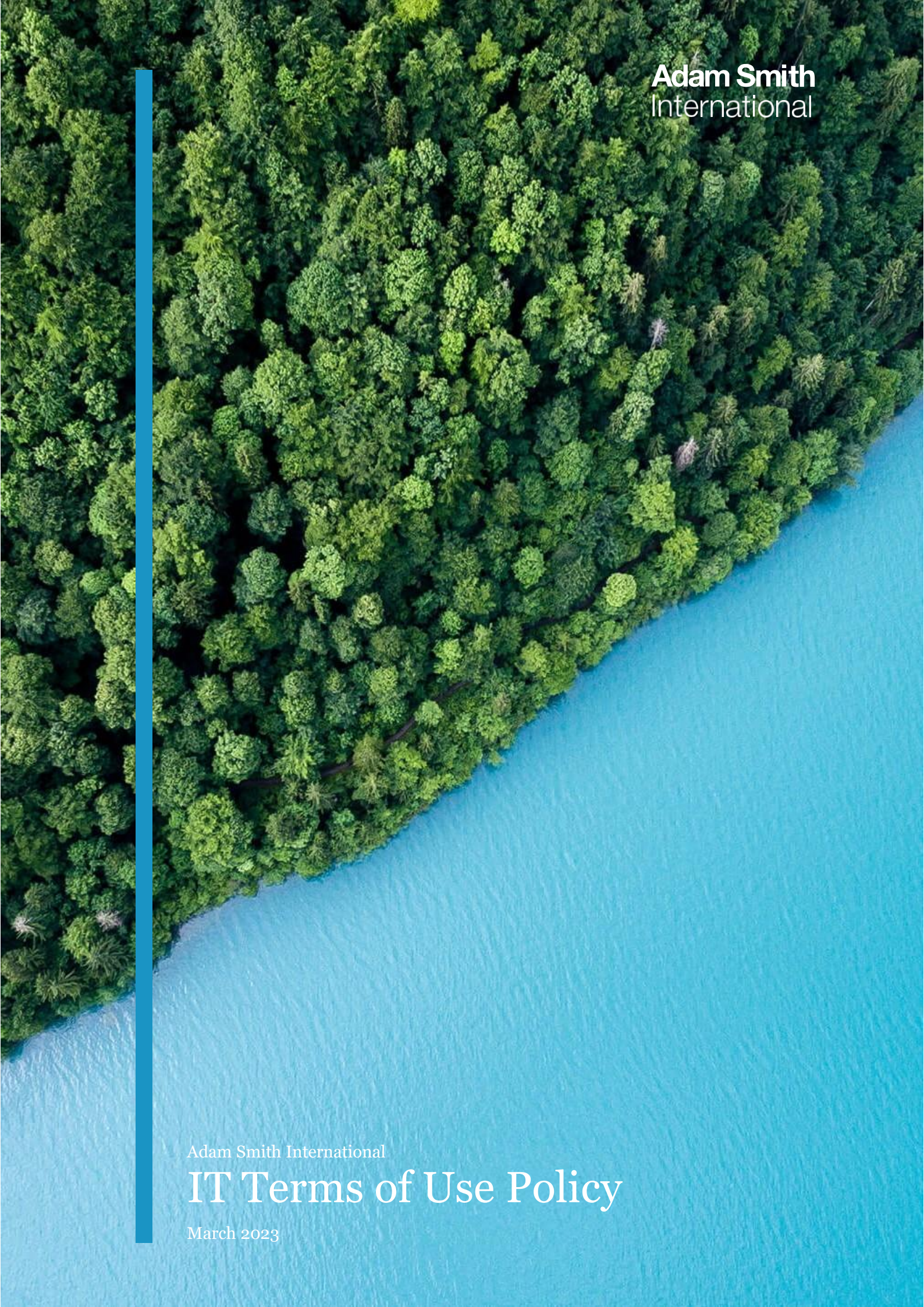

Adam Smith International

IT Terms of Use Policy

March 2023

Document version:	**v1.2** **Revised language around device security requirements**
Last review date	**March 2023**
Author	**Paul Ferrier, Information Security Officer**
Owner	**Adrian Hollister, Head of IT and Cyber Security**
Approver	**Audit Committee**
Classification	**INTERNAL**
Who does this policy apply to:	**All Adam Smith International workers**[1]

[1] Adam Smith International ("ASI") "workers" shall include both ASI Employees and ASI Associates.

Definitions

Term	Definition
Computers, phones, and similar devices	Is a collective term to describe a hardware component, irrespective of operating system and ownership that is used for transmitting, storing, accessing, or manipulating ASI data, including (but not limited to) servers, laptops and desktop computers, smart phones, printers, network switches and wireless access points.
May	This term is used to state an **optional** requirement of this policy.
Multi-Factor Authentication (MFA)	Is a further identity challenge, over and above a password, to ensure that the worker in question is the person trying to access the online services. This provides assurance around the fact the worker in question is who they say they are (MFA blocks access if a worker password is compromised).
Online services	Is a collective term covering Microsoft's, Adobe's, and other company's products, that require logging on to access, that are used by ASI's workers to perform their digital duties.
Security posture	Is the general overall health of the computer or similar device (be used to access online services) as well as the actual worker account to ensure that online services are not put at risk for all workers by an insecure device or potentially compromised, or at-risk worker account.
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.
Worker account	Is the actual digital account used to access online services, this is predominantly a project or corporate email address protected with a password and Multi-Factor Authentication (MFA).
Workers	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.

