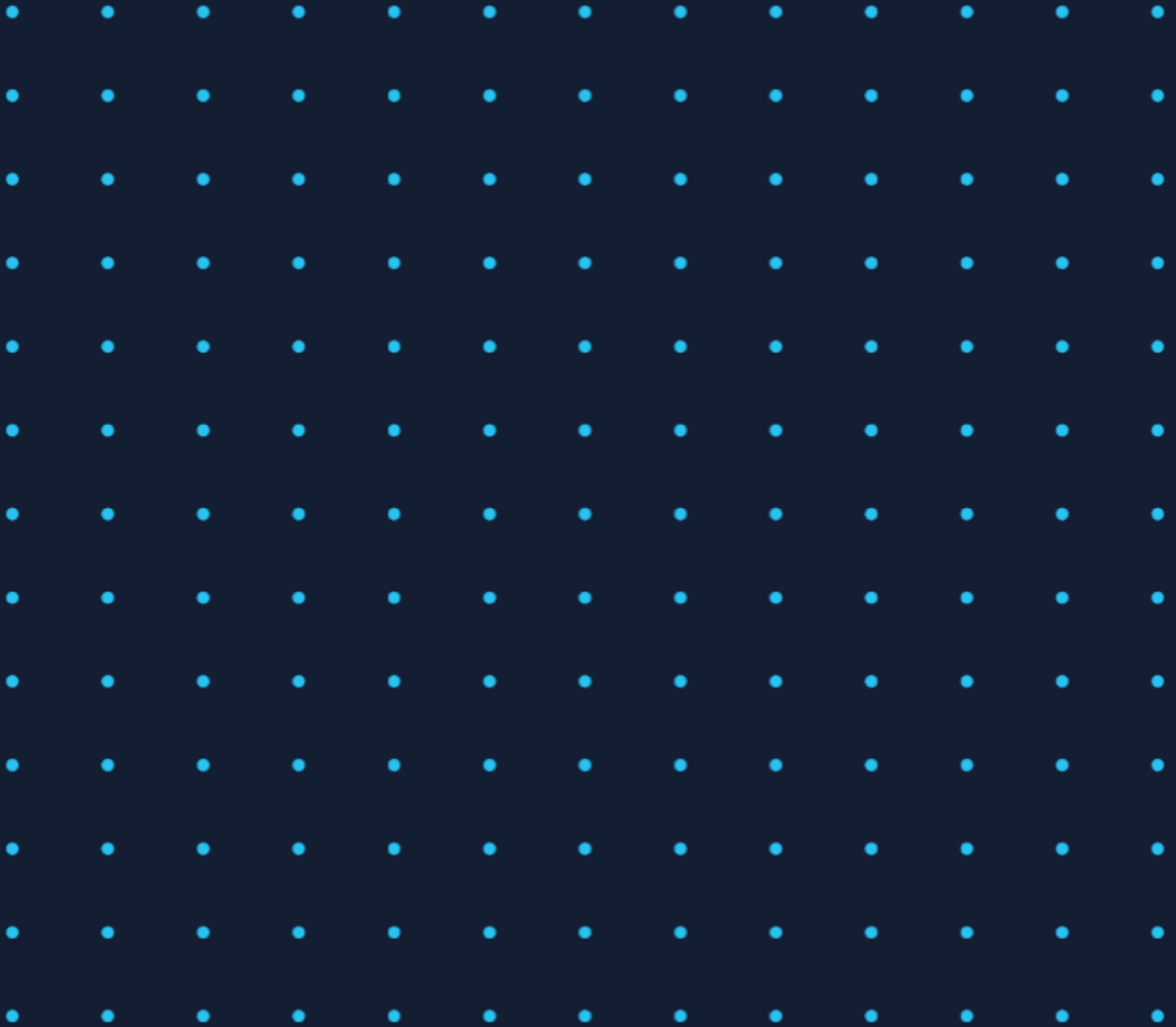


Access Intelligence Information Security Policy



Contents

[Contents](#)

[Purpose](#)

[Objectives](#)

[Relevant Corporate Objectives](#)

[Information Security Objectives](#)

[Policy Scope](#)

[Products](#)

[People](#)

[Premises](#)

[Data Centre Operations](#)

[Policy Statements](#)

[Risk Assessment](#)

[Management, Monitoring and Review](#)

[Legislative Compliance](#)

[Supplier Security](#)

[Asset Management](#)

[Acceptable Use](#)

[Access Control](#)

[Information Classification and Handling](#)

[Human Security](#)

[Information Security Training](#)

[Device Security](#)

[Secure Development](#)

[Information Security Incidents](#)

[Business Continuity](#)

[ISMS Responsibilities](#)

[Employees, Contractors and Third-Party Users](#)

[Executive Management](#)

[Senior Department/Team Management](#)

[Control Owners](#)

[Asset Owners](#)

[Information Security Officer \(Governance, Risk, Compliance\)](#)

[Information Security Officer \(Technical\)](#)

[Risk Management](#)

[Risk Assessment](#)

[Audit](#)

[Legal Compliance](#)

[Obligations](#)

[Intellectual Property](#)

[Information Lifecycle](#)

[Data Protection](#)

[Supplier Security](#)

[New Supplier](#)

[Supplier Management](#)

[Asset Management](#)

[Asset Management](#)

[Acceptable Use](#)

[Devices](#)

[Maintenance](#)

[Sensitivity Labels](#)

[Data Loss](#)

[Access Management](#)

[Access Rights](#)

[Authentication](#)

[Office Security](#)

[Workspace](#)

[Reporting](#)

[Human Security](#)

[Security Team](#)

[Management Support](#)

[Staff Vetting](#)

[Employment Contracts](#)

[Staff Training](#)

[Engineering Security](#)

[Technical Compliance](#)

[Technical Documentation](#)

[Vulnerability Management](#)

[Backup & Restore](#)

[Activity Logs](#)

[Encryption](#)

[Change Control](#)

[Engineering Security: Development](#)

[SDLC: Analysis & Design](#)

[SDLC: Development](#)

[SDLC: Testing](#)

[SDLC: Deployment](#)

[SDLC: Maintenance & Disposal](#)

[Engineering Security: Infrastructure](#)

[Data Transfer](#)

[Network Security](#)

[Infrastructure Security](#)

[Monitoring](#)

[Incident Management](#)

[External Contacts](#)

[Incident Management: Preparation](#)

[Incident Management: Assess](#)

[Incident Management: Response](#)

[Incident Management: Review](#)

[Document Version Control](#)

Information Security Policy

Purpose

The purpose of this policy is to direct the design, implementation and management of an effective Information Security Program, which ensures that Access Intelligence's information assets are appropriately identified, recorded, and afforded suitable protection at all times. This document sets forth certain principles regarding the responsible use of information by Access Intelligence and outlines the roles and responsibilities of personnel to protect the confidentiality, integrity, and availability of information assets and data.

Objectives

Corporate governance is the set of practices and responsibilities exercised by the Access Intelligence Board and Senior Management. Strategic direction is defined by corporate objectives. To be of value, information security objectives must support the corporate objectives and strategy.

Relevant Corporate Objectives

1. Protect our clients and the business growth by mitigating the risk of security incidents, legislative fines and reputation damage
2. Support our clients and the business by maintaining international standards in information security
3. Maintain governance structures and processes that support good decision-making by the Board
4. Increase security awareness of staff to protect sensitive business data and personal data
5. Promote a corporate culture that is based on data ethics, protection, and trust

Information Security Objectives

1. To ensure information assets are adequately identified, always recorded and afforded suitable protection, and that Access Intelligence can maintain full compliance with all applicable legislation, regulations and contractual requirements. *[supporting 1, 2]*
2. To implement and manage an Information Security Management System (ISMS) which is certified to ISO/IEC 27001:2022 standards. *[supporting 2, 3]*
3. To ensure that all vulnerabilities, threats and risks to information assets and supporting assets are formally identified, understood, assessed and controlled to reduce the likelihood of an information security incident. *[supporting 1, 2, 3, 5]*
4. To ensure that appropriate plans are maintained to prepare Access Intelligence for an information security incident, and, to ensure the business can continue whilst disaster recovery plans are executed. *[supporting 1, 2, 4]*

5. To ensure that Access Intelligence's employees, contractors and third-party users comply with this Information Security Policy, and all other ISMS documentation, through the provision of effective information security awareness training and ongoing support and monitoring activities. *[supporting 4, 5]*

Policy Scope

This policy covers Access Intelligence's information assets and supporting assets, including information and information systems used, managed, or operated by a contractor or other vendors and applicable to all employees, contractors, and other users of Access Intelligence's information. Including:

Products

- Pulsar
- Isentia Platform (Media Portal)
- Vuelio (UK)
- Vuelio (Australia)
- ResponseSource

People

- All Access Intelligence (Pulsar/Isentia/Vuelio) employees with access to business information.

