INFORMATION SECURITY POLICY

MAY 2025

Certified B Corporation
This company meets the highest standards of social and environmental impact

Table of Contents

Document version:	**v5**
Last review date:	**May 2025**
Author:	**IT and Cyber Security**
Owner:	**Adrian Hollister, Head of IT and Cyber Security**
Approver:	**Board**
Who does this policy apply to:	**All ASI People**

INFORMATION SECURITY POLICY

DEFINITIONS

Term	Definition
ASI's network	Refers to any connection for wired or wireless access to ASI resources, including any downstream servers (for example, email served through Office365, or digital learning environment when hosted by a third-party company).
ASI information	Is a collective term that covers corporate, and project created or manipulated information; this is the intellectual property of the organisation, and it needs to be protected against unauthorised disclosure, manipulation, or destruction. It also includes the standard definition of Personally Identifiable Information (PII) as described in the Data Protection Act.
ASI people	Refers to any person who is currently engaged in any form of employment or partnership with ASI, it also covers anyone who connects to ASI's network.
Computers and similar devices	Is a collective term to describe a hardware component, irrespective of operating system that is used for transmitting, storing, accessing, or manipulating ASI data, including (but not limited to) servers, laptops and desktop computers, mobile/smart phones, printers, network switches and wireless access points.
Corporate (or project issued) devices	This is a device that has been issued to a worker to undertake their corporate or project duties on, it is not owned by the individual themselves.
Data	Means information which: a) is being processed by means of a device operating automatically in response to instructions given for that purpose. b) is recorded with the intention that is should be processed by means of such a device. c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.
Device user	Is the worker that is using the device in question, irrespective of whether this is a personal or corporate device.
Information	Is data with meaning, for example, a spreadsheet that contains just figures is data, whereas if context is given to what the figures relate to it is considered information.
Information asset	Is a body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited effectively. Information assets have recognisable and manageable value, risk, content, and lifecycles.
IT & Cyber Security team	This term covers any party engaged in the creation, delivery, or support of Services, Systems and Servers.
May	This term is used to state an **optional** requirement of this policy.
Mobile working	Is working from a non-fixed location, for example, this may refer to working while travelling between home and a fixed work location.
Personal device	Is a computer or similar device (as above) that is personally owned but is being used to interact with corporate or project related information.
Remote working	Is working from a fixed location, for example, working from home or working from temporary accommodation.
Services, systems and servers	Are generally referred to as an interchangeable term. A service may be a discrete entity (for example, a hosted eLearning platform), or it may be comprised of a few systems (as there are many elements that interconnect to provide the overall service). A server may just be providing a single function, such as file storage, or it may form part of a system.
Shall	This term is used to state a **mandatory** requirement of this policy.
Should	This term is used to state a **recommended** requirement of this policy.
Subcontractor	Is a worker that has been engaged to work on a project, but they are contracted to their parent company during their engagement.

INTRODUCTION

The Information Security Policy is a comprehensive set of requirements and guidelines that define how Adam Smith International protects its systems and services as well as information assets from threats and risks.

SCOPE AND APPLICABILITY

This policy applies to Adam Smith International Ltd. and all its operating companies (collectively, **"ASI"**) and applies to all employees and associates of the Company (collectively, **"ASI people"**).

ROLES AND RESPONSIBILITIES

The following groups and persons have the following responsibilities:

The Boards of Adam Smith International Ltd and those of its parent company and ultimate parent company are fully committed to supporting and implementing the Information Security Policy. Each of the Boards recognises the importance of information security for Adam Smith International's business success and reputation and requires everyone to comply with the policy and report any incidents or issues to the IT Security Team. By endorsing this policy, the Boards demonstrate leadership and accountability in protecting Adam Smith International from cyber threats and risks. The Board of Adam Smith International Ltd is supported by the Executive Team to delivery and maintain the requirements of this policy.

ASI People are responsible for reading, understanding and complying with this Policy and for reporting any breaches or suspected breaches of ASI's policies.

The Executive Team ("**ET**") of Adam Smith International Ltd and, where any such ET has been established, the ET for each ASI company is responsible for ensuring that this Policy is maintained and communicated to ASI People working for or engaged by that company.

