registry direct

Security and compliance

Security and compliance are always front of mind at Registry Direct. We understand that they are core to the success of your business and ours.

We are committed to keeping your customer data secure by preventing, monitoring for and eliminating system vulnerabilities. Registry Direct is ISO 27001:2022 certified and also undergoes an external GS007 audit annually. At Registry Direct we are dedicated to continually improving our security posture and the resilience and continuity of our services. We understand that this requires both a strong technology and human focus.

Registry Direct utilises a carefully chosen suite of industry standard technologies, partner organisations, tools and practices to secure your data and keep it that way. Our people lie at the heart of this approach. All Registry Direct staff go through a rigorous selection process, undergoing background checks prior to onboarding. Every staff member then completes mandatory security training during the staff onboarding process and again in formal training sessions every 6 months. Software developers and technical staff undergo security training and upskilling on an ongoing basis.

Additional security training and preparedness is undertaken on a continual basis by the Security Review Committee which meets on a monthly basis to review and direct the security and compliance programme on an ongoing basis.

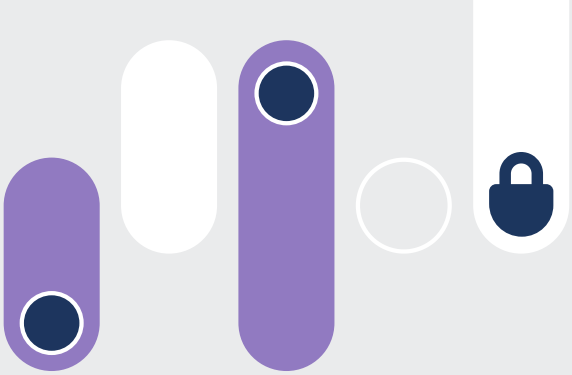
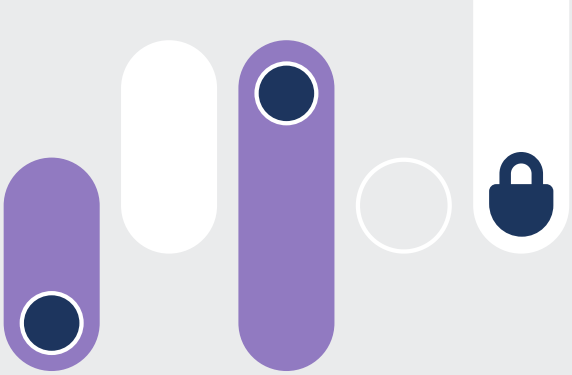


Table of contents



1. Infrastructure and network security

Registry Direct is hosted on AWS (Amazon Web Services) cloud computing platform. AWS data centres are designed and built to mitigate the risk of environmental disasters, with availability zones within a region physically separated from each other. AWS data centres feature many other design and operational measures to ensure high levels of availability and redundancy. Physical access to data centres is only granted to approved AWS employees, is time bound and done on a principle of least privilege basis. Registry Direct staff do not have physical access to AWS data centres. Physical security measures such as CCTV, secure entry points which require multi-factor authentication and advanced intrusion detection and response systems all help make AWS data centres some of the most secure in the world.

Registry Direct is the owner of our account with AWS and only a small number of authorised Registry Direct staff have access, on a least privilege basis, to be able to view and configure infrastructure within that AWS account. Access is used only when required and all login accounts have multi-factor authentication enabled. Servers are situated within a virtual private network and access requires a combination of private key authentication, encrypted VPN connection and IP whitelisting via specifically configured firewall rules. Private keys are encrypted, passphrase protected and stored securely using AWS Key Management Service.

As much as possible an IAC (Infrastructure As Code) approach is used to provision, configure and maintain Registry Direct cloud infrastructure and associated configuration.

