oneeducation

Capita One Hosted eStart Datacentre Security

April 2018

Datacentre Security

CAPITA

Revision History

Version	Published on
1.0 – April 2018	4/18/2018

Doc Ref

Capita One Hosted eStart Datacentre Security/April 2018/2018-04-18

www.capita-one.co.uk

Contacting the Service Desk

You can log a call with the Service Desk via the Customer Service tool available on My Account.

Providing Feedback on Documentation

We always welcome comments and feedback on the quality of our documentation including online help files and handbooks. If you have any comments, feedback or suggestions regarding the module help file, this handbook (PDF file) or any other aspect of our documentation, please email:

onepublications@capita.co.uk

Please ensure that you include the document name, version and aspect of documentation on which you are commenting.

Contents

01 | Hosted eStart Service Overview

Capita One hosted eStart is delivered as a Software as a Service (SaaS) solution through colocation hosting from Tier 2 and Tier 3 + datacentre facilities situated in Hampshire and Nottinghamshire, United Kingdom.

Colocation and supporting services are delivered by third party suppliers from the Capita approved supplier list, which ensures that our supply chain meets with ISO 27001 and ISO 9001 certifications, mirroring the Capita ISO 27001 and ISO 9001 certifications attained.

Capita One eStart is a browser-based solution, accessible via Internet Explorer and a fully qualified domain name (FQDN). All traffic between the customer end user and the Capita One hosted eStart application is encrypted over an SSL connection.

All equipment utilised for the delivery of the hosted eStart solution is owned outright by Capita and service delivery is managed from the Capita Bedford office by the hosted eStart team. Access to Capita's colocation assets is restricted to Capita staff, with limited physical access extended to supplier colocation support staff for operational and remote hands support activities.

Remote hands support is available to the Capita the hosted eStart team upon request where supplier colocation support staff act under instruction of the Capita hosted eStart team as our eyes and hands on site. Supplier colocation support staff have no requirement and are not permitted to connect to or attempt to login in to hosted Capita assets.

02 | Datacentre locations and facilities

Datacentre facilities are owned and managed through our approved supplier and service provider, located in Hampshire and Nottinghamshire, United Kingdom. Both datacentres are housed within secure facilities.

Datacentre sites are protected by comprehensive internal and external CCTV, monitored locally and externally. Patrolling security guards and supplier colocation staff are based on site at both facilities around the clock, 365 days per year. All areas of the datacentre facilities are secure, access is restricted through key card and biometric entry systems.

Bridge rooms are in place on each site which provides an air-gapped room that will not let you beyond the internal airlock door to the data floor until the external airlock door is closed and secure.

Power is delivered into the datacentre via redundant feeds with generator backup on auto failover. UPS serve each data floor to provide around twenty minutes of service at full capacity. UPS are tested weekly using automated testing and the supplier has maintenance contracts in place with the UPS vendors.

Two generators are connected to each datacentre and can operate for up to five days without refuelling. Generators can be refuelled whilst in use by on site fuel bowsers with capacity upwards of 10,000 litres. Priority fuel supply contracts have been put in place by the supplier for same day fuel deliveries when bowser fuel levels reach 50%.

Integrated fire detection and suppression systems cover office and datacentre space. These are FM 200 or Inogen Fire suppression based in addition to portable equipment. Activation of the fire suppression system is designed to extinguish fires by reducing the oxygen level in the datacentre, whilst allowing the safe running of hardware.

HVAC systems maintain an average temperature of 19 – 20 degrees C, average humidity is around 25% and all areas are monitored throughout the day.

Connectivity between the hosted Capita hosted network and the supplier infrastructure is provided through Cisco firewalls in a resilient configuration. The configuration permits SSL connections from the Internet to access the hosted eStart SaaS solution, everything else is blocked.

03 | Security Governance and Policies

Capita has a significant number of Information Security Policies and Standards that cover ISO 27001 clauses and controls. Compliance is enforced by the Divisional Information Security Directors and Group Risk with a local Compliance Team and Information Security Organisation documentation for all key individuals, roles and responsibilities.

Access to customer data hosted in the datacentre is controlled to ensure that the Information security controls are suitable for the privacy of customers and individuals personally identifiable information and are in accordance with the eight principles of the UK Data Protection Act 1998 and Capita Children's Services ISO 27001 certification. The Capita plc Baseline Information Security Policies and Standards have also been mandated by the Capita Board as the minimum required level of security which all Capita business units must attain and comply with.

Incident, configuration and change management

Capita maintain the assets which make up the solution using ITIL v3 incident, problem and change management processes which aligns to the ISO27001 and ISO 9001 standards. No configuration items are added or changed without the appropriate review which includes deployment and testing of the change outside of the production environment to ensure that the risks and impact are appropriately managed prior to delivery of the change into live.

Vulnerability Management

A significant number of Information Security Policies and Standards that cover ISO 27001 clauses and controls are adhered to for the triage and management of vulnerabilities. Threat information is gained from multiple sources including suppliers, software vendors, NIST and Capita Group; classifications are based on Microsoft Security Bulletin Severity Rating and CVSS score. Severity based action is taken within hours for critical, 7 days for important and 40 days for lower severity risks.

Staff Security

Staff screening performed conforms to BS7858:2012. Annual training for compliance with the data protection act is mandatory for all Capita staff and compliance with Capita Group Policies required for ISO 27001.

One Product Suite Security Testing Policy

At Capita One we take the security of our solution and the data held within it, very seriously. To help ensure the highest standards, our approach to security broadly falls into the following categories:

□ Architecture reviews – trying to identify where in the architecture could be insecure.

□ Design reviews – trying to identify where the design could be insecure.

□ Security reviews – ensuring we have followed industry security standards.

□ Penetration testing – performing vulnerability testing on the One product suite, and infrastructure

For each One release, every project must consider how to apply all of the above and provide internal evidence of the outcomes. We must resolve (fix or adequately mitigate) all issues and vulnerabilities found prior to releasing software, with the following exceptions:

a. a vulnerability that has no real world risk due to the functional nature of our system (e.g. exploiting the vulnerability only gives access to data that is public anyway, or “so what?” technology information disclosure); or

b. a vulnerability with low risk information disclosure (e.g. TCP packet timestamps) that require disproportionate effort to resolve; or

c. other exceptional circumstances that have been disclosed to and agreed with stakeholders.

If we decide to release software with exceptional outstanding or partially mitigated vulnerabilities (item c above) then:

a. a committed plan for a full fix must be agreed and in place (the issue is placed on the project development backlog); or

b. the residual risk must be logged on the divisional risk register.

To ensure we meet governmental guidance (https://www.gov.uk/government/publications/ithealth-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance), every release of our software is installed on hardened servers and undergoes vulnerability testing.

Vulnerability testing is performed by industry recognised suppliers of security testing services. All testing suppliers must be CREST (http://www.crest-approved.org/) or Tiger Scheme (http://www.tigerscheme.org/) accredited.