Security management for the student voter registration service

Author: Rhys Smith (chief technical architect, trust and identity)

Version 1.0 - dated: 21 June 2019

1 Introduction

This document describes the security of the student voter registration service (SVR). Its structure is based on the Cloud security principle from the National Cyber Security Centre.

SVR is deployed in a hybrid cloud model – all components that users interact with are hosted in the cloud on AWS, but all data is stored in Jisc’s own secure data centres with a secure link between the two.

The service operates by identifying the Electoral Registration Office that a user of the service needs to register with, collecting the required voter registration information and passing that information to the relevant Electoral Registration Office.

For the purposes of data protection law, Jisc is a processor of the personal data collected by the service, and the home organisation of the user is the controller. Full details can be found in the Terms & Conditions documents for the service, found on the Jisc SVR web page.

2 Data in transit

All communication between the user’s agent (browser) and SVR application is over encrypted SSL (TLS) connections. It ensures that sensitive information can be transmitted securely. Jisc follows best practice (e.g. as in the PCI DSS Sub-Requirements 4.1) and does not commit to using particular versions of TLS or particular ciphers as this may be limiting as new weaknesses are discovered. Instead we commit to achieving and maintaining a grade of at least A when tested by SSL Labs. You can view the current status via SSL Labs.

Jisc publishes CAA records for the jisc.ac.uk domain which limits the acceptable Certificate Authorities allowed to issue SSL certificates for that domain to those Certificate Authorities used by Jisc.

Within SVR, any transfer of data between AWS and Jisc infrastructure is conducted over a secure IPsec site-to-site connection between the AWS infrastructure and hardware encryption devices on the Jisc infrastructure.

3 Asset protection and resilience

Physical location and legal jurisdiction
The electoral registration website of the SVR service operates in Amazon Web Services (AWS) from a UK-based AWS data centre. All data storage and transformation operates on Jisc infrastructure within its own UK-based secure data centres.
All data provided to the electoral registration website of the SVR service only ephemerally transits AWS, being ultimately stored within Jisc’s data centres.

**Data centre security**
All systems physically located within datacentres operated by AWS are managed in conformance with the requirements of ISO 27001, providing Jisc and our customers with assurances of the security of the data centre and virtualisation aspects of the service. The security of the operating systems and application stack are managed by Jisc.

The security of the operating systems and application stacks physically located within Jisc's own secure data centres are managed by Jisc in line with best security practices.

Staff at Jisc are subject to our Secure Working Practices Policy that covers the physical security of information when working in an office or remotely at other locations.

**Data at rest protection**
Data is encrypted at rest within SVR via Full Disk Encryption of all volumes of the Virtual Machines running the SVR database.

All ERO account’s passwords are hashed using bcrypt with per-password salts. Jisc is responsible for the management of all cryptographic keys and material involved within SVR.

**Data sanitisation**
Jisc ensures all electoral registration data submitted is securely erased within 30 days of submission, apart from non-personally identifiable statistical usage information required for tracking service statistics.

The SVR service has a data retention policy that means that all systems are backed up daily and all backups are held for three months, This, however, excludes the core personal data submitted by users for inclusion on the electoral roll. This data is excluded from the daily backups to ensure that particular data is not held by Jisc for more than 30 days.

Backups are stored securely in a Jisc secure data centre located in the UK. After three months the backups are deleted and physically destroyed.

**Physical resilience and availability**
The SVR service runs over three availability zones in AWS (EU London) in an active-active high availability configuration using AWS Elastic load balancing and Auto Scaling Groups.

The performance of the service depends on the use of the system and AWS. We monitor the system’s performance routinely and have automated alerts. In the event of high traffic, AWS will automatically increase resources quickly to meet demand.

SVR is protected from DDoS attacks by services provided by Amazon and by Jisc.

**4 Separation between users**
SVR has three types of users: students submitting data; EROs retrieving data; and administrators. Each of those three components run entirely separately on distinct systems. Within each system, the software has controls and checks in place to ensure sessions are kept separate.

Jisc conducts periodic penetration testing of the network environment, operating system, and applications; all alerts are acted upon promptly. Jisc’s cyber security penetration testing service is CREST-accredited.

**5 Governance**
Jisc operates an Information Security Management System (ISMS), certified to ISO 9001, and many of the processes and policies used to operate SVR, and by Jisc staff, are part of the ISMS. Jisc provides a number of services that are certified to ISO 27001; SVR will be a part of this.
Jisc has an established process for handling information security incidents including data breaches. Should an incident occur, it will be handled according to this process and in line with current data protection legislation. If an incident has an impact on the security of information secured in SVR then Jisc’s Senior Information Risk Owner (SIRO), will make decisions as to whether and how customers and the Information Commissioner’s Office are notified.

