projektron
Plan. Implement. Evaluate.

INFORMATION SECURITY

Since 2008, we have been operating a quality management system based on ISO 9001 that covers the entire value chain and product life cycle – from the product idea to development, testing, documentation, and commissioning at the customer's site, as well as customer support. In 2017, we also implemented an information security management system (ISMS) according to ISO 27001.

TÜVRheinland®
ZERTIFIZIERT
Management System
ISO/IEC 27001:2013
www.tuv.com
ID 9000032687

At the beginning of 2018, we received ISO 27001 certification from TÜV SÜD and in 2021 we received renewed certification according to DIN EN ISO/IEC 27001:2017 . In 2024, we were awarded the certification ISO/IEC 27001:2013 by TÜV Rheinland with the scope of application of development, support, IT services and internal IT administration.

Highest security standards - TISAX® assessment procedure completed

The ENX Association supports with TISAX (Trusted Information Security Assessment Exchange) on behalf of VDA the common acceptance of Information Security Assessments in the automotive industry. The TISAX Assessments are conducted by accredited audit providers that demonstrate their qualification at regular intervals. TISAX and TISAX results are not intended for general public.

TISAX®
ENX ASSOCIATION
RESULT AVAILABLE

For Projektron GmbH confidentiality, availability and integrity of information have great value. We have taken extensive measures on protection of sensitive and confidential information. Therefore, we follow the question catalogue of information security of the German Association of the Automotive Industry (VDA ISA). The Assessment was conducted by an audit provider, in this case the TISAX audit provider TÜV SÜD Management Service GmbH. The result is exclusively retrievable over the ENX Portal.

The general objectives of information security apply to all areas of the business: confidentiality, integrity and availability. Our management systems cover all relevant regulations and guidelines for data protection, health and safety, environmental protection, occupational health and safety, fire protection and information security.

TABLE OF CONTENTS

BCS

Projektron GmbH

PRODUCT DEVELOPMENT

Secure software development – secure software: Information security in the development process is essential to offering a software product with BCS that provides a secure basis for your business requirements and ensures the confidentiality, integrity and availability of your information.

Access control and authentication

- ✓ **Role and rights concept** – A customizable role and rights concept is a prerequisite for restricting access to data or information to authorized persons.
- ✓ **Guidelines for passwords** – BCS supports guidelines for passwords regarding password complexity and frequency of changes.
- ✓ **Passkeys** – BCS supports Passkeys, a password-free authentication method that replaces passwords with an asymmetric procedure, thereby increasing user-friendliness and eliminating vulnerabilities such as phishing, password theft and weak passwords.
- ✓ **Single sign-on** – BCS supports authentication via SAML, Active Directory (LDAP/KERBEROS) or OAuth 2.0 with OpenID Connect.
- ✓ **2-factor authentication** – The login can be additionally secured by a second factor generated according to the TOTP procedure.

Data security and protection mechanisms

- ✓ **Encrypted connections** – Encrypted communication is possible for secure data transfer between BCS and users or external systems (https, imaps, smtps).
- ✓ **Password vault** – Passwords needed for third-party systems can be stored cryptographically secure in a password vault.
- ✓ **Brute force attacks** – User accounts are protected by waiting times or account lockout after multiple failed login attempts. Access to individual accounts can be restricted to certain IP addresses and IP ranges.
- ✓ **Secure passwords** – Passwords are secured in BCS with the PBKDF2 algorithm as well as salt and pepper.

Testing and review

- ✓ **Automated testing** – BCS is tested for both functionality and user-friendliness. Common attack patterns can be checked automatically. Automated tests are integrated into the Continuous Integration (CI) pipeline to ensure that every change to the code is tested immediately.
- ✓ **Integration tests** – We perform integration tests to ensure that different components of the software work together securely and that no new security vulnerabilities arise.
- ✓ **End-to-end testing** – We create end-to-end tests that cover the entire user story and ensure that the application works as expected and is secure.
- ✓ **Vulnerability scanning** – The software is regularly scanned for known security vulnerabilities.
- ✓ **Pentests** – Pentests are regularly carried out in collaboration with our customers. The results of these tests are continuously incorporated into the development and protection of BCS.
- ✓ **Test coverage reports** – We create test coverage reports that show the coverage of user stories by the tests and ensure that no security-critical areas remain untested.
- ✓ **Unit testing** – For each user story, we develop unit tests to verify correct functionality and security at the code level.

