360 Tender Evaluations Security Statement

INTRODUCTION

360 has been developed using modern web-application techniques with security as a focus from its core. The security measures are broad, multifaceted and intended to prevent, minimise and mitigate against:

- Data theft
- Data loss (both accidental and deliberate)
- Data corruption (both accidental and deliberate)
- System downtime
- Developer errors and oversight
- Loss of administrative control

PHYSICAL SECURITY

360 is hosted in a physical environment in Australia that has been independently verified as ISO 27001 compliant and has layers of security to protect the:

- Building
- Infrastructure
- Data
- Electricity supply

simplylogical.net®

360 Tender Evaluations Security Statement

HOST PLATFORM SECURITY

360 is hosted on a platform that is monitored by an organisation that has been independently verified as ISO 27001 compliant:

- The host platform has hardware redundancy
- Data is isolated
- Data is encrypted at rest
- A back-up regime operates on multiple tiers and with multiple cycles
- The back-up regime has passed testing

PRODUCT SECURITY

Security is applied at every layer within 360:

- 360 uses Transport Layer Security 1.1 as a minimum and 1.2 by default
- Passwords are encrypted with a highly secure one-way algorithm
- 360 does not contain data that would make it a high-value target by a large sub-set of criminals – specifically:
  - No credit card details
  - No health records
- 360 is built with sound software development practices to avoid known threats including:
  - Buffer overruns
  - Script injection
  - Cross-site script injection
  - Brute force attacks

simplylogical.net®

360 Tender Evaluations Security Statement

DEVELOPMENT SECURITY

360 is being modernised with a commercially available development framework that uses a Single Page Application (SPA) architecture.

The framework accelerates development, improves product performance, and improves product security.

Security benefits:

- The potential for developer error is greatly reduced
- Newly identified threats can be managed more easily and more quickly
- Create, Read, Update, and Delete requests are processed through strict algorithms that necessitate deliberate security-conscious decision-making before functionality is unlocked – i.e. all functionality is locked by default
- Structural alignment of data and code is automated with the effect that data storage is protected from corruption
- Data limits are applied to all requests
- Data stored and data transmitted is carefully delineated
- Exceptions (system execution errors) are managed such that:
    - Developers have sufficient information to resolve the problem
    - Hackers cannot use exceptions to identify the system's internal workings

DEVELOPER CREDENTIALS

360 is owned by and is being modernised by simplylogical.net – a Microsoft Silver Partner certified for application development.

simplylogical.net®