Hosting Q/A Index

Access provides management of the Alto hosting environment up to and including the application infrastructure layer. This includes all hardware, VMWare hypervisor software, storage, operating systems, SQL Database Servers, IIS Web Servers and RDS Servers. This document should be used in conjunction with **Access Security Q/A**

Control Subject

POLICIES

	POLICIES
Certifications	
Is there an established Information Security Management System (ISMS) (similar to that defined in ISO27001) in place in your organisation?	YES
Is the organisation PCI DSS compliant?	N/A
Are you Gcloud accredited	YES
Are you accredited on the NHS IG Toolkit	YES
Is your organisation Cyber Essentials certified or compliant	YES
Is your organisation HIPAA compliant	YES
Policies	
Do you have an Information Security Policy	YES
Is the Information Security Policy reviewed at least annually?	YES
Are all Information Security policies approved by management and communicated to all employees and relevant subcontractors?	YES
Have all the Information Security policies been reviewed and evaluated for their effectiveness, relevance and currency within the last 12 months?	
Is the ISMS subject to periodic Management reviews to ensure that its objectives are up-to-date, and aligned to the organisational objectives?	
Is compliance to these policies monitored?	YES
Do you have policies and procedures in place to allow for exceptions to the Information Security Policies?	YES

List of Policies / Instructions

Information Security Policy

Management Review Policy

Risk Assessment Process & Methodology

Mobile Security Policy

Information Security in project Management

Asset Inventory and Ownership

Email and Electronic Messaging Policy

Information Classification Policy

Internet Acceptable Use Policy

Acceptable Use Policy

Access Control Policy

Cryptograhic Controls and Key Management

Physical Security Policy

Removal of Information Assets

Antivirus and Anti malware Policy

Change Management & Control

Network Security Management Policy

Secure Development Policy

Supplier Relationships

Incident Management Process

Business Continuity Planning

Compliance with legal and contractual requirements

Records Management

Data Protection and Privacy Policy

Contact With Authorites

Remote / Teleworking

Comments	Associated documents
We have ISO27001:2013 Certification	ISO27001:2013 Certificate & Annex
We do not process Credit Cards	
Reference HJM98	
Not specifically but all the requirements for Cyber Essentials and more are covered by our ISO27001 certification - we are therefore compliant	
Relative to our US Operation	
	ISMS DOC 5.1 Information Security Policy
All policies are reviewed annually	
Within our SelectHR system and on our internal "Collaborate" site	
By all staff	
We have an acceptable risk process but it is not commonly used as we look for mitigation or termination rather than accept a risk	
	ISMS DOC 5.1 Information Security Policy
	ISMS DOC 5.2 Management Review Policy
	ISMS DOC 4.4 Risk assessment process & Methodology
	ISMS DOC 6.2.1.2 Mobile Security Policy
	ISMS DOC 6.5 Information Security in Project Management
	ISMS DOC 8.1 Asset Inventory and Ownership
	ISMS DOC 8.3 Email and Electronic Messaging Policy
	ISMS DOC 8.6 Information Classification Policy
	ISMS DOC 8.2 Internet Acceptable use policy
	ISMS DOC 8.1.3 Acceptable use policy
	ISMS DOC 9.1 Access Control Policy
	ISMS DOC 10.1 Cryptographic controls and key management
	ISMS DOC 11.8 Physical Security Policy
	ISMS DOC 11.12 Removal of Information Assets
	ISMS DOC 12.11 Antivirus and Malware Policy
	ISMS DOC 12.7 Change Management & Control
	ISMS DOC 14.1 Secure Development Policy

ISMS DOC 14.1 Secure Development Policy

ISMS DOC 15.1 Supplier Relationships

ISMS DOC 16.1 Incident Management Process

ISMS DOC 17.1&2 Business Continuity Planning

ISMS DOC 6.1.3 & 4 Contact with Authorities & Special Interest Groups

ISMS DOC 18.2 Records Management

ISMS DOC 18.6 Data Protection & Privacy Policy

ISMS DOC 6.6 Contact with Authorities

ISMS DOC 6.12 Remote Working _ Teleworking

THE ALTO DATA CENTRES

Telehouse

Certifica

- ICO registration Z8030846
- ISO/IEC 27001:2013 (Information Security Management)
- ISO 22301:2012 (Business Continuity Management)
- PCI-DSS v3 (Payment Card Industry Data Security Standard)
- ISO 9001:2008 (Quality Management system)
- ISO 14001:2004 (Environmental Management)
- ISO 50001:2011 (Energy Management)
- BS OHSAS 18001:2007 (Occupational Health and Safety Management)
- RMADS (Public Sector Compliance

