[Company]

CHANGE MANAGEMENT POLICY

The management of change

1 Document Version Control

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

2 Document Contents Page

3 Change Management Policy

3.1 Purpose

The purpose of this policy is to manage the risk posed by changes in the company.

3.2 Scope

All employees and third-party users.

3.3 A Request for Change

Requests for change are made via the company change platform and process.

3.4 Change Request Approval

Changes are approved by [redacted] team prior to implementation.

3.5 Change Register

A register of changes is maintained.

3.6 Change Prioritisation / Classification

All change requests are prioritised in terms of benefit, urgency, [redacted] on company operations.

3.7 Change Risk Assessment

Changes are assessed for risk following the Risk Management Policy and Risk Management process.

3.8 Change Impact Assessment

Changes are assessed for positive and negative impact to the customer and the company.

3.9 Testing

Changes are tested in [redacted] where feasible prior to implementation to minimise the risks to company processes, operations, security, and clients.

3.10 Version Control

Software changes and updates are controlled with version control. Older versions are retained in accordance with retention and storage processes.

3.11 Communicating Change

All users or user representatives impacted by a change are notified of the change.

3.12 Roll Back

Procedures to roll back / recover from an unsuccessful change are in place where appropriate.

3.13 Change Freeze

At certain critical times of the year, it may be necessary to impose a non-essential change freeze period.

[redacted]

3.14 Emergency Change

Emergency changes may operate outside the normal change process but must be approved by senior management.

[redacted]

3.15 Unauthorised Changes

Unauthorised changes are tracked and reported to the Management Review Team meeting and escalated to senior management as required.

[redacted]

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.