The IT & Cyber Security team is responsible for maintaining this Policy and ensuring that it remains up to date and relevant to all ASI People.

The IT & Cyber Security team also have a responsibility under this Policy to maintain the security of ASI's systems enabling ASI People to perform their duties in a safe and secure environment.

The P&T Team will arrange for delivery of training on information security and cyber security.

It is also the responsibility of the IT & Cyber Security team to work with ASI People to ensure that all reported incidents or any breaches or alleged breaches of this Policy are appropriately investigated and managed.

It is the responsibility of all ASI People, irrespective of role, type, or grade ensure that their behaviour and activities are in accordance with the requirements of this policy.

LEGAL OBLIGATIONS

There is a lot of legislation that applies to all people, following the policies and procedures that ASI publish will align with industry best practice and supplement the foundation legislations presented below.

Applicable legislation

ASI people **shall** comply with all applicable legislation wherever they reside including, but not limited to:

- Data Protection Act (2018)
- General Data Protection Regulation (2018)
- Health and Safety at Work Act (1974)
- Working Time Regulations (1998)
- Display Screen Equipment Regulations (1992) (amended by the Health and Safety (Miscellaneous Amendments) Regulation 2002)
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) (1995)
- Employment Act (2002)
- All analogous legislation relating to the subject matter of the above legislation in each of the countries in which ASI operates.

DIGITAL SERVICES

Principles and rules

Adam Smith International **shall** adopt a range of digital services to assist in the creation, storage, and transmission of information to be used throughout its projects and extend across different geographies to provide a consistent approach to manage its information assets. These services will be:

- **Designed** – in line with industry best practice, (including, but not limited to, the Principles for Digital Development)
- **Documented** – covering:
    - the system architecture
    - the classification and expected retention of information being handled
    - roles and default permission sets for users, if appropriate
    - the maintenance schedule for the service
    - detail any mission critical periods that the service needs to be available for
    - the expected lifecycle of the service and
    - periodic review or update after any significant change to the service
- **Resilient** – the service **should not** be reliant on single elements that may fail resulting in an outage. Disaster Recovery ("DR") and backups shall be defined and implemented to prevent potential data loss later. Change management shall be implemented, if required, to control the service stability.
- **Secure** – the information that the service provides, stores, or transmits **shall** be protected to preserve the availability, confidentiality, and integrity of the underlying data.
- **Auditable** – appropriate mechanisms for monitoring and reviewing the services performance, efficiency and risks assessments shall be undertaken periodically, and any recommended improvements implemented.

The use of digital services **shall** align with the strategic direction of ASI.

ACCOUNT MANAGEMENT

Principles and rules

1. A secure and unique identifier (account) for each worker will be created and issued exclusively for that worker. This account **shall not** be used by anyone other than the intended recipient. This identifier (account credentials) is comprised of:
    - An email address (to log into an account with for example, john.smith@adamsmithinternational.com) and a
    - Password (that conforms to the security requirements as detailed in the IT Password Policy)
2. This account **shall** be used to access, interact, and undertake duties to access ASI systems and to store information in ASI approved systems, such as, but not limited to, Microsoft SharePoint Online, Teams, and Outlook.
3. The account credentials will be presented to the workers' line manager and one of the first activities undertaken should be for the worker to change their password to something they set themselves.
4. This account password **shall not** be divulged to anyone, including IT staff, for any reason.
5. To protect ASI services and information, the combination of your email address and password **shall not** be used to access any other online resource (e.g., an Internet shopping site).
6. **ASI People shall** use Multi-Factor Authentication (MFA) to further protect the materials they have access to.
7. **ASI People shall** remember their password and notify IT staff if there is any suspicion that it may have been compromised when a temporary password will be issued, for the worker to change.
8. Where appropriate access to systems **shall** be automatically managed, either indirectly using groups or role-based access data controls derived from an authorised source of data (such as the human resources system). Where access is administered manually, changes (especially revocation of permissions) **shall** be performed as soon as possible following notification; it is expected that wherever possible manual processes should be minimised or replaced where applicable.
9. The use of Microsoft Office365 automated tools and security services shall be used to protect **ASI People's** accounts, this may include the temporary disablement of accounts if rules are created on the mailbox, or the signing in from multiple countries in a short space of time.
10. The misuse of ASI services or information can have a detrimental effect on other users and potentially ASI's public profile and that of its sponsors or donors. As a result of this:
    - ASI maintains the right to monitor user accounts in the pursuit of an appropriately authorised investigation.