Internal security measures

- ✓ **Internal guideline “Secure Software Development“** – The internal guideline aims to minimize security deficits and vulnerabilities in the development of BCS and to respond appropriately to them. This is done by taking into account the SANS 25, which lists the 25 most dangerous and relevant vulnerabilities in software, as well as the OWASP Top 10, which describes the ten most widespread and important vulnerabilities for web applications.
- ✓ **Team of experts in product development** – A specialized team continuously deals with current IT security issues and implements the latest security measures in BCS. This ensures that our software always meets the highest security standards.

- ✓ **Security documentation** – All security requirements, measures and tests are documented in detail.
- ✓ **Staff training** – Our developers receive regular training and are made aware of security aspects and best practices.
- ✓ **Definition of security requirements** – Security objectives and requirements are clearly defined at the beginning of the project.
- ✓ **Security planning** – We follow a detailed security plan that describes security measures and procedures.
- ✓ **Awareness programs** – We run programs to promote security awareness throughout the development team
- ✓ **Reporting** – We regularly report on the security status and any incidents that have occurred to relevant stakeholders.

Secure programming and development guidelines

- **Coding standards and guidelines** – We adhere to proven coding standards and guidelines to avoid security vulnerabilities.
- **Static Code Analysis** – Tools are used for static code analysis to find vulnerabilities in the source code.
- **Vulnerability Management** – A process has been implemented to detect, assess and remediate security vulnerabilities.
- **Code reviews and peer reviews** – The code is regularly reviewed by colleagues to identify potential security issues at an early stage.
- **Risk Assessment** – Potential security risks are identified and assessed throughout the entire development process.

Version Control and Configuration Management

- **Version control** – We use version control systems (e.g. Git) to track changes in the code and ensure traceability.
- **Configuration management** – We ensure that all configurations are securely managed and documented.

Incident response and emergency planning

- **Contingency plans** – Contingency plans have been created and are continuously maintained to enable a quick and effective response in the event of a security incident.
- **Incident response** – We have established a process for responding to security incidents, including analyzing and rectifying the causes.

HOSTING / SAAS

We know that a secure system is important to you, especially if you host BCS with us or our service provider.

Location and availability

- **Data center in Germany** – The data center is located in Germany and is subject to high security levels. It belongs to the Tier IV class with redundant ISP POP.
- **Backup and recovery** – The hosting offers backups and, if necessary, a quick recovery.
- **Certified** – Our data center and Projektron´s security-related areas are certified according to ISO 27001. The data center also has other certificates: VdS ISO 9001 NSL and IS, DIN 14675 for BMA and DIN EN 50518.
- **Availability** – We guarantee the agreed availability, which is permanently monitored.

Physical security and access control

- **Access control** – The data center may only be accessed by authorized persons who have been entrusted with the fulfillment of tasks and who have registered in advance.
- **Security** – The data center is guarded on-site 24/7, 365 days a year.

Security tests and updates

- **Automated updates** – The virtual machines and BCS are updated automatically so that they are always up to date and secure.
- **Pentest** – Our hosting is subjected to a pentest annually.
- **Maintenance window** – There are regularly scheduled maintenance windows for importing updates and patches. In the event of an acute security breach, unscheduled updates will be carried out, with two hours´ notice.

Data and access security

- **Firewall** – A centralized firewall with strict filter rules individually for each customer protects you from external attacks. A firewall for web applications can be provided upon request.
- **Separate database servers** – Customer data is stored on separate database servers. This enables better performance and the setup of individual interfaces.
- **SSL** – When hosting, you access BCS via encrypted access with an SSL certificate.
- **Secure connections via HTTPS/SFTP/SSH & SCP** – You generally only access your virtual machine via secure connections (via HTTPS/SFTP/SSH) and create backups or data copies (via SCP) in this way, for example.
- **VPN tunnel** – The virtual machines cannot be accessed via the Internet. Projektron only accesses these via VPN tunnels.