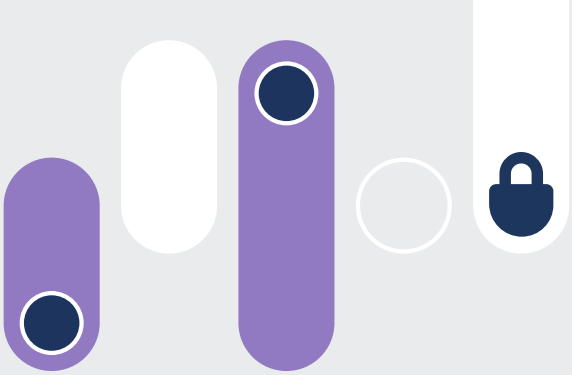
2. Penetration testing

Registry Direct commissions annual penetration testing of its platform, conducted by a reputable Australian third-party security agency. For penetration testing, an isolated high fidelity clone of the production environment is used. Registry Direct provides penetration testers with basic high level information about the system and architecture. No customer data is exposed to the agency during penetration testing.

Any information about security vulnerabilities successfully exploited through penetration testing is used to set mitigation and remediation priorities. Artefacts from the most recent penetration test report can be provided upon request.

3. Cloud infrastructure security audits

The same third-party security agency also conducts an annual cloud infrastructure security audit. This involves cloud security experts analysing and reviewing the cloud infrastructure and network configuration within the AWS Registry Direct account. Cloud architecture and security configuration is assessed against best practices (including the AWS Well Architected framework). Any information about configuration improvements or security vulnerabilities is used to set mitigation and remediation priorities. Artefacts from the most recent cloud infrastructure security audit report can be provided upon request.



4. Intrusion detection and prevention

Registry Direct leverages a variety of tools to prevent and detect suspicious network traffic, patterns and usage behaviour. These include but are not limited to the use of WAFs (Web Application Firewalls), bot protection, DDOS (Distributed Denial Of Service) protection as well as cloud based malware scanning and quarantine tools. Reducing the attack surface is also an important measure in intrusion prevention. Registry Direct utilises automated scanning tools which monitor, analyse and report on our attack surface so that we can limit its size in a proactive manner.

5. Data encryption

All customer data in the Registry Direct system is encrypted at rest. This means that if physical disks from the AWS data centre were stolen or obtained by bad actors, it would not be possible for them to decrypt and access customer data on those disks.

In addition, passwords are stored encrypted using a robust industry standard password hashing algorithm. All user facing connections (for both customers and Registry Direct support staff) are encrypted end to end over HTTPS (Secure Hypertext Transfer Protocol) and HTTPS is enforced throughout all routes in the Registry Direct web application. HTTPS utilises SSL (Secure Socket Layer) technology. Registry Direct's SSL certificate is issued by Amazon which is an established and trusted CA (Certificate Authority).

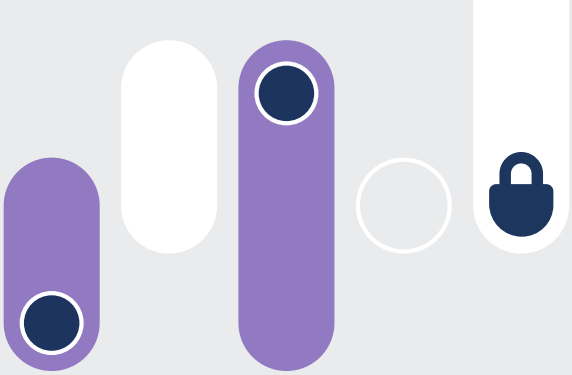
An encrypted VPN connection is used for all staff connections to Registry Direct server infrastructure.

6. Data retention, sovereignty and removal

Customer data is retained for the duration of each customer's commercial tenure with Registry Direct. When a customer leaves Registry Direct they can either download data themselves or Registry Direct can provide a full export of customer data as part of a paid offboarding package. Customer data is then permanently deleted from the Registry Direct platform. When data is deleted from the Registry Direct databases the AWS encryption-at-rest mechanism facilitates "crypto shredding" and AWS secure media destruction practices which comply with NIST 800-88 mean decommissioned media is securely destroyed when it reaches end of life. It is the customer's responsibility to comply with Austrac and other regulations with regards to data retention requirements for customer/investor data, once they have offboarded from Registry Direct.

Customers can delete registry data such as investor details, transactions and securities themselves, using the UI however an immutable audit trail is created for whenever registry data is deleted or updated.

