Platform Security Whitepaper

Updated October 2022

Keeping Your Data Safe

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 ISO27001:2013 – the information security standard. More information about ISO27001:2013 can be found here. The last audit was conducted in March 2022 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:

1. Secure Hosting: Amazon Web Services
2. Security Measures
3. Data Access and Storage
4. System Development

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 AAWS security policy and documentation which can be found here.

foundU maintains its own EC2 servers for 3 tasks:

1. Web servers (hidden behind AWS ELB):
2. Queue worker servers (not accessible via HTTP); and
3. Scheduling servers (not accessible via HTTP).

We do not maintain our own servers for Load Balancing, Databases, Object Storages or Caching/Queueing. foundU uses AWS Elastic Load Balancing, AWS Aurora, AWS S3, AWS Elasticache respectively.

The foundU corporate office network is completely separate from our platform hosted in AWS.

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 complete 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, though can be encrypted if required.

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 storage zone. 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 offsite 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 7 years, with an evaluation after the 7 years 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. Put simply, you'll need to enter a 6-digit, one-time code sent to your email or phone. 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 250ms.

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.