Premises

- Access Intelligence Headquarters, London, United Kingdom

Data Centre Operations

- Amazon Web Services, EU West 1 region (Pulsar)
- Amazon Web Services, EU West 2 region (Pulsar DR)
- Amazon Web Services, Sydney region (Isentia Platform)
- Amazon Web Services, Sydney region alternate Availability Zone (Isentia Platform DR)
- Microsoft Azure, UK South region (Vuelio)
- Microsoft Azure, UK West region (Vuelio DR)
- Microsoft Azure, Australia East region (Vuelio Australia)
- Pulsant, South London DC (Response Source)

Policy Statements

Access Intelligence shall be committed to the protection of the information assets and supporting assets as defined within the Scope of this Policy. Access Intelligence has created its Information Security Management System (ISMS) in accordance with the international Information Security Management Systems standard ISO/IEC 27001. All Security Control Policies are described in the Appendix.

After reviewing the needs and expectations of interested parties, the scope of the ISMS was defined to support these requirements. To effectively manage and deliver its ISMS, Access Intelligence shall:

Risk Assessment

Perform regular risk assessments on all information assets, and their supporting assets, as detailed within Access Intelligence's Risk Management Policy and using the control objectives and controls as documented within Annex A of ISO/IEC 27001:2022. The documented results of risk assessments shall be reviewed to understand the level of risk to information and supporting assets, and appropriate controls applied as appropriate to address any unacceptable risks that have been identified. A Statement of Applicability (SoA) shall be produced to record which controls have been selected and the reasons for their selection, and the justification for any controls not selected.

Management, Monitoring and Review

Continually monitor, review and improve the Access Intelligence ISMS, in accordance with the Management Review controls, by undertaking regular reviews, internal audits (in accordance with the Internal Audit requirements and other related activities, and taking prompt corrective actions and implementing improvement opportunities in response to the findings of these activities.

Legislative Compliance

Ensure consistently that its Information Security Management System shall support full compliance with the requirements with applicable global legislation, e.g. GDPR.

Supplier Security

Ensure that sufficient security controls and agreements are in place to protect Access Intelligence's assets that are accessible by suppliers, in accordance with the Supplier Security Management Policy. The policy shall describe what requirements must be adhered to when engaging third parties, the standard terms that should be included in supplier agreements and how Access Intelligence will monitor compliance.

Asset Management

Define and maintain a comprehensive Inventory of Assets, including all information assets and supporting assets as defined within the scope of this Policy. The Inventory of Assets shall detail a named owner for each asset, who shall fully understand their responsibilities for

the protection of the asset in accordance with the documented Access Intelligence Asset Management Policy.

Acceptable Use

Ensure that all personnel, contractors and third-party users comply with the Acceptable Use Policy which describes how information assets and their supporting assets should be used in an acceptable manner and in accordance with all ISMS related policies and processes. This policy shall describe the acceptable methods of use of information processing systems, networks (including, for example, the internet and telephone systems) and other resources within the scope of this policy.

Access Control

Ensure that all information assets, and their supporting assets, are protected with strong passwords in accordance with the password management requirements and to ensure their confidentiality, integrity and availability is maintained. Access to information assets and supporting assets shall be in accordance with Access Intelligence's Access Control Policy and be restricted to the minimum required to undertake authorised business activities, and Access Intelligence has adopted the principle that "access is forbidden unless it has been specifically and formally pre-authorised".

Information Classification and Handling

Ensure that all information assets shall be classified and handled in accordance with Information Classification and Handling Guidelines, which details how information assets of different sensitivities shall be managed, handled, processed, encrypted, stored and transmitted. Information is retained in accordance with Data Retention Policy.

Human Security

Minimise risk in the workforce by implementing security controls pre-employment in accordance with the Human Security controls for employee screening and by including Information Security responsibilities into job descriptions.

Information Security Training

Develop a regular training and education programme, in accordance with the Information Security Training Policy, which shall be mandatory for all Access Intelligence's employees, contractors and third-party users, which details their individual responsibilities to fully comply with the requirements of the ISMS policies, processes and work instructions defined within the scope of this policy.

Device Security

Reduce risk of information leakage by only working on devices provided and managed by the organisation or for specific processes. When unattended, devices must be locked, and no information should be displayed on the workstation as per Clear Desk and Screen controls.

Secure Development

Minimise risks during development by improving security controls for people and technology, in accordance with the controls for Data Encryption, Information Transfer, Secure Development & Infrastructure and Change Management Policy, so that the security of Access Intelligence's information assets is not compromised, even in an ever-changing cloud environment.

Information Security Incidents

Provide a mechanism for the swift identification, reporting, investigation and closure of information security incidents to Access Intelligence, in accordance with the Information Security Incident Management controls, and to fully analyse reported incidents to identify the root cause of issues and take advantage of any improvement opportunities which may have been identified.

Business Continuity

Ensure that information security is a key consideration within the Business Continuity Management Policy so that the security of Access Intelligence's information assets is not compromised even when faced with a wide variety of unplanned business interruptions.

ISMS Responsibilities

All individuals specified within the scope of this Information Security Policy 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.

Employees, Contractors and Third-Party Users

Within Access Intelligence, all information security responsibilities are defined and allocated in accordance with the ISMS. All employees shall understand their role in ensuring the security of information assets (and their supporting assets) by complying with information security awareness training, including:

- Creating unique, complex passwords for each user account
- Completing all assigned Information Security training
- Reviewing applicable security control documentation relevant to their role
- Considering the sensitivity of the information that they are processing and correctly classifying the document i.e., password protecting email attachments and/or choosing the appropriate information classification label when sharing documents.
- Reporting suspected and confirmed information security events to the Security Team

There are additional responsibilities defined in order that the ISMS shall operate efficiently and in accordance with the requirements of ISO/IEC 27001. These are detailed below:

Executive Management

The Chief Financial Officer (CFO) and Executive Management shall be responsible for the following activities within the Access Intelligence ISMS:

- Setting and reviewing Access Intelligence's Information Security Objectives
- Delegating appropriate resources necessary to manage and operate the ISMS effectively
- Agreeing the level of acceptable risk within the Risk Assessment Methodology
- Approving any decisions not to address any unacceptable residual risks, where identified
- Having ultimate responsibility for actions related to information security incidents breaches
- Overseeing any disciplinary action resulting from information security incidents/breaches
- Playing an active role during Access Intelligence's Risk Assessment exercises and defining risk mitigation strategies.
- Reviewing any reports of the Information Security Program implementation status or assessments
- Approving Access Intelligence's information security policies and any changes to the policies and ensuring that the overall information security posture is aligned to business requirements and risks.
- Specifically, the **Chief Technology Officer** (CTO) shall be responsible for:
 - Providing guidance and oversight for BCPs and Disaster Recovery Management for Access Intelligence and approving the Disaster Recovery Action Plans documented for implementation.
 - 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 Access Intelligence's security requirements
 - Communicating and resolving any development-related issues arising from third-party developers.

Senior Department/Team Management

Managers within Access Intelligence shall be responsible for:

- Ensuring that their team members are aware of and remain compliant with all information security policies, processes and work instructions, and they receive relevant training for their role
- The provision of a user training and awareness programme for applicable third-party users
- Supporting reviews, internal audits and risk assessments within their area of responsibility
- Specifically, the **Head of HR** for each region shall be responsible for:
 - Organising background verification checks for all employment candidates
 - Include information security compliance requirements in employment contracts
 - Ensuring all employees comply with information security awareness training

Control Owners

Security Control Owners shall be responsible for:

- The way in which their assigned control(s) are selected, implemented and operated
- Understanding which asset(s) are reliant upon each of their assigned controls
- Contributing feedback to asset owners on the operation of each control, to assist them in undertaking accurate risk assessments of their asset(s)
- Helping in the investigation, resolution and closure of any information security incident which does or does not indicate the failure of a control.

Asset Owners

As per the Asset Management Policy, designated Asset Owners shall be responsible for:

- Assessing the value of their asset(s) to the Company
- Undertaking detailed risk assessments on their asset(s), including the identification of controls and assessing their effectiveness as per the Risk Management Policy
- Addressing any unacceptable risks
- Helping in the investigation, resolution and closure of any information security incident which directly or indirectly affects the security of their asset(s).
- Reviewing and authorising the levels of access to their asset(s) which are granted to others
- Contributing to the Acceptable Use monitoring, specifically for the user of their asset(s)

Information Security Officer (Governance, Risk, Compliance)

The Information Security Manager shall have functional GRC responsibility for the Access Intelligence ISMS, and shall be responsible for the daily operational tasks of the ISMS, including:

- Ensuring an appropriate structure of ISMS policies, processes and work instructions are created and maintained for all ISMS activities
- Ensuring the ISMS operates in accordance with the current requirements of ISO 27001
- The preparation and communication of the Statement of Applicability (SoA)
- Overall management of the information security controls in production processes
- Arranging a programme of risk assessments, risk treatments and internal audits. Monitoring compliance which includes internal, external, and regulatory compliance.
- Ensuring compliance with changing laws and applicable regulations.
- Reporting any security incidents to the relevant Supervisory Authority e.g. in the UK, the Information Commissioner's Office (ICO) must be notified within 72 hours of Access Intelligence becoming aware of a data breach.
- Communicating the Information Security policies and security programs to the organisation through ongoing security training and awareness.
- Partnering with business stakeholders across the company to raise awareness of risk management concerns.
- Collaborating with various departments within the organisation to reduce risk by ensuring that technical controls and policies are implemented across the organisation.

