UKRIO
RESEARCH INTEGRITY OFFICE

Promoting integrity and high ethical standards in research
Providing confidential, independent and expert support

Rustici Software: Information Security

Dispatch to third party e-learning platforms

Version No.: 0001

Publication Date: 28/03/2025

Table of Contents

Security Governance **2**

- Security direction 2
- Audit and risk management 2
- User awareness requirements 2
- Information security policy 2

Access Management **2**

- Access control 3
- Accounts and passwords 3

Information Management **3**

- Information classification and handling 3
- Approach to privacy requirements for personal or sensitive information 4
- Physical assets 4

Infrastructure Management **4**

- Back-up processes 5
- Physical components security 5

Supply Chain Security Management **5**

- Service level agreements 5

Threat Management **6**

- Automated scans 6
- Patch management 6
- Cyber attacks 6

Incident Management **6**

- Incident management policy 7

Development Management **7**

- Source code protection 7
- Quality assurance processes 7
- Approach for software acquisition 7
- System and security testing 8
- Protection against disclosure of sensitive information 8
- Server protection 8
- Controls to support information validation 8

Physical and Environmental Security **8**

Audit and Monitoring of Security Arrangements **9**

Technical Security **9**

- Automated scanning and alerts 9
- Cryptography solutions 9

Business Continuity **10**

UKRIO
RESEARCH INTEGRITY OFFICE

Security Governance

As an overall approach to ensuring information security, Rustici Software will not have access to third party data/system because of **personally identifiable information (PII) Hashing**.

The governance arrangements in place are described below.

Security direction

Security direction is derived from the company's Information Security Mission. The Vice President of Information Security is responsible for monitoring and enforcing security mechanisms, and the Security Team (within the Hosting department), actively works to protect infrastructure and systems from threats. Additionally, the Executive Security Steering Committee is responsible for the promotion and application of security standards throughout the organisation.

Audit and risk management

Rustici Software has a documented risk management program based on the ISO-27001 framework which includes formal quarterly risk assessment processes.

Internal audits are completed quarterly and annual **ISO 27001** and **SOC 2** audits are conducted to verify compliance with information security policies and standards. See SOC 2 Type II report, ISO 27001 Certification & Statement of Applicability (SOA).

User awareness requirements

All Rustici Software employees are required to complete a privacy training course at induction and annual privacy and security awareness training provided by the company. The training is tracked via the company's internal learning management solutions.

Information security policy

Up-to-date information security policy that includes acceptable use and mandate specific controls over client data is available to all employees. See Rustici Software Security Documentation.

The company performs References and Employment Verification, Criminal Background Check (where allowed), Proof of Citizenship, Social Security Number Crosscheck, and OFAC list. The background check process is SOC 2 audited.

Access Management

Rustici Software has two different types of user groups: Admin and User. See the Access Control Policy for additional details.

Access control

The company operates all access control activities upon the principle that default permissions are set as "deny all", and specific permission is needed to grant access in line with the individual's role and *bona-fide* business needs. Role based and least privilege access. Each asset owner shall be responsible for reviewing, authorising, and recording the details of those who have legitimate access to their asset(s).

Access permissions are reviewed frequently to ensure that they remain accurate, current, and adjusted as necessary (at onboarding, termination, and at least yearly).

Remote access is only authorised via Rustici Software's owned equipment and using the pre-installed connection configuration (e.g., VPN). No user shall attempt to connect to Rustici Software's networks or IT systems using non-company equipment or non-approved software or utilities. Controls are SOC audited.

Accounts and passwords

All generic account passwords are changed. Users shall ensure that their user ID is supported by personal passwords which fully conform with Rustici Software's Password Management Policy.

Interactive accounts are not shared between users. All account credential encryption at rest will use **AES-128 encryption** or better. Keys for encryption at rest will be maintained inside Amazon Web Services (AWS) Key Management System.

Users shall not use generic user ID details to access information assets, nor shall they use super-user accounts (e.g., supervisor or administrator privileges), unless such privileged account access is essential under the prevailing circumstances.

All users are provided with unique user ID and the sign on process is secure to protect authentication credentials. There is a joiners, movers and leavers process that drives access entitlement review. The use of privileged access is audited and controlled via change control.

Information Management

Rustici Software manages all forms of information as described in the below control measures.

Information classification and handling

Documented and implemented information classification and handling regime is in place – see the Information Classification and Handing Procedure for details.

Formalised asset management process is in place. Security requirements are formally factored into the full development lifecycle. The company has a formal **Information Security Management System (ISMS)**, comprised of security infrastructure, policies, and procedures. The ISMS is derived from industry data

security and privacy best practices such as OWASP, ISO-27001, NIST, and SANS guidelines and is designed to maintain the confidentiality, integrity, and availability of data that is processed and stored within the organisation's systems. Formalised data offboarding process is in place, including secure deletion.

