AIMS

Information Security Policy

Author: Security Compliance
Date: 02/09/2022
Doc Version: 1.2a

Advanced Computer Software Group Ltd.

www.oneadvanced.com

Copyright © Advanced Computer Software Group Ltd 2022

This document contains confidential and / or proprietary information. The content must not be disclosed to third parties without the prior written approval of Advanced Computer Software Group Limited or one of its subsidiaries as appropriate (each referred to as “Advanced”). External recipients may only use the information contained in this document for the purposes of evaluation of the information and entering into discussions with Advanced and for no other purpose.

Whilst Advanced endeavours to ensure that the information in this document is correct and has been prepared in good faith, the information is subject to change and no representation or warranty is given as to the accuracy or completeness of the information. Advanced does not accept any responsibility or liability for errors or omissions or any liability arising out of its use by external recipients or other third parties.

No information set out or referred to in this document shall form the basis of any contract with an external recipient. Any external recipient requiring the provision of software and/or services shall be required to enter into an agreement with Advanced detailing the terms applicable to the supply of such software and/or services and acknowledging that it has not relied on or been induced to enter into such an agreement by any representation or warranty, save as expressly set out in such agreement.

The software (if any) described in this document is supplied under licence and may be used or copied only in accordance with the terms of such a licence. Issue of this document does not entitle an external recipient to access or use the software described or to be granted such a licence.

The development of Advanced software is continuous and the published information may not reflect the current status. Any particular release of the software may not contain all of the facilities described in this document and / or may contain facilities not described in this document.

Advanced Computer Software Group Limited is a company registered in England and Wales with registration number 05965280 whose registered office is at The Mailbox, 101 Wharfside Street, Birmingham, B1 1RF.

A full list of its trading subsidiaries is available at www.oneadvanced.com/legal-privacy

Version History

Date	Version	Issued By	Changes
03/05/2020	1.0	Security Compliance	Initial – Rewrite & restructure of ISMS Manual into Information Security & Data Protection Policy in-line with new Integrated Management System (AIMS)
05/05/2020	1.1	Security Compliance	Inclusion of AIMS document references, and simplification of document control section
13/05/2020	1.2	Security Compliance	Extraction of Data Protection into separate Policy
29/10/2021	1.2	Security Compliance	Reviewed with no change
02/09/2022	1.2a	Security Compliance	Reviewed, amended head office address

Effective and Expiry

Document Effective Date	Document Expiry Date
15/06/2020	Effective date of superseding policy

Document Publication

Filename	Location of Current Version	Minimum Retention
AIMS – Information Security Policy	Advanced Hub – Security Policies	Default

References

Number	Document	Location
1	AIMS Policy and Framework	Advanced Hub – Security & Compliance - AIMS
2	AIMS Risk Management Policy	Advanced Hub - Security & Compliance - Policies
3	<not used>	
4	AIMS Information Classification and Handling Standard	Advanced Hub – Security & Compliance - AIMS - Standards
5	AIMS Staff Security Manual	as [2]
6	AIMS Commissioning and Decommissioning Policy	as [2]
7	AIMS Personnel Lifecycle Management Policy	as [2]
8	AIMS Account and Password Management Standard	as [4]
9	AIMS Change Management Policy	as [2]
10	AIMS Monitoring and Logging Standard	as [4]
11	AIMS Encryption Key Management Standard	as [4]
12	AIMS Backup and Restore Standard	as [4]
13	AIMS Data Retention Standard	as [4]
14	AIMS Vulnerability Management Standard	as [4]
15	AIMS Software Development Standard	Advanced Hub – Security & Compliance - Secure Design
16	<not used>	not used
17	AIMS Supplier Management Policy	as [2]
18	AIMS Information Security Incident Management Process	Advanced Hub – Security & Compliance - AIMS - Processes
19	AIMS Business Continuity Management Policy	as [2]

Contents

1 Purpose & Scope

1.1 Purpose

Advanced Computer Software Group is committed to being a world class provider of software and technology solutions, via its specialist sector knowledge, that deliver quantifiable business benefit for our customers.

Through this statement Senior Management affirm their commitment to implement the associated Information Security Management System (ISMS) and the associated Privacy Information Management System (PIMS) in accordance with the applicable requirements of the International Standards ISO 27001 and ISO 27701.