Physical S

- Independent client card identification access system.
- The data centre is constructed of Block & Metal cladding
- Secure & monitored single person point of entry, physically guarded 24/7
- Integrated digital video camera surveillance.
- Proximity card access from the main Data Centre building to specific facilities management suites.
- Strict security processes in place to ensure delivery and loading of goods are secure.
- CCTV coverage for the perimeter, common areas and facilities management suites.
- Protected perimeter fence fitted with intruder sensing.
- Secure access procedures to ensure you and your nominated staff gain authorised access to the facility whenever you require, day or night.
- Windows are fitted with bomb film protection.
- Mantrap access to Data centre
- 2.3 metres min perimeter fencing with motion detection in place

Powe

- Four redundant HV power systems, from separate grids to each building on the Docklands site.
- N+1 redundant standby generators.
- Standby generators with a minimum of 24 hours autonomy at full capacity.
- 8 x 2.5MVA 11kV Generators.
- 2(N +1) redundant UPS floor by floor
- Redundant A & B power feeds to customer equipment

Cooli

- 6 x 2.7MW chillers N+2 configuration.
- Room Air Conditioning Units (RACUs) to provide down flow chilled water system at N+25%.
- RACU with bundled floor area and water leakage detection and monitoring.
- Hot aisle/cold aisle zone design.
- 800mm raised floor design with airflow space to provide the most efficient cooling.
- Free cooling operation in winter.
- Maximum external ambient temperature of 35 degrees Celsius dry bulb.
- The in-room units provide full function, closed control air conditioning, with cooling, humidity and de-humidification control.

Fire Suppr

- Data Centre areas are fitted with a fully addressable two stage fire detection system that monitors the under floor and the room.
- Detectors with 50% mix of optical and ionisation are installed split across 2 separate zonal-loops, to meet BS 5839, 6266, 5445 and 5588.
- Very early smoke detection alarms (VESDA) are installed throughout the facility.
- Dry sprinkler fire detection system to meet BS 5306, 3115 and with LFEPA approval.
- Gas suppression areas available for dedicated tenancy areas.
- Systems are designed to minimise any possible customer disruption and to ensure that any minor problems remain localised.

Connect

- System – Overhead proprietary cable tray system with multi-tier ladder rack or underfloor tray work
- Cross Connects – Enables customers to connect to other parties within an IBX data centre or IBX datacentres on a campus location using copper or fibre services
- Metro Connect – Extends choice and reach for carrier and network availability across metro areas
- Equinix Carrier Ethernet Exchange – Enables Ethernet Service Providers to interconnect to CENs and expand the reach of Ethernet services
- Equinix Connect – provides a bundled IP transit solution for Equinix customers who require a single source solution.

Equinix

tions

•SSAE16/ISAE3402 SOC-1 Type
• ISO 27001
• PCI-DSS
• FACT
• OHSAS 18001
• ISO 9001
• ISO 50001
• ISO 14001
• ISO 50001
• Renewable energy - 100% through utility green program

ecurity

• IBX datacentres are manned by onsite security on a 24x365 basis
• All doors, including cages, are secured with biometric hand geometry readers or access cards
• A silent alarm and automatic notification of appropriate law enforcement officials protect all exterior entrances
• CCTV digital camera coverage of the entire site, including cages, with archival system, integrated with access control and alarm systems
• Motion-detection for lighting and CCTV coverage
• All equipment checked upon arrival
• Visitors are screened upon entry to verify their identity, and in shared situations, are escorted to their appropriate locations
• Shipping and receiving area walled off from colocation areas

ɜr

Equinix IBX datacentres are designed with power systems that have built-in redundancy, full Uninterruptible Power Supply (UPS) systems with up to N+1 levels or greater, and backup generator systems in the event of a local utility failure.

