Jonco IT & Security

Policies

Policies

Overview

- This document contains Jonco IT & Security policies that are classified as public.
- Each policy has a document control section listing changes and review dates.
- Each policy will be reviewed at least yearly, with the document control section updated accordingly.
- Our policies are currently appropriate for the size of the company (one employee, who’s also a director). As Jonco IT & Security grows, changes will be made as required.

Contents

Acceptable Use Policy (AUP)

Version	Date	Contributors	Comment
1	2025-04-01	Director (JH)	Initial release

Scope

This policy applies to all staff and other users who have access to the organisation's IT systems. It is expected that any contractors will have similar policies and processes in place.

This policy and the law

- You acknowledge that regardless of this policy, you must, always, follow applicable laws.
- You may not obtain, or attempt to obtain, access to systems to which you have not been authorised (i.e. “hack” or “breach” systems).
- The only exception to this is where you are examining a system for the express purpose of responsibly disclosing any problem findings to the system owner. If in doubt, speak to your manager.

User accounts

- All colleagues and contractors will be issued individual, unique, login credentials.
- Users must not share their login credentials with others and must log out of systems when not in use.
- Rules for passwords are contained in the *End User Computing policy*.

Email Use

- **Professional Use:** Email should be used primarily for business-related communications. As such, colleagues must ensure that their email communications are professional and appropriate.
- **Confidentiality:** Users must not share confidential information via email unless authorised, and sharing such information should be done in line with our *data classification* policy.
- **Attachments:**
- Users should be cautious when opening email attachments, whether from known or unknown sources, to prevent malware infections.
- When sending attachments, colleagues should consider sharing the file via SharePoint, or an approved alternative, by preference.

- **Spam and Phishing:** We have anti-spam and anti-phishing systems, but colleagues must still be vigilant against spam and phishing attempts. Report any suspicious emails to your manager.
- **Emails can be binding:** Remember that the content of emails could constitute a legal agreement between parties. You must not enter into an agreement, or give the impression of doing so, without authorisation from a director.

Internet Browsing

- **Business Purposes:** Internet access should be used primarily for business-related activities. Personal use is permitted within fair use limits (see below)
- **Prohibited Content:** Accessing, downloading, or sharing illegal, offensive, or inappropriate content is strictly prohibited. Examples of such content includes:
- Pornography
- Software "warez" sites, or sites offering ways to "crack" software to allow use without paying a fee
- Sites that promote hatred of any kind
- Sites *known* to be used for malware distribution
- Content that would be deemed illegal in the United Kingdom
- **Bandwidth:** Colleagues should be mindful of bandwidth usage to ensure that business-critical applications are not impacted. Generally, access to streaming media services should be limited, especially when using company provided mobile phones and mobile data plans.
- **Filtering systems:** The company will implement suitable filtering systems (content and / or DNS) to help keep colleagues safe. These must not be bypassed without approval from a director.

Connecting to company systems over the Internet

- **Authorisation:** Before accessing company systems, colleagues must have authorisation to access the organisation's systems remotely. When connecting remotely, users must use systems provided for secure connections.
- **Data Protection:** Wherever possible, users must ensure that data transmitted over the internet is encrypted and secure. For example, by using HTTPS and SSH rather than plain-text protocols such as HTTP and Telnet.

Personal Use

We acknowledge that everyone uses company equipment and connections for personal use from time to time – for example checking the news or getting a link as part of "water cooler" / "tea break" chat. This is permitted such that:

- **Fair Use:** Personal usage is within reasonable limits. Excessive personal use that impacts work performance or network resources is prohibited.
- **Social Media:** Personal use of social media should not interfere with work responsibilities. Colleagues and contractors must not post confidential or proprietary information about the organisation. If you're unsure if what you want to post would be permitted, speak to your manager.
- **Downloads:** Users should avoid downloading large files for personal use that may affect network performance.

Compliance

- **Monitoring:** The organisation reserves the right to monitor email and internet usage to ensure compliance with this policy.
- **Violations:** Any violations of this policy may result in disciplinary action, up to and including termination of employment.

Artificial Intelligence (AI)

Version	Date	Contributors	Comment
1	2025-04-30	Director (JH)	Initial release

Scope

This policy applies to all staff.

Approved AI tools

Only the following AI tools may be used. If additional AI tools are required, these will need to go through the approved software process.

Vendor & tool	Data types	Notes
JetBrains AI	Source code, log entries, descriptive chat	This tool allows choosing upstream models, including Claude Sonnet and OpenAI ChatGPT.
Microsoft Copilot	Documents, web pages, emails *except* where a customer has explicitly opted out.	Customers can object to AI use on their own / proprietary data.