1. Introduction

1.1. The purpose of this ASI IT Terms of Use policy document is to provide exemplar guidance in line with the HMG, DFAT, EU or USAID and industry best practice, to protect computers, phones, and similar assets, and the information (or data) that they hold, process, or transmit while working for or with Adam Smith International.

1.2. All information has a value, whether it is the contact details of a single worker, a risk register or a database of information collected throughout a project. Today's workplace involves using computers, phones, and similar devices to create, amend, print, and send information, all over the world. This includes personal devices used to conduct corporate or project work, as well as devices issued by a project or centrally. To reduce the risk of the information being sent to the wrong recipient, overseen by in appropriate worker, lost or stolen, measures need to be put in place; this is what this policy document looks to lay out what is acceptable or not.

2. Scope and Applicability

2.1. This Policy applies to Adam Smith International and all its operating companies (collectively, the **"Company"**) and applies to all employees and associates of the Company (collectively, the **"Workers"**).

3. Roles and Responsibilities

3.1. The Executive Team has overall responsibility to ensure the principles of this policy are being upheld throughout the organisation.

3.2. The Internal Audit Team have a responsibility to provide independent assurance to management and the Board that the IT controls are appropriately designed and operating as intended.

3.3. The IT management team have a responsibility to design and monitor the IT controls, ensuring these controls are operational and being adhered to.

3.4. The IT team have a responsibility to maintain the security of the organisation's systems enabling workers to perform their duties in a safe environment.

3.5. The IT team have a responsibility for promoting, circulating, and raising awareness of this policy with all workers.

3.6. It is all ***workers*** responsibility to read, confirm understanding or raise queries in respect of and adhere with this policy.

4. Terms of Use

Principles and rules

All workers:

- ***Shall*** be required to agree to the IT Terms of Use, on each individual device, before being given access to online services.
- ***Shall*** be required to agree to the IT Terms of Use on a recurring schedule of *every* six months.
- ***Shall not*** use computers, phones, and similar devices to visit sites or perform tasks that are illegal (in the country where the worker is located and/or the United Kingdom), inappropriate or bring the company into disrepute.

- ***Shall not*** engage in any form of defamatory, threatening or intimidatory behaviour, this includes verbal, written and physical actions.
- ***Shall not*** break copyright or infringe on intellectual property, this refers to the donor country of origin, the UK as well as local in-country legislation where the worker is resident.
- ***Shall not*** attempt to gain access to unauthorised information or circumvent existing information security measures.
- ***Shall*** protect their computers, phones, and similar devices used to conduct company or project work against unauthorised access.
- ***Shall*** protect their computers, phones, and similar devices by meeting our minimum-security requirements:
    - Installing Operating System and application patches within **14** days of release from the manufacturer.
    - Have legal hardware and software that meet all license conditions of use.
    - Have anti-malware software active and up to date.
    - Have a software firewall active on the device.
    - Be encrypted, thus protecting all the information stored on the device.

  Failure to meet this condition, will result in the device not being able to interact with corporate and project services until remediation is completed.
- ***Shall*** protect information from being easily intercepted or accessed by others.
- ***Shall*** use Multi-Factor Authentication (MFA) to further protect their worker accounts.
- ***Shall*** inform their line manager and IT if:
    - A computer, phone, or similar device has been lost, stolen, or compromised (including having malware or virus infection, for example) immediately after discovery.
    - An account used to access corporate or project information has been compromised; and
    - Any information security near misses occurs, in order that existing measures can be reviewed and tightened if required, to prevent recurrence.
- ***Shall*** allow monitoring and reporting on baseline compliance of their digital activities to prevent misuse of both the workers computing account, the device itself and ASI's corporate online services.

5. Internal and external references

5.1. For incidents, please contact the IT team it@adamsmithinternational.com.

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

5.2.1. Mobile Computing Policy

(https://adamsmithint.sharepoint.com/:b:/r/sites/CorporatePolicies/ASI Published Policies/Mobile Computing Policy.pdf)

5.2.2. ASI Information Security Policy

(https://adamsmithint.sharepoint.com/:b:/r/sites/CorporatePolicies/ASI Published Policies/ASI Information Security Policy.pdf)

Headquarters
Tallis House,
2 Tallis Street
London
EC4Y 0AB
United Kingdom
T: +44 20 7735 6660

Europe
Adam Smith Europe B.V.
Keizersgracht 62,
Amsterdam,
1015 CS
Netherlands
T: +31 (0)20 520 7400

Africa
Westlands
Nairobi,
Kenya
T: +254 20 444 4388

Asia Pacific
Suite 103
80 William Street
Woolloomooloo
Sydney
NSW 2011
Australia
T: +61 2 8265 0000

North America
1712 N Street NW, Suite 400
Washington, DC 20036
United States of America
T: +1 (202) 873-7626

South Asia
56 Alps Building,
Janpath,
New Delhi 110 001
India