Additional services and training

- **CMS** – Our customers are automatically connected to the Configuration Management Service (CMS). This means that their configurations are managed within an SVN repository.
- **Further training** – Employees receive further training tailored to their needs in the security of hosting services.

SUPPORT PORTAL & WEB APP

The following measures provide an overview of the most important security and configuration settings that make the BCS support portal and web app even more secure and efficient. Find out how to optimally protect your data and customize the platform to suit your needs.

Support portal

- ✓ **Transport security** – Transport security in the support portal is ensured by the optional but recommended use of HTTPS.
- ✓ **Message exchange and authentication** – Messages are exchanged via SOAP, with authentication being ensured by username and password in the SOAP header. The synchronization user should be protected with a strong password because it has extensive rights. This password should be stored in the password.
- ✓ **Configuration of the Attributes to be Synchronized** – The attributes to be synchronized can be configured, whereby sensitive attributes can be excluded from synchronization.
- ✓ **Port Restrictions** – Port restrictions can be applied to specifically restrict the HTTP exchange between the systems involved.

Web App

- ✓ **Transport security** – The transport security of the web app is guaranteed, as it can only be used in conjunction with HTTPS.
- ✓ **Authentication and cookie management** – Authentication is carried out via a username and password, followed by the use of a long-lasting cookie that is stored securely in the memory and removed from the app when you explicitly log out.
- ✓ **Rights application during synchronization** – When synchronizing from the Web app to BCS, the rights set in BCS are applied.

INTERFACES

This is where you will find an overview of the central security aspects when using interfaces in BCS. Regardless of whether you are integrating Microsoft Exchange, Microsoft 365 (Exchange Online) or Jira, this is where you will learn how to ensure transport security and which authentication and authorization methods are used.

Microsoft Exchange On-Premises

- ✓ **Transport security** – Transport security for Microsoft Exchange on-premises is ensured by the optional but recommended use of HTTPS.
- ✓ **Authentication** – BCS supports the BASIC, DIGEST and NTLM authentication types, which are, however, vulnerable to certain attack patterns. BCS does not yet support the modern AD FS authentication type, which is based on OAuth 2.0 and is used by Exchange 2019.

Microsoft Exchange Online

- ✓ **Transport security** – When using Microsoft Exchange Online, transport security is guaranteed by the exclusive use of HTTPS.
- ✓ **Authentication** – Secure, token-based authentication provides additional protection when using Exchange Online.

Jira On-Premises

- ✓ **Transport security** – Transport security for Jira On-Premises is guaranteed by the optional but recommended use of HTTPS.
- ✓ **Impersonation and security** – After logging in via the sync user, impersonation is used to store actions in the context of the logged-in user.
- ✓ **Message exchange** – The message exchange is done via SOAP, where the password of the sync user must be securely protected.

Jira Cloud

- ✓ **Authentication** – In Jira Cloud, authentication is done via an API key on the user via the REST interface in BCS, whereby the API key is securely created and stored.
- ✓ **User management** – Only the administrator can manage the user assignment mappings in BCS.
- ✓ **Security recommendation** – It is recommended that Jira Cloud and BCS be installed on the same system to be able to block ports through a firewall.

IT ADMINISTRATION

Our internal IT administration also takes information security very seriously. We use state-of-the-art technology to secure our systems and continuously update our security measures.

Central software distribution and endpoint security

- ✓ **Central software distribution** – The software required on the operating computers is distributed centrally and kept up to date.
- ✓ **Patch management** – Security updates and patches for operating systems and applications are regularly installed.
- ✓ **Antivirus and antimalware software** – The antivirus and antimalware programs that are always in use on all end devices are regularly updated.

Network and perimeter security

- ✓ **Redundant network technology** – Internet lines, firewalls and central switches are redundant.
- ✓ **Network segmentation** – Networks are segmented into different segments to restrict access to critical systems and prevent attacks from spreading.
- ✓ **Firewalls** – Firewalls are used to control data traffic.
- ✓ **VPN** – VPN access is available to employees for mobile working. VPNs are used for secure remote access to internal systems.

Access control and authentication

- ✓ **Least Privilege Principle** – Access rights are granted based on the principle of minimal authorization, so that users can only access the resources they actually need.
- ✓ **Role-Based Access Control (RBAC)** – Role-based access controls have been implemented to restrict access to sensitive information.

