Access Intelligence Secure Development Policy

1.0 *Policy Objectives*

- To ensure that Access Intelligence's applications and associated systems are designed and developed to allow for the identification and mitigation of security-related issues. It defines acceptable secure development principles which, properly implemented, will prevent the compromise of data, interference from malicious activities, or damage to IT services.

- To ensure that Access Intelligence's development activities are conducted in accordance with industry best practice, including considerations for secure design, code creation, application testing (and weakness remediation) and deployments of code into live, operational environments. It also extends to considerations related to decommissioning activities.

2.0 *Policy Scope*

Access Intelligence Secure Development Policy shall include the following:

- All employees, contractors and third-party developers who are responsible for the design, development, testing, implementation, in-life support and end-of-life decommissioning of any information or technical systems which process information either for Access Intelligence itself or on behalf of one or more of its customers.

- All steps in the Access Intelligence Software Development Lifecycle (SDLC) from concept through to deployment, and decommissioning.

3.0 *Policy Statements*

3.1 *General Statements*

- Observe the '8 Principles of Secure Development & Deployment' (from NCSC)
  - Secure development is everyone's concern
  - Keep your security knowledge sharp
  - Produce clean & maintainable code
  - Secure your development environment
  - Protect your code repository
  - Secure the build and deployment pipeline
  - Continually test your security
  - Plan for security flaws

- All Access Intelligence's personnel engaged within the development of software solutions (including any contributory components related to technical infrastructure) shall maintain a thorough knowledge of the Company's approach to secure development, and the requirements of applicable external security standards (e.g. those within Section 4.0). They shall ensure that these requirements are effectively implemented within all their development activities.

- Access Intelligence's shall maintain awareness of the OWASP (Open Web Application Security Project) recommendations and regularly check the OWASP "Top Ten" vulnerabilities and promptly communicate these to all personnel involved in development activities.

- Access Intelligence promotes the creation of clean and maintainable code through definition of coding standards, and mandated peer code review of all changes.

- Access Intelligence shall ensure the security of personal and shared development and testing environments.

- Access Intelligence shall ensure strict access control to source code repositories.

- Access Intelligence shall use automated build and deployment pipelines to increase the repeatability, accuracy, and security of systems.

- Access Intelligence shall integrate regular testing for security into the software development process.

- Access Intelligence shall ensure that the SDLC includes prioritisation and remediation of identified security defects.

- Access Intelligence shall include considerations for information security in project management e.g. threat modelling, privacy protection, security controls etc. Product Managers shall include the Information Security Manager in any projects which include processing data in a new way, e.g. new supplier or tool, or involve the processing of business information, client data or personal data. Any project that could increase the risk of the confidentiality, integrity or availability of information must have approved mitigating controls in place before development.

- Access Intelligence shall maintain backups for at least 1 month. This should include point-in-time (PiT) backups for at least 7 days, where available.

- Access Intelligence shall maintain both event and access logs for at least 1 month. This should be extended where possible.

3.2 *Considerations for Secure Development*

Access Intelligence shall ensure that full consideration is given to:

- The confidentiality, integrity, and availability of data which is to be stored and/or processed.
- How the system is to be access controlled, privileges to be managed
- The requirements for monitoring user activity, automated systems processing and data imports and exports.
- Considerations for resilience, business continuity objectives, and the backing up of data.
- The sensitivity of the data, which is to be processed, and whether additional controls such as encryption or split responsibilities need to be applied.
- How data protection requirements (e.g. responding to data subject requests arising from the EU General Data Protection Regulation) can be fulfilled within specified time periods.
- Requirements for protective controls to protect the intellectual property of the code being developed.
- Securing the production environment by not disclosing software version numbers or any other system information in the source code or via remote debug mode. Where possible, HTTP response headers, e.g. Content Security Policy, Permissions Policy, Cross Origin Policies, should be implemented in order to prevent certain classes of attack and in order to improve the overall security posture of the product.
- The encryption of data in transit and at rest (**see ISDL11**). Authentication must always be encrypted.
- Securing user inputs e.g. forms with appropriate sanitisation and validation.
- Securing user uploads with appropriate malware scanning.
- Secure usage of authentication credentials. Passwords should not be coded into source code. The practice of hard coding passwords increases the risk of passwords being compromised.

- Modifications of software packages is discouraged and limited to necessary changes. Such changes should be strictly controlled and approved as per the Change Management Policy (**see ISDL54**)

- Access control to each environment is strictly controlled with restrictive privileges in accordance with the Access Control Policy (**see ISDL07**) and Password Management Policy (**see ISDL03**)

- Requirements for the preparation and release of supporting documentation when complete.

- Considerations for end-of-life or decommissioning (see Section 3.7)

3.3 *Use of Third-Party Development Resources*

- Secure development activities as required by this Policy are not limited to those undertaken in-house by Company's own personnel. The requirements of this Policy shall also be mandated for any third-party organisations engaged by Company to undertake specified development tasks, and the applicable engagement contract shall formally record this requirement.

- Where it is necessary for Company to procure the services of an external organisation, including the purchase of commercial software, application elements or bespoke development activities, then the secure development practices of the third-party shall be fully assessed prior to procurement taking place. The Company's requirements shall be communicated to the Purchasing Manager to incorporate within applicable policies and procedures.

- When using third-party software, e.g. open source, verify that the version of all software acquired is still supported by the developer or appropriately hardened and patched based on developer security recommendations.

