benify

Information Security & Data Protection

White Paper

Rev. 08/2024

A word from our CEO

Information security is of great importance to Benify and a core part of our business. You trust Benify to process your information, which means that we have a great responsibility to ensure that the data is processed securely and according to all applicable laws and regulations. This is something we take most seriously!

With this white paper, we hope to provide you and your organization with an overview of our information security and data protection program.

Joakim Alm, CEO

Contents

Compliance certification & assurance

In order to achieve a structured and strategic approach to information security, Benify runs a security program in compliance with a range of well-known industry standards. We appreciate that these attestations matter, as they provide independent assurance to our customers. We have implemented and adhere to Organizational and Technical security measures to meet legal requirements for cyber resilience.

Standard	Sponsor	Status
ISO/IEC 27001	International Organization for Standardization	***Benify is ISO 27001 certified*** for developing, hosting, and maintaining information systems and services for employee benefits and salaries management. ISO/IEC 27001 also leverages the comprehensive security controls detailed in ISO/IEC 27002. The scope of this certification is the development, implementation and continuous improvement of a rigorous security management program, including Information Security Management System (ISMS).
ISO/IEC 27018	International Organization for Standardization	***Benify is ISO 27018 certified*** as part of our Cloud security compliance program. ISO/IEC 27018 is a code of practice that focuses on protecting personal data in the cloud. It is based on the information security standard ISO/IEC 27002 and provides additional implementation guidance for ISO/IEC 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set.
ISO/IEC 27701	International Organization for Standardization	***Benify is ISO 27701 certified*** as a part of our GDPR compliance program. The design goal of ISO 27701 is to enhance the existing (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for PII Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals.

ISO/IEC 22301	International Organization for Standardization	***Benify are certified in accordance with ISO 22301***, the International Standard for Business Continuity Management Systems (BCMS). It provides a framework for organizations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents.
ISAE 3000 SOC2 (Type II)	Service Organization Controls	***Benify undergoes the ISAE 3000 SOC2 (Type II)*** examination, performed by a third-party accreditation body. The examination demonstrates how Benify achieves specific Trust Service Principles and highest standards, compliance with information- and data security, privacy, established robust controls to support operations, and our commitment to maintaining a secure environment.
CSA CCM/STAR (CAIQ)	Cloud Security Alliance	A CSA STAR Level 1 Self-assessment (CAIQ) for Benify is available for download on the Cloud Security Alliance's STAR Registry website. The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings. It thereby helps customers assess the security of cloud providers they currently use or are considering contracting with.
Cyber Essentials Plus	National Cyber Security Centre, UK	Cyber Essentials is an effective, Government-backed scheme that will help protect against a range of the most common cyber-attacks. For more information, please visit: https://www.ncsc.gov.uk/cyberessentials/overview

Information security governance

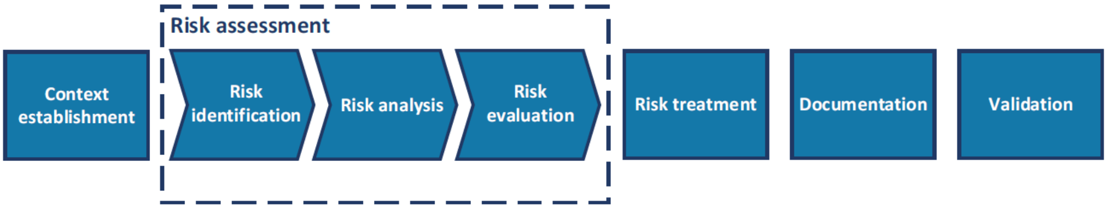
Information classification

Benify applies information classification to all information used in the organization. All IT systems/services used within the organization are classified according to the CIA model (Confidentiality, Integrity, and Availability).

