Data Protection and Retention

1. Purpose

This policy ensures information collected and stored by foundU is appropriately classified and secured. foundU has considered the requirements of AS4390 Australian Standards for Records Management and Australian Standard AS ISO15489, when formulating this protocol.

2. Definitions, terms, and acronyms

Regular Data/Information is information available on the standard foundU public website and is not Sensitive or Semi-Sensitive Data. Consent has been provided to foundU for the use of this information, which may include:

- customer/client/candidate testimonials.
- customer/client/candidate ratings.
- profile pictures.
- customer/client names and logos.

Other Data/Information includes information that foundU collects and stores that is not Sensitive Data, Semi-Sensitive Data or Regular Data (where consent has been obtained for its collection and storage).

Personal Information is any information which identifies an individual or allows their identity to be reasonably ascertained.

Semi-Sensitive Data/Information is information which may be viewed by a Platform User and foundU employees, and includes:

- candidate/employee's full name.
- customer/client company name.
- Australian Business Number (ABN).
- postal address.
- resume.
- contact information, including email address.
- date of birth.
- gender.
- demographic information.
- banking and other financial information.
- invoices.
- charge out rates.
- positions of interest.
- qualification/s and suitability notices.
- photo identification.
- work experience.
- Timesheets.
- equipment.

Sensitive Data/Information is a sub-set of personal information that is given a higher level of protection under the National Privacy Principles. It includes information or an opinion about an individual's:

- an individual's racial or ethnic origin.
- health information.
- political opinions.
- membership of a political association, profession or trade association or trade union.
- religious beliefs or affiliations.
- philosophical beliefs.

- sexual orientation or practices.
- criminal record.
- genetic information.
- biometric information that is used for certain purposes.
- biometric templates.

Employee means any person employed or contracted by foundU Holdings Limited or its subsidiaries.

User includes any person granted access to foundU ICT facilities or services, including the foundU Platform

3. Scope

This policy applies to all employees. Categories of information may change from time to time, and the onus is on all employees to regularly monitor this policy to ensure compliance.

foundU staff should only accept data from outside the organisation using OneDrive, SharePoint or Dropbox.

4. Policy statement

foundU is committed to a policy of protecting data and information in accordance with the requirements of AS4390 Australian Standards for Records Management and Australian Standard AS SIO15489.

The entire foundU server will be secured by a 256-bit SSL/TLS certificate. Further steps to secure sensitive data/information stored in the database, or in cookies/sessions on foundU devices, include encryption with a dynamically generated encryption key.

5. Protocol

5.1. Sensitive data/information

Protection Methodology: Sensitive data/information is stored on the database as an encrypted string. The encryption key is unknown as it is dynamically generated and is therefore unable to be decrypted.

Retention Processes: Sensitive data/information is retained for seven (7) years from the date of last use and then destroyed or returned to the owner.

5.2. Semi-sensitive data/information

Protection Methodology: Semi-sensitive data/information is stored on the database as an encrypted string. The encryption key is known and hidden in a password protected file. This information can be decrypted and shown to the end-user; however, it is not stored on the users' machine to prevent any malicious software on their machine from accessing this information.

Retention Processes: Semi-sensitive data/information is retained for seven (7) years from the date of last use and then destroyed or returned to the owner.

5.3. Regular data/information

Protection Methodology: Regular data/information will only be stored with the owner's consent and will not be capable of being accessed other than through the foundU website. Any bulk collection of regular data/information will be protected as per the semi-sensitive data/information methodology.

Retention Processes: Regular data/information is retained for seven (7) years from the date of last use and then destroyed.

5.4. Other data/information

Protection Methodology: foundU applies appropriate internal controls to protect other data/information it collects and stores. These controls include password protection of data accessing tools and standard server security protections.

Retention Processes: Other data/information will be retained for the relevant period under the appropriate laws and regulations and then destroyed.

Document History

Document Name	Data Protection and Retention
Document Owner	Chief Technology Officer
Approved by	foundU Board
Effective Date	01.2020
Date of Last Revision	02.2024
Version	F
History	A – Document creation (01.2019) B – Annual review (01.2020) C – Annual review (05.2021) D – Annual review & added accepting external data (02.2022) E – Annual review (04.2023) F – Annual review (02.2024)