3.4 *Testing and Release Management*

- Application testing shall be carried out in accordance with the specific requirements of the development activity, and where possible shall be undertaken by an individual other than the assigned developer. In the development environment, all code changes must be reviewed and approved by another developer, then UAT tested by a Product Manager. In testing environments, code changes must be tested by a QA specialist.

- By default, Access Intelligence only allows developers to use fictitious or sanitised data sources during testing activities, and no testing involving the use of live data shall be undertaken without the express written permission of Senior Management.

- To protect data subjects, no Personally Identifiable Information (PII) should be used in non-production environments. In development and testing environments, all PII data should be sanitised, unless with the express written permission of Senior Management.

- Email tools should be disabled during development and testing. Only fictitious or staff contacts are to be included in email testing.

- Developed code shall be periodically stored within secure repositories (e.g. GitHub), to ensure that it is properly protected from loss, theft or corruption. Such repositories shall incorporate version control, such that each version can be attributed to a named individual with a specific date and time stamp. Access to code repositories shall be recorded and regularly reviewed.

- All Access Intelligence's applications and deployment infrastructure shall be subject to independent security reviews at agreed points within their development lifecycle. These shall be conducted by a suitably experienced and credible individual or testing organisation, conducted in accordance with a suitable scope, and where possible the results aligned with current standards or frameworks such as the CVSS (Common Vulnerability Scoring System).

- Following an independent review of applications and deployment infrastructure, any identified weakness or observations shall be promptly assessed by Senior Management such that the priority, urgency and necessary resources to fully remediate such issues are agreed and communicated. Such assessment shall consider the grade or rating assigned to each issue by the independent tester, and records shall be maintained to demonstrate remediation and satisfactory re-testing.

- Once code has satisfactorily completed security testing, and any associated remedial activities have been fully completed and validated, it shall be subject to formal change management approval (**see ISDL54**) prior to being released into the live environment.

3.5 *Live Operations & Application Maintenance*

- Live applications shall be subject to applicable policies and procedures, including:
  - Ongoing monitoring for new or changing software vulnerabilities, such that prompt and effective patching and maintenance can be undertaken
  - Monitoring for any software components which vendors are retiring or discontinuing their support for, such that the application can be updated before that date

- Ongoing assessment of the developed code against applicable contractual, legislative or regulatory requirements (including changes to such requirements)
- Monitoring of the underlying hardware and software capacity to prevent overload or unacceptable performance of the application
- Monitoring of system availability, to ensure that an acceptable level of service (as specified at the commencement of development activities) can be achieved
- Reacting to the results of any business continuity or disaster recovery incident (or the results of a simulated exercise), where the application did not perform as expected
- User education on acceptable usage of the application, and the reporting of issues
- Requirements for subsequent independent security validation tests, to ensure that the application continues to operate in a secure and acceptable manner
- Available threat detection tools must be enabled in cloud hosting environments
- Regular vulnerability scanning of source code and infrastructure
- Access to production databases must be tightly controlled by Asset Owners. Production databases must not be duplicated to local machines.
- Where PII or authentication data is stored, transmitted, or processed, the underlying systems must have signature based anti-malware software and/or EDR (Endpoint Detection and Response) capabilities installed. In the case of containerised or PaaS applications, the container registry and source code should be scanned for malicious threats.

3.6 Decommissioning

During development activities, consideration shall also be given to how the source code is to be retired, and any live data associated with the application at that time is to be properly and securely managed. This shall include details as to the:

- Disposal of hardware containing the application and/or data
- Retirement of the application, and the deletion/archiving of associated code from repositories
- Sanitisation of data and code from any cloud-based systems or repositories
- Retirement of associated documentation, support functions and monitoring capabilities
- Cancellation or reallocation of associated software licenses

3.7 *Breaches of Policy*

- Failure to adhere to the requirements of this Secure Development Policy shall result in the employee concerned being subject to the Access Intelligence disciplinary action procedure.

4.0 *Secure Development Standards*

Several relevant security standards have been published, supported by "good practice guides". Some of these are recorded below for reference:

- National Cyber Security Centre **(NCSC)**
- NCSS Guide to Penetration Testing
- Open Web Application Security Project **(OWASP)**
- OWASP Top Ten Vulnerabilities
- Microsoft Security Development Lifecycle

5.0 *Responsibilities*

The Chief Technology Officer shall be responsible for:

- Specifying the secure development competencies and experience to be considered within the Company recruitment process
- Ensuring that all developers are subject to continuing professional development activities, including a requirement to maintain awareness of evolving secure development best practices
- Selecting third-party development resources based upon their proven secure development experience and their acceptance of the requirements of this Secure Development Policy

- Communicating and resolving any development-related issues arising from third-party developers.

The Information Security Manager shall be responsible for:

- Ensuring that the requirements of this Secure Development Policy are communicated to all personnel within its Scope through formal training and awareness initiatives

All developers in scope (see Clause 2.0) shall be responsible for:

- Maintaining awareness of secure development best practices (see Clause 4.0)
- Completing any assigned secure development training (see **ISDL02**)

All individuals specified within the Policy Scope of this Secure Development 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.

6.0 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	David Roud	31/10/2018	First version, in readiness for Access Intelligence ISO 27001:2013 audit
2.0	Andy Olliver	30/01/2020	ISO 27001:2013 certification needs to be achieved so document has been updated.
3.0	Adam Palmer	20/01/2021	ISO 27001:2013 certification was achieved in June 2020
4.0	Adam Palmer	22/11/2021	Additional security considerations and requirements during SDLC

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		12/03/2020
Mark Fautley	Chief Financial Officer		26/02/2021
Mark Fautley	**Chief Financial Officer**		**20/01/2022**