Information security risk management

Information security risk management is a continuous process at Benify. We perform ongoing risk assessments to evaluate risks to our environments and products continuously. Our approach to risk management includes:

- *Enterprise information security risk management* - A risk management process controls significant changes to the organization, business processes, or information processing facilities that affect information security.



- *Product development information security risk management* - Information security risk management is applied as a part of our product development framework.

- *IT service/system and supplier risk management* - Information security requirements and risks associated with new IT services/systems and suppliers are controlled by a risk management process.

- *Data Protection Impact Assessment (DPIA) - When personal data processing is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment (DPIA) is being* performed to ensure appropriate personal data protection.

Information Security Audits

As part of the Benify Management System, we continuously conduct Information Security and Business Continuity Management audits to ensure compliance with relevant security industry standards, best-practice frameworks, and applicable legislation and regulations.

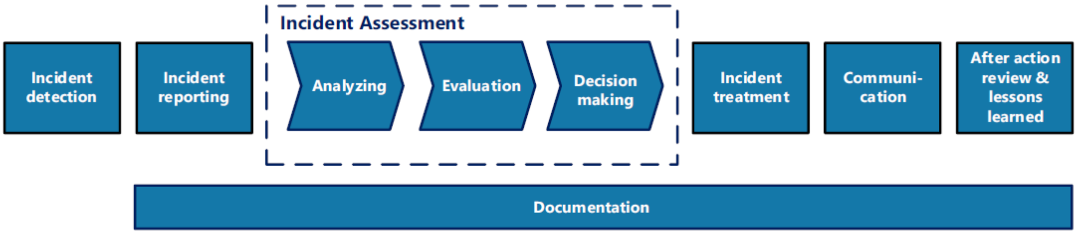
Audits performed annually by external independent auditors:	Audits/compliance checks and self-assessment performed by Benify:
• Internal information security audit • ISO 27001, ISO 27018, ISO 27701 certification audits • ISO 22301 • ISAE3000 SOC2 type 2 • Cyber Security Essential Plus	• Consensus Assessments Initiative Questionnaire (CAIQ) • PCI-DSS (SAQ D) • CIS Top 20 Critical Security Controls • Accounting, bookkeeping, Anti-Money Laundering, and Counter-Terrorism Financing (AML/CTF).

Information Security and Privacy Incidents

All security and data protection incidents are managed by Benify's Operation Quality and Incident Management Team according to established policies and procedures.

Benify's security and data protection incident management process includes:

- Incident detection
- Incident reporting
- Incident assessment
  - Analyzing
  - Evaluation
  - Decision making
- Incident treatment
- Communication
- After action review & lessons learned



Supplier assessments

To ensure compliance with information security policies and data protection legislation, Benify has system and supplier acquisition process and policies to review and assess all new IT systems/services introduced in our organization.

Supplier reviews include but are not limited to the following:

- Review of Benify's security and data protection questionnaire.
- Collection and review of certifications and accreditation reports (ISO, ISAE 3000 SOC 2 (Type II), etc.)
- Review of industry-standard questionnaires and frameworks (CAIQ, CIS Top 20, etc.)
- Review technical reports (penetration tests, vulnerability scannings, etc.)
- Legal compliance (GDPR, E-privacy, AML/CTF etc.)

Governing documents & Policy management program

We have structured our policies to cover all the domains of the ISO standards and other frameworks we have adopted. Our policy management program shall ensure that all policies are:

- Approved by management
- Communicated to all employees
- Documented and readily available
- Defining security objectives
- Showing commitment to meet our regulatory obligations
- Focused on continual improvement
- Reviewed annually

Information security awareness

As a part of our continuous awareness training program, we educate, train, and test all employees as regards information security & data protection policies and procedures. In addition, we also perform specific training sessions such as Security Talks, Phishing campaigns, etc.

Employee vetting

All our employees are covered by information security agreements and non-disclosure agreements.

