International Associates Limited establishes the acceptable usage guidelines for all technology resources. These resources can include, but are not limited to, the following equipment:

- Computers (Laptops, Desktop Computers, Mobile Devices, Servers, etc.)
- Network Equipment (Routers, Wireless Devices, Fiber Optic Lines, VoIP Phones, etc.)
- Audio/Video Equipment (Cameras, Projectors, Security Cameras, Digital Cameras and Camcorders, Scanners, Printers, Copiers, Fax Machines, etc.)
- Software (Operating Systems, Application Software, etc.)
- Resources (Drive File Storage, Website File Storage, Email Accounts, Social Networking Accounts, etc.)

This policy applies to all employees, contracted employees, contractors, and sub-contractors, at International Associates, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by International Associates.

Failure to comply with this policy would be a breach of company protocols, and users could be subject to disciplinary procedures.

While **International Associates** desires to provide a reasonable level of freedom and privacy, users should be aware that all equipment, network infrastructure, and software applications are the property of International Associates and, therefore, are to be used for official use only. Also, all data should be treated as such and protected from unauthorised access.

The following activities provide a general guideline to use International Associates resources in an acceptable manner:

- All passwords used to access International Associates systems must be kept secure and protected from unauthorised use.
- No user account can be shared between individuals. Authorised users are responsible for the security of their own passwords and accounts.
- Do not transfer personally identifiable information on equipment, cloud drives and storage devices.
- All computers residing on the International Associates network shall be owned by IA, and shall be approved with virus-scanning software with a current, up-to-date virus database and also a software firewall.
- Employees must use extreme caution when opening email attachments received from unknown senders.
- All electronic works should be completed or transferred via International Associates email accounts so that no data is transferred off-network.
- All workstations should be kept secure. Users should lock the workstation when not attended to protect unauthorised users from accessing secure files.
- Social media and chat apps shall not be used for business processes.

- All hardware shall be disposed of, accounting for recycling requirements and data protection breaches.

Under no circumstance shall an employee of International Associates be authorised to engage in any activity that is illegal under local or international law while utilising International Associates resources. The lists below are to provide a framework for activities that fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, and the installation of any copyrighted software.
- Exporting software, technical information, encryption software or technology, in violation of international or local export control laws is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
- Introduction of malicious programs into the network or server environments.
- Revealing the account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using any machine to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any International Associates account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access unless these duties are within the scope of regular duties.
- Executing any form of network monitoring which will intercept data unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
- Any form of harassment via email or telephone.
- Unauthorised use, or forging, of email header information.

- Use of unsolicited email originating from within International Associates' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by International Associates.

Passwords

When setting password users, the strength is normally determined within the settings of the system. However, the user should:

- Shall be a minimum of 9 characters in length containing UPPER, lower, numbers and symbols.
- Avoid choosing obvious passwords (such as those based on easily discoverable information).
- Not to choose common passwords (use of technical means, using a password blacklist recommended).
- Should not re-use a password.
- Shall not record passwords to store and retrieve them securely.
- Shall use only authorised password management software (available via the IT manager).
- All passwords must be memorised and not recorded anywhere.
- Must be unique for each application.

Remote Working

This policy applies to all persons employed or contracted who may be required to, or have the opportunity to, work from home. In all cases, homeworking should only be considered when there is a defined business need.

Users shall be included in the Cyber Essentials security checks, including security, anti-virus, passwords, wi-fi, updates and patches etc.

Where possible, users should use company-provided IT equipment; if this is not possible or practical, the user shall ensure that all security requirements are implemented on the equipment being used.

Hard copies of documentation shall not be printed at remote working locations.

Access to the IA systems is limited for remote workers to online tools and cloud-based systems; no direct access, VPN or other remote networking to the company servers/network shall be allowed.

Support may be given by IA using MS Teams to remotely control IT equipment. Users should not allow any other external support personnel remote access to their equipment.

No files of any kind shall be saved locally on Non-company IT equipment.

COVID Supplement

Due to the coronavirus (COVID-19) outbreak, we have added additional IT requirements to our policies; we have re-examined our disaster preparedness plans and planned and prepared for risks that may be involved with business continuity interruptions, cancelled business travel plans, possible data loss, unplanned downtime, more people working remotely and also the conducting of Remote Audits.

The IA policy is aligned with the IAF MD 4:2018 – IAF Mandatory Document for the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes.

Administrative Account Usage

Administrative accounts are to be used solely for administrative purposes and should not be employed for every day user activities.

Administrative accounts are granted elevated privileges within the IT environment to perform critical system management, configuration, and security tasks. These accounts have the potential to significantly impact the organisation's IT infrastructure and data security. To ensure the integrity, confidentiality, and availability of IT resources, it is imperative that administrative accounts are used judiciously and exclusively for their intended administrative functions.

Policy Guidelines:

1. Purpose of Administrative Accounts:

   Administrative accounts should only be used for tasks that require elevated privileges to maintain, configure, monitor, or secure IT systems, networks, and resources.

2. Prohibited Activities:

   Administrative accounts must not be used for routine or everyday user activities, such as web browsing, email, social media access, or non-administrative software installations.

   Administrative accounts must not be used for testing or experimentation unless specifically required for administrative purposes, and with appropriate approvals.

3. Accountability:

   Users with administrative privileges are responsible for their actions when using administrative accounts. Any changes or actions taken using administrative accounts must be logged and monitored for security and auditing purposes.

4. User Accounts:

   Each IT user should have a separate standard user account for their everyday activities. These standard accounts should not have administrative privileges.

5. Password Security:

   Administrative account passwords must adhere to the organisation's password policy, including complexity requirements, expiration intervals, and uniqueness.

Remote Audits

During remote audits, only the following conferencing systems shall be used: -

- Microsoft Teams
- WebEx
- Zoom

No social media systems shall be used when conducting audits.

Video Capture / Screen Shot may be required by the Lead Auditor to meet the requirements of the scheme being audited. Client confirmation shall be confirmed prior to this being completed.

Meetings shall be set up by the lead auditor so that security and permissions can be managed.

The following permissions shall be enforced for attendees: -

- No recording of the audit
- No video capture/screenshot by attendees
- Access to authorised attendees only.

Documentation

Documentation shared for the audit in advance shall be covered by the standard IA policies on data protection and privacy. Any documentation from the client shall be sent by email or, if required, via the IA secure OneDrive document request link.

Documentation shared during the audit required to be retained shall be retained on company equipment/storage devices only. All other documentation shall be deleted at the end of the audit.

Martin Coles

Martin Coles

Operations Director of International Associates Limited

Date: 22/09/2023