Approach to privacy requirements for personal or sensitive information

The Client (i.e., UKRIO) is the **Data Controller** and Rustici Software is the **Data Processor**. The company processes all data in accordance with written direction from the client organisation via contract or order form. Also see

- Rustici Software's Privacy Policy and details related to Data Privacy Framework certification
- UKRIO's Privacy Policy and details related to data protection

Rustici Software's security controls and policies are derived from industry data security and privacy best practices such as OWASP, ISO 27001, ISO 27701 (privacy), NIST, and SANS guidelines.

Physical assets

Sensitive physical information is managed according to Rustici Software's Physical Security Policy. The company has a documented Asset Management policy that addresses inventory and ownership of assets as well as roles and responsibilities.

Client data is prohibited from storage on removable media. USB data-write is disabled by domain security policy. Writing to removable media is restricted.

Additional details are provided in the Acceptable Use Policy.

Infrastructure Management

Infrastructure management processes and systems includes server and network device configuration, firewalls, wireless access, backup, and change management.

All infrastructure changes go through change control, which includes testing as appropriate. SDLC and change management processes apply to infrastructure as code. Access is role based and least privilege. Additional details provided in the Secure Engineering Principals.

See the System Hardening Guidelines for information on how servers are configured to function as required and to prevent unauthorised or incorrect updates.

Secure hardening standards are in place to manage virtual servers. See also the Cryptographic Control Policy.

AWS and Cloud network storage arrangements are in place.

Formalised Vulnerability Management Policy is in place for maintenance of key components supporting:

- Critical/High vulnerabilities – treated within 30 days
- Medium vulnerabilities – treated within 90 days

With consideration for performance and capacity management.

Back-up processes

Formalised Backup Policy in place, aligned with industry standards.

Default firewall configuration is set to deny all. See the System Hardening Guidelines for additional details.

Physical components security

All customer data storage and processing is done in AWS; AWS controls are described in the Data Center Controls document. See the Rustici Physical Security Policy for the office.

Supply Chain Security Management

Applicable supply chain security management processes and systems relate to acquisition, outsourcing, cloud computing, IaaS, PaaS, SaaS etc.

To manage potential risks at third parties, a comprehensive vendor management process is in place; new vendors are reviewed and classified in relation to the services rendered and audited annually thereafter.

Technical controls are described in the System Hardening Guidelines and are aligned with industry best practices. Controls are SOC 2, ISO 27001 & ISO 27701 (privacy) audited annually.

A comprehensive vendor management process is in place including ensuring proper data controls are in place and aligned with industry standards. new vendors are reviewed and classified in relation to the services rendered and audited annually thereafter. Applicable contracts and/or DPAs are required. Additional details provided on the Third-Party Vendor List.

Service level agreements

To the extent applicable, subcontractor **service level agreements (SLAs)** are aligned with service and client commitments.

All open source is fully licensed, and DAST scans check third party libraries including open source for vulnerabilities.

Threat Management

Rustici software has a comprehensive vulnerability management program is in place to identify and remediate technical vulnerabilities in the service. Staff responsible for assessing vulnerability reports are sufficiently skilled and trained.

Automated scans

Automated configuration audits in place include:

- static;
- dynamic;
- penetration testing; and
- software composition analysis

Patch management

Standard vulnerability management process is in place which covers all vulnerability remediation inclusive of patching. Remediation SLA for:

- critical and high vulnerabilities is 30 days
- medium severity vulnerabilities is 90 days

There are no current outstanding exceptions for Critical or High patches.

Security event monitoring and management processes

Alerts are integrated into central logging and SIEM, and alerts are configured to notify on-call personnel. SIEM deployed over centralised logging facility, which incorporates all relevant logs.

Zero day protection and advanced malware protection is in place. Threat modelling is incorporated within the SDLC as appropriate.

Cyber attacks

A formalised risk management process is in place that assesses full range of cyber threats, tracking risk treatment as appropriate. **Information Security Awareness** training is conducted annually and covers all relevant topics. See the Incident Management Policy for additional details.

Incident Management

Management of security incidents includes:

- mechanism for raising a security incident

- prioritisation of security incidents

Incident management policy

An information security incident management framework has been developed, deployed and maintained. See the Incident Management Policy for details.

Incident response training is incorporated into standard information security awareness training.

Incident response process is tested annually. Notifications of incidents that may impact service are delivered in alignment with legal and contractual obligations

A Security Operations Centre is in place to support the management of information security incidents.

Process to deploy emergency fixes that are needed as part of incident response is in place.

Security incident response process incorporates forensic analysis, inclusive of engaging specialised third party forensics providers

Development Management

Formalised SDLC process is in place for application protection and system development management (e.g., the system development life cycle).

Specific development/test environments that are isolated from production processing client information is in place.

Source code protection

Commercial grade source management system is utilised; all access is role based. SDLC and change management processes apply to infrastructure as code. Integrity checks are in place as part of release process. See also the Change Management Policy.

