Security Requirements for Customers

TIS Security Team

Table of Contents

End User Device Security

Operating System and Browser

Use a supported version of your operating system and keep it up to date on all recommended patches. The same applies to the internet browsers of the users. TIS Support can provide you a list of supported browsers.

Computer

Do not use computers in public areas and third parties (i.e., Internet cafes, airports, etc.). Use computers provided by your company.

Anti-Virus and Firewall

Install and use up-to-date antivirus software to prevent, detect and remove malware of all kinds. We recommend modern antivirus technologies able to detect and mitigate advanced cyber threats (EDR, Endpoint Detection and Response)
Utilize anti-spam, anti-phishing, firewall and intrusion detection services as additional security layers for blocking and identifying potential online attacks.

Authentication and Login

TIS Internet Address and Website

Use the TIS services only through the TIS website (www.tispayments.com) and never through links displayed on other websites, search engines or in e-mail messages.

Single-Sign-On

We advise to enable Single Sign-On with your own identity provider, to ensure that your company's policies are enforced at all times. This technology:

- Allows users to log-in with the account they already have in your company,
- Allows you to enforce your company's Password Policy and Multi-Factor Authentication requirements,
- Allows you to track login activity in your own audit logs, for usage in your security tools,
- Ensures that users disabled in your central systems immediately lose access to TIS systems as well,
- Allows you to follow the principle of Zero-Trust, for instance enforcing that your users only connect from trusted devices, etc.

For more information, please contact TIS support.

IP Address Filtering

Use IP filtering to allow logins from selected IP addresses or network ranges. The settings are defined in the Administration Area under Security Settings.

Exception: CashOptix does not IP filtering to restrict the login from unwanted IP addresses

Manual and automated log-out

It is recommended to set a user session timeout of max. 5 minutes in the Administration Area under Security Settings. The user session timeout defines how long a session is active if no user interaction occurs.

Users are additionally advised to select "Logout" instead of directly closing the browser window.
Exception: CashOptix does not support the option to set a custom user session timeout.

User Passwords within TIS

This only applies if you do not wish to use Single Sign-On.
Use strong passwords that comply with current security standards. Discourage password-sharing among users. Do not store your passwords on your laptop, instead use a password vault. In case TIS' password policy does not meet your security requirements, we encourage customers to activate single sign-on using your own identity provider (item 2.9).

Exception: It is not possible to set a password expiration period in CashOptix, we encourage customers to activate Single Sign-On using your own identity provider to apply your own password policy.

Multi-Factor Authentication within TIS

This only applies if you do not wish to use Single Sign-On.
In general, any user of TIS should use multi-factor authentication (via TIS token or your own, via single sign-on – please refer to item 2.9). For user roles such as *Company Administrators*, *Approvers* and *Administrators* two-factor authentication is mandatory.

Exception: CashOptix doesn't support two-factor authentication, we encourage customers to activate Single Sign-On using your own identity provider to have MFA.

Hardware Tokens

TIS delivers to its customers a timed one-time-password token for two-factor authentication upon request. Make sure that the receiver of the tokens confirms with TIS the delivery of the tokens. Only when confirmed the tokens are assignable to users. After the activation at TIS the tokens are assigned to users in the User Management via its serial numbers.

Exception: CashOptix doesn't support hardware tokens

Software Tokens

TIS provides an option to use software tokens. For more details, please contact the respective Customer Success representative.

Exception: CashOptix doesn’t support software tokens

User Management and Authorization

4-Eyes Principle

Make sure that any approval process is properly secured with a 4-eyes principle. Avoid single approval rights for productive bank accounts. The 4-eyes principle should be enabled for administration area after go-live. Any changes to master data should be covered by a 4-eyes principle as well.

User Groups and Permissions

With TIS' user group and permission concept you can customize for each user role the exact set of assigned read, create, update and delete permissions for any master data or transactional object. TIS recommends assigning to each user group only the minimum required permissions, always considering the least privilege and role-based access control principles. Users associated to specific organization entities should only be granted permissions for objects within the scope of this entity.

We encourage you to review periodically users access rights to avoid any illegitimate access to the platform.

Workflows

The functionality to manage another user's workflows should be disabled before go-live.

Secure Store

Tenant Password

The Tenant Password is used to encrypt sensitive customer data such as banking access parameters. Save the password at a secure place and choose a complex secure password. This password cannot be recovered by TIS. In case of loss, it will require re-initialization of all bank connections.

Information Exchange and Data Management

E-Mail

As a general rule, TIS does not send out any e-mails asking their customers to disclose confidential access and transaction data such as usernames, passwords, and other confidential information etc. or to scan QR codes outside of our platform.

Disclosure of Information

Do not send company confidential information or personal data to any employee of TIS, neither through e-mail nor via the support portal.

Excel Import/Export

Disable the Excel-Import / Export functionality before going live to avoid non-governed master data management processes.

Test-System

Do not use productive data in the TIS test systems. Make sure that your ERP test system is connected to the TIS test system. Never process productive payments on the test systems.