- We are obliged to monitor and fulfil our responsibilities regarding EU, UK, and in-country laws. This includes, but is not limited to, Police investigations, Data Protection and GDPR.
- Monitoring of accounts shall be automatically conducted through Microsoft's audit capabilities; it provides a route to diagnose problems that are struggling to access services.
- If additional monitoring is required, over the out of the box services, this can only be authorised in agreement of two of the following: Director of IT and Cyber Security, Director of Legal, Ethics and Compliance and/or Director of People and Talent.
- To aid in the protection of accounts, monitoring of the Dark Web is performed for domains that are registered in our Microsoft environment. If account credentials are discovered, it allows the IT team to support affected workers.

DEVICE MANAGEMENT

In today's digital society we all use devices in our personal and work lives, appropriate measures **must** be taken to prevent the information that the device holds from being easily accessible to anyone.

To protect ASI systems and information, devices that are used to directly access ASI information **should not** be left unattended if they are logged in and unlocked.

Devices that are used to conduct ASI business, **shall** have the following software installed or present, active, and up to date:

Solution	Description	Corporate or project issued devices		Personal devices	
		Responsible	Accountable	Responsible	Accountable
Anti-malware software	Protection against both viruses and malware	ASI IT & Cyber Security team	ASI IT & Cyber Security team Device user	Device user	Device user
Firewall software	Provides boundary protection to the device itself, examining inbound and outbound communications to prevent unauthorised access	ASI IT & Cyber Security team	ASI IT & Cyber Security team Device user	Device user	Device user
Full disc encryption	Prevents the information stored on a devices' hard drive being freely available when connected to another device without security measures being met	ASI IT & Cyber Security team	ASI IT & Cyber Security team Device user	Device user	Device user
Password protection	When not in use, devices should be protected by a password, PIN, passphrase, or biometrics before access to the held information is provided	ASI IT & Cyber Security team	ASI IT & Cyber Security team Device user	Device user	Device user
Operating systems and applications kept up to date	Vulnerabilities in both the Operating Systems and applications are being continually discovered; the manufacturer of the software periodically patches vulnerabilities to prevent exploitation	ASI IT & Cyber Security team	ASI IT & Cyber Security team Device user	Device user	Device user
Microsoft (Intune) Company Portal / Jamf Pro	Provides a gateway for deployment of configurations to meet compliance needs, deliver software, and to report the device security posture for remediation activities, where required. Additionally, provides a remote wipe mechanism (for corporate devices) if the device is lost or stolen.	ASI IT & Cyber Security team	ASI IT & Cyber Security team Device user	Device user	Device user

Devices issued by ASI and their contents remain the property of ASI. Upon leaving ASI, all corporate or project devices **shall** be returned to your line manager. The device will then be prepared for redeployment by the IT & Cyber Security team. Any personal data on the device **should** be removed, but any ASI data **shall not** be erased as this remains the property of ASI.

Devices **shall** be re-used where possible up until the end of their current working life.

Laptops provided by ASI **shall** be issued with a standard software build, and the person will use a standard (non-administrative) account.

SUBCONTRACTORS

ASI People that are subcontracted also need to be able to attest that their devices meet the minimum-security requirements; this can be performed by either of the following mechanisms:

- Provide a valid Cyber Essentials Plus certificate of assurance for the subcontractors' parent company; or
- Enrol their work devices with ASI's Microsoft Company Portal for automated compliance and assessment services.

REPORTING LOSSES, THEFT, OR VANDALISM

All **ASI People** have a duty to report the loss, suspected loss, vandalism, or suspected unauthorised disclosure of any information asset through the IT & Cyber Security team (it@adamsmithinternational.com), or directly with the Director of IT and Cyber Security, at the earliest opportunity.