The ISMS and PIMS seek to ensure the legal, proportionate and secure processing of information, the protection of this processing from both internal and external threats, with the objective of preventing or minimising the impact on internal and external stakeholders.

1.2 Scope

As part of the Advanced Integrated Management System (AIMS) this policy is applicable to the divisions, operational sectors, personnel and locations identified as being within the scope of the AIMS Policy and Framework [1].

2 Policy Management

2.1 Organisation of Information Security

Organisational roles and responsibilities for the ongoing management and maintenance of the ISMS and PIMS, along with the operational structure, are detailed in the AIMS Policy and Framework [1].

2.2 Policy Enforcement, Audit and Review

In accordance with the AIMS Policy and Framework [1].

- Adherence to Advanced Policy is mandatory unless approved as part of policy exception management.
- Exceptions and evidence of adherence to, or breaches of, policy are formally managed, recorded, reported and reviewed.
- Reviews of this policy are formally undertaken and recorded.

3 Information Security Policy

3.1 Management of Information Security Risks

In accordance with the AIMS Policy & Framework [1] and AIMS Risk Management Policy [2]:

- All operational areas must identify, manage, record and report Information Security and Data Protection risks in relation to their scope of operation or responsibility.
- Risk management must include risks relating to breaches in the availability, integrity or confidentiality of information, and risks associated with the failure to process information in accordance with relevant legal, regulatory or contractual requirements.
- Risks must include the assessment of impacts to all affected stakeholders.

3.2 Information and Data Governance

Information must only be processed for legitimate/legal purposes in accordance with relevant legal and regulatory requirements.

Information must only be processed with the authority of the data owner (data controller or data subject for personal data).

Information must only be processed for the purposes for which it was obtained/created

Information must not be processed for longer that is necessary and/or for which authority permits

Information must not be shared without authorisation and/or approval from the data owner (data controller or data subject for personal data)

All stakeholders must be made aware of the purposes of processing, have visibility of risks associated with the processing, and information relating to controls implemented to mitigate those processing risks.

3.3 Information and Data Integrity

Information accuracy and completeness must be maintained in accordance with any relevant legal or regulatory requirements.

In accordance with the AIMS Risk Management Policy [2]:

- Risks to all stakeholders associated with the inaccuracy, corruption or lack of completeness of must be identified and mitigated.

3.4 Asset Management Security

All information assets, and systems used to process information assets, must be recorded in a suitable inventory and have a nominated asset owner.

The asset owner is accountable for ensuring that Information Security risks are assessed and managed, and that all assets are appropriately used and secured. Risks related to the protection of information on mobile assets must be identified and managed.

All Information Assets must be classified and labelled, and handled in accordance with this classification in accordance with AIMS Information Classification and Handling Standard [4].

Acceptable use of assets must be formally documented in the AIMS Staff Security Manual [5] and communicated to all users.

User registration and induction processes must include awareness and education on information handling and the acceptable use of assets.

All assets must be returned when no longer required, or upon employment termination.

Assets must only be used for legitimate purposes, and using approved methods and processes.

Use of removable media is prohibited for the transferring and storing of confidential, client and personal information without encryption and permission of the data owner.

Information assets must only be used in accordance with the AIMS Data Governance Policy [section 3.2] and AIMS Staff Security Manual [5].

All information and system assets must be disposed of in accordance with AIMS Commissioning and Decommissioning Policy [6].

All information assets, or systems containing information, must be purged of data, or otherwise render data irretrievable, prior to disposal or reuse.

3.5 Information Classification and Labelling

All information must be classified, labelled and handled to mitigate identified risks in the processing of the data, and to comply with mandated legal, regulatory or contracted standards - as per the AIMS Information Classification and Handling Standard [4].

3.6 Human Resources Security

In accordance with the AIMS Personnel Lifecycle Management Policy [7]:

All employees and contractors must be made aware of their Information Security and Data Protection responsibilities prior to, during, and post-employment.

- Standard Terms and Conditions are written into the contract.
- Awareness of responsibilities must be renewed and recorded in accordance with stakeholder mandated requirements. Awareness training must be proportionate to the level of access to, and classification of data being processed.
- All personnel must be suitable for their roles, must be trustworthy, and must have successfully completed required background and employment checks necessary for the processing of information prior to being given access to relevant information.
- All personnel must have, and continue to have, successfully completed any security clearances or vetting requirements mandated by Advanced or other stakeholders.
- Personnel must not undertake multiple roles, or have multiple responsibilities, that are identified as having conflicts of interest.

