foundU

Platform Security White Paper

Updated January 2025

Table of Contents

Overview

The team at foundU has built our organisation, culture and technology with security as a guiding principle. Our HRIS and payroll Platform requires our customers to entrust us with sensitive corporate and employee information. This White Paper outlines our approach to security.

We will refer to the 'Platform' throughout this Paper however the measures, controls and certifications discussed apply to foundU as a company and to all our associated products and internal processes.

As well as providing information regarding the security measures taken by foundU to protect customer data this Paper will identify specific access points required by the product and the proper controls at all levels of data storage and access.

foundU's Information Security Management System is certified to ISO27001:2022 – the information security standard. More information about ISO27001:2022 can be found here. The last audit was conducted in January 2025 where no major or minor non-conformances were found. foundU can provide a copy of our certification on request.

This Paper covers the following topics:

- Secure Hosting
- Security Measures
- Data Access and Storage
- System Development
- Business Continuity
- Third-Party Risk Management
- Employee Security Training
- Data Breach Notification Protocol

Secure Hosting

Amazon Web Services

The foundU Platform is built and hosted exclusively on the Amazon Web Services (AWS) platform. As a result, the physical securities of foundU are equivalent to that of AWS, which many of Australia's leading organisations, as well as Federal, State and Local Governments use. For more information regarding AWS security, please view AWS security policy and documentation which can be found here.

AWS operates under a shared security model with its customers. That means that depending on the AWS service consumed, some of the security responsibility is owned by AWS and some of it is owned by its customer. foundU often opts to host with AWS services where most of the security and uptime responsibility resides with AWS thus lowering our surface area for attack, increasing uptime and decreasing the cost for our customers. For an AWS environment to be secure, periodic reviews are performed to ensure that everything is configured to the evolving recommend standards.

Common questions about our hosting environment:

Q: What firewall do you use?

A: AWS WAF (Web Application Firewall) in conjunction with AWS ALB (Application Load Balancer). No servers are directly exposed to the internet.

Q: If your office network is compromised, can an attacker get to our data?

A: No, our office network is not directly attached to our secure cloud network.

Q: How is your application code hosted?

A: Our code is deployed with AWS Code Deploy in a Blue/Green deployment pattern. We use AWS AMI's for hosting our core application and AWS Fargate for hosting assistive service applications. The AMI's are built and patched automatically using AWS Image Builder.

Q: Where is our data located?

A: foundU is hosted exclusively in AWS Sydney, spread across 3 Availability Zones. We also keep off cloud, on premise backups. No data is stored outside of Australian borders.

Security Measures

Encryption in Transit

To protect sensitive information transmitted over the web, the foundU Platform is only available via the HTTPS protocol and as a standard practice, is secured using the industry standard 256-bit strength SSL certificates. This ensures that data transmitted is encrypted and secure all the way from leaving user browser to server and back. All data such as financial information can only be sent to and stored on the server across encrypted sessions.

Encryption does not start at the browser and end at the web server either. foundU's entire AWS infrastructure communicates with encrypted traffic. All the traffic flowing between the web servers, databases, object storage and caching servers is encrypted.

Encryption at Rest

Data is encrypted at rest when it is in our database servers, caching servers and our object storage in AWS. For further safety, we also keep a copy of our object storage backed up on premises. Our on-premises backup is encrypted on disk using the GELI protocol.

Data Access and Storage

At foundU, securing and protecting user information is our priority. The foundU Platform enforces strict, industry

tested measures to increase overall security and to validate all entered data.

To avoid any risk of SQL injection (common database hack), Cross-Site scripting and any malicious input, all incoming data is filtered and safely escaped before entering the database system and again safely escaped before outputted on the user screen. User information is further secured by the database encryption process which encrypts the entire DB instance. In the event of the database being accessed directly, the data shown is just random encrypted characters which can only be decrypted with special keys. Keys are used to encrypt/decrypt information and passwords are hashed using “bcrypt”. Information that is deemed not to be private/confidential is stored normally in plain text.

The foundU platform is unique in its approach to data management. Whilst we deliver a multi-tenanted SaaS application, we isolate each customer’s database and data into a separate and completely private database schema. This isolation provides far superior security to a shared storage and shares databases that combine data from many customers into a single place. Multi-tenanted software provides economies of scale, enabling customers to share one version of software, gain immediate access to the latest enhancements and security updates as they become available, without having to compromise on data security. These controls are in addition to the rich, logical security model in the application itself.

