Information Security Policy

Document Classification:	**Public**
Document Ref.	**ISMS-DOC-1**
Version:	**2.0**
Dated:	**10 May 2018**
Document Author:	**Hilmi Sunay**
Document Owner:	**Hilmi Sunay**

Revision History

Version	Date	Revision Author	Summary of Changes
2.0	10 May 2018	Hilmi Sunay	Major review to make the policy in-line with GDPR requirements and updates to make it available to any relevant third parties

Distribution

Name	Title
Hilmi Sunay	Technology and Information Security Director
Tony Heard	Managing Director
Management Team	

Approval

Name	Position	Signature	Date
Tony Heard	Managing Director	N/A	17 May 2018

Contents

1 Introduction

Abintegro is committed to maintaining the highest possible data protection standards and ensuring, at all times, being compliant with ISO/IEC 27001:2013 and other relevant legislation.

Abintegro is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of its clients and other third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO 27001.

This top-level information security policy is a key component of the Abintegro overall information security management framework which outlines Abintegro's approach to information security management and sets the security goals within Abintegro. It should be considered alongside more detailed information security documentation including, supporting system specific policies, code of practice, security guidance, protocols or procedures and statement of applicability.

This policy and other system level policies for information security shall be reviewed at planned intervals, at least annually, or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

2 Objectives, Aim and Scope

2.1 Objectives

The objectives of the Abintegro Information Security Policy is to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2 Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Abintegro by:

- Providing an information security framework for establishing suitable levels of information security for all Abintegro information systems and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2.3 Scope

This policy applies to all information, information systems, networks, applications, locations and users of Abintegro or supplied under contract to it. It will be communicated to all staff and relevant third parties who interact with information held by Abintegro.

3 Responsibilities for Information Security

- Ultimate responsibility for information security rests with the Managing Director of Abintegro, but on a day-to-day basis the Technology and Information Security Director shall be responsible for managing and implementing the policy and related procedures.
- Information and physical security is also a key responsibility of all employees, and this shall be regularly communicated and reinforced through an ongoing security education and training programme.
- Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:
    - The information security policies applicable in their work areas
    - Their personal responsibilities for information security
    - How to access advice on information security matters
- All staff shall comply with information security procedures including the maintenance of data confidentiality, data availability and data integrity. Failure to do so may result in disciplinary action.
- Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.
- Each member of staff shall be responsible for the operational security of the information systems they use.
- Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

4 Legislation

Abintegro is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Abintegro, who may be held personally accountable for any breaches of information security for which they may be held responsible. Abintegro shall comply, for example regarding data protection, with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The General Data Protection Regulation (Regulation (EU) 2016/679)
- and any equivalent or replacement legislation in the UK

5 Policy Framework

5.1 Management of Information Security

- At board level, responsibility for Information Security shall reside with the Technology and Information Security Director.
- Abintegro's Technology and Information Security Director shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.2 Internal Organisation and Segregation of Duties

- Allocation of information security responsibilities shall be done in accordance with the information security policies. Responsibilities for the protection of individual assets and for carrying out specific information security processes shall be identified.
- Care shall be taken that no single person can access, modify or use assets without authorisation or detection. The initiation of an event shall be separated from its authorisation. The possibility of collusion shall be considered in designing the controls.
- Whenever segregation is not possible due to the size of the organisation, other controls such as monitoring of activities, audit trails and management supervision shall be considered.
- Appropriate contacts with relevant authorities shall be maintained.

5.3 Contracts of Employment

- Employee security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- All new employees shall undergo pre-employment screening for criminal background, employment and education verification, and reference checks.
- Information security expectations of staff shall be included within appropriate job definitions.
- Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
- Changes of responsibility or employment shall be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

5.4 Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education, training and regular updates in organisational policies and procedures, as relevant for their job function.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

5.5 Security Control of Assets

- Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
- Each asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset and the classification shall be identified.
- Employees and external party users using or having access to the organisation's assets shall be made aware of the information security requirements of the organisation's assets associated with information and information processing facilities and resources. They shall be responsible for their use of any information processing resources and of any such use carried out under their responsibility.
- The termination process shall be formalised to include the return of all previously issued physical and electronic assets owned by or entrusted to the organisation. In cases where an employee or external party user purchases the organisation's equipment or uses their own personal equipment, procedures shall be followed to ensure that all relevant information is transferred to the organisation and securely erased from the equipment.

