Security Overview

A guide to data security at AIMES Data Centres

www.aimesgridservices.com TEL: 0151 905 9700 enquiries@aimes.net

Contents

Protecting our clients data

AIMES provides specialist ISO 27001 data centre services to a range of industries, including Health, Pharmaceutical, Automotive, Professional Services and the Digital and Creative sectors. Our Data Centre information security management system (ISMS) was audited by BUREAU VERITAS and granted ISO 27001 certification in December 2007 (Certificate No: IND14.1053U), and has passed further annual audits each year between 2008 & 2016.

For us maintaining our ISO 27001 certification is just as much about running our data centre securely as it is about providing our clients with evidence of our compliance. At AIMES, we continually seek to improve our processes and systems to protect our business and to offer the best possible service to our customers.

The security regime and security standards that we adhere to can be summarised into four main headings:

- Information Security
- Data Centre Security
- Rack Security
- Staff Security

The following document provides specific details on each of these aspects of security at AIMES. If you still have any questions or queries regarding our security, then please do not hesitate to contact me using the details below.

Paul Langan

Paul Langan
Information Security Manager
0151 905 9700
Paul.langan@aimes.net

Information Security

ISO 27001 Information Security Management System (ISMS)

ISO27001 Certification is one of the most widely recognized independent global standards for security an organization can achieve. Certification to the standard involves a lengthy process whereby every facet of the business is examined from a security and process standpoint. All of AIMES business systems, technologies, processes and data centres have been carefully examined to ensure they are compliant to the highest security and management standards

We have implemented and had audited 135 individual security controls at our data centres to ensure security and to protect our client's information assets. These controls are grouped under the following categories:

Security Policy:
Organisation of Information Security
Asset Management.
Human Resources Security.
Physical and environmental security.
Communications and operations management.
Access control.
Information systems acquisition, development and maintenance.
Information security incident management.
Business Continuity Management.
Compliance.

Benefits to AIMES customers

- It provides basis for sharing information with other organisations in a secure manner
- A system for due corporate governance and a framework for legal compliance
- Ensures that we keep our customer's confidential information secure
- Managing & minimising our customer's risk exposure

We publish a "Statement of applicability" document each year which identifies the security controls chosen for our data centres, and explains how and why they are appropriate. If you would like to receive a copy ISO 27001 certificate or statement of applicability then please contact our Information Security Manager.

NHS IG Toolkit Compliant

AIMES meet the NHS criteria for information security and governance. AIMES (Organisation Code 8J121) complete the Department of Health's Information Governance Toolkit on an annual basis and our version 14 submission for 2016/17 has been reviewed and classed as meeting the NHS criteria for information security and governance (Level 3). Our status can be viewed on the IG Toolkit website via the IGT Reports section: http://tinyurl.com/pocrc32

G-Cloud Assured Supplier

AIMES is a G-Cloud Assured supplier and has been selected by the Government Procurement Service to deliver key elements of the G-Cloud program through the G-Cloud Framework Agreement. The G-Cloud Framework delivers fundamental changes in the way the public sector procures and operates ICT and allows all UK public sector organisations flexibility and freedom of choice in procuring cost effective, industry-leading cloud based services.

HSCIC accredited Commercial N3 Aggregator

In addition to the toolkit compliance, AIMES are an accredited and approved NHS N3 Aggregator and are entrusted by the Health and Social Care Information Centre (HSCIC) to monitor and maintain security of organisations connecting to the NHS' N3 Network on their behalf. Aggregator status is only awarded to organisations who have undertaken an enhanced set of security requirements.

Data Centre Alliance Class 3 Facility

AIMES has been named as the first data centre in the European Union to be awarded the new Data Centre Alliance (DCA) certification. Having successfully passed a rigorous data centre audit carried out by the industry body in conjunction with a member of its approved expert firms, Certios, AIMES was awarded the level 3 classification for its award-winning facility at Liverpool Innovation Park.

European Code of Conduct (EUCOC)

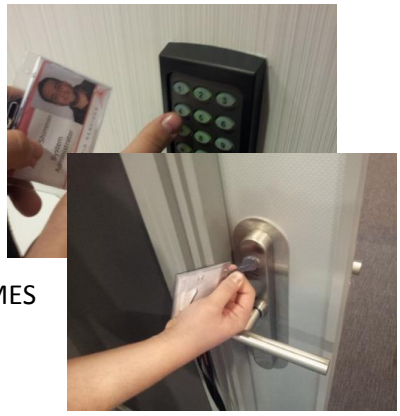
The European Code of Conduct has been created in response to increasing energy consumption in data centres and the need to reduce the related environmental, economic and energy supply security impacts. AIMES is an ethical and environmental conscious organisation that has adopted the best practices of the code and become an official participant. The EUCOC ensures that AIMES operational procedures regarding the management of a data centre are appropriate and the energy saving initiatives the company adopts meet the objectives of the European Union.