Customer data and AI use

Care must be taken when submitting customer data to AI tools and large language models:

- Ensure the customer is aware AI tools will be used
- Customer provided Personally Identifiable Information (PII) must not be submitted to the AI tool *unless* the customer has explicitly approved this use case
- Ensure the AI tool does not use customer provided data to train and improve the model / tool

Customer right to object to AI use

Customers have the right to object to their data (including source code) being passed to an AI model. If the customer exercises this right then any AI processing of customer data will cease immediately.

Backup

Version	Date	Contributors	Comment
1	2025-04-06	Director (JH)	Initial release

Scope

This policy applies to all systems and data owned or managed by *Jonco IT & Security Ltd*.

Data storage and availability for backup

- Unless the data is for test purposes (e.g. labs or other ephemeral / temporary data), under no circumstances must data exist only in one place (e.g. on a single laptop).
- Company data should exist on company provided storage, e.g. Microsoft SharePoint (part of Microsoft 365 for business).
- If an exemption is needed, for example due to a customer requirement, a director must be made aware and accept the risk.

Backup Frequency

- **Cloud services:** Services such as Microsoft 365 for Business will follow vendor managed backup schedules.
- **SharePoint:** A copy of SharePoint will be taken at least monthly.
- **End user devices:** If images of employee computers are taken, these will be refreshed at most every six months.
- **Virtual machines:** Backups will be taken at least weekly.
- **Source code:** The git versioning system is by its nature distributed and retains multiple versions. Backups will be taken at least monthly (where relevant).

Backup Retention

- **Cloud services:** As managed by the vendor.
- **SharePoint:** Full copy retained for at least three months, at most one year.
- **End user devices:** At least two images will be retained, at least six months apart, for at most one year.
- **Virtual machines:** At least two backups will be retained, up to a maximum of one year.
- **Source code:** Versions are managed by git. Backups of the repository will be kept for at least three months, at most one year.

Backup Encryption

- All backup data must be encrypted using industry-standard encryption methods (e.g., AES-256) to protect against unauthorised access.
- The encryption used must be equivalent (or better) to the original encryption of the source data.

Test Restores

- **Annual Test Restores**: Test restores will be conducted at least annually to ensure backup integrity and the ability to recover data.
- **Documentation**: Results of test restores, including any issues encountered and corrective actions taken, will be documented.

Responsibilities

- **Directors**: Responsible for implementing and maintaining the backup procedures.
- **Data Owners**: Ensure that critical data is identified and included in the backup process.

Bring Your Own Device (BYOD)

Version	Date	Contributors	Comment
1	2025-04-06	Director (JH)	Initial release

Scope

This policy applies to all staff and contractors with access to company data.

Device Requirements

- **Supported Operating Systems:** All personal devices used for BYOD must run a supported and up-to-date operating system (e.g., Windows, macOS, iOS, Android).
- **Approved Applications:** Only official Microsoft Office applications or other vendor-provided apps may be used to access company data.
- i.e. If the vendor “Contoso” provided a note taking service, only the “Contoso” app should be used to access the data, rather than other compatible apps.
- e.g. The Microsoft Outlook app must be used, rather than Apple Mail or Gmail.
- **App updates:** Apps must be kept up to date.

Security Measures

- **Encryption:** Devices must be encrypted to protect company data.
- **Password Protection:** Strong passwords or biometric authentication must be used to secure devices.
- **Antivirus Software:** Where available, devices must have up to date antivirus software installed.
- **Mobile device management:** Where available, controls will be applied to apps that access company data to ensure that they are locked to prevent unauthorised use, and to permit erasure of company data.

Usage Guidelines

- **Downloads:** Company data should not be downloaded to personal devices for extensive periods.
- Ideally, company data should only be downloaded to company owned & managed devices.
- If a download is required to a personal device, it must be securely deleted as soon as possible after it is no longer needed.
- **Data Access:** Access to company data should be limited to what is necessary for job functions.
- **Compliance:** Users must comply with all company policies regarding data security and confidentiality.

- **Data erasure:** Employees acknowledge that, where supported, the company may erase company data from BYOD. It is the employee's responsibility to ensure they have suitable backups of their own data, to prevent against the unlikely event their personal data is impacted by the erasure.
- **Support:** Note that the company will only provide limited support on personal devices. Any actions performed on an employee's personal device will be undertaken with the employee present and at their risk.

Responsibilities

- **Employees:** Ensure their devices meet the requirements and report any security incidents immediately.
- **Directors:** Provide support and ensure compliance with this policy.