5.6 Classification of Sensitive Information

- Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
- An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.
- Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.

Information Classification Definitions

The following table provides a summary of the information classification levels that have been adopted by Abintegro and which underpin the principles of information security

defined in this policy. These classification levels explicitly incorporate the General Data Protection Regulation's (GDPR) definitions of Personal Data and Special Categories.

Confidential	"Confidential" information has significant value for Abintegro, and unauthorised disclosure or dissemination could result in severe financial or reputational damage to Abintegro. Data defined by the GDPR as Personal Data falls into this category. Only those who explicitly need access must be granted it and aligned with the "need to know" and "least privilege" principles. "Confidential" information must always be protected with strong access controls in align with information security policies.
Internal	"Internal" information is relatively private in nature, either to an individual or to the organisation and, whilst its disclosure or loss is unlikely to result in significant consequences, it would be undesirable. "Internal" information can be disclosed or disseminated by its owner to appropriate members of Abintegro, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.
Public (or unclassified)	"Public" information can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

5.7 Media Handling

- Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.
- Media shall be disposed of securely when no longer required, using formal procedures. Formal procedures for the secure disposal of media shall be established to minimise the risk of confidential information leakage to unauthorised persons. The procedures for secure disposal of media containing confidential information shall be proportional to the sensitivity of that information.
- Media containing information shall be protected against unauthorised access, misuse or corruption during transportation. Encryption shall be used across all digital media.
- Removable media use shall be restricted on end-points.

5.8 Access Controls

- An access control policy shall be established, documented and reviewed based on business and information security requirement established in this document.
- Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

5.9 User Access Controls

- Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.
- A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
- Formal user access provisioning process shall be in place for all Abintegro information systems and services. This process shall apply to new starters, leavers and those moving roles. Authorisation for access to key systems shall be governed by the Technology and Information Security Director.
- Level of access granted shall be verified and be appropriate based on business purposes and other security controls.
- The allocation and use of privileged ("super-user") access rights shall be restricted and controlled.
- Unique user IDs shall be used in order to link actions to a specific individual.
- All vendor-supplied default accounts shall be removed or disabled.
- A central record of access rights granted shall be maintained.
- Authorisations for privileged access rights shall be reviewed at least quarterly.

5.10 Computer Access Control

- Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.11 Application Access Control

- Access to data, system utilities and source code libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. software developers, system or database administrators.
- Access to source codes shall be managed by the Technology and Information Security Director and Head of Software Development.
- Software developers shall be authenticated with their unique user identifiers before making changes to source-controlled code.
- Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

- Managed secure encrypted password storage system shall be in place with unique identification per employee, password strength policies, password generator (with quality standards imposed) and forced regular password changes.

5.12 Equipment Security

- In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.
- Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.
- Users shall ensure that unattended equipment has appropriate protection.
- Key systems processing and storing client data shall be hosted in ISO 27001 certified data centres.

5.13 Computer and Network Procedures

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Technology and Information Security Director.

5.14 Cryptography

- A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
- Based on a risk assessment, the required level of protection shall be identified taking into account the type, strength and quality of the encryption algorithm required.
- A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle. Policy shall include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.
- Cryptographic algorithms, key lengths and usage practices shall be selected according to best practice. Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.
- All cryptographic keys shall be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys shall be physically protected.

5.15 Information Risk Assessment

- Identification and quantification of information security risks are required in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.
- Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks.
- The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of Abintegro's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.16 Information security events and weaknesses

- All information security events and suspected weaknesses are to be reported to the Technology and Information Security Director. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.17 Protection from Malicious Software

- The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy.
- Restrictions shall be applied to block users installing software on the organisation's property.
- Users shall not install software on the organisation's property without permission from the Technology and Information Security Director. Users breaching this requirement may be subject to disciplinary action.

5.18 Backup

- Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
- The backup policy shall define the retention and protection requirements.
- Adequate backup facilities shall be provided to ensure that all essential information and software can be recovered following a disaster or media failure.
- Backup media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary; this shall be combined with a test of the restoration procedures and checked against the restoration time required.
- In situations where confidentiality is of importance, backups shall be protected by means of encryption.