Data Privacy

If your company operates in or collects and processes data from citizens of countries where data protection laws regulate the careful handling of personal information, pay special attention to where you store such data within the TIS application. Do not misuse general text fields, such as comment or title columns, for personal data. Keep track of where you put such information and implement the necessary processes in your company to handle these occurrences accordingly. This includes (but may not be limited to) the following areas:

Custom Fields

Customers can configure custom fields at various company levels in the application in order to store additional information together with most master data. TIS is not aware of the nature of the content entered into such fields. Keep the personal data stored in such fields to a minimum, especially on higher levels where a larger group of people has access to it. Enter such information only in places where it is expected, set permissions accordingly, and keep track of these within your company. You are responsible for correcting, blocking, and deleting such data as well as providing information about it if necessary. Please note that the General Information History may also contain an audit trail of custom field values.

Attachments

Similar to custom fields, attachments can be uploaded at different locations within the application. Again, TIS is not aware of the nature of such content and thus cannot automatically identify personal information within attachments. Keep personal data within attachments to a minimum and keep track of where you upload such documents. It is your responsibility to correct, block, and delete these files as well as provide information about their existence if requested. Please note that the Attachment History also contains references to uploaded documents even after they were deleted. Remove entries from this audit trail on demand. For providing links to payments and/or files, keep track what links you provide. It is your responsibility to provide links only to secured sites and documents.
Advise all employees that personal attachments uploaded to their user profile have to be managed by the individual user and must not contain personal data for which no consent was given. This also includes a user's profile picture.

Reports/Exports

Delete reports and data export files generated in the background from the Jobs view. These documents are accessible as result of finished background jobs and may contain personal information, depending on the execution context.

Templates

Do not include personal information within Excel report or Word templates.

Certification and PGP Keys

Do not store personal data in the details of security certificates and cryptographic keys. If issuer or user ID fields contain such information, remove or replace it as legally required.

Data Integrity and Process Monitoring

Payment Processing

When a payment file is uploaded to the TIS platform the file is stored in the Temporary Storage before it is processed by the Bank Transaction Manager Application. If a payment file cannot be processed (e.g., because of syntactical or semantic errors) the payment file stays in the Temporary Storage in status error including an error message. TIS recommends customers to monitor payment files in the Temporary Storage Monitor within the Administration area of the TIS Platform and ensure that payments are processed in time.
The protection of payments from unauthorized manipulation is ensured by signing the payment with a customer specific key within the Bank Transaction Manager application. Payments are not processed if the signature of a payment is not valid. It is strongly recommended to verify the correctness and validity of the data before approval. It is recommended also to enable 'Signing with token' for additional security upon approval (subject to license). The status of the payment indicates if the transmission is successful. This can be verified in the Bank Link Configuration in the Administration area of the TIS Platform as well. TIS strongly recommends checking the status especially for time critical payments to ensure payments are transmitted on time.

Payment Status Report

Payment status reports, which are delivered by the bank, can be downloaded and processed by the TIS Platform. a successful download can be monitored either at the Bank Link Configuration or on the payment itself where the status of the payment is updated accordingly. The pull status shows all successful and failed download operations at the bank. The files are stored in the Temporary Storage before they are processed by the Bank Transaction Manager application.

Bank Account Statement Processing

Bank account statements are downloaded by the TIS application from the respective bank and stored in a canonical data model within the TIS application. Successful and failed downloads of account statements can be monitored in the Bank Link Configuration in the Administration Area of the TIS Platform. The bank account statement files are visible in the Temporary Storage before they are processed by the Bank Statement Manager application. If a bank account statement cannot be processed (e.g., because of syntactical or semantic errors) the account statement file will stay in the Temporary Storage with an error status. TIS recommends monitoring the status in both areas to ensure account statements are processed on time.

Customers can connect client systems to automatically download bank account statement files from the TIS Platform. In those cases, customers can monitor the successful download at the Client System Configuration in the Administration Area of the TIS Platform.

File Downloads from TIS Platform

TIS provides an Application Programming Interface (API) which allows to download files such as bank account statements. When customers use their own implementation to connect to TIS, the download must be confirmed by the client system. Customers must ensure that the file is correctly downloaded to the target location before providing confirmation to TIS. TIS Agent and SAP ERP Add-on already have this process implemented.

Annex A: Document History

Version	Date	Author	Changes
1.0	15.08.2019	Security Team	Draft version created
1.1	22.08.2019	Security Team	Approved version published
1.2	10.08.2020	Security Team	General, yearly review
1.3	01.07.2021	Security Team	“Authentication and Login” and “Secure Store” chapters edited
1.4	15.09.2022	Security Team	Aligned password recommendation to better fit NIST recommendations. Highlighted recommendation to use SSO instead of platform stand-alone accounts. Changed MFA for administrators and approvers to be mandatory. Added recommendation of ‘signing with token’ for payment approvals. Added responsibility of providing safe links. Changed recommended value of timeout.
1.5	19.09.2023	Security Team	Updated sections 2.2 IP Address Filtering 2.4 Session Timeout 2.5 User Passwords 2.6 Two-Factor Authentication 2.7 Hardware Token 2.8 Software Token
1.6	24.07.2024	Security Team	General, yearly review