Data Classification, Encryption, and Protective Marking

Version	Date	Contributors	Comment
1	2025-04-30	Director (JH)	Initial release

Scope

This policy applies to all staff.

Classification

- All data and documents should have a classification.
- Classifications are to be set by the data / document owner, or a director.
- Encryption and handling of data should respect the classification level.
- There are four classification levels (below).

Classification levels

Public

- Document or data may be disclosed to external parties without consequences.
- Data may be accessible without login (anonymous access).
- It is *recommended* to encrypt the data at rest and in transit.
- Examples include: public website, brochures, marketing material.

Internal

- Document or data should not be shared with third parties.
- May be shared within the company.
- Should be encrypted at rest and in transit.
- Examples include: internal processes, team communication sites.

Customer Confidential

- Document or data has been prepared for a customer, and may be shared with the customer and others within Jonco IT & Security as required.
- The data is shared on a need-to-know, where the customer has an automatic need-to-know.
- Data may not be shared with a third party without the consent of the customer and Jonco IT & Security.
- Unless otherwise agreed with the customer, all customer data is customer confidential.
- Should be encrypted at rest and in transit.
- Examples include: customer contracts, proposals, reports.

Confidential

- Document or data is internal only, so may not be shared with external parties.
- Document or data could do the company harm if it was inappropriately shared.
- Where an exception is required, for example as part of an audit, this must be approved by a director, and Non-Disclosure Agreements may be required.
- Access is on a need-to-know basis.
- Should be encrypted at rest and in transit.
- Examples include: company accounts, staff records, detailed network diagrams.

Encryption

- Industry standard encryption must be used (i.e. Jonco IT & Security will not “roll its own” encryption).
- Encryption must be appropriate to current good practice (i.e. if an encryption algorithm is known to have been broken, or considered weak, it must not be used).
- When using Transport Layer Security (TLS), version 1.2 or higher should be used.
- Where there is a need for lesser TLS versions this must be agreed by a director. The exception must be recorded, along with its justification, and the exception must be reviewed yearly.

Protective marking

- The data owner is responsible for classifying the data or document and applying markings.
- For documents, markings should be placed in the header (where possible / appropriate) of each page.
- If it is not possible / appropriate to mark the document in the header, the classification must be clearly stated elsewhere.
- Not all data can be marked within the data itself (for example a database table). Instead, the infrastructure itself should be “tagged” (e.g. in a cloud computing environment) and the classification should be documented.
- Lists of data classifications are classified as confidential.

Unmarked documents

- If a document has no protective markings, it must be treated at the highest level of classification (**Confidential**).
- Unmarked documents should be updated with a classification as soon as is practical.

End User Computing

Version	Date	Contributors	Comment
1	2025-04-06	Director (JH)	Initial release

Scope

This policy applies to all staff. References to devices relate to company issued devices. For employee-owned devices, see the *Bring Your Own Device (BYOD) policy*.

Jonco IT & Security Ltd expects that contractors will have suitable equipment that aligns to equivalent or better security standards / controls.

General statement

- The company firmly believes that providing good quality equipment is fundamental to staff feeling valued, and has a direct impact on their wellbeing.
- All staff will be provided equipment to allow them to efficiently and effectively perform their job role.
- Should additional equipment, or upgrades, be needed, this should be discussed with the employee's manager. If agreed necessary equipment will be provided where possible.
- Colleagues must use equipment in line with the *Acceptable Use Policy*, and other policies where relevant.

Data storage

- In line with other policies, data should not only exist on an employee's assigned device.
- The exception to this is ephemeral (temporary) data, e.g. labs.
- Colleagues should store data on company provided systems, such as Microsoft SharePoint or Microsoft OneDrive for Business.

Device builds

- **Trusted media:** Operating Systems must be installed from trusted media, such as that from the vendor's official site or via the vendor's delegated distribution channel.
- **Security controls & management:** Company owned devices must be configured by device management tools, or by company directors, in such a way that they meet security requirements.

Encryption of devices

- All devices must be encrypted using industry-standard encryption.

- Examples include Linux Unified Key Setup, Microsoft BitLocker, Apple MacOS FileVault, Apple iOS and Android built-in encryption.

Hardware replacement cycles

We believe we must protect our environment (see our *environment & transport policy*, so we do not arbitrarily replace end user equipment on set schedules. Instead, we will provide "well specced" equipment that should meet the need for at least five years. When an employee thinks they need an upgrade, this should be discussed with their manager.

An exception to this rule is for faulty, unreliable, or broken equipment. Such equipment will be replaced or repaired as is most appropriate.