All registry data resides within Australia, in the ap-southeast (Sydney) region of AWS.



7. Secure development lifecycle

In securing the software development lifecycle Registry Direct takes a DevSecOps approach in which we endeavour to "shift left" so that security is baked into the software delivery process. This starts with developer security training and awareness. This involves developers using modern secure coding training platforms as well as studying the OWASP Top 10 and staying abreast of new incident case studies and attack vectors by following prominent security experts and bulletins. Third-party libraries and frameworks are carefully selected for their security credentials, leveraging built in and proven protections for common attack types like XSS (Cross Site Scripting), SQLi (SQL Injection), clickjacking and CSRF (Cross Site Request Forgery).

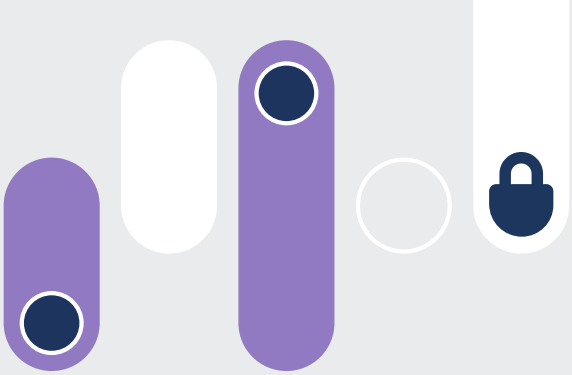
For new features and improvements security considerations are always front of mind during the requirements, design and QA steps. Code review on every PR (pull request) is mandatory, with any critical sections which could have security implications, highlighted for additional scrutiny. When it comes to shipping code, a continuous delivery approach underpins the SDLC at Registry Direct with SAST (Static Application Security Testing) running as a mandatory step in our CI/CD (Continuous Integration/Continuous Delivery) pipeline. Automated vulnerability checking of our software supply chain ensures that any potential vulnerabilities in our dependency chain are patched quickly. Automated deployments enable us to fix issues quickly, achieve repeatability and mitigate the risk of human error introducing unexpected problems.

8. Patching

In the ever changing, rapidly evolving threat landscape which modern SaaS applications are exposed to, it is essential to maintain a continuous, automated approach to patching. Registry Direct leverages AWS Systems Manager and other automated upgrade functionality to ensure cloud infrastructure is patched on a continual basis, protecting against known CVEs (Common Vulnerabilities and Exposures). LTS (Long Term Support) versions of major software dependencies and operating system platforms are chosen to ensure the best possible support for security updates. Registry Direct uses automated tools to monitor End Of Life horizons within our infrastructure and software supply chain to ensure that any required major version upgrades can be planned and tested ahead of time.

9. Secrets detection and management

All secrets are stored securely, in industry standard secrets management solutions (not in source code repositories). This prevents secrets from leaking and ensures that access can be tightly controlled. Centralized secrets management also facilitates easier management of the secrets lifecycle, including secret creation, rotation and revocation. Automated monitoring is used within the cloud computing environment to scan and detect any secrets which may be exposed in an unsafe way. Similar tooling is used in the CI/CD pipeline to monitor for any changes which may introduce unintended secrets exposure during the software development lifecycle.



10. Application security

Registry Direct is continually improving the security measures in our SaaS platform. Below are some key security measures which are in place at the application level.

Role-based access control: Access to data is controlled using a role-based access control model. This ensures that users only have access to view and change the data which their role entitles them to have access to. This also enables us to implement more rigorous multi-factor security schemes for user roles which have more privileged access.

Multi-factor authentication: Users with the issuer admin, client admin or issuer read-only user role are subject to mandatory token-based multi-factor authentication using an authenticator app (e.g. Google Authenticator, Microsoft Authenticator or Authy). These users must provide an OTP (One Time Password) verification code from an authenticator app in order to log into the system and are forced to re-verify after a period of 24 hours regardless of the device they are logging in from. Users who only have the investor role are subjected to a step-up model of multi-factor authentication in which they must enter a unique one-time verification code which is SMS'd to their linked and verified mobile phone, whenever they wish to change any of their investor details or change password/username/linked mobile number.

