Information Security & Data Protection

WHITE PAPER

benify

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 in ensuring that the information 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, we run our 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.

Standard	Sponsor	Status
ISO 27001	International Organization for Standardisation	***Benify is ISO 27001 certified*** for the scope of development, hosting and maintenance of information systems and services for management of employee benefits and salaries. ISO/IEC 27001 also leverages the comprehensive security controls detailed in ISO/IEC 27002. The basis of this certification is the development and implementation of a rigorous security management program, including the development and implementation of an Information Security Management System (ISMS).
ISO 27018	International Organization for Standardisation	***Benify is ISO 27018 certified*** as parts of our Cloud security compliance program. ISO/IEC 27018 is a code of practice that focuses on protection of 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 27701	International Organization for Standardisation	***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.

ISAE3000 Type II	Service Organisation Controls	To ensure the physical security in Benify's co-location data centers we issue ISAE3000 Type II reports. The report is certified by a third party and demonstrate how Benify achieves specific Trust Service Principles according to SOC2. The purpose of these reports is to help you and your auditors understand the controls established to support operations and compliance at Benify.
CSA CCM / STAR	Cloud Security Alliance	A CSA STAR Level 1 Questionnaire for Benify is available for download on the Cloud Security Alliance's STAR Registry web site. The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping customers assess the security of cloud providers they currently use or are considering contracting with.

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. In order to continuously evaluate risks to our environments and our products, we perform on-going risk assessments. Our approach to risk management includes:

- *Enterprise information security risk management* - Significant changes to the organization, business processes or information processing facilities that affect information security is controlled by a risk management process.

- *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/system and suppliers is 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 be performed to ensure appropriate protection of personal data.

Information security audit

Benify continuously undertakes information security audits to ensure compliance to standards, best-practice frameworks, legislations and regulations.
Audits performed by external independent auditors:

- Internal information security audit (annually)
- ISO 27001, 27018, 27701 certification audits (annually)
- ISAE3000 report type 2 - Physical security for Data centers (annually)

Audits/compliance checks performed by Benify:

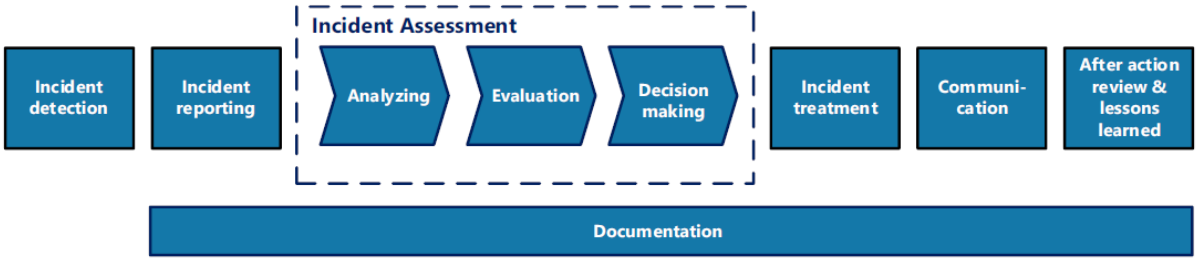
- (CAIQ) Consensus Assessments Initiative Questionnaire (continuously)
- CIS Top 20 (continuously)

Incidents

All security and data protection incidents are managed by Benify's security and data protection organization according to establishes policies and procedures and are aligned with Benify's organizational wide incident management process.

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

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



Supplier assessments

In order to ensure compliance to information security policies and data protection legislations Benify have processes and policies in place to review and assess all new IT systems/services that are introduced in our organization.

Supplier reviews include but is not limited to:

- Review of Benify's security and data protection questionnaire.
- Collection and review of certifications and attestation reports (ISO, ISAE 3000 etc.)
- Review of industry standard questionnaires and frameworks (CAIQ, CIS Top 20 etc.)
- Review of technical reports (penetration test, vulnerability scanning etc.)
- Legal compliance (GDPR, E-privacy 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 easily 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 every months. In addition to monthly trainings 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 employee's and temporary staff. Our background check includes:

- 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. Each of our users are assigned a unique user ID in order to provide accountability. 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 to this annual access control reviews are undertaken. Access control reviews includes both role permission reviews and assignment reviews.

Singel sign on (SSO)

Access can be managed through single sign on (SSO) using SAML 2.

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/or 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 authenticator
- Sms private
- Sms business
- Email private
- Email business
- Push notification

For our Swedish customers authentication can be done using BankID.

Passwords

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

All password hashes are match to a database of weak, well-known or breached passwords to encouraging 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 users pre-registered email address. Reset links direct the user to secure page were a new password is set. Old reset links expire upon generation of a new reset link.