Passwords, MFA, and biometrics

- Passwords must:
- Be different per account
- Not be shared between employees
- Meet the following requirements:
- Minimum 12 characters
- Have three out of four character classes: lower case letters, upper case letters, numbers, special characters
- If you think your password has become known to another person, it must be changed immediately.
- Wherever possible, Multi Factor Authentication (MFA) **must** be used.
- Hardware security token (e.g. Yubikey)
- Push notification to app
- One time password generated by app
- "Magic link" or code sent to company email
- **Do not** use SMS or phone call MFA unless this is the only available option
- Biometrics may be used to facilitate the logon process.
- Microsoft Hello for Business
- Apple FaceID
- Fingerprint

Printing

- Where possible, printing should be avoided. This is for environmental and security reasons.
- If printing is necessary, the paper copy must be disposed of securely in a cross-cut shredder.

Removable media

- Generally, use of removable media is prohibited.
- For file sharing, use tools such as Microsoft SharePoint.
- Where removable media *must* be used it should be encrypted (e.g. BitLocker To Go, or hardware encrypted devices).
- If encrypted media is not possible, for example in a camera:
- Only non-confidential / non-sensitive data should be stored.
- Unencrypted media should be accompanied at all times, or securely stored, until company data can be removed.

Environment & Transport

Version	Date	Contributors	Comment
1	2025-04-06	Director (JH)	Initial release

Scope

This policy applies to all staff.

Environmental statement

We believe we must protect our environment and make efforts to reduce our negative impacts on it.

IT equipment

- IT equipment has a high environmental impact.
- Where possible, IT equipment will be sourced that uses recycled materials, and that is designed to permit repairs by users (e.g. the Framework series of laptops).
- Where appropriate, IT equipment will be repurposed rather than purchasing new (including purchasing reconditioned / renewed hardware).

Disposal

- Items will be disposed in-line with the law and relevant local regulations.
- When contracting disposals, only registered waste carriers will be used.
- Items will be recycled wherever possible.

Recycling & re-use

- **Recycle:** Staff are encouraged to recycle at home, co-working spaces, and offices.
- **Re-use:** Where there is an option for re-usable items vs single-use, the re-usable item should be preferred.

Transport

- **Public transport:** Where practical in terms of cost, time, and safety, public transport will be used.
- Where public transport allows the booking of a seat, colleagues are encouraged to do so.
- **Flying:** When flying, which should be the option of last resort, staff (of all levels) will fly:
- Economy for short-haul flights.
- Business class for long-haul flights (if preferred).
- Never first class.

- **Purchasing tickets:**
- Tickets should be purchased as far in advance as possible in order to secure the best value (likely a cheaper price).
- When travelling by train, first class *may* be used if this is cheaper.
- **Cycling:** When cycling, staff will:
- Ride a cycle that is in a roadworthy condition.
- Use cycle routes where possible.
- Wear a helmet (and other safety gear where deemed appropriate).
- Have working lights for riding at night.
- Observe the rules of the road and ride with due consideration to other road users. This includes **not** riding on pavements or in pedestrianised zones.
- **Driving:** It is acknowledged that public transport is not always suitable. When driving, staff will:
- Ensure they have appropriate business insurance.
- Have a valid driving licence.
- Drive a vehicle that is in a roadworthy condition, including with a valid MOT (unless exempt due to young vehicle age) or appropriate service.
- Plan routes to allow for environmentally friendly driving.
- Observe the rules of the road and drive with due consideration to other road users.
- **Fines:** Except for in exceptional circumstances, employees will be personally liable for fines incurred while transporting themselves (e.g. receiving a penalty charge notice for incorrectly parking, fines for speeding).

Privacy & Cookies

Version	Date	Contributors	Comment
1	2025-05-07	Director (JH)	Initial release
2	2025-05-15	Director (JH)	Update to include feedback survey

This policy is published on our website and is separate to this document.

Please view the policy at https://www.jonco-it.co.uk/privacy-cookie-policy/ .

HR & Recruitment

Version	Date	Contributors	Comment
1	2025-04-06	Director (JH)	Initial release

Scope

This policy applies to all staff.

Reduced HR policy set

Our HR policies are currently appropriate for the size of the company (one employee, who's also a director). As *Jonco IT & Security* grows, changes will be made as required. In the interim, the ACAS guidance applies.

Impact on contractors

Jonco IT & Security Ltd expects contractors to follow good HR practices (for companies) and within the law.