Monitoring / security monitoring

- ✓ **Security updates** – Internal services are monitored permanently to ensure availability and to be able to react quickly to problems.

Data encryption and security

- ✓ **Cryptography** – The recommendations of the BSI Technical Guidelines (BSI TR-02102) are audited annually.
- ✓ **Encryption during transmission** – Encryption technologies are used to protect data during transmission.
- ✓ **Internal certification authority** – Internal services are encrypted via their own certification authority.

Email security and backups

- ✓ **Backup & recovery** – Internal services are backed up daily and can be quickly restored to the state of the last backup. The recovery process is tested every six months.
- ✓ **E-Mail** – Incoming mail traffic is monitored and, in case of doubt, initially placed in quarantine.

Organizational measures

- ✓ **Regular training** – We provide training for IT staff and end users on the latest security threats and best practices.
- ✓ **Documented security policies** – Security policies and procedures are created, documented and regularly updated.
- ✓ **Security awareness programs** – We run continuous programs to raise employee awareness of information security.
- ✓ **Compliance** – We ensure compliance with relevant legal and regulatory requirements as well as internal security policies.

Procedural measures

- ✓ **Incident response and emergency management** – We have emergency plans in place that include measures to restore systems in the event of an incident. We regularly conduct exercises to prepare for security incidents and review the effectiveness of our emergency plans.
- ✓ **Risk and vulnerability management** – We regularly conduct risk assessments to identify and evaluate potential threats. We have implemented a process to detect, assess and rectify vulnerabilities in the IT infrastructure.

SUPPORT

We use our own support portal to provide technical support to our customers. In doing so, we always pay attention to the quality and, above all, the security of the information we handle.

Support portal and configuration management

- ✓ **Support portal** – The support portal for customers is used for the secure exchange of information and the transfer of data. Communication takes place via tickets with an internal system storage for the data exchange.
- ✓ **Configuration versioning service (CVS)** – The configuration versioning service (CVS) is a central configuration store for customers and Projektron itself. The configurations are managed within an SVN repository.

Authentication and access control

- ✓ **Access authorization** – The customer´s contact persons have personalized access to the support portal.
- ✓ **Role-based access control (RBAC)** – Access rights are assigned based on the roles of the users in order to restrict access to sensitive information.
- ✓ **Strong authentication** – A two-factor authentication (2FA) is used to access the support portal.
- ✓ **Secure password policies** – We have implemented secure password policies, including minimum length, complexity, and regular change.

Encryption and data protection

- ✓ **Encryption** – Access to the support portal is only possible via encrypted access.
- ✓ **End-to-end encryption** – It is ensured that data is encrypted during the entire communication between customers and support staff via the support portal.
- ✓ **Data minimization** – Only the customer data necessary for order processing is collected and stored in the system.
- ✓ **Data protection compliant processes** – Processes have been implemented in accordance with the General Data Protection Regulation (GDPR) and other relevant data protection laws. These processes are consistently adhered to.

Staff training and security information

- ✓ **Further training for our employees** – Our support staff receive regular and needs-based further training on the security of the software used and interfaces to third-party systems that can be connected to BCS.

- ✓ **Security information for customers** – Support staff receive regular training on the topics of information security, data protection and the secure handling of customer data and are made aware of the issues.

- ✓ **Regular training** – Support staff receive regular training on the topics of information security, data protection and the secure handling of customer data and are made aware of the issues.

- ✓ **Awareness programs** – We continuously implement programs to promote security awareness and compliance with security policies.

Procedural measures and emergency management

- ✓ **Security policies and procedures** – Policies and procedures for information security in the support portal are consistently enforced and continuously adapted. In addition, security reviews and audits are regularly carried out to ensure compliance with security standards.

- ✓ **Logging and monitoring** – All activities in the support portal are logged in detail and the logs are regularly checked for suspicious activities.

- ✓ **Incident response and emergency plans** – We follow a clear process for reporting, analyzing and rectifying security incidents. We have emergency plans in place in the event of a security incident, which are regularly updated.

- ✓ **Customer data management and anonymization** – To increase the protection of customer data, we anonymize or pseudonymize data wherever possible.