Tritax Management LLP

IT Security Policy

Version	2.0
Classification	Internal - confidential
Effective Date	27/06/2022
Date for Review	27/06/2023
Document Owner	*Chase French*
Document Approver	*TML Operations Committee*
Document Summary	This document defines Tritax Management LLP's baseline security requirements and controls to support our Information Security Principles.

Tritax Management LLP
3rd Floor, 6 Duke Street St James's, London SW1Y 6BN
T: +44 (0)20 7290 1616 E: enquiries@tritax.co.uk www.tritax.co.uk

Table of Contents

Policy

It is the policy of Tritax Management LLP that information, as defined below, in all its forms - written, spoken, recorded electronically or printed - will be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. This protection includes security over the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for an appropriate period, according to the type of data. Holding periods appear in the Annex to this document. All documentation must be periodically reviewed for appropriateness and currency at a frequency to be determined by each entity within Tritax Management LLP.

Adherence to this Policy forms part of employees contract of employment and can be enforced accordingly.

Scope

- The scope of information security includes the protection of the confidentiality, integrity and availability of information.
- The framework for managing information security in this policy applies to all relevant individuals all involved systems
- This policy and all standards apply to all protected information and other classes of protected information in any form.

Responsibilities

- It is Tritax Management LLP's responsibility to ensure there are robust controls in place for IT security. A nominated individual is to ensure this security and report to the Partners who will be responsible for oversight.

Risk Management

- A thorough analysis of Tritax Management LLP's information networks and systems will be conducted on a periodic basis by Tritax Management LLP to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic - that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.
- From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be decided accordingly.
- Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

Information Security Definitions

Availability: Data or information is accessible and usable upon demand by an authorised person.
Confidentiality: Data or information is not made available or disclosed to unauthorised persons or processes.
Integrity: Data or information has not been altered or destroyed in an unauthorised manner.
Involved Persons: All staff. This includes employees, contractors, temporary staff, interns, etc.
Involved Systems: All computer equipment and network systems that are operated within Tritax Management LLP's environment. This includes all platforms (operating systems), all computer sizes (desktops, mainframes, smartphones etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification, the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format.

The following levels are to be used when classifying information:

- **Confidential Information**
  - Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.
  - Examples of Confidential Information may include: personnel information, key financial information, closed-period related information, confidential tenant strategy and planning, system access passwords and information file encryption keys.
  - Unauthorised disclosure of this information to people without a business need for access may violate laws and regulations (in particular, MAR – Market abuse regulation), or may cause significant problems for Tritax, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.
- **Internal Information**
  - Internal Information is intended for unrestricted use within Tritax Management LLP, and in some cases within affiliated organisations such as Tritax Management LLP's business partners.
  - Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.
  - Any information not explicitly classified as Confidential or Public will, by default, be classified as Internal Information.

- Documents intended as public information whilst in draft form, for example presentation material, prospectus material etc must remain internal until they are signed off as compliant and added to the Financial Promotions register.
- Unauthorised disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions. In the case of promotional material, this could make Tritax vulnerable to a mis-selling claim.

- **Inside Information**
  - Tritax Management LLP manages Funds listed on the FTSE indices and therefore has information from time to time which, if it were made public, would be likely to have a 'significant effect' on share price. The Company Secretariat is responsible for advising individuals when they are in receipt of inside information and how to treat it. For more information on inside information, refer to the Market Abuse Policy and the Dealing Policy.
- **Public Information**
  - Public Information has been specifically approved for public release by the nominated individual. Examples of Public Information may include marketing brochures and material posted to Tritax Management LLP's website.
  - This information may be disclosed outside Tritax Management LLP.