3.7 Mobile Working

Personnel are permitted to work from remote or mobile locations where:

- Their contract or employment permits remote, home or mobile working
- They have been issued with the facilities to work remotely
- All remote or mobile working is compliant with the AIMS Staff Security Manual [5].

3.8 Access Control

Users must only be provided with access to the network and network services that they have been specifically authorized to use. In accordance with the AIMS Account and Password Management Standard [8], access to Information must only be provided:

- For legitimate purposes
- To confirmed roles
- On a Need-to-Know basis
- For the minimum required period
- With the minimum required permissions and rights
- Upon confirmation of identity
- Upon receipt of authorised approval
- For individual use

Access control changes must be made in accordance with the AIMS Change Management Policy [9]. Access must be monitored and logged in accordance with the AIMS Monitoring and Logging Standard [10].

3.9 Cryptography and Encryption Key Management

Use of cryptographic controls to mitigate risks, or for compliance with legal or regulatory requirements must be formally managed, and must include the safe custody of encryption and decryption keys.

Risks relating to the loss, corruption or breach of encryption key integrity must be assessed and actions identified as part of Incident management and Business Continuity Management processes.

Use of encryption technology must conform to any geographical, national, government or regulatory mandates and in accordance with AIMS Encryption Key Management Standard [11].

3.10 Physical and Environmental Security

Physical access to Information Systems, and Information Assets must be controlled to ensure access is limited to authorised personnel.

Physical controls must proportionate to the classification and criticality of the assets, in accordance with the AIMS Information Classification and Handling Standard [4].

All Information Assets or systems deemed critical or sensitive by stakeholders, must be located in secure areas, with a defined security perimeter, and must be protected with appropriate security barriers and entry/exit controls.

Controls must be implemented to ensure or minimise the risk of equipment theft or unauthorised removal.

Clear desk and clear screen practices, including the use of screen security filters and window filters, must be promoted and implemented as required.

Risks to the operation and/or security of Information assets and systems from environmental and natural sources must be identified and managed.

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Equipment is sited, maintained and protected to reduce the risks from:

- environmental threats and hazards
- power failures and other disruptions
- interception, interference or damage
- opportunities for unauthorized access.

3.11 Change Management

All changes to operational processes, procedures, and systems must be documented and follow a formal change management process, in accordance with the AIMS Change Management Policy [9].

All changes must have a recorded approval from an authorised person.

All changes must be tested prior to implementation (where possible), and must have agreed documented back-out/recovery plans in cases of change failure.

3.12 Capacity and Availability Management

System resources must be monitored and reported to ensure ongoing availability of systems, and ongoing ability to meet operational service levels.

Indicators or trends which identify potential lack of resources must be escalated and associated availability risks managed.

IT systems and services must be monitored to ensure their ongoing availability.

Service delivery incidents, or incidents affecting the operation or availability of services or systems must be documented and managed to maintain expected service levels.

Service delivery incidents must be analysed to identify underlying problems.

All operational systems must be backed-up at a frequency required to restore operations to an acceptable and stable state, and in accordance with AIMS Backup and Restore Standard [12].

Backups must be retained for as long as is deemed necessary by the business to enable restores, and to allow for incident investigation.

Backups must not be retained for longer that the maximum period defined in the AIMS Data Retention Standard [13].

3.13 Malware Protection

Security controls must be implemented on all perimeter systems to prevent and detect malicious code. All IT systems and end–user devices must implement malware and illegal code prevention and detection controls in accordance with AIMS – Security Configuration Standard.

All solution designs, and changes, must be risk assessed to identify and manage the risks associated with the introduction of malicious or illegal code in accordance with:

- AIMS – Security Configuration Policy
- AIMS – Vulnerability Management Policy
- AIMS – Solution Commissioning and Decommissioning Policy
- AIMS – Change Management Policy

User awareness training must include guidance on the prevention of malicious code infection, in accordance with the AIMS Personnel Lifecycle Management [7].

Privileged accounts must not be used for standard user activities (including but not limited to reading e-mail, web browsing) in accordance with the AIMS Staff Security Manual [5].

3.14 Communications Security – Network Controls

Networks must be managed and controlled to protect information in systems and applications.

Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced.