Air Conditioning & Cooling

Precision HVAC systems cool the most demanding high-power deployments. The HVAC system provides appropriate airflow, temperature, and humidity to provide optimum conditions for equipment operation and to minimise downtime due to equipment failure.

ng

Precision HVAC systems cool the most demanding high-power deployments. The HVAC system provides appropriate airflow, temperature, and humidity to provide optimum conditions for equipment operation and to minimise downtime due to equipment failure.

ression
HI-FOG pre-action water mist triggered via double knock detection of fire alarm
tivity

OPERATIONAL SECURITY

	Response
Hardware	
Are default Passwords changed on commission of hardware	YES
Are management Interfaces accessible only via a management network VLAN	YES
All unused ports are set to administratively disabled by default	YES
Are all your operating systems currently supported	YES
Are the following components subject to policy by default? -	
• Disablement of all unused services/protocols	YES
• Disablement of all unused accounts (Guest etc.)	YES
• Renaming of used Default Accounts i.e. Administrator Account	YES
• Removal of unused software components	YES
• Installation of Client Firewall Components	YES
• Installation of File System Anti-Virus	YES
• Installation of centralised Patch Management Software	YES
• Installation of centralised Monitoring Software	YES
Are all system user accounts assigned uniquely to the individual ?	YES
Are system priviledges controlled and ensured as being appropriate for the function being perform	YES
Do you ensure that production systems are logically seperated from development and test systems	YES
Do you update 3rd party software components used to provide the service regularly	YES
Do you have a policy or procedure that controls changes to the environment ?	YES
Are all firewall and router rules reviewed at least every six months to ensure the rules are still required?	YES
Are changes to firewall rules logged and do the logs identify the administrator performing the change and when the change occurred?	YES
Are console administrative ports restricted to authorised staff members?	YES
Are network diagrams, data flow diagrams, and physical/facility security diagrams maintained and restricted to authorised personnel?	YES

Are new systems and devices configured with current security updates/patches and hardened before being put into production?	YES
Are production system audit logs retained for a minimum of 6 months?	YES
Are routine quarterly scans performed to detect unauthorised wireless network connections or access points even if wireless technologies are not permitted?	YES
If a virtual private network (VPN) is implemented, is a process in place to ensure that access by non-employees (consultants, vendors, support personnel etc.) is reviewed at least every 12 months?	YES
Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?	YES
Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyperjumping, etc.)?	YES
Do you allow for administrators or employees to use personal devices to manage systems or provide support of the production environment?	No

Comments
And stored off-site in encrypted format in an encrypted database requiring 2FA Authentication
Also subject to 2FA authentication (IPSEC VPN)
All unused ports are set to administratively disabled by default
Yes We do not operate for production usage any unsupported operating systems for security and compliance reasons they include Microsoft Windows 2012 R2, Microsoft Windows 2016, Redhat Enterprise Linux, Centos and Ubuntu server.
All accounts are uniquely assigned and are assigned permissions appropriate to the function being performed using the least priviledge methodology
Permissions and systems rights are managed through active directory where possible by the Access Control Team. Access and rights to systems and services are provided on a “role based” methodology only. Access to systems and services above role based entitlement has to be agreed by the user’s manager and authorised by the system / service owner. Test environments are provided as a separate installation / database although they may exist on the same server All 3rd party software components are updated quaterly in respect of normal updates and within 14 days for critical updates
All operational systems, services and applications are subject to Change Control. All staff are responsible for submitting completed change requests to the change authorisation board (CAB) using the change request form. Change request forms, before submission to the CAB must be peer reviewed and pre authorised by the appropriate system service owners and team managers. All changes are recorded, tested and verified prior to implementation (where possible) and are communicated to relevant members of staff and users as appropriate.
Yes, access control is defined by Role-Based Access Control (RBAC) and limited to authorised network ranges or MFA authentication

Yes, hardening is at a level designed by Access in line with the 14 principles of computer security and CIS guidelines. Additionally systems are enforced via VMWARE Configuration Manager applications on a pro-active basis.

Retention levels vary dependant on systems in use. System logon events and privileged access logs are retained for 12 months as a minimum.

No, wireless connections are not available in the data centre- Protection against wi-fi is built into the physical infrastructure

Yes, directly connected access (VPN’s / dedicated lines) & Management networks are segregated, encrypted and limited to specific operational ports only. Both are subject to risk assessment and authorisation, and periodic review (minimum of 90 days).

We utilise PVLAN and separate management and hardening controls to protect against these attacks.

No - all connections to the environment is restricted to company provided devices by policy.