Information Security Officer (Technical)

The CTO shall be the ISMS technical lead and be responsible for implementing cyber security controls throughout Access Intelligence's IT infrastructure, including:

- Overall management of the cyber security controls in production processes
- Managing and improving Business Continuity Planning (BCP) and Disaster Recovery (DR) preparedness of the organisation
- Ensuring that Business Continuity Plans (including disaster recovery options) are regularly reviewed, tested and audited, and that any identified corrective actions or improvement opportunities are promptly identified, addressed and resolved.
- Monitoring continuous security improvements; reviewing and recommending applicable changes in the security policies and processes.

Appendix: Security Controls

Each Policy Statement may contain several Security Controls which have their own Control Requirements.

All Controls are mapped to the international standard for Information Security, ISO 27001, and managed in the Access Intelligence Information Security Management System (ISMS).

Risk Management

Both information assets and their supporting assets are subject to a wide variety of threats, each of which has the potential to exploit a vulnerability and produce an event that damages or disrupts the normal, secure existence or operation of the asset. Threats can originate from inside an organisation as well as external sources and may be the result of accidental or deliberate events. A vulnerability alone cannot harm an asset: rather it is a condition or state that could allow a threat to exploit it and consequently cause harm. Therefore, threats and vulnerabilities need to combine to create an incident that can damage or disrupt the normal, secure existence or operation of the asset.

Access Intelligence shall ensure it has a robust risk management methodology that is effective in mitigating risk to information security.

Control Mapping	Control Requirements
<p>Risk Assessment</p> <ul style="list-style-type: none"> • <i>ISDL31 Risk Management Policy</i> • <i>6.1: Actions to address risks and opportunities</i> 	<ol style="list-style-type: none"> 1. All information assets must be documented in the ISMS so that asset evaluations and risk assessments can identify the most appropriate security controls to protect them. 2. Asset evaluations involve reviewing the impact to the business from a loss of: <ol style="list-style-type: none"> a. <i>Confidentiality</i> – if the information was leaked b. <i>Integrity</i> – if the information was damaged c. <i>Availability</i> – if the information was deleted 3. If a high impact is identified, a Risk Assessment must determine the Likelihood of the Impact. 4. A Risk Matrix provides a formalised and repeatable methodology of assessing risk. This 5X5 matrix will score each risk from Very High to Very Low. 5. If a Risk scores Medium or above it must have Controls applied to manage the risk or reduce it to acceptable levels. 6. Full documentation of the Risk Management must be stored in the ISMS.
<p>Audit</p> <ul style="list-style-type: none"> • <i>ISDL14 Internal Audit Policy</i> 	<ol style="list-style-type: none"> 1. Access Intelligence shall compile and communicate in advance, a programme of internal audits 2. Internal audits and spot checks shall be carried out by the Security Team on a regular basis. The scope of the technical audit does not need to be agreed with the Asset Owner prior to the audit.

<ul style="list-style-type: none"> • <i>A.8.34: Protection of information systems during audit testing</i> 	<ol style="list-style-type: none"> 3. External audit requirements for access to systems and data will be agreed upon with the Security Team. This includes penetration tests and external ISO 27001 audits. The scope of technical audit tests will be agreed upon prior to the audit. 4. All staff must comply with audit requests and treat them as a priority 5. Internal Audits shall be undertaken by suitably qualified, experienced and competent Internal Auditors. 6. Auditors shall not undertake (or be asked or be 7. expected to undertake) audits which include their own work. 8. Audit findings shall be promptly and accurately documented in the ISMS and presented to the appropriate Manager. 9. The Manager shall be required to investigate and resolve any reported non-conformance by implementing permanent corrective and/or preventive actions within the requested timescales. 10. Audit, pen test and vulnerability report details are classified as SECRET. This information is not suitable to be shared externally. However, the Security Team can approve the release of a report summary.
---	---

Legal Compliance

To ensure that Access Intelligence can operate a trusted, established Information Security Management System, it shall identify all legislative, regulatory and contractual requirements relevant to achieving the lawful functioning of the business and maintain compliance with all applicable requirements for the duration of Access Intelligence's operations.

Control Mapping	Control Requirements
<p>Obligations</p> <ul style="list-style-type: none"> • <i>ISDL390 Statutory Regulatory and Contractual</i> 	<ol style="list-style-type: none"> 1. Applicable global legislation that could cause a loss of availability to part/all of Access Intelligence services shall be recorded in the ISMS by the Legal Team 2. Compliance activities should be documented in the ISMS with clear ownership identified

<p><i>Compliance Policy</i></p> <ul style="list-style-type: none"> • <i>A.5.31: Legal, statutory, regulatory and contractual requirements</i> 	<ol style="list-style-type: none"> 3. Employment, client and supplier contracts shall include requirements for applicable legislations 4. Relevant training shall be provided to all employees to understand their legal and contractual obligations e.g. GDPR 5. Employees shall be made aware of all relevant legal, contractual and statutory requirements via policies, codes of conduct and relevant training programmes 6. Access Intelligence shall engage the assistance of 3rd party professionals to objectively evaluate and advise on Access Intelligence's standard of compliance with statute, regulation and relevant contractual obligations.
<p>Intellectual Property</p> <ul style="list-style-type: none"> • <i>A.5.32: Intellectual property rights</i> 	<ol style="list-style-type: none"> 1. Access Intelligence's intellectual property (IP) includes source code, product plans, business strategies, domain names, data sets etc, and must be protected effectively by all employees. 2. Third party IP must be protected inline with contractual and legal requirements. 3. Open source libraries are used inline with their licence. This should be reviewed by the Security Team and documented in the ISMS. 4. Trial software must be approved before installation by the Security Team 5. Purchased software must be documented in the ISMS.
<p>Information Lifecycle</p> <ul style="list-style-type: none"> • <i>ISDL15 Data Retention Policy</i> • <i>A.5.33: Protection of records</i> • <i>A.8.10: Information deletion</i> 	<ol style="list-style-type: none"> 1. Security is everyone's responsibility. Digital records are preferred over paper-based records and files. 2. Access to information records should be protected, especially in transit e.g. email attachments 3. If information has a business value, it must be backed up with a cloud supplier 4. Data records should only be retained for as long as they are useful or that there is a legal requirement to keep them. 5. CRM, employment and financial data must be retained for 7 years. 6. Client data must be removed within 100 days of the contract expiring.

<p>Data Protection</p> <ul style="list-style-type: none"> ● <i>ISDL13 Data Protection Policy</i> ● <i>A.5.34: Privacy and protection of PII</i> 	<ol style="list-style-type: none"> 1. "Personal Data" or Personally Identifiable Information (PII) includes any private or publicly available data that can be used to identify an individual. This includes name, email, social media IDs, usernames, tracking cookies etc. This also includes two pieces of unidentifiable information e.g. job title and place of work. PII is classified as CONFIDENTIAL and shall be handled accordingly. 2. Access Intelligence shall appoint a Data Protection Officer (DPO) to manage UK GDPR compliance activities 3. The DPO shall: <ol style="list-style-type: none"> a. Monitor compliance with the UK GDPR b. Map other global data protection laws to UK GDPR requirements c. Maintain a full and accurate record of processing activity which is under its control. d. Maintain clear and concise Privacy Notices, and related information for data subjects. e. Ensure that all data processing activities are subject to full and accurate Privacy Impact Assessments f. Ensure all employees receive regular data protection and privacy training g. Manage the Privacy Team that will respond to applicable Data Subject Access Requests (DSARs) within 30 days h. Promptly report any actual or suspected data breaches internally, and to the Supervisory Authority and data subjects within the required timeframes. 4. All employees shall complete awareness training covering data protection and privacy principles. 5. The Legal Team shall consult the DPO on data protection matters to ensure that information which is transferred between suppliers, clients or Group entities, is adequately protected.
--	--

Supplier Security

Access Intelligence uses third party suppliers to provide services and goods. The effective management of these suppliers is essential in the provision of services to Access Intelligence's clients and ensuring the security of systems and data.

Control Mapping	Control Requirements
<p>New Supplier</p> <ul style="list-style-type: none"> • <i>ISDL19 Supplier Security Management Policy</i> • <i>A.5.19: Information security in supplier relationships</i> • <i>A.5.20: Addressing information security within supplier agreements</i> • <i>A.5.21: Managing information security in the ICT supply chain</i> • <i>A.5.23: Information security for use of cloud services</i> 	<ol style="list-style-type: none"> 1. New suppliers must be: <ol style="list-style-type: none"> a. Reviewed by the Legal Team to ensure confidentiality and compliance with applicable legislation b. Documented in the ISMS with assigned Supplier Relationship Owners c. Reviewed to ensure compliance with security and data protection requirements d. Provided with a copy of the Access Intelligence Supplier Code of Conduct 2. A full security assessment maybe required which could result in additional security clauses being added to the contract. 3. If the supplier processes personal data, the Procurement Manager may be required to complete a DPIA prior to approval. 4. No supplier agreement is to be approved that may increase the overall risk to information security
<p>Supplier Management</p> <ul style="list-style-type: none"> • <i>A.5.22: Monitoring, review and change management of supplier services</i> 	<ol style="list-style-type: none"> 1. Supplier Relationship Owners must ensure ISMS documentation is maintained and accurate. 2. If a supplier experiences a security incident which impacts Access Intelligence, they must inform us within 24 hours of discovery. Supplier Relationship Owners must ensure such notifications are escalated to the Security Team immediately. 3. Supplier changes must be reviewed by the Relationship or Asset Owner and escalated to the Security Team for review.