Hashing is a one-way methodology to store data. Password hashing used for information within the database is a mixture of SHA1, bcrypt and salting. As users login over time, we will continue to update the hashing mechanisms to the latest available.

Data acquired through the foundU Platform is to be stored and archived using two main methods; archive tables and off cloud backup. This data will be stored in archive tables that will be continually monitored and modified if the data is required at any point. The platform has multiple automated backups occurring at regular intervals across 24 hours. This backup will be a snapshot of the entire system, including archives. All backups are stored on offsite Australian storage locations.

All data will be stored for a minimum period of 12 months post-platform termination, with an evaluation after the 12 months determining the importance of the data. If the data is deemed to be unusable and obsolete it will be permanently removed and destroyed. foundU’s IT policies are available on request.

Defence Mechanisms

foundU has implemented proactive security measures such as perimeter defence and network intrusion detection and prevention systems, together with anomaly detections algorithms that alert team members. foundU restricts access to the platform based on which country the user is in.

Vulnerability assessments and penetration testing of the foundU platform are evaluated and conducted on a regular basis by both foundU team members and a trusted external third-party vendor. These vulnerability assessments are in addition to the secure coding practices, static code analysis and security reviews undertaken internally.

Authorisation Controls

The foundU platform enforces role-based security for authorisation. Role-based security allows customers to grant or restrict user access to functionality, business processes, reports and data on a user-by-user basis.

Single Sign-on Support

SSO (Single Sign-on) is an authentication tool that allows a user to login to several independent software systems using one single Login ID. The SSO integration foundU supports is via SAML.

If you currently use a single sign-on provider in your business, you may want to set this up for accessing foundU.

If you don't currently use SSO you may consider it as benefits include:

- Users can access their applications and software systems faster
- Your admins won't have to memorise several passwords including foundU
- Centralised user management across all systems for an employer, this allows a user to be deactivated across multiple software systems at once

Multi-Factor Authentication

When you log in, you will be asked to verify your identity through multi-factor authentication (MFA). Put simply, you'll need to enter a 6-digit, one-time code sent to your email or phone. While it is your choice whether you use SMS or Email. **We highly recommend the use of SMS only for MFA**. This is to ensure your confidential data remains secure and is in line with requirements from the Australian Taxation Office (ATO).

This applies to both admin users and employees when updating confidential information such as banking and tax file details.

Web Application Firewall (WAF)

The web servers that power the foundU Platforms are not exposed to the internet directly. All traffic from the outside world is filtered through a Web Application Firewall built by AWS. The WAF is filtering out traffic from malicious activities in real time. We maintain a list of known malicious IP addresses to filter, the WAF also looks for SQL injection attacks and XSS attacks as they occur.

We also monitor all traffic from overseas and filter out countries that should not be accessing our product. All traffic also is transported via an Elastic Load Balancer which gives the platform another layer of security.

Access Logging

Encryption, hashing and firewalls are all important aspects of securing a web application, but it does not prevent malicious users performing actions. For this reason, we track all activity that occurs in the foundU Platform and specifically which user initiated the action. Our software allows admin users to impersonate employees and perform actions on their behalf. We log this information and use it when investigating incidents that occur.

Software Development

The foundU Platform is built on the Laravel framework. Laravel's queueing system makes the application scalable and allows our response time for web requests to stay under our 250ms target.

The foundU development team has comprehensive procedures in place for developing, testing, and deploying new code. We use the OWASP Top 10-2021 principles to mitigate web application security risks (OWASP).

Technical Architects and Tech Leads analyse software design to advise against security risks including: cross-site scripting injection, SQL injection and improper access to application functions.

Technical Architects and Technical Leads perform static code analysis to ensure against security risks and issues.

Quality Assurance engineers run through multiple steps to make sure the foundU products meet the stated requirements. Any change request to the foundU Platform is first pushed through our testing servers and the QA team assures the product meets the stated requirements by performing system testing and then on successful completion, changes are pushed to the production system.

Business Continuity

At foundU, ensuring the continuity of our services and safeguarding customer data are top priorities. We maintain a Business Continuity Plan (BCP) that is designed to maintain operational resilience and minimise downtime in the event of disruptions.

Service Uptime is available in your foundU Agreement terms.

Infrastructure Resilience

foundU leverages Amazon Web Services (AWS) for its cloud infrastructure, with servers strategically located across Australia. AWS provides high availability, redundancy, and robust failover mechanisms, supported by their own backup and disaster recovery protocols. This geographically diverse setup mitigates the risk of regional outages and ensures consistent service delivery.