Computer and Information Control

All involved systems and information are assets of Tritax Management LLP and are expected to be protected from misuse, unauthorised manipulation, and destruction. These protection measures may be physical and/or software based:

- **Ownership of Software:** All software developed on behalf of Tritax Management LLP or licensed for Tritax Management LLP use is the property of Tritax Management LLP and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.
- **Installed Software:** All software packages that reside on computers, laptops, smartphones, tablets etc and networks within Tritax Management LLP must comply with applicable licensing agreements and restrictions.
- **Licensing:** Unauthorised copying of software or other copyrighted material such as photographs, music, books, videos or other resources for which Tritax Management LLP or the end user are not appropriately licensed is strictly prohibited.
- **Virus Protection:** Virus checking systems approved by the nominated individual must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorised to turn off or disable virus checking systems.
- **Patch Management:** Automated patch management systems will automatically deploy security and critical updates. Users are not authorised to turn off or disable patch management systems.
- **Access Controls:** Physical and electronic access to Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by staff, a variety of security measures will be employed as recommended by the nominated individual and approved by

Tritax Management LLP. Mechanisms to control access to Confidential and Internal information include (but are not limited to) the following methods:

- **Authorisation:** Access will be granted on a "need to know" basis and must be authorised by the immediate supervisor and application owner with the assistance of the nominated individual. Any of the following methods are acceptable for providing access under this policy:
  - *Context-based access:* Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.
  - *Role-based access:* An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organisation's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
  - *User-based access:* A security mechanism used to grant users of a system access based upon the identity of the user.
  - **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.
  - Users access the network with strictly controlled passwords. (Appendix 1 – Password Control Standards),
  - Users must secure their authentication control (e.g. password, token) such that it is known only to that user.
  - Users must log off or secure the system when leaving it.

- **Data Integrity:** Tritax must ensure that Confidential and Internal Information has not been altered or destroyed in an unauthorised manner. It should be able to provide evidence that such measures are in place. Listed below are some methods that support data integrity:
  - encryption of data in storage
  - Data Backup
  - Email backup and Archiving
  - Data access permissions
- **Transmission Security:** Technical security mechanisms must be put in place to guard against unauthorised access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:
  - encryption, where deemed appropriate
  - *Firewall as a perimeter security measure to the network*
  - *AV protection, server and device level*
- **Remote Access:** Access into Tritax Management LLP network from outside will be granted using Tritax Management LLP approved devices and pathways on an individual user and application basis.

Cloud based computing is also encrypted both on the transmission of data and at rest.

Further, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within Tritax Management LLP network.

- **Physical Access:** Controls need to be implemented and operated to prevent the physical loss, damage, theft or compromise of important assets. The following requirements are to be met at all locations that host Tritax Management LLP information systems.
    - Sensitive equipment such as servers, routers and the telephony control systems shall be protected from unauthorised physical access by locating in a secure communications room or data centre.
    - Data centres and communications rooms shall be protected from:
        - Extremes of temperature and humidity
        - Fluctuations in quality and failure of power supplies
        - Fire via smoke and heat detection alarms and fire suppression systems
        - Unauthorised physical access via a secure perimeter, with appropriate security barriers, recoded and monitored CCTV, intruder alarms and entry controls.
    - Power cabling shall be installed by competent installers to current legislation and accepted good practice.
    - Physical access to Tritax Management LLP sites and offices must be authorised by an appropriate manager and on a business needs basis.
    - Unauthorised staff or external contractors who require temporary access to restricted areas must be duly authorised by an appropriate manager and always accompanied by an authorised person. All such access must be logged.
    - Food, drink or other 'wet' items (e.g. coats and umbrellas) are not allowed in Tritax Management LLP Communications Rooms.
    - Equipment no longer required will be decommissioned and removed from Tritax Management LLP Communications rooms as soon as possible.
    - Doors into and within Tritax Management LLP's Communications rooms must not be left unlocked or propped open at any time.
    - Computer rack doors must remain locked and closed always except during maintenance.
- **Emergency Access:**
  The Tritax infrastructure is hosted in AWS data centers. For continuity this ensures that in the event of a disaster data is accessible from alternative locations. Tritax have backup copies of the infrastructure to different Regions. If the office was out of service, users would be able to log into cloud systems from home via company issued laptops and use exactly the same data and services as within the office. Employees may also log in via their own devices but strictly in accordance with the Tritax BYOD Policy.

Equipment and Media Controls:

The disposal of information must ensure the continued protection of Confidential and Internal Information. Tritax Management LLP uses licensed shredding firms to destroy physical data.

Electronic data can be permanently deleted from systems. The data may still be available but only via data back-up. The copy of this data is no longer available after the retention period of 90 days. Once the retention period for backup has passed (currently 90 days) the file/data in question is no longer available. Any request for accessing the data backups is audited and tracked via Priority One IT's ticketing system where an engineer will action the request. This allows Tritax to adhere to GDPR requirements to destroy data that is no longer required, as the availability of the data post-deletion is strictly controlled.

