BitaBIZ Information Security Policy

BitaBIZ is committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets throughout our organization and we continuously seek to improve the protection of our customers.

The purpose of this Policy is to ensure that BitaBIZ will apply a consistent, business risk based and cost efficient approach in order to manage information security.

BitaBIZ will identify and manage risks to information, applications, and technology applying Information Security Management System (ISMS) intended to follow and conform to the best practice standards. Protecting information assets addresses all stocks of information, the network, the people that use them, the processes they follow, and the physical computer equipment used to access them.

BitaBIZ management is responsible for this Policy and it applies to all full- or part-time employees, sub-contractors, project consultants and any other person who works under the authority of BitaBIZ.

1. SaaS Platform and Data Retention

- BitaBIZ SaaS Services are delivered via a Microsoft .NET technology platform. Our Microsoft resources are always updated with the latest security updates.
- Azure tools continuously scan for vulnerabilities. This enables us to identify and remove vulnerabilities.
- Our Azure Cloud Services and Virtual Machines are protected by Cloudflare Web Application Firewall (WAF).
- Platform monitoring is performed directly in Azure with automated security alarms.
- Databases are encrypted with Encryption-at-rest by default.
- Database encryption key is protected by a built-in server certificate.
- Microsoft Antimalware and Defender are installed on our Azure Cloud Services and Virtual Machines.
- Login to our production environment is only via Microsoft Azure Just-in-Time that provides audit logs for all activity.
- Point in time backups are stored 1 month, and weekly backups are stored for 2 months on Zone redundant storage (ZRS) on 3 different Azure data centres. Backups can be restored if needed.
- Data Portability and Data Management for Customers
    - BitaBIZ has built-in tools that allow the customer to respond to data subjects (employees etc.) requests to delete personal information if the information is no longer relevant.

2. Authentication & Access control

Network security

- BitaBIZ is HSTS (HTTP Strict Transport Security) enabled, and all requests are forced to use https.
- SAML 2.0
  - Single Sign-on (SSO) allows your company to authenticate users in your own systems without requiring them to enter login credentials to BitaBIZ.
- Manual Password and Credential Storage
  - Password-based authentication; user passwords are encrypted using the protocol SHA1 or later version.
- Authentication Controls
  - Measures are implemented to restrict the number of login attempts.
- Session timeout
  - Session timeout is implemented.
- SCIM
  - User provisioning allows your company to control and manage user creation and access control from your own systems.
- Rest API
  - The industry-standard protocol for authorization OAuth 2.0 is used.

Product security

User Role Permissions (Privacy by Design)

BitaBIZ has built-in settings and permission management.

- Permission roles include:
  - System admin
  - Global payroll admin
  - Local Payroll admin
  - External admin
  - HR statistics
  - Approver role
  - User role
- Settings management:
  - Default settings
  - GDPR/Anonymous settings
  - User settings
  - Global settings

3. Encryption

- At rest: Azure databases are encrypted with Encryption-at-rest by default and the database encryption key is protected by a built-in server certificate.

- In transit: All data in transit to or from BitaBIZ is encrypted using 256-bit encryption. API and application endpoints are TLS only. The newest TLS version is always used when supported by the clients.

4. Internal security

- **Confidentiality**
  - All employee contracts, consulting agreements, vendor agreements, or service delivery agreements include confidentiality clauses to set forth a duty of secrecy and security of customer data and personal data even after the engagement with BitaBIZ ends.
- **Internal permissions and authentication**
  - Access to customer data is limited to authorized employees who require it for their job.
  - BitaBIZ has a Single Sign-On (SSO) policy for all business resources. SSO is a requirement for implementing a business resource. We manage resource access from one central portal. Access to a resource is only granted if relevant for the job function.
  - We monitor and audit log login to all company resources.
  - All actions taken on production consoles are logged.
  - We have strong password policies.
- **Staff Training**
  - All our employees have received security awareness training and more specialized staff have received appropriately specialized information security training.
- **Policies**
  - Our setup does not allow our staff to access business resources outside our implemented Information Security Policy.
- **Hardware**
  - All BitaBIZ devices are compliance managed centrally with MSFT Intune.
  - All employees have company paid PC and Mobile secured with company managed firewall and security scan.
  - Data must only be saved on company managed SharePoint/OneDrive.

5. Annual Review of Security Management & Policies

As a part of our overall security management and company policies, BitaBIZ reviews all policies including the Information Security Policy annually as a part of the annual ISAE 3000 GDPR Audit.