Access Intelligence Change Management Policy

1.0 *Policy Objectives*

- To ensure that Access Intelligence implements standardised methods and procedures for efficient and prompt handling of all changes to control IT infrastructure and deployed components, while managing associated risk.
- To ensure that Access Intelligence implements a Change Management program that includes:
    - Accurate Documentation – Identify the information relevant to a specific change that needs to be collected throughout the change management process.
    - Continuous Oversight – by Change Advisory Board (CAB). The CAB is tasked with balancing the need for change with the need to minimize risks.
    - Formal, Defined Approval Process – All changes will follow the established multiple level approval process to ensure routine changes are completed with minimum restrictions while complex, high impact changes receive the oversight necessary to guarantee success.
    - Scope – Establish the specific areas that this policy will cover.

2.0 *Policy Scope*

The scope of the Change Management Policy or Change Control Policy and associated procedures is applicable to all members of Access Intelligence and are related to the management of changes to all managed live IT systems or services. No employee is exempt from this policy.

This policy covers the data networks, servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorized to access the company's data networks. This policy also covers use of IaaS and PaaS Cloud hosting services in use by the company.

3.0 *Policy Statements*

Access Intelligence shall ensure that all in-scope changes follow the defined change management workflow. No in-scope change should be implemented without:

- A request for change (RFC) ticket being raised in the appropriate change management system.

- The RFC must have the correct Change Type specified. This indicates which CAB to use.
- There are several RFC Change Control Types in use, all require different approval checks:
    - **Source Code** – must be approved by 4 separate CAB members from:
        - Engineering
        - Product Management
        - Quality Assurance
        - Support
    - **Infrastructure** - must be approved by 2 separate CAB members from either:
        - Infrastructure
        - IT
        - Security
        - Engineering
    - **Internal IT** – must be approved by 2 separate CAB members from either:
        - Infrastructure
        - IT
        - Security
        - Engineering
- Approval by the Change Advisory Board (CAB) associated with the change.
- An approved, documented plan of the sequence or steps for implementing and releasing the change into the live environment.
- Evidence demonstrating the fact that this change has been tested in a pre-live/staging environment first.
- A rollback/mitigation plan in case of failure.
- A post-change test being documented to check that the change has been successfully applied.

4.0 Responsibilities

This policy document defines specific activities that shall be performed by:

- Information Security Manager
- All Assigned Asset Owners
- All Engineering Staff with operational roles related to live systems.
- The IT Service Provider

The Information Security Manager shall be responsible for:

- Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries.
- Co-ordinate the overall communication and awareness strategy for change management.

The CAB shall be responsible for:

- Review and approve RFC in a timely manner.

IT Service Provider, Asset Owners, Engineering Staff shall be responsible for:

- Comply with all information security policies, standards and procedures for change management and control
- Keep any Change Control Boards up-to-date
- Report all deviations.

All individuals specified within the scope of this Change Management Policy (see Section 2.0) shall have individual responsibility for complying with every aspect of this policy. The requirement to comply with Access Intelligence policies is included within the Terms and Conditions of Employment and is noted within each individual user's job description. Any failure to adhere to the requirements of this policy shall result in disciplinary action being taken.

5.0 ***Document Version Control***

This policy needs to be reviewed annually as an absolute minimum, or if required changes ae identified to address one or more of the following:

- An identified shortcoming in the effectiveness of this policy, for example because of a reported information security incident, formal review or audit finding.
- A change in business activities (e.g. mergers and acquisitions) which will or could possibly affect the current operation of the Access Intelligence Information Security Management System, and the relevance of this document.

- A change in the way in which Access Intelligence manages or operates its information assets and/or their supporting assets, which may affect the validity of this document.

The current version of this policy, together with its previous versions, shall be recorded below

Version History

Revision	Author	Date	Reason for issue
1.0	Andy Olliver	18/12/2019	First version to supplement policies already in place in order to meet requirements for ISO 27001:2013
2.0	Adam Palmer	20/01/2021	ISO 27001:2013 certification was achieved in June 2020
3.0	Adam Palmer	13/08/2021	Change Control Types

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		21/01/2020
Mark Fautley	Chief Financial Officer		20/01/2021
Mark Fautley	**Chief Financial Officer**		**20/01/2022**