ISAIC Security Information Summary

Operating as a unit within the University of Alberta ensures that all applicable university cybersecurity policies and best practices are followed. Periodic security assessments are undertaken with the university CISO (Chief Information Security Office). The following table summarizes various security features and standards implemented within ISAIC's environment (Infrastructure as a Service). The purpose of this table is to provide information to clients regarding ISAIC's security standards and capabilities. The table is largely based on a security evaluation developed for post secondary research institutions by EDUCAUSE (HECVAT), for purposes of evaluating vendor cyber-security.*

Security Control	ISAIC Environment
Access Control	ISAIC provides infrastructure-as-a-service (IaaS) to multiple clients. Each client is provisioned a dedicated VM (virtual machine) within the ISAIC cloud. Each client is provided full administrative access to their environment, and is able to limit/grant access to user accounts and applications within the environment that they maintain and manage. The provision of dedicated VMs means that there is a sufficient level of abstraction within the ISAIC cloud to ensure that clients are not able to access any other VM other than the one(s) assigned to them. Provisioned VMs are accessed by clients using public key infrastructure (PKI). Secure encrypted connections are established through SSH to access the client VM, and SSH tunneling for application communications such as Jupyter Notebook.
Firewall	ISAIC infrastructure is protected by two levels of firewall; one at the University perimeter managed by the central IT group; and one at the ISAIC cloud level. Additionally, each provisioned VM has a set of firewall rules controlled by the client.
Passwords	Access to ISAIC dedicated virtual machines is controlled through PKI (public key, private key infrastructure), therefore eliminating the use of traditional passwords. PKI is a more secure means of authentication and access control. On-demand services are accessed through a web portal with the option of setting a user password (strong password requirements).

Physical Security and Protections	The physical data centres (DC) for ISAIC cloud infrastructure are located on the University of Alberta campus with secure keycard access, restricted to authorized staff only. Backup power is available through both UPS and generator. The purpose-built DCs are monitored and maintained by UofA Facilities & Operations, 24x7.
Vulnerability Scanning	At ISAIC we have automated two scans to run every three months, and two Sysadmin are independently notified of the results. One scan is run internally on the infrastructure using OpenSCAP; the other scan using OpenVAS is run on the public facing interface. In addition to the above noted internal and external exposure system scans, ISAIC also works with the University Chief Information Security Office (CISO) to conduct periodic independent security scans using Rapid 7 Nexpose. We then work with the CISO to address and mitigate any reported vulnerabilities.
Data Backups, Disaster Recovery and Business Continuity	The ISAIC cluster is protected with many redundant components (UPS, power supplies, hard drives, internet connection), to ensure high availability. Additionally, storage nodes are mirrored across two physically separate DCs. Compute nodes are also physically distributed across two DCs, allowing for a degree of business continuity for clients that cannot tolerate significant downtime. As noted in the ISAIC Terms of Service, it is the client's responsibility for data backups, however scheduled backups can be arranged as needed. ISAIC services are provided on a best-effort basis, and any planned outages are communicated well in advance. ISAIC infrastructure-as- a-service (IaaS) is provided as a secure sandbox environment for development and proof of concept.

* Higher Education Community Vendor Assessment Toolkit (HECVAT);
https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

University of Alberta Information Security Policy & Standards,
https://www.ualberta.ca/information-services-and-technology/security/information-security-policy-standards.html
https://policiesonline.ualberta.ca/PoliciesProcedures/Pages/Information-Management-and-Information-Technology.aspx

For further information please contact support@isaic.ca