5.19 Logging and Monitoring System Access and Use

- Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
- An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.
- Controls shall aim to protect against unauthorised changes to log information and operational problems with the logging facility.
- System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
- The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source. External and internal requirements for time representation, synchronisation and accuracy shall be documented. Such requirements can be legal, regulatory, contractual requirements, standards compliance or requirements for internal monitoring. A standard reference time for use within the organisation shall be defined.
- Abintegro reserves the right monitor activity where it suspects that there has been a breach of policy.

5.20 Control of Operational Software

- Procedures shall be implemented to control the installation of software on operational systems.
- Systems shall be setup with restricted user accounts by default where installation of any software shall be blocked.
- The updating of the operational software, applications and program libraries shall only be performed by members of technology team upon appropriate management authorisation.
- Where possible, a central configuration management system shall be used to keep control of all implemented software as well as the system documentation.
- Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organisation shall consider the risks of relying on unsupported software.

5.21 Technical Vulnerability Management

- Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
- Internal and external facing infrastructure shall be tested against vulnerabilities at least monthly.

- Web applications shall undergo penetration testing by an independent authority at least annually.
- Any critical or high risk issues shall be remediated as high priority. Where a remediation not possible, associated risks shall be discussed and documented.
- Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

5.22 Network Security Management

- Controls shall be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access.
- Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
- The ability of the network service provider to manage agreed services in a secure way shall be determined and regularly monitored, and the right to audit shall be agreed.
- Groups of information services, users and information systems shall be segregated on networks.

5.23 Information Transfer

- Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
- Agreements shall address the secure transfer of business information between the organisation and external parties.
- Information involved in electronic messaging shall be appropriately protected.
- Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.
- Confidentiality or non-disclosure agreements shall address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to external parties or employees of the organisation. Elements shall be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information.

5.24 Acquisition of Information Systems

- The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the Technology and Information Security Director before they commence operation.

5.25 Security in Development and Support Processes

- Rules for the development of software and systems shall be established and applied to developments within the organisation.
- Secure programming techniques shall be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices.
- Secure coding standards shall be considered and where relevant mandated for use, e.g. OWASP Top 10 requirements. Developers shall be trained in their use and testing and code review shall verify their use.
- If development is outsourced, the organisation shall obtain assurance that the external party complies with these rules for secure development.
- Formal change control procedures shall be documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts.
- When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.
- As far as possible and practicable, vendor-supplied software packages shall be used without modification.
- Secure information system engineering procedures based on security engineering principles shall be established, documented and applied to in-house information system engineering activities. Security shall be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology shall be analysed for security risks and the design shall be reviewed against known attack patterns.
- Organisation shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
- The organisation shall supervise and monitor the activity of outsourced system development.
- Testing of security functionality shall be carried out during development.
- System acceptance testing shall include testing of information security requirements and adherence to secure system development practices. The testing shall also be conducted on received components and integrated systems. Organisation can leverage automated tools, such as code analysis tools or vulnerability scanners, and shall verify the remediation of security-related defects.
- The use of operational data containing personally identifiable information or any other confidential information for testing purposes shall be avoided at all times.

5.26 Supplier Relationships

- Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.
- The organisation shall identify and mandate information security controls to specifically address supplier access to the organisation's information in a policy.
- All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.
- Supplier agreements shall be established and documented to ensure that there is no misunderstanding between the organisation and the supplier regarding both parties' obligations to fulfil relevant information security requirements.
- Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
- Organisation shall regularly monitor, review and audit supplier service delivery.
- Monitoring and review of supplier services shall ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.
- Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

5.27 Information Security Incident Management

- Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
- Information security events shall be reported through appropriate management channels as quickly as possible.
- All employees and contractors shall be made aware of their responsibility to report information security events as quickly as possible. They shall also be aware of the procedure for reporting information security events and the point of contact to which the events shall be reported.
- Employees and contractors using the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
- Handling information security incidents shall be detailed in a separate information security incident management policy and shared across the organisation.

5.28 Business Continuity and Disaster Recovery Plans

- The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.
- The organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

5.29 Compliance

- All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.
- The specific controls and individual responsibilities to meet these requirements shall also be defined and documented.
- Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
- A form of pseudonymisation shall be applied to personal information stored in the databases aligned with GDPR requirements.

5.30 Intellectual Property Rights

- The organisation shall ensure that all information products are properly licensed and approved by the Technology and Information Security Director.

5.31 Reporting

- The Technology and Information Security Director shall keep the Managing Director informed of the information security status of the organisation by means of regular reports and presentations.