Associated documents

NETWORK SECURITY	Response
Antivirus	
Do all Windows Operating Systems have resident supported Anti-Virus installed that is controlled and managed via a centralised management portal	YES
Are Definitions updated from a centralised location every 5 minutes against local and supplier repositories	YES
Are all servers set to run a scheduled AV scan of all files and settings regularly	YES
Does Access Alto manage alerts from the AV software	YES
Do you have controls in place to prevent the AV software being disabled or changed	YES
Firewalls	
Does the basic design of your network utilise 1 or more firewalls to segment the network into a DMZ/Presentation Zone and a Secured Zone?	YES
How do you protect internal systems from network threats	
Do network security products used by the provider (specifically firewalls) have Common Criteria certification? If so at which level?	YES
Do you regularly review firewall rules	YES
Encryption & Pseudonomisation	
Is Data encrypted in transit	YES
Is Data encrypted at rest	YES
Do you have procedures to support split encryption key custodians so no individual (or, in certain cases, no two individuals) have access to a functional encryption Key?	YES
How is Pseudonymisation managed in the Access Alto enviroment	
Security Testing	

Does Access Alto carry out regular Penetration testing	YES
Does Access Alto carry our Vulnerability scans?	YES
Are security controls enforced throughout the environment and how is this performed	YES
Intrustion Detection	
Does Access Alto run intrustion Prevention services on its environment	YES
Is there a process to maintain and/or update the network IDS or IPS signatures to ensure current vulnerabilities and exploits are monitored within the network?	YES
Does Access Alto logically separate environments when delivering services to customers	YES
Does Access Alto perform any network flow monitoring for performance or security reasons	YES

Comments	Associated documents
alerts are generated by non-compliant devices e.g. devices that have not updated recently or have un-acknowledged alerts	
This runs every night	
We have centralised alerting to our Network Operations Centre and Security Officer from managed clients	
All resident AV has Tamper Protection deployed to prevent the disablement or alteration of local policies without authorisation from the central management portal	
This is performed via Cisco ASA Firewalls with IDS (Fire-Power) modules connecting to a switching fabric to provide logical seperation. Internal network zones are protected by VLAN and VRF zones and host based firewall controls.	
Through a combination of host based firewalls at the Guest Layer, Distributed Firewalls to protect internal East-West Traffic, and network based Access Control rules and firewalls to protect North-South Traffic.	
We use Cisco ASA appliances. All external firewalls are Common Criteria EAL4+ certified	
All rules are reviewed quaterly by our Network Administration Team, Additionally internal switching configuration is enforced through the ue of ACI Based contracts	
With SSL offloaded on Brocade Traffic Managers, supporting TLS 1.2.	
SSL certificates are signed by a commercial root CA with 2048-kit keys and AES256 encryption.	
All data is encrypted at rest using industry standard multi-node 256bit encryption and supports authentication and secure erase	
Management and storage of the keys is handled by staff who are not involved in the active management of systems therefore there is segregation of responsibility – No staff have access to the keys unless they require a particular key as part of their job role.	
Pseudonymisation techniques employed against Database Names and Company Information using an externally held coding structure.	

Access carry out penetration (Pen) tests in addition to the standard quality assurance processes that form part of our agile software development. The penetration tests are undertaken by an external Crest Registered 3rd party company who are specialists in the field of Internet security. The Pen tests are segregated between infrastructure (networks, firewalls, ports etc.) and individual application tests (cross site scripting, SQL injection etc.). Penetration tests are scheduled to occur regularly and dovetailed with major software version releases.

Access also carry out weekly automated vulnerability scans from a CREST approved supplier. This is an additional level of defence to automatically check if changes to the environment have exposed new vulnerabilities.

Through a combination of internal Group Policy enforcement at the Guest Layer and VMWare Configuration Manager at the underlying Hypervisor Layer

IPS Service analyses at the firewall level all traffic into and out of the environment. It performs this by inspecting the nature of the network data for known malicious or unwanted patterns of network behaviour.

Internal / External Vulnerability scans are undertaken monthly to ensure vulnerabilities have not been introduced to the systems and the effectiveness of the patching cycles.

Environments and trust zones will be logically separated by employing Ethernet 802.1q VLAN technology and will require supporting rules within the firewalls to permit access as deemed necessary. Data between zones is denied unless specifically allowed.

Access uses a combination of physical and logical segregation methods to segregate information, systems, services and users

All network flows are monitored actively through our border exist devices. Monitored traffic is analysed through our aggregation engine for anomolous traffic either by destination or volume

ACCESS CONTROL	Response
Access is provided on a “least privilege” basis, by role. Elevated rights can only be given with business justification, and requires Director Level approval. Elevated access has an expiry date or is reviewed every 3 months. All other access is reviewed at 6 monthly intervals or annually based on classification of system	
Does Access Alto enforce policies to control/limit/permit access to computers, services and systems?	YES
How are user accounts stored in the Alto Hosted Environment	
How are user accounts stored in the Alto Hosted Environment	
Are all system, application and device password files encrypted using an industry standard encryption algorithm?	YES
Are default system accounts (e.g., guest, administrator) disabled or renamed upon initial system build?	YES

Is there a function responsible for administration of Access Control	YES
Are accounts created with Pseudonomisation	YES

Data Logs and Auditing

Does Access Alto ensure that access to systems is audited and logged?	YES
What is the information used for?	