Where data loss is likely to have occurred, ASI **shall** formally investigate the impact of the loss and may need to report findings to the ICO and/or relevant authorities as well as the data subjects affected by the loss or breach.

Where serious data loss is likely to have occurred, ASI **may** suspend the worker's account while the breach is being triaged and investigated.

Where devices have been provided to conduct work on and they are damaged while in the possession of a worker, the IT team will evaluate the damage, assess the remediation costs, and will work with the People and Talent and Legal, Ethics, and Compliance teams to consider recovering some or all the costs to repair the device.

EXTERNAL MEDIA

The use of external storage devices, such as (but not limited to) USB drives or external hard drives **shall** be assessed and approved before purchase by the IT team and registered as an information asset, both against the project asset register and centrally within IT. The information on these devices **shall** remain the property of ASI and **shall** be returned to ASI for secure and recorded erasure when no longer required.

MOBILE PHONES

The use of calls, texts, and data usage on mobile phones **shall** be monitored for cost overruns. Excessive use may result in limitations to your service and be recharged as stated in the Corporate Mobile Policy (see Internal References).

Mobile phones issued by ASI **may** be used for limited amounts of personal use. Excessive personal use will result in referral to People and Talent and/or Legal, Ethics, and Compliance, where disciplinary action or reimbursement for costs may be sought.

Repair or replacement of devices will be on a like for like basis.

Excessive and/or deliberate damage to ASI property **may** be referred to People and Talent and/or Legal, Ethics, and Compliance where costs of repair **may** be the responsibility of the user.

UNACCEPTABLE USE OF SERVICES

Principles and rules

To provide acceptable levels of service to all workers, it is important to highlight what is determined as unacceptable behaviour and any breach of these conditions may lead to disciplinary action being taken:

- Any illegal activity or activity that knowingly breaches the security of ASI information or users.
- Creation or transmission, of any offensive, obscene, or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or materials.
- Creation or transmission of material with the intent to cause annoyance, inconvenience, or needless anxiety.
- Creation or transmission of material with the intent to defraud.

- Creation or transmission of defamatory material or any such content that may bring ASI into disrepute.
- Creation or transmission of any material which infringes copyright.
- Any attempt to knowingly gain unauthorised access to facilities or information.
- Any attempt to knowingly undermine the security or integrity of ASI's information and systems, including:
    - Corrupting or destroying other user's data
    - Violating the privacy of other users
    - Attempting to bypass security measures, such as, but not limited to:
        - Password capturing / cracking programs
        - Packet sniffing / analysing programs
        - Port scanning
        - Using false (or spoofed) IP address(es) or domain names
- Providing access to facilities or information to those who are not entitled to access it (including sharing passwords or accounts).
- Downloading pirated media content
- Any irresponsible or reckless handling or unauthorised use and or modification of information.
- Attempt to import, or access data that they are not authorised to use or access.
- Remove, print or copy any data from ASI systems that they are not authorised to remove, print or copy at the end of their employment or engagement or otherwise.
- Exceed the limits of their authorisation or specific business need to interrogate ASI's Systems or data.
- Hold and/or process any information to which the individual and/or Adam Smith International has no legal rights.
- Any intent to bully, harass, intimidate, or otherwise cause alarm or distress to others.
- Sending unsolicited and unauthorised bulk email (spam).
- Using software which is only licensed for limited purposes or otherwise breaches software licensing agreements.
- Using ASI facilities for direct or indirect personal commercial gain.
- Failing to comply with a request from a member of IT & Cyber Security team to desist from any activity which has been deemed by IT to be detrimental to the operation of ASI facilities.
- Knowingly failing to report any breach or suspected breach of information security to IT.
- Failing to comply with a request from a member of IT & Cyber Security team for you to change your password.
- Follow an instruction issued by the IT & Cyber Security department.

DATA AND INFORMATION MANAGEMENT

A risk-based approach will be taken to protect and manage data and information within ASI.

All primary data sources, for example (but not limited to) the human resources or finance systems **shall** have a designated Information Asset Owner identified and documented. That designated Asset Owner will act as local guardians for the information assets.

Any concerns that are raised by the introduction or modification of services, systems, or processes **shall** be added and managed through either the IT risk register or specific project risk registers. Any specific project IT related risks should be escalated to the Director of IT & Cyber Security.