Email security: Email notifications from the Registry Direct SaaS platform are automatically sent when key user actions are undertaken. This ensures that users are alerted to any potentially unauthorised changes. These along with other email notifications are sent from the Registry Direct domain which has SPF (Spam Protection Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting, and Conformance) protections in place in order to prevent spoofing, spam and phishing attempts coming from the Registry Direct domain.

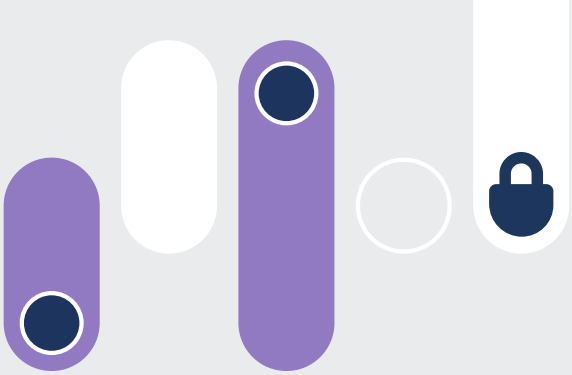
Two step approval: For key user actions a two step approval process is required, with immutable audit logs created for each step of the process.

Session timeout: Idle users are automatically logged out after a set period of inactivity.

Password strength requirements: A minimum password length of 8 is required in combination with user attribute similarity, common password and other robust password strength validation measures.

11. Immutable audit trail logging

In the financial services and regulatory technology domain, immutable, detailed and clear audit trails are considered a core requirement. That's why the Registry Direct platform provides customers with a comprehensive view of changes to registry data as well as logs of user actions within the system. Known as the Registry Direct "activity log", this audit trail is accessible to issuer and client admin roles and is searchable and exportable for compliance and forensic purposes. A colour-coded side-by-side "diff" view is available for each activity log entry to make it simple to see what exactly has changed, who changed it and when. This includes all user login activity which also captures IP address and device user-agent information.



12. Corporate security

Endpoint protection: Industry standard antivirus and malware protection is installed and configured on all staff devices. Full disk encryption is enforced on all staff laptops. Biometric and/or strong password authentication is required on all staff devices as well as screen lock and automatic operating system updates to ensure device OSes are equipped with the latest security patches.

Multi-factor authentication: Authenticator app based multi-factor authentication is required for all third-party applications used by Registry Direct staff. Account provisioning and de-provisioning is managed as part of a documented on and off boarding process.

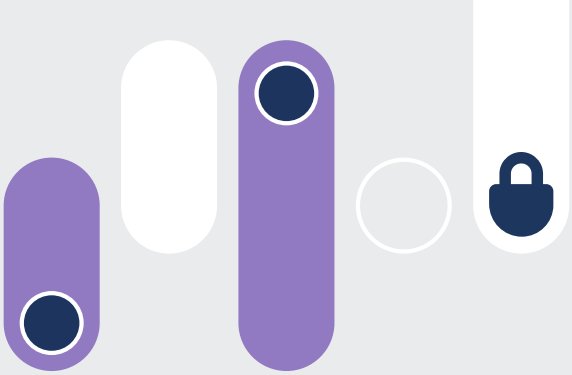
Secrets management: An industry leading zero trust, zero knowledge encrypted password manager is used to securely store login credentials for third-party systems. This enables audited centralized management, role based access control as well as quick and easy revocation as part of staff offboarding procedures.

Privileged access: Privileged access to production systems and administrative capabilities in third-party tools is only granted to a select number of Registry Direct staff and only if strictly required. Granting and revocation of privileged access is documented and tracked in staff on and off boarding checklists. A formal review of privileged user access is conducted quarterly.

Third-party vendor assessment: Third-party vendors and services are carefully assessed to ensure they meet necessary security and compliance requirements prior to being adopted. An annual review of existing third-party vendors is conducted to maintain compliance.

Security policies: Registry Direct maintains a suite of internal security and compliance related policies which form the basis of our ISMS (Information Security Management System). These include but are not limited to: Access Management Policy; IT Systems Security Policy; End User Security Policy; Supplier Management Policy; Risk Management Policy; ISMS Governance Framework.