Quality assurance processes

Regimented release and change management process, ensuring appropriate testing is performed prior to release.

Approach for software acquisition

Formalised asset management process is in place, ensuring entire lifecycle is maintained from acquisition to disposal and end of life. System build documents are maintained.

System and security testing

Static, dynamic, penetration testing and software composition analysis are in place. Formalised SDLC decommissioning process is in place.

System Hardening is in place to process client information and protect against invalid connections.

Alerting is in place for all forms of operational failure. Standard reporting/alerting/logging measures apply. Seamless failover to alternative availability zone within hosting region.

Protection against disclosure of sensitive information

All access is role based, tailored to least privileged. Integrity checks are in place as part of release process. Enforcement of OWASP Principals incorporated throughout SDLC. ISMS is derived from industry data security and privacy best practices such as OWASP, ISO-27001, NIST, and SANS guidelines and is designed to maintain the confidentiality, integrity, and availability of data that is processed and stored within the organisation's systems.

Server protection

Comprehensive antivirus & malware protections are in place across all applicable production components. System Hardening standards are in place and encryption by default.

Browser based applications are protected through Admin abilities (such as browser proxy settings) and are only accessible to IT. Implementation details are not shared externally. Business continuity planning (BCP) and disaster recovery (DR) plans are SOC and ISO audited.

Controls to support information validation

Rustici software is obligated to provide adequate security to protect and ensure the integrity and availability of client's data processed on its systems. However, the content and accuracy of their data is the responsibility of clients.

End user developed applications are not utilised.

Physical and Environmental Security

All customer data storage and processing is done in AWS; AWS controls are described in the Data Center Controls document. See here for the Rustici Physical Security Policy for the office.

Risk assessment has been undertaken to cover physical and environmental factors that might impact the delivery of services.

See the AWS Data Center Controls & Rustici Physical Security Policy for controls that are in place to manage visitor/third party access to areas where client information is processed.

Power and other utilities required to deliver services are protected and resilient. BCP and DR plans are reviewed and tested annually.

Audit and Monitoring of Security Arrangements

A defined audit process is in place. SOC 2 Type II, ISO 27001 & ISO 27701 (privacy) audits are conducted annually.

Technical Security

Technical security infrastructure includes details of malware protection, anti-virus, cryptographic controls etc.

- Comprehensive antivirus & malware protections are in place across all applicable production components.
- System Hardening standards are in place and encryption by default.
- Zero day protection and advanced malware protection are in place.

All operating systems are required to have anti-virus / anti-malware protection with continuous monitoring to ensure the protection is operational and up to date.

Users involved in delivery of services cannot disrupt the operation of malware protection solutions.

Automated scanning and alerts

Security monitoring is in place, inclusive of configuration drift detection. Alerts are integrated into central logging and SIEM, and alerts are configured to notify on call personnel. Standard reporting/alerting/logging measures apply .

Commercial grade EDR solution is deployed on all devices for intrusion detection. Implementation details are not shared externally.

Appropriate content filtering and DLP controls are in place to protect against information leakage.

Cryptography solutions

See Cryptographic Control Policy. Formalised encryption key lifecycle management process is in place.

Zero day protection and advanced malware protection are in place to protect services and access to data.

Business Continuity

Rustici Software operates on resilient technology environments. Business continuity planning (BCP) and disaster recovery (DR) plans for crisis management was last tested in December 2023.

Post incident reviews are implemented into DR plans which are tested annually and results shared with executive management.

DR training is role specific and delivered to all staff involved in the plans as part of their role-based training.

UKRIO
RESEARCH INTEGRITY OFFICE

Promoting integrity and high ethical standards in research
Providing confidential, independent and expert support

The UK Research Integrity Office (UKRIO) is an independent charity, offering support to the public, researchers and organisations to further good practice in academic, scientific and medical research. We pursue these aims through a multi-faceted approach:

- Education via our guidance publications on research practice, training activities and comprehensive events programme.
- Sharing best practice within the community by facilitating discussions about key issues, informing national and international initiatives, and working to improve research culture.
- Giving confidential expert guidance in response to requests for assistance.

Established in 2006, UKRIO is the UK's most experienced research integrity organisation and provides independent, expert and confidential support across all disciplines of research, from the arts and humanities to the life sciences. We cover all research sectors: higher education, the NHS, private sector organisations and charities. No other organisation in the UK has comparable expertise in providing such support in the field of research integrity.

UKRIO welcomes enquiries on any issues relating to the conduct of research, whether promoting good research practice, seeking help with a particular research project, responding to allegations of fraud and misconduct, or improving research culture and systems.

UK Research Integrity Office

Impact Hub London Euston, 1 Triton Square, London NW1 3DX
Email: info@ukrio.org Web: www.ukrio.org
Registered Charity No: 1147061 Registered Company No: 7444269

For the full list of UKRIO publications, visit www.ukrio.org