The information created and stored within ASI's information systems **shall** be retained for no longer than the maximum periods (as denoted in Internal References - Information Retention Policy) to meet both legal and business requirements.

Information regarding **ASI People**, suppliers, and others dealing with ASI is to be kept confidential and **shall** be protected and safeguarded from unauthorised access and disclosure.

All ASI information **should** be categorised as either **Public, Internal, Confidential** or **Highly Confidential** in accordance with the Information Classification Policy (see Internal References).

Documents that are identified as **Highly Confidential** and have a restricted audience **should not** rely on the integrity or availability of other documents or data files over which the author may have no control. Key documents **should** be self-contained, holding all the pertinent information in one place.

REGISTERS

All projects **shall** register their major assets (for example, devices, furniture, office equipment etc.) and information assets (for example, databases, paper records etc.) either centrally with IT, or with the project that is funding and/or managing the asset itself.

Damaged digital storage devices that contain **confidential** or **highly confidential** information **shall** undergo a risk assessment to determine whether it should be repaired or destroyed.

- Disposal procedures **shall** be followed, and certificates of destruction retained for audit purposes.

PAPER DOCUMENTS

All **ASI People should** seek to minimise the production and retention of paper-based copies of **confidential** or **highly confidential** documents.

Confidential or **highly confidential** paper documents **shall not** be left on desks overnight, they **shall** be kept securely in lockable cabinets to prevent unauthorised access. Where feasible, a clear desk approach **shall** be maintained.

Documents that are no longer required **shall** be destroyed using an appropriate shredder and subsequently placed into standard (ASI office, client or personal) recycling bags or bins.

Where printing of **confidential** or **highly confidential** information is permitted, for example, disciplinary proceedings or other such documents, secure print functionality **shall** be used (for example, printing to a secure print queue and releasing the job to print with a designated identity card).

EXTERNAL DATA

When working with external partner or government data, additional password management requirements, for example, shorter timescales for password alteration **may** be required as part of any data sharing agreements or contracts.

FILE STORAGE

ASI information **should only** be stored on company approved systems, including Office365 (comprising Teams, SharePoint Online etc.) and ASI IT approved locations.

Any information that is essential to ASI that is created or stored (in a temporary capacity, as it **should not** be held there for the long term) on a device's hard drive **shall** be copied to a suitable company approved file store at the earliest available opportunity. (Please refer to Internal References - Information Retention Policy, queries should be directed to service.desk@adamsmithinternational.com)

Storage of information on any other sources, including personal instances of Office365 products as well as USB and external drives, Google Drive, and DropBox, for example, **shall** need to be approved by the Director of IT and Cyber Security prior to use and the services and **shall** meet GDPR and Data Protection Act guidelines. If approved, these services may also require additional security measures to be in place as well.

Cyber Security prior to use and the services and **shall** meet GDPR and Data Protection Act guidelines. If approved, these services may also require additional security measures to be in place as well.

Any storage media used for archiving purposes **shall** be appropriate to its expected longevity, for example, long term storage on magnetic tapes when the tape readers are discontinued in case of existing failure.

RECORDING OF PREMISES OR INFORMATION

Taking photographs or filming is **not permitted** in any ASI office or working area, except with express permission from the local country lead.

All participants are to be notified in advance whenever telephone conversations or videoconference events, such as company briefings, are to be recorded.

EVIDENCE

Where necessary to gather evidence to support an investigation relating to a worker or an organisation, any such evidence shall be collected and presented to conform to the relevant rules of evidence.

SECURE WORKING

All **ASI People shall** be mindful of their immediate environment when discussing work related matters or materials that could be overheard.
When **ASI People** are connecting to services containing **confidential** or **highly confidential** information from potentially insecure networks (such as public, hotel, conference, or home wireless networks) a secure (VPN) connection **shall** be used to protect information.
Additional security measures, if required, will be reviewed, and authorised by the Director of IT & Cyber Security.

THIRD PARTY ENGAGEMENTS

Third parties are external organisations or individuals other than Adam Smith International's own workers.