Tritax engage a Managed Service Provider, Priority One IT, who are able to assist in the secure disposal of hardware at the end of its life.

Removable Media:

Removable media is taken to include:

- CDs / DVDs
- USB memory sticks and flash memory (SD-Cards)
- Backup Tapes
- Any other removable media

Any removable media that is used to transfer / store Confidential Data must be encrypted.

If data is not classified, regard it as Confidential.

Users may not introduce non-Tritax Management LLP owned removable media to Tritax Management LLP systems without obtaining clearance from the Head of Risk & Compliance. This is to ensure that media is properly scanned for malicious software and that data can be loaded into an appropriate network location.

Any storage of personally identifying information on removable media must be strictly limited to only the information necessary and for the shortest time necessary. The media must always be encrypted and securely deleted when no longer needed.

If you have a requirement for an encrypted USB memory stick to use to carry data, please request this through the Head of Risk & Compliance who can arrange provision.

Disposal of Equipment & Media

Tritax Management LLP data can be compromised through careless disposal of equipment. All items containing storage media, e.g. hard disks, drives, etc. must be checked prior to disposal to ensure that any data and licensed software is removed or overwritten.

- All Tritax Management LLP IT hardware assets must be handed to the Head of Risk & Compliance or Line Manager for proper reassignment / disposal.
- All removable media (e.g. CD-ROMs) should be disposed of properly according to the sensitivity of the data that is stored upon it. For further information on disposal of assets, contact the Head of Risk & Compliance.

Data backup and Storage:

Back-up controls shall ensure that the availability of information assets can be sustained in line with the identified business requirements.

Data Transfer/Printing:

- **Electronic Mass Data Transfers**: Downloading and uploading, Confidential, and Internal Information between systems must be strictly controlled.
- **Other Electronic Data Transfers and Printing**: Confidential and Internal Information must be stored in a manner inaccessible to unauthorised individuals. Confidential information must not be downloaded, copied or printed.
- **Oral Communications**: Tritax Management LLP's staff should be aware of their surroundings when discussing Confidential Information. This includes the use of mobile telephones in public areas. Tritax Management LLP staff should not discuss Confidential Information in public areas if the information can be overheard. This is further covered in the TML Market Abuse Policy.
- **Audit Controls**: Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use confidential information must be implemented.
- **Evaluation**: Tritax Management LLP requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic information to ensure its continued protection.

Commented [JT|PO1]: Does this exist?

Contingency plan:

Controls must ensure that Tritax Management LLP can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain Confidential, or Internal Information

The IT Security Policy applies to all users of Tritax's information, this includes all members of staff and Partners. Failure to comply with Information Security Policies and Standards by employees, volunteers, and outside affiliates may result in disciplinary action.

Password Control Standards

Tritax Management LLP's requires the use of **strictly** controlled passwords for accessing Confidential Information (CI) and Internal Information (II).

Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for accessing the Tritax Management LLP IT Environment

Users are responsible for complying with the following password standards:

- Passwords must be a minimum of 8 characters.
- Azure AD joined PC's must have a minimum 6 digit PIN to unlock the device.
- Where technically possible Multi-Factor Authentication must be enabled.
- Passwords must not be re-used.
- Do not share your password with anyone, keep it confidential.
- Do not include a password in any automated log-on procedures.
- Do not use the same password for different services, in particular passwords for personal and Tritax Management LLP accounts must be different.
- Passwords should be randomly generated.
- A User who forgets their password must reset it by the Customer Support Desk, their Line Manager or, where possible, using self-service reset options.
- Users are personally accountable for any activity that takes place using their account.
- If you believe that your password has been compromised, you must change it immediately, and promptly inform the Head of Risk & Compliance.
- All pre-installed default, administrative, or test passwords must be changed or removed before any computer, device or system is used by Tritax Management LLP.

Document History

Revision Version	Revision Date	Description of Revision	Revision Author(s)
1.00		Initial Live Document	Catherine Fry
2.00	27/06/2022	Reviewed and updated	Priority One IT