Groups of information services, users and information systems are segregated on networks. Agreements address the secure transfer of business information between the organization and external parties.

Information involved in electronic messaging is appropriately protected.

3.15 Vulnerability Management and Secure Configuration

Vulnerabilities within systems, software, processes and procedures must be identified and rectified in a timely manner, as determined by the criticality of the vulnerability, and in accordance with the AIMS Vulnerability Management Standard [14].

Vulnerabilities which cannot be managed in accordance with vulnerability management standards must be escalated as risks for formal risk treatment.

Regular checks on vulnerabilities must be undertaken to confirm adherence to vulnerability management standards and relevant legal, regulatory or contractual requirements.

Secure configuration standards for all systems must be documented and implemented.

Regular checks on secure configurations must be undertaken and reported to confirm adherence to secure configuration standards.

3.16 Logging and Monitoring

Use of assets, and the operational of security controls, must be monitored and reported to ensure effective operation and compliance with this policy, and in accordance with the AIMS Monitoring and Logging Standard [10].

Audit trails and logs must be created to confirm user activity, and to provide evidence of security events or compliance with security control operation.

Audit and activity logs (including CCTV) must utilise consistent and accurate timestamps.

Audit and activity logs must be protected from accidental or deliberate tampering.

Audit and activity logs must be kept for a period necessary to evidence activity, or to investigate security events or incidents.

Monitoring and logging, including the protection and retention of logs, must comply with all relevant legal and regulatory requirements.

3.17 Information Systems Acquisition, Development and Maintenance

The Standard Project Management template includes a section on information governance, Information Security risks are assessed as part of project and programme management, and control objectives formally included as project or programme deliverables. Operating procedures are documented and made available to all staff if required.

Information Security risks and associated control implementation and operation must be included in the overall business cases for organisational and/or operational changes or projects.

All software development must be undertaken in accordance with the AIMS Software Development Standard [15].

Development and pre-production testing environments must be segregated from live/operational environments where possible. Live, un-redacted data, or data that has not been anonymised, must not be used for development or pre-production testing.

All systems and services must be tested and confirmed as meeting security requirements prior to deployment to live environments.

All systems must be commissioned and/or decommissioned in accordance with the AIMS Commissioning and Decommissioning Policy [6].

All systems and infrastructures used for the processing of Information must be maintained in accordance with;

- Asset licence agreements
- Asset usage or acceptable use agreements
- Legal/regulatory or contractual timescales/schedules
- Asset Criticality

All maintenance activities must be scheduled and logged

No assets or systems, including software, must be used that are out of support from their manufacturer, or that is used outside of licencing and usage agreements, or manufacturer or supplier instructions.

Changes to operational processes, procedures, or systems must only be undertaken in accordance with AIMS Change Management Policy [9].

3.18 Supplier Management

All suppliers shall be assessed and confirmed as meeting all relevant legal, regulatory and operational requirements, in accordance with the AIMS Supplier Management Policy [17].

Contracts with suppliers and partners must include mandatory legal or regulatory security requirements, and adherence to Advanced security policies and standards (or greater).

Contracts must include the provision of, and measures to be used as evidence of compliance with, security requirements and notification mechanisms for Security Incident management.

All contracts must include relevant confidentiality clauses, non-disclosure agreements, and Information/Data Sharing Agreements.

Suppliers' service provision shall be reviewed against defined and agreed service levels.

3.19 Information Security Incident Management

All Information Security incidents must be reported, recorded, and managed in accordance with the AIMS Information Security Incident Management Process [18].

Security Incident management must follow a documented and approved process, and must include approved Incident Response Plans.

Security Incident Management must include actions to identify, contain, correct and investigate incidents, as well as all communications that must be undertaken.

Incident response plans must include any mandatory timescales for actions as required by legal, regulatory or contractual requirements.

Final Incident reports must be generated that provide sufficient information to review the effectiveness of controls, and review relevant Information Security risks.

3.20 Information Security Aspects of Business Continuity Management

Business Continuity Management must include the ongoing provision of Information and services/system required to access Information.

Business Continuity Management must include the continuity of, or equivalent operation of security controls within Business Continuity Plans in accordance with the AIMS Business Continuity Management Policy [19].

Information Security risks associated with the implementation or operation of Business Continuity Plans must be identified, recorded and managed as per Business-as-Usual operations.