16 06 2026

Security Requirements for Customers

Contents

Contents 1
End User Device Security 3
- Operating System and Browser 3
- Computers 3
- Anti-Virus and Firewall 3
- TIS Website 3

Authentication and login 4
- Single Sign-On 4
- IP Address Filtering 4
- Session timeout, log-out 4
- User Passwords within TIS 4
- Multi-Factor Authentication within TIS 5

User Management and Authorization 6
- 4-Eyes Principle 6
- User Groups and Permissions 6
- Workflows 6

Secure Store 7
- Tenant Password 7

Information Exchange, Data Management 8
- E-Mail 8
- Disclosure of Information 8
- Master Data Import/Export 8
- Customer Test-System 8

Data Privacy 9
- Custom Fields 9
- Attachments 9
- Reports/Exports 9
- Templates 9
- Certification and PGP Keys 9

Data Integrity and Process Monitoring 10
- Payment Processing 10
- Payment Status Report 10
- Bank Account Statement Processing 10
- File Downloads from TIS Platform 10

Owner:	Security Team	**Classification:**	Public
Document:	Policy	**Status:**	Final
Version	1.8	**Date:**	16.06.2026

Specificities for customers using SWIFT 11
Context 11
Implementation when performing SWIFT sensitive tasks 11
Implementation when accessing SWIFT-related data 11
Annex A: Document History 13

Owner:	Security Team	**Classification:**	Public
Document:	Policy	**Status:**	Final
Version	1.8	**Date:**	16.06.2026

End User Device Security

Operating System and Browser

All users must use a supported version of their operating system, kept up to date on all recommended patches. The same applies to internet browsers. TIS Support can provide you with a list of supported browsers.

Computers

Users must not connect from public computers (i.e., Internet cafes, airports, etc.), but from computers provided by their company.

Anti-Virus and Firewall

All users must have a device with 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.

TIS Website

Users must always verify they are on the legitimate TIS website, and access it directly through their bookmarks, rather than clicking links displayed on search engines or e-mails.

Authentication and login

Single Sign-On

We advise enabling Single Sign-On with your own identity provider, to ensure that your company's policies are always enforced. This technology allows:

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

For more information, please contact TIS Support.

IP Address Filtering

TIS allows you to implement IP filtering to restrict logins to selected IP addresses or network ranges. This setting may be redundant if you take advantage of Single Sign-On where you can restrict connections from trusted networks and locations.

Exception: TIS Cash does not provide an IP filtering feature.

Session timeout, log-out

TIS allows you to set a user session timeout 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.

TIS recommends a session timeout of maximum 10 minutes.

Exception: TIS Cash 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,
- Use a password manager.

In case TIS' password policy does not meet your security requirements, we encourage customers to activate single sign-on using your own identity provider (see above).

Multi-Factor Authentication within TIS

TIS recommends implementation of multi-factor authentication for all users. If you use Single Sign-On, make sure MFA is enabled at your identity provider's level. If you can't use Single Sign-on, TIS provides built-in support for software tokens and for TIS-provided hardware tokens, both allowing you to display a rolling code.

Hardware Tokens

TIS delivers to its customers a Timed One-Time-Password (TOTP) token for multi-factor authentication upon request. Make sure that the receiver of the tokens confirms with TIS the delivery of the tokens, as tokens can only be assigned once confirmed. Configuration takes place in the User Management section via its serial numbers.

Exception: TIS Cash does not support hardware tokens.

Software Tokens

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

User Management and Authorization

4-Eyes Principle

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

Master Data Import/Export

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

Customer Test-System

Do not use productive data in the TIS customer test systems. Make sure that your ERP test system is connected to the TIS customer 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 handling of personal information, pay special attention to where you store such data within the TIS platform. 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 platform to store additional information together with most master data. TIS is not aware of the nature of the content entered into such fields. Keep 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 platform. 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. 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 reports 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.

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 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 platform from the respective bank and stored in a canonical data model within the TIS platform. 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.

Specificities for customers using SWIFT

Context

Under SWIFT's Provider Security Controls Framework (PSCF control 4.2), TIS is obligated to enforce Multi-Factor Authentication for all Customer users accessing SWIFT-related data. And under SWIFT's Customer Security Control Framework (CSCF control 4.2) the customer must use a Multi-Factor Authentication for interactive user access to TIS SWIFT-related services. The requirement mandates that "the device used to generate the second factor must not be the same as the device used to enter the first factor. As such, using an app to generate the second factor on the same device/PC used to enter the first factor (password) is not sufficient".

TIS is also obligated to enforce a **session timeout** that cannot be set lower than 15 minutes.

Implementation when performing SWIFT sensitive tasks

TIS enforces that your users use a SWIFT-compliant MFA solution based on **dedicated hardware tokens** at the time they perform SWIFT sensitive tasks, such as confirming sensitive business transactions.

Implementation when accessing SWIFT-related data

The requirement in the PSCF and the CSCF also applies when accessing SWIFT-related data, even when not performing a sensitive operation. There are two possible implementations, depending on whether your tenant **does or does not use Single Sign-On**:

- **For users not logging-in with Single Sign-On**, TIS enforces usage of TIS-provided **dedicated hardware tokens** at each log-in for all users of the tenant. The options to use software tokens (TOTP) or to remove MFA are not available.
- **For users logging-in with Single Sign-On**, the Customer must comply with the rules described below. **If you are not technically able to enforce the below rules, you must use dedicated, TIS-provided hardware tokens for all your users**.

1. **Multi-Factor Authentication implemented by your identity provider must be required at each log-in to the TIS Application**

Note, this is stronger than having MFA enabled on your company account – it specifically means that you must configure your identity provider to require MFA **at each log-in** to TIS.	**Examples of valid implementations**	**Examples of invalid implementations**
	EntraID Conditional Access Policy that mandates MFA at **each** connection to the TIS service, with short session timeout.	Automated, seamless login based on Single Sign-On based on an existing session, or previously satisfied MFA.

2. **Multi-Factor Authentication implemented by your identity provider must use a separate device for the second factor**

Note that if your users have multiple MFA options, it is possible to restrict which one can be used for TIS through the "authentication strength" options of EntraID Conditional Access Policies (if applies to you), so to only apply these higher requirements to log-in to TIS.	**Examples of valid implementations**	**Examples of invalid implementations**
	Using a phone as MFA: -MFA on an Authenticator app on phone (TOTP). -Passkey-based MFA on Microsoft Authenticator on phone. Using a hardware key: Hardware-based MFA such as a YubiKey or other passkey.	-Rolling code (TOTP) that the user is allowed to store in a password manager on their laptop -Windows Hello and equivalent macOS passkey and passwordless: even when using biometrics, these solutions **alone** do not satisfy the requirement to have a separate device for MFA (but you satisfy the requirement with Windows Hello + MFA on phone for the TIS service).

Please contact TIS if you are using Single Sign-On but not able to comply with the rules above, so we can enforce usage of TIS-provided hardware tokens for each log-in.

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
1.7	23.05.2025	Security Team	Yearly review. Wording updates.
1.8	16.06.2026	Security Team	Specificities for customers using SWIFT