Data Centre Security

Secure Location

AIMES is located in a designated technology park, which is surrounded by secure metal fencing. There is a single point of entry, with a security lodge that is manned on a 24-hour basis. Within the security lodge guards control the external CCTV and perimeter protection cameras and carry out hourly foot patrols of the park.

Two form factor authentication & anti tailgating security lobby



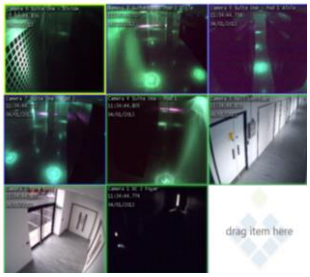
Access to our Kilby House Data Centre is achieved using secure 2 factor authentication access controls. Pin Code and personalised access control passes are used to secure entry. AIMES has eliminated the threat of tailgating by locating an anti-tailgating security lobby in between each of the two access controlled doors. The enclosed area has one door in the public area and another door into the secure area. In addition the 2nd door providing entry into the secure Data Centre area cannot be opened until the 1st door is fully closed and AIMES trained security personal have ensured that they have not been followed into the security lobby.

Tablet based Photo ID Access Control

Kilby House uses a Photographic ID Records Application for Visitor Sign in. All individuals are required to check-in at the reception upon arriving at the AIMES Data Centre. If it is their first visit, clients must produce identification. They will then be photographed and required to sign the Data Centres Terms & Conditions in order to gain access to their designated cabinet or cage.

On following visits they will be photographed again, and this will be checked against the photograph provided during their first visit to ensure it is the same authorized individual requesting access.

CCTV Monitoring



Data Centre CCTV monitoring of our data centre buildings 24 hours a day, 365 days a year is vital and we have put in place some of the very latest security technology to protect the data centre from any unauthorised access.

Rack Security

AIMES provide bespoke rack based security controls based on client's individual security requirements. Security controls can be applied at the Rack, Cage and POD level.

Secure Rack

42 U Standard Rack space (1.75 inches X 19 inches) provided in Kilby or Baird House. Cabinets are individually secured with key locks front and back or alternatively, can be secured by a proximity card system, if required. A cost effective solution for installation of customer's rack mounted equipment. We can accommodate single or multiple racks in a secure controlled access suite.

Secure Cage

Dedicated cages are ideal for organisations with a corporate security policy that specifies the need for a segregated caged environment. A private cage from AIMES is a cost effective way of securely managing your colocation.

The cages provide reasonable clearance, both front and rear, to allow technicians to perform maintenance on the systems. AIMES provide these cages on a custom built basis and they are suitable for two or more racks.

Secure Pod

A Pod is a secure segregated area in a suite containing a number of racks grouped together and which may or may not contain cages depending on the client's specific security requirements. Ideal for organisations who have a significant number of racks and require greater flexibility & Security than that can be achieved through utilising a cage. The Pod's are designed to your specific requirements in terms of multi layered security access controls, power supply and fast, resilient connectivity.

Your Pod is provided as a physical separated area with a solid but grilled wall in one of our suites and provided with its own separate entrance with swipe card controlled access.

Staff Security

To ensure the security of client data, AIMES has introduced controls that deal with staff security prior to, during and after employment. The procedures have been successfully audited and are detailed below:

- ***Prior to* Employment*:*** AIMES has introduced a number policies and procedures that ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

    - **Roles and responsibilities:** AIMES ensures that the security roles and responsibilities of its employees, contractors and third party users are defined and documented in accordance with the organization's information security policy.
    - **Screening:** AIMES ensures that background verification checks on all candidates for employment, contractors, and third party users are carried out prior to employment
    - **Terms and conditions of employment:** All AIMES employees, contractors and third party users have signed the terms and conditions of their employment contract, which state their and the organization's responsibilities for information security.

- **During employment:** AIMES has introduced a number policies and procedures that ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support the organizational security policy

    - **Information security awareness, education and training:** All employees of AIMES receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
    - **Disciplinary process:** AIMES has a formal disciplinary process for employees who have committed a security breach.

- **After Employment:** AIMES has introduced a number policies and procedures that ensure that employees, contractors and third party users exit our organization or change employment in an orderly manner.

    - **Termination responsibilities:** AIMES ensure that all responsibilities for performing employment termination or change of employment are clearly defined and assigned.
    - **Return of assets:** AIMES ensures that all employees, contractors and third party users return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
    - **Removal of access rights:** AIMES ensures that the access rights of all employees, contractors and third party users to information and information processing facilities are removed upon termination of their employment, contract or agreement.

Contact

If you want to discuss any aspect of our Information security policies and procedures then please contact us.

We will be happy to provide more detail on any of the elements and provide you with a more complete outline of our security policies, procedures and on-going strategy

ARRANGE A VISIT

If you would like to inspect our Data Centre facilities and security arrangements in person, please contact us to arrange a tour.

We will be happy to show you around the data centre and discuss any aspects of our policy in more detail with you.

Head Office: 0151 905 9700
London Office: 020 3598 8083

enquiries@aimes.net

http://www.aimes.uk