Benify performs background checks on all new employees and temporary staff. Our background check includes the following:

- Education
- Employment verification
- References
- For certain positions, criminal records

Benify application security

Access control

Access control is role-based and limited to a need-to-know basis. To ensure accountability, each user is assigned a unique user ID. The unique user ID applies to all employees, including system administrators and operators.

Benify has procedures in place to change or revoke access rights immediately following a change to an employee's employment status or position. In addition, annual access control reviews are undertaken. Access control reviews include both role permission reviews and assignment reviews.

Single sign-on (SSO)

Federated authentication can be managed through Single Sign-On (SSO) using SAML 2, OpenID Connect (OIDC).

Multi-factor authentication

Multi-factor authentication is enforced on all Benify's administrators, and access is only granted when authenticated with at least two factors.

Multi-factor authentication can also be enabled for customer administrators and end-users. With a second login factor enabled, any login method, including single sign-on, can be protected with two-factor authentication using a variety of different options:

- Google/Microsoft authenticator
- SMS
- E-mail
- Push notification

For our Nordic customers, authentication can be done using Mobile BankID, BankID, MitID.

Passwords

Benify users have individual user accounts and must be authenticated with at least a username and password. Benify has a baseline password policy to enforce strong passwords. The password policy can be customized to fit specific customer requirements.

All password hashes match a database of weak, well-known, or breached passwords to encourage users to practice good password hygiene. This will also mitigate threats such as password guessing and malicious parties reusing leaked credentials.

Password reset is done by request and is sent to the user's pre-registered email address. Reset links direct the user to a secure page where a new password is set. Old reset links expire upon generation of a new reset link.

The application only allows a limited number of password reset requests before the account is locked. The user account will also be locked after several failed log-on attempts. The account will remain locked for an extended period until a new password is set or when a Benify administrator manually opens an account.

Protection of Authentication Information

Authentication information stored within the Benify application is hashed, salted, and stored in a separate database with strictly limited access.

Encryption – Data-in-transit

Communications between end-user computer clients and Benify’s servers are encrypted via industry best practices HTTPS and, at minimum, Transport Layer Security (TLS) 1.2 over public networks.

Customer integrations such as file transfers and API calls are protected using SFTP/HTTPS. Payload/file encryption is possible using PGP.

Encryption – Data-at-rest

Application data is protected by enabling data-at-rest encryption in the database using InnoDB Data-at-rest encryption. InnoDB enables data-at-rest encryption by encrypting the database's physical files. Data is encrypted automatically, in real-time, before writing to storage and decrypted when read from storage. As a result, hackers and malicious users are unable to read sensitive data from tablespace files, database backups, or disks. InnoDB uses industry-standard AES algorithms.

Data-at-rest Encryption Key Management

Encryption keys are stored in a secure and resilient Key Management System. Benify´s Key Management Service uses FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints, which provide independent assurances about confidentiality and integrity.

User inactivity

All users are automatically logged off after 30 minutes of inactivity.

Separation of customer data

All customer data is logically separated for each customer to ensure confidentiality and integrity between customers. Every customer has a unique company key used to separate data. Every row in the database is tagged with a unique company identifier.

Sensitive data

According to Benify’s information classification policy, all customers' data is classified as Strictly confidential. In addition to this, information such as salary, bonuses, etc., is classified as sensitive in the Benify application.

Access to sensitive information is only allocated according to the principle of least privilege. Sensitive information is, by default, masked for all Benify administrators. Permission to view masked information is controlled by the role permissions.

Access to sensitive information is a part of the annual role permission review.

Event logs

All activities in the application are logged. Our logs include information about the user, time and dates, user activity, and critical security events (such as authentication attempts to violate the rules of authentication).

To protect our logs against tampering, an integrity check mechanism protects the logs, and access rights are strictly limited.

Application time is synchronized using Network Time Protocol (NTP).

Dynamic Application Security Testing (DAST)

Automated web application vulnerability scans (including OWASP top 10) are performed weekly. All vulnerabilities are documented, classified, and mitigated according to internal policies and procedures.