All third parties who are given access to ASI's information systems, whether as suppliers, customers, or otherwise, **shall** agree to follow the relevant policies of the organisation, prior to access being provided.

Non-Disclosure Agreements (NDAs) or suitable contractual terms **shall** be used in all situations where the confidentiality, sensitivity, or value of the information being disclosed is categorised as **Confidential** or **Highly Confidential**.

All contracts with third parties to supply, manage, or facilitate services are subject to ASI performing audits (either directly, or via a specialist third party auditor) to ensure compliance with information security requirements. This may be in the form of a planned or no-notice inspections.

All contracts **shall** include appropriate provisions to ensure the continued security of information if a contract is terminated or transferred to another supplier.

Any contracting third parties **shall** disclose fourth (and/or subsequent) parties that they themselves subcontract to for the understanding of complete supply chains that are used.

BACKUP AND RESTORATION

Where services are hosted by third party companies, the backing up and restoration of information **shall** be included as part of the contract for service provision and align with ASI's security policies and retention schedule.

DEVELOPMENT, MAINTENANCE, AND SUPPORT

All **ASI People** responsible for commissioning outsourced development of IT services or systems **shall** use reputable companies that operate in accordance with quality standards, as denoted by ISO27001 accreditation or equivalent.

Any maintenance undertaken on any ASI IT services and systems by a third party, **shall** be agreed, and timetabled with all concerned parties, including the IT & Cyber Security team, prior to the engagement in any work itself.

All **ASI People shall** ensure that all third parties shall use discretion when creating or managing credentials to administer the service, specifically:

- Default usernames can only be used when no alternative is available
- Passwords shall be randomly generated and meet ASI's password complexity requirements
- Default system passwords **shall** never be used in development, test, or production services

REMOTE ACCESS

If remote access is required to ASI services or systems, communications **shall** be secured through approved mechanisms for remote access and/or data transfer.

INFORMATION SECURITY BREACHES

Any information security breaches that occur against a third-party provider of service **shall** be conveyed to ASI through the IT & Cyber Security Team (it@adamsmithinternational.com) or the Director of IT and Cyber Security, within the agreed priority one incident level (as denoted in the Service Level Agreement) or at the earliest available opportunity (whichever is sooner).
Following the remediation of the breach, a report detailing the steps taken and any measures that have been altered or implemented that **should** prevent the breach for occurring again must also be provided to the IT & Cyber Security team, within a maximum period of ten working days.

INTERNAL AND EXTERNAL REFERENCES

INTERNAL REFERENCES

If a suspected or actual data breach occurs, this **shall** be reported **immediately** to ASI's IT & Cyber Security Team (it@adamsmithinternational.com).

Policies that should be read in conjunction with the Information Security Policy include:

- Mobile Computing Policy
- Corporate Mobile Policy
- Information Classification Policy
- Information Retention Policy
- Artificial Intelligence Policy

EXTERNAL REFERENCES

Resources that support this policy

- Principals for Digital Development
- National Cyber Security Centre

ASI

UK

ADAM SMITH INTERNATIONAL
16-18 NEW BRIDGE STREET
LONDON
EC4V 6AG
UNITED KINGDOM

EU

ADAM SMITH EUROPE B.V.
KEIZERSGRACHT 62,
1015 CS AMSTERDAM,
NETHERLANDS

NORTH AMERICA

ADAM SMITH US LLC
1724 20TH ST NW,
WASHINGTON DC 20009
UNITED STATES OF AMERICA

AFRICA

ADAM SMITH INTERNATIONAL
2ND FLOOR, 48 WESTLANDS ROAD
PO BOX 26721-00100
NAIROBI
KENYA

ASIA PACIFIC

ADAM SMITH INTERNATIONAL
SUITE 305, 100 WILLIAM ST
WOOLLOOMOOLOO
NSW 2011
AUSTRALIA

SOUTH ASIA

ADAM SMITH INTERNATIONAL
AVANTA BUSINESS CENTRE
402 STATESMAN HOUSE,
BARAKHAMBA,
NEW DELHI 110 001
INDIA

ASI ADAM SMITH INTERNATIONAL

WWW.ADAMSMITHINTERNATIONAL.COM