Asset Management

Access Intelligence shall, as an essential element of its Information Security Management System ensure that all its information assets are always identified and protected. This extends to those

supporting assets upon which information assets depend for their confidentiality, integrity and availability.

All assets shall be subject to risk assessment, and appropriate controls identified and applied to ensure that risks are fully managed. Security controls shall operate both efficiently and effectively in an authorised manner to ensure that Access Intelligence's information and supporting assets are protected.

Control Mapping	Control Requirements
<p>Asset Management</p> <ul style="list-style-type: none"> ● <i>ISDL05 Asset Management Policy</i> ● <i>A.5.9: Inventory of information and other associated assets</i> 	<ol style="list-style-type: none"> 1. All information systems and components shall be documented in the ISMS Asset Inventory 2. All information assets must have an owner 3. Asset Owners must: <ol style="list-style-type: none"> a. Document the asset Criticality and Sensitivity to represent Business Value and Asset Classification b. Document a Risk Assessment to represent Risk Rating c. Ensure ISMS documentation is maintained d. Review and approve all user access to their asset e. Ensure their Asset conforms to this Information Security Policy
<p>Acceptable Use</p> <ul style="list-style-type: none"> ● <i>ISDL06 Acceptable Use Policy</i> ● <i>A.5.10: Acceptable use of information and other associated assets</i> 	<ol style="list-style-type: none"> 1. Occasional personal use of business equipment and access to the Internet is permitted 2. Unless online posting is part of business duties, social media posts by employees using a work email address must contain a disclaimer stating that "the opinions expressed are strictly their own and not necessarily those of the organisation". 3. Employees posting from personal accounts should be aware that this could still be indirectly linked back to the business, therefore content should not be considered offensive or bring the business into disrepute. 4. Information systems and devices must not be used to shall not be used to download, process, store, upload or transmit any material that is obscene, threatening, abusive, offensive to others, defamatory, indecent, racist, sexist, libellous, hateful or connected to criminal or illegal actions or intentions. In addition, acts relating to breaching copyrighted material, trade secrets or violating intellectual property shall also be prohibited.

	<p>5. Employees shall not:</p> <ul style="list-style-type: none">a. Install software without approval from the IT teamb. Send business information to their personal email accountsc. Transfer business information to a personal cloud storage accountd. Share passwords or allow use of their accounts by otherse. Work on personal laptops if they have been provided with a company laptopf. Bypass security controls <p>6. Employees shall:</p> <ul style="list-style-type: none">a. Conduct themselves in a professional manner with courtesy, integrity and professionalism, which aligns with Access Intelligence's corporate standing.b. Primarily work from their company owned device but are able to "Bring Your Own Device" (BYOD), e.g. access non-critical systems on personal smart phones, for reading work email or booking holiday requests. <p>7. Employees should be aware that:</p> <ul style="list-style-type: none">a. For security and network maintenance purposes, authorised individuals within the organisation may monitor equipment, systems, and network traffic at any time.b. Unacceptable use of business assets may be escalated to HR for disciplinary proceedingsc. Employees should check the sender's email address before reading an email and that any links target an expected URL before clicking them.d. Employees must use extreme caution before opening email attachments received from unknown senders. If the attachment requests for "Macros to be enabled" this must be declined.e. Employees that are unsure as to the suitability of a device, supplier, asset, should proactively spread to the Security Team <p>8. All employees must ensure their company devices are:</p>
--	---

	<ul style="list-style-type: none"> a. Protected with passwords etc b. Updated regularly and security updates are installed immediately c. Monitored by Anti-Virus software with daily updates <p>9. All software must be:</p> <ul style="list-style-type: none"> a. Approved by the IT Team b. Supported by the vendor c. Used in accordance with the vendor's licence
<p>Devices</p> <ul style="list-style-type: none"> ● <i>ISDL30 Mobile and Personal Device Policy</i> ● <i>A.8.1: User endpoint devices</i> ● <i>A.7.10 Storage Media</i> ● <i>A.5.11: Return of assets</i> ● <i>A.7.14: Secure disposal or re-use of equipment</i> 	<ul style="list-style-type: none"> 1. All devices (including personal/BYOD devices accessing company data e.g. email) must: <ul style="list-style-type: none"> a. Use an operating system that is still supported by the vendor b. Anti-virus software must be enabled whenever possible c. Auto lock within 10 minutes of inactivity 2. All Access Intelligence laptops must comply with the above list, and: <ul style="list-style-type: none"> a. Endpoint Detection and Response software must be installed on all company owned endpoints b. Hard drives must be encrypted 3. Devices should only connect to untrusted networks, e.g. when remote working, when using a VPN 4. Removable media must be disabled on all end-points e.g. USB sticks in laptops 5. Individuals leaving the business must return their laptop and any other information assets prior to their leaving date. 6. Any access granted to an individual or supplier must be disabled within 24 hours of the agreement ending. 7. Old redundant devices must be securely destroyed to ensure accidental unauthorised disclosure or misuse of information is not possible. A formal destruction certificate must be obtained.

<p>Maintenance</p> <ul style="list-style-type: none"> • <i>A.7.13: Equipment maintenance</i> 	<ol style="list-style-type: none"> 1. All devices e.g. laptops, firewalls etc must be patched regularly 2. Any equipment repairs requiring external expertise must include formal confidentiality clauses e.g. NDA. 3. Any equipment repairs requiring an asset to be transferred off-site must be documented in the Asset Inventory 4. Any personal/BYOD devices e.g. smart phones, that may require repair must first have any business information deleted e.g. company email app
<p>Sensitivity Labels</p> <ul style="list-style-type: none"> • <i>ISDL52 Information Classification and Handling Guide</i> • <i>A.5.12: Classification of information</i> • <i>A.5.13: Labelling of information</i> 	<ol style="list-style-type: none"> 1. All business controlled information must be classified to ensure appropriate controls for sensitive data. 2. If a system doesn't provide labelling built-in, adding the label to the top of the document is sufficient 3. Labels available are: <ol style="list-style-type: none"> a. PUBLIC: Can be shared publicly without additional controls. b. CONFIDENTIAL: Can be shared to trusted individuals. Recipients should be under contractual obligation and attachments should be password protected. c. INTERNAL: Not intended for individuals external to the business. Information should be encrypted in the cloud and access should be via a password protected work account. d. SECRET or RESTRICTED: Not intended for internal or external sharing outside of the initial recipients. Information should be password protected and encrypted in the cloud. 4. Unlabelled information should be classified by default as: <ol style="list-style-type: none"> a. Emails from Legal, HR or Finance teams are CONFIDENTIAL b. Google Workspace documents are INTERNAL c. All other unlabelled information is PUBLIC.

<p>Data Loss</p> <ul style="list-style-type: none"> • <i>A.8.12: Data leakage prevention</i> 	<ol style="list-style-type: none"> 1. Classified information, i.e. a document with a sensitivity label, should have technical controls configured to enforce the labels handling requirements and protect against data loss 2. Collaboration tools e.g. Google Workspace, Office 365 etc should have public sharing options disabled 3. Company email systems must display a notification when: <ol style="list-style-type: none"> a. Emails are received by an external sender b. Emails are to be sent to an external recipient c. An email is suspected as Spam or Phishing
--	---

Access Management

All information assets, and their supporting assets, shall be afforded such protection as is necessary to ensure that their confidentiality, integrity and availability can be maintained to required levels. This shall include the selection and implementation of suitable controls to prevent loss or damage by unauthorised access, unauthorised amendment, and deliberate and accidental damage.

