



## Security Information

TSANet Connect is the system Members use to make a collaboration request with another Member. The system was designed to be simple to use and meet the requirements of data protection including GDPR. This document explains key system design decisions and provides answers to common security questions that Members may have about the system.

### Data Privacy

The system was designed to reduce the risk of storing sensitive information about our Members Employees or Customers. To accomplish this the following decisions and policies were created.

1. The system only maintains basic contact details for a user (Name, Email, Phone)
2. The system has single sign-on capabilities so Members can use their own employee identity management systems
3. The system does not allow attachments
4. The system removes all customer data that was part of a request after 30 days
5. After the connection is made between Members they work within their own systems and use their own internal policies while working the issue
6. Only endpoint meta-data is stored in the system and members can link back to their internal systems with their case number
7. TSANet will follow best practices for security and maintain ISO 27001 certification

### ISO 27001 Certification

ISO 27001 is a globally recognized standard mandating numerous controls for the establishment, maintenance, and certification of an information security management system (ISMS).



TSANet's certification was issued by BSI, an independent, third-party auditor that confirmed TSANet possessed the formalized information technology (IT) security policies, procedures, and technical controls necessary to meet the standard. [View TSANet ISO 27001 Certification](#)

Below are common questions and answers on Data Privacy

**1. *What document defines the TSANet Data Protection and Privacy?***

View TSANet Data Protection & Privacy Statement at <https://tsanet.org/legal-policy/>

**2. *What legal documents define how TSANet and Members work together to solve common customer issues***

View legal documents including the code of conduct at <https://tsanet.org/legal-documents/>

**3. *What Employee information do you store in the system***

The user profile requires Name, Email and Phone number. Members can also use Single Sign-on from their own identity management systems including support for just in time user provisioning and can control what information is sent to the TSANet Connect system

**4. *What Customer information do you store in the system***

Members can define what common customer information they require when receiving a request. All customer data is removed from the system after acknowledgement and the system will remove all customer data after 30 days leaving only the request metadata below

Submitted By, Case Number, Priority, Summary, Date Requested, Date responded

**5. *Do you encrypt data in transit and at rest***

Data in transit is encrypted with SSL and data is encrypted at rest with AES-256.

## System development

The system was developed using best practices defined in the OWASP Secure coding practices guide. The Open Web Application Security project OWASP defines best practices for coding secure web applications. For more information on OWASP see <https://owasp.org/>

Some specifics of this best practice include:

1. Best practices for administration of the system including 2-factor authentication to all development and system administration environments
2. Encryption on the transmission of all data
3. Best practices for API development and access

## Network and Host Security

The system is hosted at Linode: <https://www.linode.com/>

Linode provides a complete solution including physical and environmental security that includes both networking and host operating environments up to and including the hypervisor. Linode is a SOC 2 certified environment and more details on Network and Host security practices can be found at <https://www.linode.com/legal-security/>

## Penetration Testing

TSANet has contracted with Security Metrics <https://www.securitymetrics.com/> to do penetration quarterly automated and annual manual testing on the TSANet Application. This testing includes both network and authenticated application penetration testing.

## System uptime and Support

The system is designed to provide 99.99% uptime. The following document provides information on the support process

<https://tsanet.org/tsanetconnect-support>