

SIACO

protecting your security spend

Version: 1/Apr25

Cyber Security Policy Statement

It is the duty of all employees, associates and suppliers of SIACO Limited to support and maintain effective cyber security measures across the business. These measures will safeguard our assets as well as protect our client's information. This will be achieved through cooperation, vigilance and compliance with standards, direction and policy.

Cyber security risks will be identified, assessed, documented and mitigated to as low as reasonably practicable throughout the business. We expect all employees, associates and suppliers to report security concerns, breaches and non-compliance as quickly as possible.

All cyber security matters shall be directed to admin@siaco.co.uk

Purpose

The purpose of this policy is to:

- 1) ensure cyber security measures are understood, implemented and maintained
- 2) protect assets, systems and data from unauthorised access
- 3) mitigate cyber vulnerabilities

This policy covers approved software, mobile devices, passwords and leavers. It does not cover new starters, network configuration and security, asset management, software licensing or wider cyber security strategy.

Scope

This policy applies to all employees, associates and suppliers who have access to any IT system in the business, including software, mobile devices and other forms of technology.

Compliance

This policy shall be reviewed annually, or earlier if deemed necessary and its implementation will be monitored regularly. Non-compliance with this policy may result in further action being taken against employees, associates and suppliers of SIACO Limited.

Approved Software List

SIACO has an approved software list that details which software is approved across computer and phone devices. All unnecessary software and services are removed or disabled. Any software that is not approved is forbidden to be downloaded or operated on SIACO devices without requesting and obtaining written approval from admin@siaco.co.uk

Software Restrictions

- There must be a business-case for all software used
- Software use will be reviewed every 90 days
- Software must have sufficient security updates
- Only administrators can download or remove software from devices
- Only vendor supported software can be used or software will be removed
- Software must be updated regularly
- SIACO reserve the right to remove software from devices without warning

SIACO

protecting your security spend

Mobile Devices

- Mobile devices are supplied for work and light personal use only
- All mobile devices supplied will be managed and restricted
- Mobile devices must be switched on during working hours
- Mobile devices and equipment such as chargers must be kept in working order
- Mobile devices must not be left unattended or insecure
- Sim cards must not be removed under any circumstances
- Mobile devices must not have NFC technology enabled
- Mobile devices must not be used to distribute or view material that is inappropriate or offensive
- All data held or processed by any mobile device is subject to Data Protection Policy and associated statutory requirements
- In all cases of faults, loss, damage or theft, please notify admin@siaco.co.uk

Passwords

SIACO recommend generating a password in our approved password manager. This password should not be used for any other account. It should include:

- 8 characters minimum
- Lowercase characters
- Uppercase characters
- Numbers (0-9)
- Symbols

Passwords should not relate to birthdays, family-life or work.

- Passwords can only be stored in an approved password manager
- The password manager access password must be unique and meet the requirements above
- If you believe your password has been compromised, please phone 0208 137 0675 and contact admin@siaco.co.uk

Leavers

The following will apply to all new leavers:

- A full backup of accounts will take place
- Director will advise admin@siaco.co.uk if access is to be reduced
- Once agreed, revised access to be communicated to leaver
- Increased monitoring of leaver to be completed by admin@siaco.co.uk
- On final day, all devices to be returned
- All login sessions to be closed
- All passwords to be changed
- Director to advise on account closure timeframe within 28 days

Ratification

Lewis Loveless

Lewis Loveless, Director