Control Mapping	Control Requirements
<p>Access Rights</p> <ul style="list-style-type: none"> • <i>ISDLO7 Access Control Policy</i> • <i>A.5.15: Access control</i> • <i>A.5.16: Identity management</i> • <i>A.5.18: Access rights</i> • <i>A.8.2: Privileged access rights</i> • <i>A.8.3: Information access restriction</i> • <i>A.8.18 Use of privileged utility programs</i> 	<ol style="list-style-type: none"> 1. Users will be allocated the least amount of access to meet their business requirements 2. Access requests must be approved by a Senior Manager or Asset Owner 3. Privileged accounts should be separated from non-privileged accounts 4. User accounts should not be shared 5. Access rights will be monitored by the Asset Owner 6. A user's access rights must be removed within 24 hours of them leaving the business

<p>Authentication</p> <ul style="list-style-type: none"> ● <i>ISDLO3 Password Management Policy</i> ● <i>A.5.17: Authentication information</i> ● <i>A.8.5: Secure authentication</i> 	<ol style="list-style-type: none"> 1. Password complexity rules: <ol style="list-style-type: none"> a. 8 characters minimum (12 characters preferred) b. Combination of upper and lower case, number and symbols. 2. Passwords should be unique for each system 3. Multi-Factor Authentication (MFA) must be configured (if available) 4. Biometrics e.g. finger prints, facial recognition, can be used to secure devices instead of a password 5. Passwords or authentication tokens must not be stored in plain text. Password Managers are preferred. 6. If passwords need to be communicated externally, they must be sent in a separate email to the username 7. If account compromise is suspected, change the password immediately and report to IT
<p>Office Security</p> <ul style="list-style-type: none"> ● <i>A.7.1: Physical security perimeter</i> ● <i>A.7.2: Physical entry</i> ● <i>A.7.3: Securing offices, rooms and facilities</i> ● <i>A.7.4: Physical security monitoring</i> ● <i>A.7.8: Equipment siting and protection</i> ● <i>A.7.11: Supporting utilities</i> ● <i>A.7.12: Cabling security</i> 	<ol style="list-style-type: none"> 1. Access Intelligence Group Headquarters are based in London, UK. 2. The building entrance must be covered by CCTV 3. The building reception should be staffed during business hours 4. Building access should be controlled via access cards 5. Office access must be controlled via access cards 6. Key code pads shall be used to protect sensitive areas on the Office 7. Office cleaners must be vetted inline with other contractors 8. All Visitors to the office must be logged. The Log Book is maintained by Office Reception staff. 9. Visitors must be accompanied whilst in the office at all times 10. Visitor/Guest Wi-Fi must be separate from the Employee Wi-Fi and not be connected to any file stores or intranets. 11. Network equipment must be stored in secure areas e.g.

<ul style="list-style-type: none"> ● <i>A.8.22: Segregation in networks</i> 	<p>rooms secured with key pads</p> <ol style="list-style-type: none"> 12. Network cabling should be protected (or hidden) to ensure they are secure 13. The office must have effective supporting utilities to protect employees and ensure business continuity: <ol style="list-style-type: none"> a. Smoke alarms b. Fire extinguishers c. Surge protection extension leads 14. After risk assessment, the following may also be applicable: <ol style="list-style-type: none"> a. UPS power supply b. Dual internet connection 15. Supporting utilities must be tested annually to ensure they are still effective.
<p>Workspace</p> <ul style="list-style-type: none"> ● <i>ISDL16 Clear Desk and Clear Screen Policy</i> ● <i>A.7.7: Clear desk and clear screen</i> ● <i>A.6.7: Remote working</i> ● <i>A.7.9: Security of assets off-premises</i> 	<ol style="list-style-type: none"> 1. Device screens displaying Confidential information must be positioned so that it cannot be read by unauthorised people 2. Working on Wi-Fi should utilise Secure & Trusted Wi-Fi networks i.e. office wifi or an employees home network. 3. If working remotely and a Trusted Wi-Fi Network is unavailable, employees should create a Secure Hotspot on their personal mobile phones and tether to that. 4. If this is not an option, employees must: <ol style="list-style-type: none"> a. Take steps to validate the source of the Untrusted Network e.g. double check the Wi-Fi name with venue staff b. Login to the Company VPN to add a layer of privacy to network traffic. Do not use Personal VPNs. 5. All devices must have a lock screen enabled within 10 minutes of inactivity 6. Employees should not leave Confidential information unattended on their desks or in meeting rooms e.g. print outs, note books, whiteboards etc. 7. Confidential information which is visible to others on a screen must be protected with a Privacy Screen or blocked from view 8. Printed documents containing Confidential information

	<p>must be disposed with a cross cut shredder</p> <p>9. Any equipment taken off site that a user is not already responsible for requires prior approval from Senior Management</p>
<p>Reporting</p> <ul style="list-style-type: none"> • <i>A.6.8: Information security event reporting</i> 	<ol style="list-style-type: none"> 1. All employees are responsible for reporting information security events to the IT Service Desk. 2. Security events include: <ol style="list-style-type: none"> a. Data leak b. Security breach c. Ineffective security control d. Human error e. Access violations f. Vulnerabilities 3. Anonymous reporting is available via the Whistleblowing Policy

Human Security

Access Intelligence shall ensure that employees are suitable for the roles for which they are considered. Background verification checks should be carried out, proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Access Intelligence shall provide appropriate training which ensures that all employees and contractors are aware of the threats to information security that Access Intelligence faces and are aware of their personal involvement in minimising information security risks.

Control Mapping	Control Policy
<p>Security Team</p> <ul style="list-style-type: none"> • <i>ISDL10 Roles and Responsibilities</i> • <i>A.5.2: Information security roles and responsibilities</i> 	<ol style="list-style-type: none"> 1. The ISMS shall document all security roles and accountable individuals 2. The Security Team will include the CTO and heads of IT, infrastructure, development and data protection. 3. Access Intelligence will appoint a head of Information Security to manage the ISMS who is suitably qualified e.g. CISM, CISSP, CISA 4. All security roles and responsibilities will be documented in the ISMS 5. Access Intelligence will separate duties to ensure there is

<ul style="list-style-type: none"> ● <i>A.5.3: Segregation of duties</i> 	<p>no conflict of interests when carrying out security responsibilities</p> <p>6. Access Intelligence will ensure that the Executive Management receive monthly updates of ISMS activity</p>
<p>Management Support</p> <ul style="list-style-type: none"> ● <i>ISDLO9 Management Review Policy</i> ● <i>A.5.4: Management responsibilities</i> 	<ol style="list-style-type: none"> 1. Top management must act as role models for information security. 2. Management must ensure that: <ol style="list-style-type: none"> a. Access Intelligence undertakes regular, formal management reviews of its Management Systems, to validate that they are operating as planned and remain relevant to business activities. b. Access Intelligence has defined participants, responsibilities and structure of all formal management reviews, including the format and distribution of documented records. 3. Management shall ensure that employees, contractors and suppliers understand: <ol style="list-style-type: none"> a. their information security responsibilities when accessing company information b. are provided with policies and guidelines to state security expectations of their role c. achieve a level of awareness on security relevant to their role d. are provided with a confidential whistleblowing channel 4. Regular Management Review meetings shall include: <ol style="list-style-type: none"> a. significant risk assessments completed over the previous period b. any significant risk treatment activities over the previous period c. internal audits and non-conformances raised over the previous period d. ISMS metrics 5. Annual Management Review Meetings shall include consideration of: <ol style="list-style-type: none"> a. the status of actions from previous management reviews

	<ul style="list-style-type: none"> b. changes in external and internal issues that are relevant to the information security management system; c. changes in needs and expectations of interested parties that are relevant to the information security management system; d. feedback on the information security performance, including trends in: <ul style="list-style-type: none"> i. nonconformities and corrective actions; ii. monitoring and measurement results; iii. audit results; iv. fulfilment of information security objectives; e. feedback from interested parties; f. results of risk assessment and status of risk treatment plan; g. opportunities for continual improvement.
<p>Staff Vetting</p> <ul style="list-style-type: none"> ● <i>ISDL55 Employee Screening Policy</i> ● <i>A.6.1 Screening</i> 	<ol style="list-style-type: none"> 1. Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements. 2. The HR Team will screen all candidates that the Hiring Manager wishes to hire. This includes: <ul style="list-style-type: none"> a. Confirmation from the applicant as to the accuracy of their CV b. Validating competence either via interview tests and/or on receipt of 2 satisfactory character references c. Confirmation of claimed academic and professional qualifications where there is a role requirement d. Independent identity verification (passport or similar document) e. Checking legal entitlement to work in a particular country f. Criminal disclosure record where there is a role requirement) 3. When verification cannot be completed in a timely manner,

	<p>we take a risk based approach based on the role and the individual in question, and implement one or more of the following controls until the review is finished:</p> <ol style="list-style-type: none"> a. Delayed onboarding b. Delayed deployment of corporate assets c. Onboarding with reduced access d. Termination of employment <ol style="list-style-type: none"> 4. Employees with access to UK Police data shall be vetted to: NPPV Level 3 + SC. 5. Employees with access to AUS Police data shall be vetted with a Police Check.
<p>Employment Contracts</p> <ul style="list-style-type: none"> • <i>ISDL53 Adding Information Security Responsibilities into JD</i> • <i>A.6.2: Terms and conditions of employment</i> • <i>A.6.5: Responsibilities after termination or change of employment</i> • <i>A.6.6: Confidentiality or non-disclosure agreements</i> 	<ol style="list-style-type: none"> 1. Employees, contractors and third-party users should have their information security roles and responsibilities formally documented in accordance with the organisation's Information Security Policy. 2. Information Security terms shall include: <ol style="list-style-type: none"> a. Awareness of the Information Security Policy b. Descriptions of any additional security role responsibilities e.g. asset owner etc. c. Consequences for disregarding information security 3. Data Protection terms shall include: <ol style="list-style-type: none"> a. Confidentiality and nondisclosure of business and client data b. Clarity over copyright and other assets c. Data protection and handling requirements d. Incident notification instructions e. Consequences for disregarding data protection 4. If an employee is promoted or moves teams during employment, the Line Manager should review if any access requirements have changed and notify the IT Team 5. If an employee leaves the business, the HR Team shall notify the IT Team immediately to ensure all access can be disabled within 24 hours.

