Version: SEP2023

TARGIT SECURITY SPECIFICATIONS

This document specifies the organisational and technical security measures pertaining to TARGIT's provision of services and processing of data, including through TARGIT Cloud, TARGIT Insight and Support and/or Consultancy Services in relation to these services or any on premise license to the TARGIT Decision Suite.

1. APPLICABLE FOR ALL SERVICES

Technical and organisational security measures		
Area	**Measure**	**Description**
Access control – TARGIT network	Access from external locations	Access to systems is secured by log-on procedures to prevent unauthorized access to systems and applications.
	Access management process	Access management processes ensures that access is granted solely based on a work-related need and on a least access principle. Procedures are established for the establishment, closure and ongoing review of allocated rights based on the principle of a work-related need as well as segregation of duties.
	Identity and access management	Identity and access management is implemented by use of individual user accounts. All accounts are protected by MFA and are monitored for suspicious activity. Workstations are only accessible with individual usernames and passwords.
	Passwords	All employees are required to make secure passwords in accordance with the internal policy for passwords, and passwords shall be encrypted when stored. There are requirements to the formation of passwords. Users are notified when their password must be changed.
	Encryption	Data in transmission is encrypted using TLS (SSL) encryption. Azure file-shares, storage accounts and Cosmos DB is encrypted at rest and in transmission.
	Firewalls	Firewalls are installed to protect against unauthorised access.
	Penetration Tests	Annually recurring activity.

	Protection from malware	Antivirus software is installed on all computers and all downloaded software is monitored.
	Anti-spam and anti-phishing	Anti-spam and anti-phishing software are implemented on the internal mail system.
	Clean desk policy	Physical documents are rarely used, and all physical documents are securely stored away when not used.
	Brute-force attacks	Accounts are locked out after a defined number of incorrect password attempts.
Access control – Customer Data	Customer control	Only designated persons of Customer who as per Customer's instruction to TARGIT have received a login to the Service by TARGIT have access. In general, TARGIT employees do not have access to Customer Data. Customer can grant TARGIT employees a user login (issued by Customer) to enable the TARGIT employee to access Customer Data. A limited number of TARGIT employees with administrator rights to the cloud solution can access Customer Data if it is necessary for operation of the system.
	Authorisation system	Customers can setup an authorisation system with roles with differentiated access and assign these roles to specific users.
	Confidentiality and separation	TARGIT's access to Customer Data is secured through contracts, declarations of confidentiality and ensuring functional separation to minimize errors and misuse of data.
	Encryption	Data in transmission is encrypted using TLS (SSL) encryption. Azure file-shares, storage accounts and Cosmos DB is encrypted at rest and in transmission.
	Login security	Customers are able to use two factor authentication (MFA) when logging in to the system when using OpenID identity providers.
	Erasure	Customer Data can be removed by Customer or at Customer's request at any given time. Any stored Customer Data will be deleted when Customer cancels the subscription.
Personnel	Employee accounts	Procedures and automated scripts ensure that accounts for new employees are set up correctly with multi factor authentication and access levels.

	Awareness, training and education	Employees receive training in IT systems and education in IT security, GDPR and internal policies on security and privacy. Participation in training and education is mandatory for all employees. TARGIT has an established process ensuring that any person performing work for TARGIT and who has access to Customer Data knows about their responsibilities in relation to information security. TARGIT ensures that any natural person performing work for TARGIT and who has access to Customer Data only processes Customer Data in accordance with Customer's documented instructions unless other processing is required under applicable law.
	Withdrawal of access rights	Access rights are withdrawn when an employment is terminated and procedures are in place to ensure that employee accounts are closed correctly.
	Non-disclosure agreements	NDA's form part of the agreements with employees, external consultants and other business partners when relevant.
Physical security	Access control procedures	TARGIT prevents unauthorized access to TARGIT's physical locations via access control procedures.
	Physical protection	TARGIT has organized and established physical protection of TARGIT's physical locations, including against natural disasters, malicious attacks, or accidents.
	Burglar alarms	Alarms are installed at all physical premises to prevent theft or vandalism.
	Fire prevention	Indoor fire sprinklers are installed.
	Remote access	Remote access to any data processor's resources requires VPN.
Policies, procedures, and security organisation	Laws and regulation	Continuous follow-up on current and new legislation and practices.
	Privacy policy	All employees are required to read and follow TARGIT's privacy policy containing guidelines on how to process Customer Data, including personal data in compliance with the GDPR and national regulations.
	Security incident procedure	A security incident procedure is implemented which all employees are required to read and follow.
	Security policy	TARGIT has an internal management approved information security policy.

		The security policy is revised annually and updated as needed. All processing activities are carried out in accordance with internal guidelines establishing the specific security requirements, including rules for authorisation, access administration and access control and logging of login attempts.
	Risk assessment	TARGIT carries out risk assessments on an ongoing basis, based on the developments in the information security field and reviews and implements changes to its technical and organizational measures to address identified risks.
	Security organisation	TARGIT has in its organisation a defined division of roles and responsibilities to ensure information security.
	Business disaster recovery plan	A business disaster recovery plan is implemented and tested regularly.

2. APPLICABLE FOR TARGIT INSIGHT FOR TARGIT DECISION SUITE ON PREMISE CUSTOMERS, ONLY

Logs concerning the use of documents in the TARGIT Decision Suite are stored in local files on customer's server.

When enabling TARGIT Insight, these files are transferred to the TARGIT Insight hosting environment in Microsoft Azure. TARGIT Insight then entails the following:

- An encrypted database specifically for the customer is created in TARGIT's Microsoft Azure SQL server (the "**Azure SQL Database**").
- SQL user and password will be automatically generated for use by the Azure SQL Database and are not shared with customer or TARGIT employees.
- TARGIT Insight will send connection information to the customer's server. This information is not stored locally and only kept in memory. This connection is read-only.
- The only personal data TARGIT Insights stores are usernames and user's access to reports/documents. The username is the same username, which an agent or employee of the customer uses to sign-in to its TARGIT client.
- The data of the transferred customer files are processed and stored in the Azure SQL Database.
- All communication between the customer server and the Azure SQL Database is SSL TLS encrypted.
- Access to the Azure SQL Database is limited through security groups, and only TARGIT employees who are involved in supporting or providing services to the customer will get access and only on a need-to-have basis.