Axeten Security Policy

Introduction

The purpose of this policy is to ensure that Axeten implements and maintains technical and organizational measures to protect Personal Information that it holds about customers, suppliers and employees and to provide security for the company assets and customer relationships.

Axeten security measures include a complex set of technical and organizational procedures and policies to ensure the best level of protection and security against unauthorized access, accidental or unlawful loss or destruction, modification, theft or disclosure of personal and/or corporate information.

Policy Statement

Axeten is committed to preserving the integrity of all systems and confidentiality all information that it holds and processes to operate its business, in compliance with the UK Data Protection Act 2018 (DPA), and EU Regulation 2016/679 (GDPR).

To read or download our GDPR compliance documentation, please go to

https://www.axeten.com/sites/default/files/files/axeten-data-protection-compliance-statement.pdf

Security Measures

So that we are compliant with the legal requirements for the safe keeping of data and information, and so that we comply with the IASME Cyber Essentials standards, Axeten has developed and implemented a series of organizational and technical measures.

On an organizational level, the following security measures are implemented:-

- Axeten has installed electronic access control to the company premises which allows movement to be controlled by a card reader system, so that;
- access to the company premises is achieved by swiping an authorised card through the card reader, and;
- access to the company premises is restricted to employees that have clearance to work there, and;

- access records are reviewed by management regularly, and;
- our after hours cleaners have access by dedicated swipe card and are vetted by our security company, and;
- we have human security on site during working hours and the building is locked down at night, and;
- video surveillance system at the main access, work area and server room; suppliers are not permitted to progress beyond the reception area unattended, and;
- access to the server room is restricted to designated approved personnel who are key holders, and;
- mobile storage media is forbidden (CD / DVD, USB Stick, Portable HDD), and;
- all employees access company computers with identification and authentication, and;
- all employees ensure that the company computer is logged off or locked when the work station is left unattended, and;
- Axeten performs pre-employment screening on potential employees to verify that they have the requisite skills and experience to carry out their roles, and that there are no legal issues or other matters which indicate that Axeten may be unduly exposed to risk, and;
- employees have been trained to ensure that all handling of personal data is compliant with DPA and GDPR. The training covers areas such as data protection principles, data subject rights, confidentiality and security of personal data. For additional information, please see our compliance documentation, and;
- all access rights of former Axeten employees are disabled within one working day of the date of their unemployment.

On a technical level, the following security measures are implemented:

- Axeten holds Cyber Essentials security accreditation,and;
- Axeten owns and operates a range of Virtual Private Networks for all external access to the WAN, and;
- SSH access is protected through key-based authentication deploying non-standard ports, and;
- firewall, only the ports that need to be exposed are exposed, and;
- use of a secure socket layer (https) on all Axeten websites, and;
- Axeten offers secure e-mail to all customers that require a secure service, and;

- the Axeten e-mail service is protected from threats at the server level, and;
- the Axeten mail server has an anti-virus engine for detection of trojans, malware and other malicious threats. The mail server checks all incoming and outgoing messages for malicious entities and automatically quarantines or deletes any suspicious message, depending on the threat level, and;
- internal connections are allocated secure ports, where access is restricted to specific IP addresses, and;
- strong passwords are applied to all systems and applications; we use a password manager to generate passwords which include numbers, special characters, lower and upper case letters, and;
- all hosted services are supplied by Axeten, so that the company has no reliance on any third party management service or application, and;
- Axeten hosted services have live monitoring, where each access is recorded in a log file that identifies the user with a time-stamp and record of the activity performed, and;
- all databases are incrementally backed-up to local storage, and;
- the Axeten back-up service cannot be accessed from the internet, and;
- a separate and secure Wi-fi network is supplied for guests and employees while on a work break, and;
- Bluetooth functionality is disabled on all company computers and devices, and;
- all data that is transferred is encrypted by default, and only unencrypted for delivery to a customer. Each customer has the option to request encrypted files, and;
- Axeten does not store customer data other than to administer a contract, with exception of research for customers , and;
- our deletion is set-out in the Framework Data Processing Agreement available at https://www.axeten.com/documents
- archives are stored on remote Virtual machines that are purchased and managed by the Axeten technical team. We backup to dedicated VMs and to a local drives.

Printed Document Security Policy

Axeten prints only what it is legally obliged to print. Other than contracts and agreements that have been printed for the purpose of applying a 'wet ink' signature, no other documents relating the the supply of a service to a customer are printed.

Printed documents are stored behind a locked door in the open plan facility where only the business manager or a member of the executive has right of access to the document repository. Printed documents are shredded before disposal.

Clear Desk and Clean Workstation Policy

Within the facility, a high level of security is maintained.

No personal smart phones are permitted in the work area. The company provides each employee with a dumb mobile handset for incoming emergency calls. Personal smart phones are stored in the cloakroom area and may be accessed, only in the break-out rooms and kitchen/dining areas. No personal USB sticks are permitted on the premises.

From their work-stations, employees are forbidden to access their private e-mail or social media accounts. Work-station logging is deployed. Logging acts an effective deterrent.

Hardware Disposal Policy

Where a printer, work-station, or server hard-disk or RAM is end of life, it is destroyed by the technical manger before disposal.

Changes to this policy

The effectiveness of this policy shall be monitored and reviewed annually, to reflect any changes to our security practices in accordance with changes in legislation, best practice and technology enhancements.

Please check this policy regularly. It is publicly available on https://www.axeten.com/documents