References & background checks

- **References:** When recruiting, the recruiting manager / director will take up **two** references for the prospective employee.
- One reference should be for the immediately previous employer, unless agreed otherwise with a director.
- **Background checks:** Unless required by law, or as appropriate to a specific role, background checks (e.g. DBS) will not be required.

Recruitment

- We believe that an employee should be hired based on their merits (e.g. skillset, experience, how well they fit with the team).
- We will not discriminate between candidates based on a protected characteristic (see *Equality Act (2010)*), i.e. all candidates will be treated fairly.

Remote working

Version	Date	Contributors	Comment
1	2025-04-06	Director (JH)	Initial release

Scope

This policy applies to all staff and contractors.

Being observed or overheard

- Care must be taken when working remotely to ensure that screens are not observed by external parties, to prevent the leaking of sensitive information.
- External parties may overhear conversations – you must consider the content of your conversation, and the impact of it being overheard.
- If necessary, re-schedule the call.
- Be aware of external parties “shoulder surfing” for passwords on company information, and take steps to prevent this.

Safe working environments

- The employee is responsible for ensuring the remote working environment is safe.
- Ensure there is adequate lighting, and that the temperature is comfortable.
- Take steps to avoid trip hazards, such as cables run across floors.
- Have your screen at the correct height to avoid straining your neck.
- Where possible, use an external keyboard and mouse.
- Take regular breaks to stretch.

Unattended equipment / data

- Screens must be locked (via PIN, password, or biometrics) when not in use.
- Print outs must be locked away when unattended.
- Hardware must not be left unattended if it is at a greater risk of theft (e.g. on a cafe table).
- If equipment or data is left in a car, it must not be visible, and the vehicle must be locked.
- Ideally, the equipment and data should be brought inside the house / hotel room.

Use of WiFi

- Home WiFi should be well configured:
- Require a password (at least 12 characters) or certificate.
- Use WPA 2 or greater (WEP or WPA 1 must not be used).
- Care should be taken to use WiFi that is not at additional risk of malicious tampering.

- It is acknowledged that employees cannot know the configuration of public WiFi / WiFi offered at venues.
- Airports and cafes *may* present a greater risk, however, there is no one-size-fits-all approach.
    - If you receive certificate warnings / errors in your browser or within an app, **do not proceed through the warning** and disconnect from the wireless network.

Relationship with other policies

While remote working, all other policies still apply.

Software Usage & Approvals

Version	Date	Contributors	Comment
1	2025-04-06	Director (JH)	Initial release

Scope

This policy applies to all staff and contractors, although contractors may use appropriate software per their own approvals process.

Software approvals

- **Approved software:** Only software listed as approved on the software list is permitted for use.
- This list will be maintained and regularly updated by the directorate.
- Software may have further restrictions on use, which will be recorded on the list.
- **Prohibited software:** The approved software list may include software that is prohibited for use on a particular platform (or all platforms). Such software must never be used.
- **Licencing:** Only correctly licenced software may be used.
- **Review process:** A director will review software regarding its suitability, security, and development practices. So long as this process doesn't highlight significant concerns, the software may be approved if it's deemed beneficial to the company.

Software Requirements

- Software used must be actively developed and receive regular updates to ensure security and functionality.
- Once software reaches the end of its supported lifecycle it will be moved to the prohibited list.
- Software must only be obtained from the vendor, or the vendor's delegated distribution mechanism.
- Torrents, warez sites, other non-official third parties may not be used.

Responsibilities

- **Employees:** Must use only approved software and report any software needs or issues to a director.
- **Directors:** Responsible for maintaining the Software List and ensuring all software meets the required standards.

Training

Version	Date	Contributors	Comment
1	2025-04-06	Director (JH)	Initial release

Scope

This policy applies to all staff. We expect that contractors will have appropriate training and follow their own training policies.

Training policy

- All staff will be given general training on security (covering good practice) and data handling (covering GDPR and Data Protection Acts).
- Security and data handling training will be refreshed annually.
- Other training will be refreshed as needed or recommended by the course provider.
- Where a role requires specialised training, this shall be sourced from an appropriately accredited provider, or otherwise one that meets the needs of that role / requirement Security.
- It is expected that all colleagues will participate in training and continual professional development (CPD) activities.
- Time will be provided for this
- CPD may take many forms, including attendance at events, webinars, face-to-face training courses, in-house training, reading journals / industry relevant blog posts / magazines / books, etc.

Record keeping

- A training record will be kept for each employee.
- Any training undertaken by the employee, along with relevant CPD, should be recorded along with the date.
- Managers are responsible for ensuring their team remain current with mandatory courses (security and data handling).
- Anonymised training records may be provided to customers as policy evidence.