OVERVIEW:

TNZ Group utilizes multiple methods to ensure the best possible security across the product suite:

- **Email**

By default, email sessions are encrypted using STARTTLS where possible, with an option to enforce encryption if required.

In addition to email encryption, other security measures include SPF, PTR, DKIM and DMARC sender verification.

- **Web (Dashboard, API)**

Access to the tnz.com.au dashboard and APIs are encrypted (HTTPS) with support for TLS (v1.2+) encryption.

Dashboard logins use a tiered structure, limiting information viewable based on a user's access level. Privileged users can view message information, billing data and perform configuration changes.

- **FTP**

FTP services support both SFTP and FTPS encryption.

IMPLEMENTATION:

When interfacing with TNZ services, connections will be via the following IP/Subnets:

52.62.254.254/32
52.65.188.40/32
60.234.34.112/28
60.234.61.16/29
175.45.87.23/32
175.45.87.44/30

Common ports:

80 (HTTP)
443 (HTTPS)
20 (FTP)
21 (FTP)

This document will be updated as IPs are added/removed.

POLICIES:

A summary of TNZ's security policies:

- **Data Storage (In-House Encryption, NoArchive, PGP Encryption)**
Fax and email content is encrypted using TNZ Group's In-House Encryption software. It is then Base64 encoded to further deter intruders retrieving the fax data and reassembling the fax image. At the point of distribution to the end user (email or web retrieval) the fax image decrypted and delivered as a PDF/TIF image.
NoArchive is a recommended option for enterprise clients. When enabled, fax image data will be securely purged (using an overwrite routine) as soon as practicable following fax delivery. Call Detail Records (Caller IDs, times/dates, number of pages, etc) will be kept. This limits the window of vulnerability for data loss.
PGPEncryption is an additional option that enables PGP Encryption of received faxes (additional costs apply). This option is built to PCI-DSS compliance criteria.

- **Data Retention**
By default, live data is stored online and accessible via the Web Portal for three months. Target retention for warm archive data is 12 months, stored in attached offline storage. Target retention for cold archive data is three years, stored in disconnected offline storage. NoArchive data is stored for the minimum period of time required to complete message transmission (typically 5-20 minutes).

- **Closed Networks, DMZs and VPNs**
TNZ Group's networks are restricted.
Physical access is granted for authorised personnel only using industry standard access restrictions (keycards with separate keys, surveillance, etc).
Where remote IP access is allowed, access is restricted to VPN only (2048-bit certificate).

- **WAN File Transfers**
WAN file transfers (where files are transmitted to servers outside the main core network, typically for final delivery via SMS, Fax, Email or Voice) are done so via a fully encrypted session using In-House applications. The file is encrypted, broken into segments, then transmitted and reassembled at the receiving end. This ensures the upmost security when your data may be transmitted over a connection that is not controlled by TNZ Group.

- **Business Continuity & Incident Reporting**
TNZ Group operates with a regularly reviewed Business Continuity plan to ensure resiliency against outages. Should an incident occur, the Incident Management Plan includes instructions to identify, verify, contain, analyse, recover and report on the incident.

Should you wish to be notified of any scheduled or unscheduled outages, contact support@tnz.com.au

- **Server Security**

TNZ administrators follow a regimented Server Security Policy. Contact your account manager for access to this policy.