Staff Training

- *ISDL02 Information Security Training Policy*
- *A.6.3: Information security awareness, education and training*

1. All employees will receive regular awareness training covering, at a minimum:
 - a. Secure remote working
 - b. Incident reporting
 - c. Phishing
 - d. Password management
 - e. Data protection
2. Training content will be sourced from:
 - a. Training providers e.g. MetaCompliance
 - b. ICO
 - c. NCSC
 - d. ACSC
 - e. SANS
 - f. NIST
3. The Security Team is responsible for training content and publishing.
4. The HR Team is responsible for staff training communications.
5. All new starters will receive information security training in their first 2 weeks
6. All employees will receive regular refresher training throughout the year
7. If a user suspects or has actually been infected by malware (including viruses, ransomware, worms, trojans etc.) they must:
 - a. Immediately disconnect the machine from the network i.e. turn off Wi-Fi and unplug network cables.
 - b. Do not turn off the power as this will destroy any evidence stored in temporary memory e.g. RAM
 - c. Take a photo of any ransomware message or pop-ups as evidence.
 - d. Stop using the machine until informed that it is safe to do so.
 - e. Report the security event to the IT Service Desk

Engineering Security

To ensure that Access Intelligence's applications and systems are designed and developed to allow for the identification and mitigation of security-related issues.

Control Mapping	Control Requirements
<p>Technical Compliance</p> <ul style="list-style-type: none"> • <i>A.5.36: Compliance with policies, rules and standards for information security</i> 	<ol style="list-style-type: none"> 1. Senior Engineering Staff should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. 2. Cloud services must be hardened against threats and have vulnerability reporting enabled 3. Asset Owners and Senior Engineering Staff should be aware of the vulnerability reports from their information assets and mitigate according to the Risk Management policy.
<p>Technical Documentation</p> <ul style="list-style-type: none"> • <i>A.5.37: Documented operating procedures</i> 	<ol style="list-style-type: none"> 1. Documented Operational Processes (DOPs) or Standard Operating Procedures (SOPs) shall ensure correct and secure operations of information processing facilities. 2. Documented procedures should be prepared: <ol style="list-style-type: none"> a. When an activity needs to be performed in the same way by many people; b. When an activity is performed rarely; c. When an activity is new to the organisation; d. Prior to handover of an activity to new personnel.
<p>Vulnerability Management</p> <ul style="list-style-type: none"> • <i>A.8.8: Management of technical vulnerabilities</i> 	<ol style="list-style-type: none"> 1. All Access Intelligence products will be tested by a CREST certified penetration tester at least once per year. 2. The London office (HQ) IT infrastructure will be scanned by a third party at least once per year. 3. All production infrastructure and software must be scanned to identify possible weaknesses. 4. Vulnerability scanning should be continuous by must be no less than once per quarter. 5. Identified vulnerabilities shall be regularly reviewed by the Security Team. Risk Assessments will determine if action should be taken immediately or scheduled within the

	<p>following timeframes:</p> <ol style="list-style-type: none"> a. <i>Critical</i> – No later than 2 weeks from identification b. <i>High</i> – No later than 4 weeks from identification c. <i>Medium</i> – No later than 6 months from identification d. <i>Low</i> – No later than 12 months from identification <ol style="list-style-type: none"> 6. All anti-virus/anti-malware/EDR software should have virus definition files updated each day. 7. All end-points should have automated patch discovery in place 8. Patches should be installed on a monthly cycle 9. Emergency patches, identified from the SOC or Security Team, should be installed immediately
<p>Backup & Restore</p> <ul style="list-style-type: none"> • A.8.13: <i>Information backup</i> 	<ol style="list-style-type: none"> 1. Production backups are crucial to business continuity and are considered Critical Assets 2. Backups must contain enough data to restore all client accounts and products in a disaster scenario 3. All products should have: <ol style="list-style-type: none"> a. Point in Time (PiT) backups configured for at least 7 days b. Weekly backups should be retained for at least 28 days, although 90 days is preferred 4. Backups should be stored in a separate environment to the source data to protect them from the risk of Malware spreading 5. Access to backups should be restricted, logged and require MFA 6. All backups should be encrypted and immutable 7. Engineering Teams shall: <ol style="list-style-type: none"> a. regularly review backups to determine that they are adequate and accurate b. Test that backups are effective by testing the restoration process at least once per year

Activity Logs

- *A.8.15: Logging*

1. Production logs are crucial to incident investigations and are considered Critical Assets
2. For correlation of system and event logs, clock synchronisation shall be configured within information processing systems and applications
3. Access to logs should be restricted, logged and require MFA
4. All logs should be encrypted and immutable – even to admins
5. Product logs should contain:
 - a. Successful login attempts
 - b. Unsuccessful login attempts
 - c. All logoffs
 - d. Attempts to perform unauthorised functions
 - e. User actions and data changes/events
 - f. Errors
6. Admin logs should contain all of the product log requirements, plus:
 - a. Additions, deletions and modifications to user and system accounts/privileges
7. If possible, logs should aggregate to the SEIM
8. All logs in production environments should be protected with the following requirements:
 - a. Log files should be stored in a separate location to the source data.
 - b. Access to log files must be restricted, recorded and require MFA where possible
 - c. Consideration should be given to additional protection of sensitive data within the log files such as data masking or encryption.
 - d. Logs should be retained for at least 30 days, although 90 days is preferred

<p>Encryption</p> <ul style="list-style-type: none"> • <i>ISDL11 Data Encryption Policy</i> • <i>A.8.24: Use of cryptography</i> 	<ol style="list-style-type: none"> 1. Access Intelligence will only use standardised, currently accepted, and extensively reviewed encryption algorithms. 2. Cryptography implementations must be kept up to date to avoid emerging weaknesses. 3. All critical or sensitive data transferred outside of the organisation should be encrypted. 4. Company laptop hard drives must be encrypted. 5. Access credentials must be encrypted in transit. 6. Secure File Transfer Protocol (SFTP) should be used for file transfers to relevant bodies 7. Secure Shell (SSH) should be used for securing connections to remote devices 8. Data in Transit must be encrypted using TLS 1.2 (or later) 9. Data at Rest should be encrypted using 256-bit Advanced Encryption Standard (AES) encryption 10. Senior Engineering Staff are responsible for key management 11. The key must be of the type RSA and be 2048 bits. The private key must have a passphrase which at least conforms to the minimum requirements for passwords.
<p>Change Control</p> <ul style="list-style-type: none"> • <i>ISDL54 Change Management Policy</i> • <i>A.8.32: Change management</i> 	<ol style="list-style-type: none"> 1. Changes to software, infrastructure, suppliers, shall be managed and executed according to a formal change control process. 2. The control process will ensure that the changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner. 3. If a change is planned to a system that stores or processes personal data, a Privacy Impact Assessment (PIA) or Data Protection Impact Assessment (DPIA) should be conducted in compliance with relevant privacy legislation. 4. No changes can be made to operational systems without approval from the Senior Engineering Team 5. All change requests shall be logged 6. The approval of all change requests and the results thereof shall be documented e.g. GitHub commits must be approved by another developer 7. The Approver is responsible for Quality Assurance (QA) of source code, technical review of applications and

	<p>security/privacy checks</p> <p>8. Senior Managers should:</p> <ul style="list-style-type: none"> a. Ensure that all team members are aware of their teams change control procedures b. Coordinate awareness strategies and rollouts to effectively communicate changes. c. Continually improve change management controls as necessary
--	--

Engineering Security: Development

Access Intelligence's products shall be developed in accordance with industry best practice, including considerations for secure design, code creation, application testing, weakness remediation, and deployments of code into live, operational environments.