Third-party library vulnerability scans

To identify project dependencies and check for any known, publicly disclosed vulnerabilities in third party libraries, Benify utilizes a software composition analysis tool. This tool is integrated into our CI/CD pipelines and vulnerability management process to identify vulnerabilities and licensing issues throughout the software lifecycle.

Penetration testing – Web application

At least annually, we engage an external independent security company to perform application penetration tests. Penetration tests are performed using automated and manual testing that is carried out in accordance with the latest (development) version of the OWASP Web Security Testing Guide and, where applicable, other international benchmarking projects and standards. During testing, the source code is examined to facilitate the penetration test.

Penetration testing – Mobile application

At least annually, we engage an external independent security company to perform mobile application penetration tests. The tests are performed using both dynamic and static analysis methodology. Automated and manual analysis of communications towards the backend systems, Blackbox static analysis of the built applications, and Whitebox review of the application code and configuration settings. All assessment strategies are performed in line with the OWASP MSTG.

Client-specific security testing

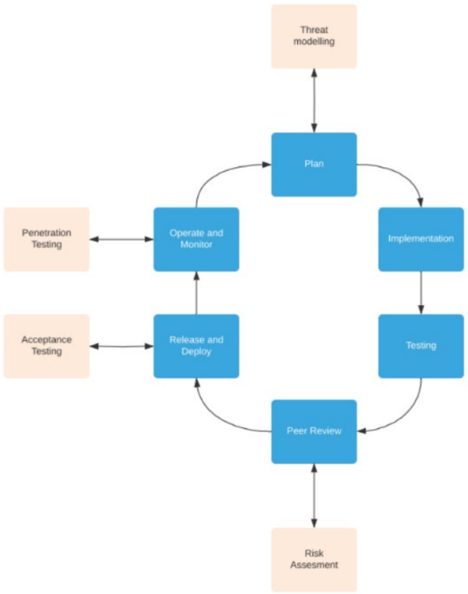
Clients (or their chosen third parties) are not permitted to conduct vulnerability scans, penetration tests, or other code or port scans against Benify's company network or applications. However, Benify is happy to share our independent test reports with clients upon request.

Secure Software Development Lifecycle (SSDLC)

The Benify application is developed according to good engineering practices. Benify aims to optimize our processes for quality, security, and efficiency.

Security is an integrated part of our SSDLC and includes but is not limited to the following:

- Threat modeling
- Risk assessment
- Acceptance testing
- Static code analysis
- Penetration testing
- Segregation of duties
- Peer review



Operations Security

Access control

Privileged access to IT infrastructure assets, such as servers, monitoring, etc., is protected by multi-factor authentication.

IT infrastructure event logs

IT infrastructure assets are logged, collected, and managed by a syslog management platform centrally managed by Benify’s IT Operations team. The platform collects, indexes, and analyses syslog in a centralized location.

Back-up

Production data is backed up daily, with monitoring in place. Daily backups are retained for a week, weekly backups for a month, and monthly backups for a year.

Backup data is stored encrypted and physically separated from production data at Benify's secondary data center, with additional copies held in a cold storage/off-site, air-gapped location with no external connections.

Backup recovery tests are performed and verified quarterly.

Security patching

Common vulnerabilities and exposures (CVEs) are monitored, and patches are classified and applied according to internal policies and procedures.

IT environments

Benify has separate environments for application development, testing, and production.

Performance monitoring

Benify IT Operations monitor performance, uptime, and resource usage for production servers and services.

Automatic failover

The Benify application is running on several servers. By using several servers, we can effectively avoid any downtime in case of a server failure. If one server is down, all users will be automatically and transparently redirected to the other server.

Media Disposal

Approved software and degaussing equipment are used for secure data erasure.

Disaster recovery

Benify has a disaster recovery plan, which is tested annually to verify Benify’s capacity to recover and protect the business IT infrastructure in the event of a disaster.