Comments	Associated documents
Access Alto uses a comprehensive Group Policy implementation in order to apply and enforce these policies The policies are applied in a hierarchical model that are used to define access rights, interactive logon privileges, software restriction policies, folder redirection and firewall policies	
• SQL – user accounts are stored as security accounts tied to the specific database (SQL Authentication) • Application – user accounts are stored within the application you are accessing. • Windows Active Directory – an industry standard authentication platform from Microsoft	
S**QL** Access to SQL account is restricted to Access System Administrators and Database Administrators only The application controls this access by assigning roles to users which defines what users are allowed to access and administer. **Active Directory** In the case of Active Directory, access is restricted to Access System Administrators, Software Support engineers and Implementation Engineers only. Access is controlled by Group Membership and is subject to audit and change control procedures requiring manager level approval. **Application** In the case of user accounts stored in the application, these are subject to the controls present in the application and are beyond the scope of this document. Access Alto engineers do not have access to these accounts or Super-User access to system.	
Yes, Access use encryption techniques (TLS 1.2 256bit) for all sensitive information as appropriate and as such the risk of interception is minimised.	

Active Directory
The management of the user accounts in Active Directory are under the management and control of Access System Administrators, Software Support engineers and Implementation Engineers only
SQL
Creation, amendment or deletion of SQL User Accounts is subject to change control authorisation and is conducted by one of the groups above. There is no provision for self-service for SQL accounts
Applications
The management of user accounts in the Application is not under the control of Access Alto

User accounts are created with a level of pseudonominisation by default. Tenant OU using secure coding / user accounts are prefixed with a unique code / SQL customer codes are stored off system in a secure location and are unique to the customer.

Using our SIEM platform installed on the Alto platform. This information is used in combination with other collected information to monitor access to the environment by all users, potential breaches or change in system state or attacks on the environment (for example multiple failed logons)

This information is used for Security Audit purposes only and in order to maintain forensic and operational controls this information cannot be amended or deleted once it has been collected.

BUSINESS CONTINUITY	Response
Two datacentres run in an Active-Active mode, all services run within the primary active datacentre and can be failed over to the active secondary datacentre automatically. This gives an enterprise level of resiliency which is far in excess of the traditional cold standby disaster recovery datacentre. The solutions operate in a near continuous state across both datacentres minimising data loss in the event of a total data centre blackout. This is achieved using Zerto Virtual Replication and VMWare vSphere being delivered as a service to the Access user. The connections between the two datacentres are based upon Dark Fibre DWDM (Dense wavelength division multiplexing), this provides an exceptionally fast connection with a low latency of less than 10ms.	
Does Access Alto have a back up strategy for its clients	YES
Does Access Alto conduct regular restore testing	YES

Does Access Alto ensure ongoing the performance and reliabilty of the platform?	YES
Does Access have processes to ensure the compliance and reliability of the platform	YES

Comments	Associated documents
	Hosting BCP & DR Information
The solution has been designed to cater for disasters ranging from a database restore through to a complete datacentre outage. The backup architecture used is critical to being able to respond to the diverse set of restore scenarios that may be required. The design of the architecture means that all data is simultaneously available in both the primary datacentre and the secondary datacentre meaning data is always backed up to another geographically diverse site. All Servers are backed up on a daily basis at 10pm as standard. For SQL Servers we also operate 15 minute transaction log backup in addition to the nightly backup. These backups go directly to storage in the DR Datacentre to ensure off-site availability. Backups are stored on disk, in a multi tenancy data vault and are encrypted at rest. The Retention Period for all backups are shown below 15-min SQL 28 days Daily 28 days Weekly 3 months Monthly 1 year for non-financial data /7 years for financial data Replication - The virtual machine images and virtual machine storage is replicated between the two datacentres using the Zerto Virtual Replication.	
Weekly	

In order to maintain the performance and reliability of the platform We operate a number of server monitoring platforms that collect system state information about the servers and components deployed onto the Alto platform. Information collected is aggregated to a central monitoring platform that is restricted by RBAC control and also generates email and API alerts on non-conformance to both internal and external systems.

In order to maintain the operational effectiveness and compliance of the platform we monitor the platform from the Hypervisor level through the usage of VMWare Native Reporting provided by VMWare VRealize, VMWare Operations Manager and VMWare Log Insight.