simplylogical.net

Authors of high-quality software in Canberra since 2002
Proudly supporting 360 – the procurement manager's dream solution

web: **simplylogical.net/360** email: **support@simplylogical.net** socials: **@SL360au**
office: **+61 2 51 004 009 | Unit 11, Level 3, 161 London Circuit Canberra City ACT 2601**
mail to: **Ngunnawal Country, 12 Wangara Street Aranda ACT 2614**
ABN: **84 099 636 709** ACN: **099 636 709**

PUBLIC SECURITY STATEMENT

360 – Quote & Tender Evaluation Software

This document is for users and potential users of 360 who are interested to know how their information is kept secure once entered into 360. For the benefit of Australian Government entities, we have another version of this document that is aligned with the Protective Security Policy Framework's requirements. The document can be provided to suitably vetted security managers.

CONTENTS

1. INTRODUCTION TO THE SOFTWARE AND ITS SECURITY

360 – Quote & Tender Evaluation Software ("the Software") is owned, developed, and managed by simplylogical.net – a Microsoft Silver Partner certified for application development[1].

The Software is cloud-based and is used by private sector entities and all levels of government ("Buyers") to request quotes, tenders and other information from providers of goods and services ("Providers"). The information entered into the Software is treated as commercial-in-confidence and procurement-in-confidence.

In determining the type and value of the data and the security objectives for the Software based on an assessment of the impact if it were to be compromised, simplylogical.net has adopted security practices so that the software can receive and store information with **OFFICIAL**, **OFFICIAL: Sensitive**, and **PROTECTED** classifications. The Software is **not** to be used for data of a higher classification than **PROTECTED**.

[1] Microsoft has announced changes to its partnership program in 2022 that require sales generation for Microsoft that is beyond simplylogical.net's capacity. The current certification will transition to a legacy certification in August 2023.

simplylogical.net has zero tolerance for security risks rated High or Critical using the Common Vulnerability Scoring System scale. The Software has been developed using modern web-application techniques with security at its core. The implemented security measures are broad, multifaceted and 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

In determining whether to host the Software on-premise or using cloud services, simplylogical.net concluded that cloud-based services are far superior from a security perspective. The Software utilises the cloud-provider's scalability, back-up services, redundancy, physical security, denial of service defences, encryption, and monitoring systems to protect against:

- Hardware theft
- Data loss
- Data corruption
- System downtime
- Loss of administrative control

2. Governance

2.1 Risk Assessment

The Software is designed to facilitate best-practice procurement activities – i.e. requests for tender. The system contains:

- Requests for tender within their various stages which are broadly defined as: in preparation, open for responses, being evaluated, finalised.
- Business details including staff contact details
- Contract details

The risks associated with information being lost, destroyed, damaged, compromised or misused are:

- **Probity leak**: unauthorised access to the details of a request for tender that potentially gives a business an unfair advantage when a tender is issued, thus compromising and potentially invalidating a procurement activity, as well as potentially having further impacts on the commercial practices of any business(es) whose commercial-in-confidence information is compromised.
- **Industrial espionage**: unauthorised access to commercial-in-confidence information that a business has entered into the Software trusting that it will be made available to the evaluation team alone, only for the purposes of the procurement activity.
- **Privacy breach**: unauthorised access to business and personnel contact details[2] intended only for access and use in line with the terms and conditions for use of the software.
- **Data corruption**: by an external 'hacker' or through authorised users not protecting their log-in credentials, leading to, for example, manipulation of evaluations scores or other aspects of a procurement activity, to alter an outcome.

simplylogical.net incorporates security measures during all stages of the Software development and has undertaken independent external testing to identify vulnerabilities. simplylogical.net has zero tolerance for security risks rated High or Critical using the Common Vulnerability Scoring System scale.

2.2 Parties Responsible for Information Security

There are four parties responsible for protecting the in-confidence information within the Software:

1. simplylogical.net's infrastructure host is responsible for physical and some of the host platform security. The terms of use and licences stipulated by the host and simplylogical.net delineate responsibilities and accountabilities for each party – see sections:
    - Physical Security on page 65
    - Host Platform Security 6
2. simplylogical.net has the responsibility for ensuring the information is only accessed by authorised personnel in accordance with best-practice procurement workflows. To this intent:
    a. simplylogical.net has implemented measures that apply to all staff and all software development. These include, but are not limited to:
        i. Quality assurance processes
        ii. System access controls
        iii. The management of passwords and other secrets

[2] Limited to the names, email addresses, and phone numbers of staff and business directors

        iv. Email and other internet service usage (i.e., identifying and avoiding phishing)
    b. the Software's technical support team has:
        i. Mitigations to ensure its help-desk activities do not compromise security, for example, using data within the Software to verify a caller's identity
        ii. Technological restrictions and procedures so that the technical support team cannot access in-confidence information without the consent of an authorised user (and only when necessary)
        iii. Security controls so that only qualified and authorised staff can access the Software's servers to perform second-tier support and system maintenance
        iv. Records in the form of:
            1. Help-desk communications trails
            2. Notification and event logs stored in the Software's database
            3. History tables in the Software's database
        v. A 'check-if-unsure' culture in which staff confirm the best approach with the Director if they are unsure when responding to support requests

3. Buyers have responsibility for ensuring:
    a. Procurement probity controls are maintained
    b. In-confidence materials are protected when downloaded onto their systems[3]
    c. Current and former staff and contractors have the correct levels of access for the in-confidence information
    d. Email addresses and other contact details are accurately recorded (to avoid information being sent to the wrong people and so that the technical support team can verify identities)
    e. Staff and contractors are sufficiently trained so that they adopt information safety practices appropriate for internet-based software holding commercial-in-confidence information (for example: protecting passwords and using multi-factor authentication)
    f. No information classified higher than PROTECTED is entered into the Software
4. Providers have responsibility for ensuring:
    a. Current and former staff and contractors have the correct levels of access for the in-confidence information
    b. Email addresses and other contact details are accurately recorded (to avoid information being sent to the wrong people and so that the technical support team can verify identities)
    c. Staff and contractors are sufficiently trained so that they adopt information safety practices appropriate for internet-based software holding commercial-in-confidence information (for example: protecting passwords and using multi-factor authentication)
    d. No information classified higher than PROTECTED is entered into the Software

The technical support team will never ask for your password – do not share it!