Communications and network security

Access control and authentication

Authentication to business networks with access to internal resources and information is managed by device-specific certificate-based authentication. Network traffic is encrypted using the latest non-vulnerable standards and algorithms.

All remote access to Benify's LAN requires a VPN connection using multifactor authentication.

Encryption

All site-to-site communication within Benify is encrypted using IPSEC tunnels.
All VPN traffic to Benify networks is encrypted. Internal traffic from Benify computer clients to Benify production services is encrypted.

Firewalls

Our networks and IT environments are equipped with redundant stateful inspection firewall clusters to ensure their protection. To further enhance our security measures, Benify uses specific web application firewall (WAF) functionality that filters, monitors, and blocks traffic to and from our web application. By inspecting network traffic and utilizing WAF, we can prevent attacks that exploit known web application vulnerabilities such as SQL injection, cross-site scripting (XSS), file inclusion and improper system configuration.

Intrusion detection and prevention

Benify uses artificial intelligence algorithms and world-leading anomaly detection machine learning to protect our networks from malicious intruders.

Security Operations Center (SOC)

Benify utilizes a 24/7 external SOC service to monitor our networks, clients, and applications. Our external cyber analysts are experts in threat intelligence, threat hunting, and incident response, and they provide 24/7 SOC support to Benify.

Network vulnerability scans

Benify performs network vulnerability scans weekly using automated vulnerability scanners. All vulnerabilities are documented, classified, and mitigated according to internal policies and procedures.

Separation of networks and tiers

The Benify application production environment is located in a network separated from other Benify internal systems. The application consists of 3 tiers:

- Load balancing/front end
- Application servers
- Database servers

Redundancy

Benify has redundant network suppliers and can re-route communication in the unlikely event of network failure.

Endpoint protection

Benify's endpoints, such as computer clients and servers, are protected with a centrally managed and monitored solution that unifies next-generation antivirus (NGAV), endpoint detection and response (EDR), device control, vulnerability assessment, and IT hygiene.

Physical security

Data center security

Data centers hosting the Benify application have high physical security, which includes security controls such as:

- Strict physical multi-factor access control
- Access logs
- Dedicated- and locked server cabinets
- Security alarms
- Fire detection and prevention controls
- Climate control systems and alarms
- Emergency power
- Uninterrupted power supply (ups)
- Lightning protection
- Redundant networks
- Video surveillance (CCTV)

Our data centers are separated across various physical locations to achieve geo-redundancy.

Workplace security

Benify’s offices are protected by access controls, security, and fire alarms. Security at Benify’s physical locations is managed according to Benify’s Physical security policy and Workplace security policy.

Data center compliance

ISO27001 compliance and ISAE3000 SOC 2 (Type II) assurance report.

Privacy

Privacy policy

Read more about how Benify processes personal data related to the Benify application in our Privacy Policy.

GDPR

The purpose of the EU General Data Protection Regulation (GDPR) is to reinforce the rights of individuals by improving the processes through which personal data is being processed.
Benify has processes and infrastructure in place to meet the requirements detailed in the GDPR.
Benify has an information security & data protection team that continuously works to improve policies and processes for data protection.

Benify is ISO 27701 certified as a part of our GDPR compliance program.

Storage Location

All personal data processed by the Benify application is stored on servers that are owned and controlled by Benify. Our servers are located in physically separated and independent data centers in Sweden.

Personal Data Retention

To ensure that personal data processing is limited to what is necessary, Benify has a personal data retention policy implemented in the Benify application.
This policy aims to adapt the Benify application to the GDPR requirement of data protection by design and by default and the principles of data minimization and storage limitation.

The policy is based on the following scenarios:

- Automatic erasure for active customers and end-users
- Erasure due to termination of agreement
- Erasure due to termination of employment
- Individual’s right to erasure and restrict processing