management system.

3.3 Principle

The information security management system is continually improved and enhanced through addressing incidents and non-conformities with an effective corrective action and management process.

3.4 Audit

3.4.1 Internal Audits

Internal audits are conducted to assess the effectiveness of the information security management system and the controls documented in the Statement of Applicability.

Internal audits are conducted based on risk and business need.

Internal audits are conducted by individuals independent of the area being audited.

Internal audits are planned for the year.

Internal audit results are reported to and overseen by the Management Review Team.

Internal audits may result in a nonconformity requiring a corrective action or identifying an opportunity for improvement.

3.4.2 External Certification Audits

External certification audits are conducted to assess the effectiveness of the information security management system and the controls documented in the Statement of Applicability.

External certification audits are conducted based on the certification body requirements.

External certification audits are planned for the year.

External certification audits results are reported to and overseen by the Management Review Team.

External certification audits may result in a nonconformity requiring a corrective action or identifying an opportunity for improvement.

3.4.3 Client and Third-Party Audits

Client and third-party audits are conducted to assess the effectiveness of the information security management system and the controls documented in the Statement of Applicability.

Client and third-party audits are conducted based on agreement and subject to a contract and / or non-disclosure agreement being in place.

Client and third-party audits results are reported to and overseen by the Management Review Team.

Client and third-party audits may result in a nonconformity requiring a corrective action or identifying an opportunity for improvement.

3.5 Incidents

Incident management may result in a nonconformity requiring a corrective action or identifying an opportunity for improvement.

3.6 Change Management

Change management will consider and may identify an opportunity for improvement.

3.7 Management Review Team

The management review team as part of the structured management review team agenda consider opportunities for improvement.

3.8 Review of Objectives

The review of information security objectives will consider and may identify an opportunity for improvement.

3.9 Legal, Regulatory and Information Security Standards Change

Changes as a result of legal and regulatory requirements or changes to applicable standards for information security will consider and may identify an opportunity for improvement.

3.10 Improvement as a result of Non-Conformity

A non-conformity is a deviation from the norm. This is defined as a deviation from policy and / or process.

Nonconformity to process or policy is identified by the audit process and the occurrence of incidents.

When a nonconformity occurs, action is taken to correct it and deal with the consequences.

Nonconformities are evaluated for the need to eliminate the causes of the non-conformity in order that it does not reoccur or occur elsewhere:

- Reviewing the non-conformity
- Determining the cause of the non-conformity
- Determining if similar nonconformities exist or could potentially occur.

Nonconformities are reported through the Management Review Team.

Nonconformities are recorded, documented, and tracked in the incident and corrective action log.

The effectiveness of corrective actions is reviewed.

3.11 Management of Improvement

Changes to the information security management system are planned and managed.

Changes to the information security management are recorded in the incident and corrective action log or in a change log, as appropriate and relevant.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.