2.3 Mitigation Measures

The list below itemises some mitigation measures simplylogical.net has implemented for the Software on top of those that apply to the technical support team:

1. The Software encourages users to use multi-factor authentication (MFA) and allows buyers to set security rules:
    a. Mandating MFA

[3] Clauses within simplylogical.net's Software as a Service agreement regarding keeping confidences exist beyond the term of the agreement

   b. Forcing passwords to be changed regularly
   c. Disallowing password reuse
2. The Software has reminders in its user interface to:
   - Inform users when, and why information will be made available and to whom
   - Remind its users to be mindful of confidential information
   - Remind its users of the source of downloadable files and the potential for the files to contain malware
3. The Software has security roles that Buyers and Providers can apply to their staff and contractors and documentation that explains what each role is for[4]
4. The Software automatically notifies users if administration tools are used to perform security-specific actions such as resetting a password or changing a user's email address
5. See measures specified in section Product Development Security on page 7

3. Personnel Security

The Software is owned, developed, and managed by Sharrowlane Pty Ltd t/a simplylogical.net.

simplylogical.net does not have a formal information classification system or staff security clearance system, however:

1. In determining the type, value and security objectives for the Software based on an assessment of the impact if it were to be compromised, simplylogical.net has adopted security practices so that the software can receive and store information with **OFFICIAL**, **OFFICIAL: Sensitive**, and **PROTECTED** classifications. The Software is **not** to be used for data of a higher classification than **PROTECTED**.
2. All employees are trained and are contractually obligated[5] to treat the data in the Software as commercial-in-confidence
3. simplylogical.net withdraws all access rights and recovers all company-issued assets when staff leave
4. Staff have restrictions that apply to the office and elsewhere
5. The Software's development team consists wholly of people who have passed an Australian government approved vetting process
6. The Director monitors and manages the ongoing suitability of personnel with respect to all facets of their work roles, including security considerations
7. Only staff with Australian citizenship have access to administer the Software's servers

[4] https://simplylogical.atlassian.net/servicedesk/customer/portal/2/article/475234305

[5] Clauses within simplylogical.net's employee contract regarding keeping confidences exist beyond the period of employment and staff are reminded of these clauses on departure

4. Physical Security

Physical security applies to:

1. simplylogical.net's office and equipment (including remote access)
2. The Software's source code and documentation
3. The Software's data

simplylogical.net's equipment is located in an office to which only staff have access and home offices. Staff are not permitted to use equipment outside of the approved offices (such as cafés) except when travel requirements make working from an approved location impossible.

The Software's source code and documentation is stored using secure cloud-service providers. The office equipment, source code, and documentation stores do not contain the Software's data.

simplylogical.net outsources the physical security of the Software's data to an organisation that implements and maintains technical and organisational security measures applicable to its cloud infrastructure services under globally recognized security assurance frameworks and certifications, including IRAP, ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, and SOC 1, 2, and 3. These technical and organizational security measures are validated by independent third-party assessors, and are designed to prevent unauthorised access to or disclosure of customer content.

The Software is hosted in a physical environment in Australia and has layers of security to protect the:

- Building
- Infrastructure
- Data
- Electricity supply

5. Host Platform Security

simplylogical.net outsources its host-platform security to the same organisation that protects the Software data's physical security. The organisation's platform architecture and its organisational security measures ensure:

- The host platform has hardware redundancy
- Data is isolated
- Data is encrypted in transit and at rest
- Disaster-recovery back-ups are geographically dispersed

Using the host-platform described above, simplylogical.net ensures:

- Firewalls and other security controls are configured as recommended by the host platform provider
- Software updates are applied in a timely manner
- Only trained simplylogical.net staff have access[6]
- A back-up regime operates on multiple tiers and with multiple cycles
- The back-up regime has passed testing[7]
- Snap-shots (for disaster recovery) are taken multiple times a day.

[6] Only Australian Citizens who have passed security checks can access the servers
[7] Last tested: 15 January 2020 (passed – no configuration changes since tested)

6. Product Development Security

simplylogical.net engages qualified penetration testers to test the software's security. The test methodologies used by the penetration testers is compliant with standards published in the Australian Government Information Security Manual for web application development – specifically the Open Web Application Security Project (OWASP)[8].

Report specifics are not included in the public security statement. The penetration tester identified no HIGH or CRITICAL vulnerabilities in its 27 September 2022 report.

Security is applied at every layer within the Software:

- The Software uses Transport Layer Security (version 1.2 by default)
- Passwords are encrypted with a highly secure one-way algorithm
- The Software is built with sound software development practices to avoid known threats including:
  - Buffer overruns
  - Script injection
  - Cross-site script injection
  - Brute force attacks
  - Phishing

The Software does not contain highly sensitive and valuable information that alone would make it an attractive target for opportunistic cyber-criminals – specifically the Software does not store:

- Credit card or bank account details
- Health records
- Classified research
- Individuals' residential address details

The Software is being modernised with a 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 mitigated 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
- Exceptions (system execution errors) are carefully managed to provide simplylogical.net with diagnostic data without exposing the system's internal workings to hackers

[8] Australian Government Information Security Manual (www.cyber.gov.au/ism), June 2020, p 100