Data Backup and Recovery

In addition to AWS's backup systems, foundU performs daily backups of all customer data. These backups are securely stored on our on-premise servers, providing an additional layer of data protection. This dual-backup strategy—cloud-based and on-premise—ensures data integrity and availability even in the face of unexpected events. We also conduct regular virtual restoration testing to verify backup integrity and preparedness.

Incident Response and Failover

foundU has a designated Incident Response Manager responsible for coordinating responses to security incidents. In the event of an incident, our platform is equipped with automated failover capabilities to redirect to operational servers within our AWS environment, ensuring minimal disruption to service availability. Our Incident Response Team, which includes our CTO, manages investigation and recovery efforts, ensuring swift resolution and communication with stakeholders.

Data Breach Notification Protocol

In the event of a data breach, foundU has a structured Data Breach Notification Protocol in place. This includes:

- Immediate assessment and containment of the breach
- Notification to affected individuals and relevant regulatory bodies in accordance with legal requirements
- Transparent communication with stakeholders outlining the breach impact, actions taken, and measures to prevent recurrence

Recovery Objectives

Our BCP defines clear Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to guide our response efforts:

- **RTO:** We aim to restore core platform functionalities within a minimal timeframe to reduce operational impact, with critical services targeted for recovery within 4 to 12 hours depending on the affected system.
- **RPO:** Daily backups ensure that data loss is limited to a maximum of 24 hours in the unlikely event of a major incident.

Business Impact Analysis

foundU conducts regular Business Impact Analyses (BIA) to identify critical business functions and assess the potential impact of disruptions. Key thresholds include:

- **Customer access to the system:** Impact if unavailable for more than 48 hours
- **Implementation team access to systems:** Impact if unavailable for more than 2 weeks
- **Software development efforts:** Impact if disrupted for more than 2 days
- **Services team access to data systems:** Impact if unavailable for more than 1 week
- **Management team access to corporate systems:** Impact if unavailable for more than 1 week

These thresholds help prioritise recovery efforts and resource allocation.

Roles and Responsibilities

Role	Responsibility
CEO	• Triggers BCP implementation • Assembles and leads the Business Continuity Team • Manages response and recovery processes • Oversees communication with regulators and stakeholders
CTO	• Coordinates IT and development teams • Assesses network and system statuses • Determines recovery requirements for critical functionalities • Maintains system integrity during recovery
COO	• Communicates with customers regarding incident status • Advises on service prioritisation • Ensures support services are operational
System Administrator	• Assesses facility conditions • Coordinates internal communications • Ensures non-disclosure and confidentiality protocols are upheld

Recovery Timeframes

The following timeframes guide recovery efforts after a major incident:

1. **Disaster Identification and Declaration:** Immediate upon detection
2. **BCP Activation:** Within 1 hour of disaster declaration
3. **Incident Assessment and Damage Prevention:** Initial report within 2 hours
4. **Restoring IT Functionality:**
    - Recover domains: 4 hours
    - Rebuild web servers: 4 hours
    - Rebuild login servers: 2 hours
    - Recover databases: 12 hours
    - Restore customer files: Up to 3 days, depending on data volume

Preparedness and Continuous Improvement

To enhance our recovery capabilities, foundU maintains redundancy of primary customer-facing infrastructure at separate locations from our main data centres. We also perform:

- **Annual BCP Testing:** To validate effectiveness and identify improvement areas
- **Regular Risk Assessments:** To address emerging threats and vulnerabilities
- **Continuous Plan Refinement:** Incorporating lessons learned from tests and real incidents

This proactive approach ensures foundU's resilience, securing continuous operations and safeguarding customer data.

Third-Party Risk Management

All third-party providers integrated by default within the foundU Platform have undergone rigorous security assessments. These reviews are conducted under the Australian Privacy Principles to ensure compliance with data protection standards. We continuously monitor and reassess third-party vendors to maintain the integrity and security of our platform.

Employee Security Training

All foundU employees undergo comprehensive background checks, including mandatory police checks, prior to employment. Additionally, we enforce regular security awareness and training programs for all staff. This training covers topics such as data privacy, phishing awareness, secure coding practices, and incident response procedures, fostering a security-first culture within the organisation.

Conclusion

At foundU, security is an ongoing commitment. We continually assess and enhance our practices to safeguard customer data and ensure operational resilience. Supporting internal policies and detailed documentation are available upon request to provide further insights into our security framework.

For more information or to request specific policies, please contact us at privacy@foundu.com.au.