Security training: All staff undergo compulsory security training as part of their onboarding process and then every 6 months on an ongoing basis. All staff also review, acknowledge and are bound by the IT Systems Security Policy and End User Security Policy. All staff must also complete mandatory workplace conduct training. Software developers study the OWASP Top 10 and undertake specialised secure coding training as well as examining key case studies to learn from real world security incidents and disaster recovery scenarios.



13. Disaster recovery, business continuity and data breach response planning

The Registry Direct platform is architected to be highly available, with redundant servers, load balancers, database replicas and file storage/distribution infrastructure all designed to work across multiple availability zones within the ap-southeast (Sydney) AWS region.

The following backup regime is in place:

- Nightly snapshots are taken of the production database via an automated process and stored securely within the virtual private cloud on AWS. This allows for point in time restoration of the database up until the point at which the snapshot was taken. Nightly backups are deleted after 30 days.
- For the time between nightly snapshots, WAL (Write Ahead Logging) is in place which allows for recovery to a point-in-time up to the second.
- Weekly and monthly full database backups are also created via an automated database backup process. The monthly backups are then GPG encrypted and securely copied to long term storage within AWS.
- Server instances and cloud file storage data stores are also backed up on a nightly basis.
- Restoring from the backups is tested on a monthly basis

If customers also wish to maintain their own independent backup regime then sufficiently privileged users can extract registry data themselves for backup purposes.The Registry Direct operations team can also provide a full encrypted export of customer data for a fee on request.

Registry Direct maintains a detailed Business Continuity Plan document which is reviewed and tested on an annual basis. Disaster recovery scenarios and case studies are reviewed by the Security Review Committee on an ongoing basis in order maintain disaster recovery preparedness.

Our Data Breach incident Response Plan is also maintained and reviewed on an annual basis. In the unlikely event of a breach or suspected breach incident, preparedness is essential. The response team roles and responsibilities are clearly defined in the plan as are the response process steps: Contain, Assess, Notify, Review and Record. Registry Direct maintains a relationship with an industry-leading Australian cyber security firm who can be called upon to assist in our incident response efforts if required.

14. Privacy Policy and Terms Of Use

Registry Direct maintains and regularly reviews a publicly available Privacy Policy which can be viewed here.

Additionally, Registry Direct requires that all of our customers read, review and agree to our publicly available Terms of Use prior to using our products and services.

15. ISO 27001 certificate

intertek SAI GLOBAL

CERTIFICATE OF REGISTRATION

This is to certify that the management system of:

Complii FinTech Solutions Ltd

Trading as

Complii FinTech Solutions Ltd

Registry Direct Limited

Main Site: Suite 6.02, Level 6, 56 Pitt Street, Sydney, New South Wales, 2000, Australia

has been registered by INTERTEK SAI Global as conforming to the requirements of:

ISO/IEC 27001:2022

The management system is applicable to:

Information security during the design, development, operation, delivery, maintenance and support of SaaS products of Complii Fintech Solutions Ltd in accordance with the Statement of Applicability version 2.0 dated 15/12/2023.

Certificate Number:
ITGOV40497

Initial Certification Date:
20 December 2023

Date of Certification Decision:
20 December 2023

Issuing Date:
29 December 2023

Valid Until:
19 December 2026

Certified System ISO 27001

JAS-ANZ

WWW.JAS-ANZ.ORG/REGISTER

Calin Moldovean
President, Business Assurance

SAI Global Certification Services Pty. Ltd.
Level 7 Suite 7.01
45 Clarence Street
Sydney NSW 2000
Australia

The most powerful online registry software at a competitive price

- One set monthly fee with no hidden extras.
- No charge on bulk emails to investors with email addresses.
- Free report downloads.
- Meetings and corporate actions set up and processed at a fraction of the cost of our competitors.

Try Registry Direct for free

Our free trial allows you to explore our platform using demo data and upload your own registry data. Or, if you prefer to chat with one of our account managers, contact us for a demo.

www.registrydirect.com.au
registry@registrydirect.com.au

registry direct