Control Mapping	Control Requirements
<p>SDLC: Analysis & Design</p> <ul style="list-style-type: none"> ● <i>ISDL77 Secure Development Policy</i> ● <i>A.8.25: Secure development life cycle</i> ● <i>A.5.8: Information security in project management</i> ● <i>A.8.26: Application security requirements</i> 	<ol style="list-style-type: none"> 1. Product development plans should include a risks and mitigations to ensure the risk to information security & data privacy does not increase 2. Security and Privacy requirements, e.g. encryption, logging, backup etc, should be included in project plans i.e. non-functional requirements 3. Any development plans which identify a high risk should be discussed with the Security/Privacy Team 4. Any new data or tech suppliers must be reviewed by the Legal Team 5. Any new source code library must be licenced, appropriately hardened and supported by the vendor e.g. receives security updates 6. No source code changes shall be made to third party software libraries which could be overwritten on future updates

<p>SDLC: Development</p> <ul style="list-style-type: none"> ● <i>A.8.25: Secure development life cycle</i> ● <i>A.8.4: Access to source code</i> ● <i>A.8.31: Separation of development, test and production environments</i> 	<ol style="list-style-type: none"> 1. Access to source code must require MFA 2. All developers must maintain an awareness of the OWASP Top 10 Vulnerabilities and mitigations. 3. All developers shall ensure that these requirements are effectively implemented within all their development activities 4. System documentation is to be maintained 5. Development must be carried out in a separate environment 6. All source code changes must be version controlled 7. Version control must document who changed what and when i.e. no shared accounts
<p>SDLC: Testing</p> <ul style="list-style-type: none"> ● <i>A.8.25: Secure development life cycle</i> ● <i>A.8.33: Test information</i> ● <i>A.8.11: Data masking</i> ● <i>A.8.29: Security testing in development and acceptance</i> ● <i>A.8.30: Outsourced development</i> 	<ol style="list-style-type: none"> 1. Testing shall be carried out on all changes to ensure the security, robustness, correctness and performance of the application e.g. unit tests, negative testing, load testing and impact testing as appropriate to the level of change 2. All development changes must be reviewed & approved by a separate developer and only deployed once all testing and authorisation has been completed. 3. When outsourced development is used, any development changes must be approved by a senior manager. 4. No production data must be used in non-production environments 5. No client data must be used in testing 6. PII/personal data should be must be masked or obfuscated wherever possible e.g. delete the first 3 characters of all PII strings in the database 7. Email tools should be disabled during development and testing. Only fictitious or staff contacts are to be included in email testing.
<p>SDLC: Deployment</p> <ul style="list-style-type: none"> ● <i>A.8.25: Secure development life cycle</i> 	<ol style="list-style-type: none"> 1. Only approved change requests can be deployed. 2. Engineering teams should develop automated build and deployment pipelines to increase the repeatability, accuracy, and security of systems 3. Product environments are classified as SECRET and should be handled according to this policy 4. Consideration must be given to limit the amount of access

	granted in production environments.
SDLC: Maintenance & Disposal <ul style="list-style-type: none"> • <i>A.8.25: Secure development life cycle</i> 	<ol style="list-style-type: none"> 1. Developers must: <ol style="list-style-type: none"> a. Maintain an awareness of their software vendors and alert the Security Team of any changes which could increase risk to information security b. Ensure software and source code libraries are patched effectively c. Mitigate any identified source code vulnerabilities according to the timeframes documented in this policy 2. Developers should maintain awareness of their assets and ensure that information assets that are no longer useful are "hard" deleted.

Engineering Security: Infrastructure

Access Intelligence's applications and operational infrastructure shall be designed and developed to allow for the identification and mitigation of security-related issues. This includes acceptable secure development principles which, properly implemented, will prevent the compromise of data, interference from malicious activities, or damage to IT services.

Control Mapping	Control Requirements
Data Transfer <ul style="list-style-type: none"> • <i>A.5.14: Information transfer</i> 	<ol style="list-style-type: none"> 1. The classification of information transferred, e.g. email attachments, must be considered and appropriate protection applied e.g. password protected files, email encryption 2. FTP is suitable for information classified as PUBLIC. 3. SFTP is preferred for information classified as CONFIDENTIAL 4. Google Workspace apps are preferred for information classified as INTERNAL or SECRET 5. Data in transit should use TLS to create HTTPS sessions. Minimum requirements: <ol style="list-style-type: none"> a. TLS 1.3 is preferred but TLS 1.2 is sufficient b. Use a 2048 bit RSA key or an elliptic curve 256 bit ECDSA key c. Key material is signed using SHA-256 with RSA or

	<p style="text-align: center;">ECDSA Encryption</p> <p>6. Email tools within the products must comply with the following requirements:</p> <ol style="list-style-type: none"> a. TLS 1.2 (or higher) encryption in transit b. 2048 bit DKIM certificate c. SPF records configured d. DMARC, if possible (p=reject) e. If possible, MTA-STS
<p>Network Security</p> <ul style="list-style-type: none"> ● <i>A.8.20: Networks security</i> ● <i>A.8.21: Security of network services</i> ● <i>A.8.23: Web filtering</i> 	<ol style="list-style-type: none"> 1. Access Intelligence shares responsibility with cloud providers according to the Infrastructure as a Service (IaaS) model. Cloud hosting providers are therefore responsible for physical and environmental controls, network service availability etc. 2. Offices must be protected with firewalls 3. Products must be protected with Web Application Firewalls (WAFs) 4. Firewalls must be configured to deny-all incoming connections with allowed connections being specified in rules or white-lists 5. Logs from firewalls should be reviewed by a SOC 6. Web filtering shall be used to block access to websites with known malicious content or illegal materials. 7. Installation of software is restricted to device admins 8. Baseline configurations for network devices must be documented 9. Network devices should also adhere to the following requirements: <ol style="list-style-type: none"> a. Administrative interfaces must require authentication and encryption b. Vendor default passwords must be removed, disabled or changed c. Sample applications or scripts must be removed from web servers d. All systems and applications must be patched regularly e. Security configuration baselines are defined,

	<p>implemented and monitored across all endpoints.</p> <ul style="list-style-type: none"> f. Network devices should be configured to log sufficient detail to support an incident investigation g. Infrastructure security configuration reviews must be performed regularly to validate compliance with security standards h. All high-risk security patches must be applied to network devices where available i. Endpoint Detection and Response (EDR) software must be installed on all end-points j. All EDR logs should aggregate into a Security Event and Incident Management (SEIM) solution. k. Virus definition files must be updated daily l. The 'auto run' feature of the OS must be disabled wherever possible
<p>Infrastructure Security</p> <ul style="list-style-type: none"> ● <i>A.8.27: Secure system architecture and engineering principles</i> ● <i>A.8.9: Configuration management</i> ● <i>A.8.6: Capacity management</i> ● <i>A.8.7: Protection against malware</i> ● <i>A.8.19: Installation of software on operational systems</i> 	<ol style="list-style-type: none"> 1. Access to all cloud infrastructure must require MFA 2. All access (success & failures) should be logged 3. VPNs must be regularly patched and require MFA 4. Configuration scanning must be installed on all product infrastructure and be measuring compliance against vendor best practice or Centre for Internet Security (CIS) standards. 5. Scanning must notify the Security Team if a misconfiguration has been identified. Mitigation of which is prioritised. 6. Only the services that are required are to be enabled. Services must: <ul style="list-style-type: none"> a. Be available only within the network and offer limited connectivity to wider networks as needed; b. Be minimally configured to perform its role (e.g. unnecessary features must be disabled where possible); c. Require authentication and encryption where necessary. 7. Cloud hosting providers offer greater flexibility for capacity planning. Automatic scaling shall be configured where possible.

	<ol style="list-style-type: none"> 8. EDR software must be installed on all end-points e.g. laptops, servers etc 9. Device security updates shall be applied in accordance with severity or in line with monthly patching cycles 10. Vulnerabilities shall be analysed to discover how we can avoid similar vulnerabilities occurring in the future 11. Security issues shall be addressed at root level 12. The Senior Engineering Team shall oversee all installations on operational systems. 13. Patches shall be applied on a monthly basis following testing in non-production environments during the preceding week. 14. Emergency patches (e.g. to fix incidents) may be deployed outside of the regular schedule following authorisation from the CTO.
<p>Monitoring</p> <ul style="list-style-type: none"> • <i>A.8.16: Monitoring activities</i> • <i>A.8.17: Clock synchronization</i> 	<ol style="list-style-type: none"> 1. Access Intelligence shall ensure that boundary protection processes and procedures are established. 2. Endpoint Detection & Response (EDR) software must be installed on every end point 3. Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS) must be configured 4. User and network activities, exceptions, faults and information security events shall be logged, monitored, reviewed and acted, upon on a regular basis 5. Local logging shall be enabled on all systems and networking devices. 6. Access Intelligence shall use various monitoring software tools: <ol style="list-style-type: none"> a. Cloud hosts - monitoring of access, changes and improvement recommendations. b. End-points - Protection & Response software c. Systems - Configuration compliance monitoring d. Products - Vulnerability scanning e. Internet traffic - physical firewalls and Web f. Application Firewalls (WAF) g. Email - email attachment scanning

	<ol style="list-style-type: none"> 7. Logs from critical assets and EDR shall be aggregated in a Security Event & Incident Management (SEIM) 8. A Security Operations Centre (SOC) shall monitor the SEIM. 9. Alerts must be configured for Critical and High events 10. Clock synchronisation on workstations and laptop devices is done from an internet accessible atomic clock via NTP.
--	---

Incident Management

To ensure that Access Intelligence has an effective mechanism in place to promptly identify, report, investigate and resolve information security incidents affecting information assets. This shall include Disaster Recovery Plans and a Business Continuity Plan. Such capability shall be appropriate to restore normal operations and service in the event of an unplanned interruption being experienced.