6 Operational security

Configuration and change management
Jisc is responsible for maintaining the security of the operating systems and application stacks used to provide SVR.

Jisc’s Trust and identity services operate under an internal change control system as part of our planned ISO 27001 certification, where all changes are categorised, approved, implemented, monitored, and closed.

Emergency changes for critical issues, such as critical vulnerabilities, can be fast-tracked to ensure the overall security of SVR.

Vulnerability management
Vulnerability and patch management is carried out on a regular schedule accordance with our vulnerability management processes. The systems are regularly scanned for vulnerabilities by automated systems and are subject to periodic penetration testing of both the network environment, operating system, and application. All issues discovered are prioritised and accordingly addressed.

Protective monitoring
All SVR systems have internal application level monitoring, machine level monitoring, cloud monitoring, and external availability monitoring. Diagnostic logging is streamed off-server to a centralised log aggregation facility for the purposes of proactive monitoring and post-incident analysis.

Incident management
All incidents will be managed through internal processes.

Jisc encourages third parties to work with us to resolve any security vulnerabilities discovered – please e-mail information.security@jisc.ac.uk for more information.

Communications related to breaches will arrive through Jisc’s normal communications channels. Jisc will never ask you to provide passwords and other authentication information by e-mail.

7 Personnel security

All new staff at Jisc, including casual staff, are given a contract of employment containing a confidentiality clause and are made aware of their responsibilities toward personal data as part of their induction process. All staff at Jisc are subject to our “Secure Working Practices Policy” that communicates their responsibilities towards information security, as well as providing advice and guidance on common security threats. All Jisc staff involved with providing the SVR service are provided with information security training.

8 Secure development

All elements of the SVR service, from overall architecture to application implementation, were conducted by staff highly experienced in secure design; security was a fundamental requirement of the service and all design and implementation used this as a core principle.

The overall application and systems architecture was independently reviewed by experts within the cyber security division within Jisc.

9 Supply chain
No third-party suppliers are used in SVR, other than for infrastructure provision as previously discussed.

10 Secure user management

Authentication of users to management interfaces and support channels
When subscribing to the service, data providers (e.g. Universities) and consumers (i.e. EROs) go through the standard organisational checks conducted by Jisc, and contacts within each organisation able to request changes and report faults are registered. This process is all part of the ISO 9001 and forthcoming ISO 27001 certification.

Jisc publishes SPF and DMARC policies for the jisc.ac.uk domain. Operators of e-mail systems wishing to improve the reliability and trust of e-mail delivery from SVR can use these DMARC policies to identify authorised senders for this domain.

Separation and access control within management interfaces
Physical, logical, application and network access-control for all Jisc managed systems that hold personal data are managed on a least-privilege, need-to-know, basis.

All management interfaces are protected in several ways, including strong authentication requirements, access control, and have been penetration tested by Jisc’s CREST-accredited cyber security penetration testing service.

11 Identity and authentication

All users of the SVR service’s submission component authenticate securely and pseudonymously using their home organisation’s credentials via federated access using the SAML protocol enabled by the UK Access Management Federation. No local credentials for SVR are required. All members of the UK federation have agreed to the service’s Rules of Membership.

All Electoral Registration Officers (EROs) enrolled into SVR to consume the data are assigned usernames and passwords. The password must be changed on first login and be suitably complex.

SVR issues a cookie to reference session information when users log in. The session cookie does not include user information, is strictly necessary to fulfil SVR services, and is not retained once the browser is closed. The AWS Load Balancers also set a time-limited cookie that maps a session to a particular instance; this contains no user information and is also strictly necessary to fulfil SVR services.

12 External interface protection

All external interfaces to SVR are hosted on public cloud with appropriate protections previously in place (see previous sections for details). All internal interfaces are secured with TLS for authentication and encryption, firewalls for minimising access, and comprehensive log management for analysis.

13 Secure service administration

Access to SVR systems and to the data stored within SVR is strictly limited within Jisc to SVR technical teams. This access is only permitted when necessary for the investigation of operational issues, or when required by law.

Jisc conducts periodic penetration testing of the network environment, operating system, and applications; all alerts are acted upon promptly. Jisc’s cyber security penetration testing service is CREST-accredited.

14 Audit information for users

Comprehensive audit information is available to Jisc for the use of SVR but will not be disclosed to third parties, other than as agreed for reporting purposes to subscribers to the SVR service.

15 Secure use of the service
All users of the SVR service’s electoral submission website component are subject to their home organisation’s Acceptable Usage Policies, and their home organisation is subject to the UK Access Management Federation’s Rule of Membership.

All ERO users must keep their account details secure and MUST download records via the portal at regular intervals - any data not downloaded within 30 days of submission.