USERBACK

# Information Security Policy

Version: 2

---

# Encrypted Transmission

All browser connections and communication is transmitted over HTTPS, ensuring data privacy and integrity. Our servers only support the highest level of encryption 256-bit cipher suites TLS 1.2 or TLS 1.3, protecting against unauthorized disclosure, modification, and replay attacks.

- All non-essential ports and external network interfaces blocked by default
- No financial data or credit information is stored in any Userback system
- All account passwords are stored as one-way hashes
- All account data is encrypted and securely stored in database

# Key Management

Userback maintains a strict policy for assigning and distributing keys which may access any production or development systems.

- Access keys to the production servers are only distributed to CTO and Sys Admin Lead
- Keys are never stored in any online system
- Keys are never stored anywhere as plaintext
- Individual access keys are generated per employee with developer only access

# Source Code

- We perform static code analysis of all production code
- We perform third party security assessment
- All sub-dependencies have been vetted for security and performance issues
- We follow strict compliance with source code licensing and open-source licensing
- We do not use production data in our test or development environment

# Datacenter security

We use a third-party, top-tier datacenter that maintains several industry-recognized certifications, including FedRAMP, ISO, SOC, PCI, and more.

Our hosting provider is also compliant with numerous regulations, privacy standards, and frameworks, including HIPAA, HITECH, GLBA, the EU Data Protection Directive, EU-US Privacy Shield, FISMA, and more than 30 others.

# Full Disk Encryption

All infrastructure used by the Userback product uses industry standard full disk encryption.

All Userback portable computing devices are required to employ full disk encryption regardless of their intended use or the data stored on them.

# Awareness and training

All staff and contractors go through a vetting process where they are subject to background checks and confidentiality agreements.

We provide an ongoing program of security awareness training designed to keep all members of staff informed and vigilant of security risks. This includes regular assessment of comprehension to measure the program’s effectiveness.

## Secure Workstations

- All company pcs and laptops use encryption for storing of any potentially sensitive data
- All company pcs and laptops use anti-malware and antivirus software

## Compliance

Userback adheres to the Australian Privacy Act 2003, Section 2 of the Information Privacy Act 2009, the Australian Privacy Principles and is compliant with the EU GDPR legislation.