Control Mapping	Control Requirements
<p>External Contacts</p> <ul style="list-style-type: none"> ● <i>ISDL04 Information Security Incident Management Policy</i> ● <i>A.5.5: Contact with authorities</i> ● <i>A.5.6: Contact with special interest groups</i> ● <i>A.5.7: Threat intelligence</i> 	<ol style="list-style-type: none"> 1. All staff have a responsibility to contact the emergency services in an emergency situation 2. Access Intelligence will document relevant non-emergency external contacts in the ISMS 3. Responsibility will be assigned for contacting external contacts 4. Membership of professional bodies, security and industry specialist forums, is encouraged. 5. The Security & Privacy Team will subscribe to UK's NCSC and ICO communications 6. The Infrastructure Team will subscribe to critical supplier communications e.g. AWS 7. A Security Operations Centre (SOC) shall be established to review threats to the organisation on a daily basis and will alert the Security Team when necessary 8. The SOC shall produce monthly reports on threat intelligence and system monitoring

Incident Management: Preparation

- *ISDLO8 Business Continuity Policy*
- *A.5.24: Information security incident management planning and preparation*
- *A.5.29: Information security during disruption*
- *A.5.30: ICT readiness for business continuity*
- *A.8.14: Redundancy of information processing facilities*

1. Incidents may include:
 - a. Loss of information availability due to IT system failure
 - b. Loss of information availability due to external attack
 - c. Data corruption caused by software malfunction or user error
 - d. A loss of data confidentiality/privacy, which would be considered a personal data breach, may include:
 - i. Access by an unauthorised third party
 - ii. Deliberate or accidental action (or inaction) by a controller/processor
 - iii. Sending personal data to an incorrect recipient
 - iv. Computing devices containing personal data being lost or stolen
 - v. Loss of availability of personal data
2. The Security Team is responsible for defining common Attack Vectors, organising mitigating actions and defining the approach to incident management
3. Preparation for Incident Management should ensure that all staff are aware how to report an incident and that Incident Response staff are suitably competent in dealing with those incidents.
4. Information assets shall have effective logs and monitoring in place to support incident investigations
5. Critical suppliers should have their own Business Continuity plans. Access Intelligence can choose to rely on them, and wait for recovery.
6. Communications tools and practices should be established that support remote collaboration, and remote monitoring of key activities.
7. Teams should avoid 'key-person dependency' as this creates operational challenges when a person is not available to work i.e. teams should identify who will restore the asset if the main person is unavailable. Various strategies can help with this:
 - a. Identify critical knowledge, and skills related to critical business processes.

	<ul style="list-style-type: none">b. Elicit critical knowledge, in order to create training materials and share with others.c. Identify critical skills, and identify individuals suitable as back-up. <p>8. Access Intelligence should prepare for ICT resilience by:</p> <ul style="list-style-type: none">a. Infrastructure should have a highly available redundant Internet connection.b. Infrastructure should distribute key systems (such as backend databases) over multiple availability zones.c. All employees will have a portable laptop as their primary device.d. All employees have the ability to work from home.e. Offices may benefit from dual Internet connections and/or UPS backup power <p>9. Access Intelligence products must be recoverable.</p> <p>10. Access Intelligence ISMS shall include documentation for:</p> <ul style="list-style-type: none">a. Business Continuity Planb. Disaster Recovery Planc. Incident Response Plan <p>11. Plans should include:</p> <ul style="list-style-type: none">a. Productsb. Critical systemsc. Loss of critical personneld. Data corruptione. Cyber extortion threatsf. Compromised network performance e.g. outagesg. Breach of privacy regulationh. Ransomware <p>12. The DR Plan must include:</p> <ul style="list-style-type: none">a. Reporting and Escalation Proceduresb. Digital Forensics
--	---

	<ul style="list-style-type: none"> c. Incident Management Lifecycle d. Designated Security Incident Response Team e. Crisis Communications / Public Relations f. Designated Legal subject matter expert g. Designated HR subject matter expert h. Organisation-Wide Communication Plan i. Unique, specific, and applicable data breach notification requirements, including timing of notification (e.g. notification requirements to supervisory authority) <p>13. Plans should be tested detailing the technical steps to be enacted.</p> <p>14. Plans should be available in multiple systems to ensure they are available during any disaster.</p>
<p>Incident Management: Assess</p> <ul style="list-style-type: none"> • <i>A.5.25: Assessment and decision on information security events</i> 	<ol style="list-style-type: none"> 1. All confirmed security incidents must be recorded in the ISMS with a member of the Security Team assigned as Incident Manager 2. The Incident Manager must take immediate steps to gain a full understanding of the incident 3. Once a full understanding has been obtained, the CTO will categorise the incident as: <ul style="list-style-type: none"> a. <i>Critical</i> – Organisation is no longer able to provide some critical services to any users e.g. a product is unavailable for all users. b. <i>Major</i> – Organisation has lost the ability to provide a critical service to a subset of system users e.g. part of a product is unavailable for some users. c. <i>Minor</i> – Minimal effect; the organisation can still provide all critical services to all users but has lost efficiency 4. Any security incident which involves personal data of individuals in the UK/EU must be reported to the Data Protection Officer (DPO) 5. If the incident represents a high risk to individuals, the DPO is to organise notifications for: <ul style="list-style-type: none"> a. Data Controllers (clients) within 24 hours after detection






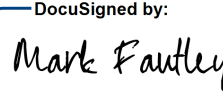
	<p>b. Supervisory Authorities (e.g. ICO) within 72 hours after detection</p>
<p>Incident Management: Response</p> <ul style="list-style-type: none"> ● <i>A.5.26: Response to information security incidents</i> ● <i>A.5.28: Collection of evidence</i> 	<ol style="list-style-type: none"> 1. The Disaster Recovery Plan (DRP) prioritises the recovery of critical systems and infrastructure in the event of a system outage or business distribution. 2. If the incident involved or originated from a cloud service, the Asset Owner takes a leading role to support the Incident Manager. 3. The Incident Manager is responsible for restoring a normal level of security whilst: <ol style="list-style-type: none"> a. Collecting evidence e.g. preserve log files b. Communicating updates internally to the Security Team, and possibly, the DPO and Senior Management c. Reducing weaknesses found to cause of contribute to the incident e.g. <ol style="list-style-type: none"> i. Disabling infected end-points ii. Blocking breached user accounts iii. Reset user passwords iv. Identify relevant backups v. Improving source code vi. Patching systems 4. For security incidents which may lead to legal or disciplinary action, the Security Team must: <ol style="list-style-type: none"> a. Create a chain of custody. This can be a separate file store which only the CTO has access to. All evidence added must be logged. All access granted to the file store must be logged. This is crucial for legal and regulatory purposes. b. Create two hashed images to protect data integrity. <ol style="list-style-type: none"> i. One hash should be generated for the original data to verify its integrity during the investigation. This should be stored in the Chain of Custody. This helps ensure that the data has not been altered or tampered with. ii. Another hash can be generated for a working copy of the data that investigators

	<p>or analysts might use. This ensures the integrity of the working copy and provides a reference point for comparison.</p> <ol style="list-style-type: none"> 5. All clients affected by the incident must: <ol style="list-style-type: none"> a. Be notified within 24 hours b. Receive a report within 1 week of the initial notification 6. The incident report will provide the following information where applicable: <ol style="list-style-type: none"> a. Date and time of incident, date and time of incident discovery and reporting b. Nature of incident; categorisation and description of the data involved c. Description of incident d. Disclosure of any data processors, sub-processors or third parties involved with the breach e. Breakdown of immediate actions and resolutions, including steps to reduce further breaches f. Root cause analysis g. Supervisory Authority notification actions undertaken h. How data subjects have been affected
<p>Incident Management: Review</p> <ul style="list-style-type: none"> • <i>A.5.27: Learning from information security incidents</i> 	<ol style="list-style-type: none"> 1. Incidents show us where our system is weakest. It is important that we use these as learning opportunities. 2. Any incident due to a failure with an asset or system must be reviewed by the Incident Manager and Asset Owner. 3. Any incident due to a failure with a security control must be reviewed by the Incident Manager and Control Owner. 4. Identified improvements should be documented in the ISMS Improvement Board.

Document Version Control

This policy shall be reviewed annually as an absolute minimum, or if required changes are identified to address an identified weakness, a change in business activities which may affect the validity of this document.

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

Version	Change	Author	Approver	Signature
1.0	Original version, to enable Access Intelligence to achieve ISO 27001:2013 accreditation	David Roud DPO 31/10/2018	Mark Fautley CFO 21/01/2019	
2.0	Change of leadership team, outsourced IT Service Provider has changed to new company	Ato Abraham IT Manager 26/11/2019	Mark Fautley CFO 21/01/2020	
3.0	ISO 27001:2013 accreditation was achieved in June 2020. Updated roles and responsibilities and included references to ISDL10, ISDL13, ISDL19, ISDL54, ISDL77, ISDL390	Adam Palmer Information Security Manager 19/01/2021	Mark Fautley CFO 20/01/2021	
4.0	Updated Senior Management structure. Included references to ISDL03, ISDL11, ISDL16, ISDL30, ISDL53, ISDL54, ISDL325	Adam Palmer Information Security Manager 22/11/2021	Mark Fautley CFO 20/01/2022	
5.0	Refreshed objectives, responsibilities and included reference to ISDL15	Adam Palmer Information Security Manager 12/09/2022	Mark Fautley CFO 20/01/2023	
6.0	Updated scope. Combined all 20+ supporting policies into 1 document. Update all security controls to ISO 27001:2022 requirements.	Adam Palmer Information Security Manager 20/11/2023	Mark Fautley CFO 21/2/2024	DocuSigned by:  699D2FDC0288475...