The application only allows one password reset request per 30 minutes.
User accounts will be locked after five failed log-on attempts. Accounts will be locked for 24 hours, until a new password is set or when an account is manually opened by a Benify administrator.

Protection of authentication information

Authentication information stored within the Benify application are hashed and salted and stored in a separate database with a 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 Transport Layer Security (TLS) over public networks. Benify also strongly recommends that all customer integrations and file transfers are protected using SFTP/HTTPS and file encryption such as 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 physical files of the database. Data is encrypted automatically, in real time, prior to 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 the confidentiality and integrity.

Web application vulnerability scans
Automated web application vulnerability scans (including OWASP top 10) are conducted against the Benify application each week. All vulnerabilities are classified and mitigated according to internal policies and procedures.

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 which is used to separates data. Every row in the database is tagged with the unique company identifier.

Sensitive data
All customer's personal data is according to Benify's information classification policy classified as Strictly confidential. In addition to this, information such as salary, bonuses etc. are 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. Permissions to view masked information is controlled by the role permissions.

Access to sensitive information is a part of 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 the logs are protected by an integrity check mechanism and access rights are strictly limited.

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

Third party library vulnerability scans
To identify project dependencies and check for any known, publicly disclosed vulnerabilities in third party libraries, Benify regularly performs OWASP Dependency-Check.

Penetration testing – Web application
We engage an external independent security company to perform application penetration tests every second quarter. 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 test can be shared with customers upon request.

Penetration testing – mobile application
We annually 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

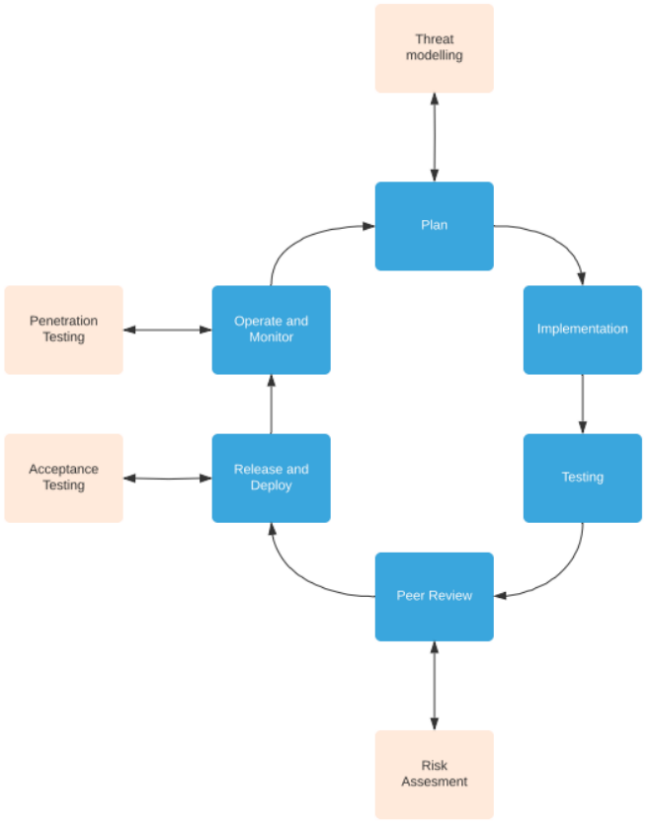
of the application code and configuration settings. All assessment strategies are performed in-line with the OWASP MSTG.

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.

Secure Software Development Lifecycle (SSDLC)
The Benify application is developed according to good engineering practice. Benify aim to optimize our processes for quality, security, and efficiency.

Security is an integrated part of our SDLC and include but is not limited to:

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



DevOps 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 and the logs are collected and managed by a syslog management platform which is centrally managed by Benify's IT Operations team. The platform is used to collect, index and analyze syslog on a centralized location.

Back-up
Back-ups of production data are undertaken daily and are monitored.
Daily back-ups are stored for at least a week. Weekly back-ups are stored for at least a month and monthly back-ups are stored for at least a year.

Backup data is stored encrypted and physically separated from production data at Benify's secondary data center.

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, test and production.

Performance monitoring
Performance, uptime and resource usage for production servers and services are monitored by Benify IT Operations.

Media disposal
Approved software and degaussing equipment is used for secure data erasure.

Disaster recovery
Benify has a disaster recovery plan which is tested annually in order 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 VPN connection using multifactor authentication.

Encryption
All site-to-site communication within Benify is encrypted using IPSEC tunnels.
All VPN traffic to Benify networks are encrypted.

Internal traffic from Benify computer clients to Benify production services are encrypted.

Firewalls
Our networks and IT environments is protected by redundant stateful inspection firewall clusters.

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

Network vulnerability scans
Benify weekly perform network vulnerability scans using automated vulnerability scanners. All vulnerabilities are 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 consist of 3 tiers:

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

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

Endpoint protection
All 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 a high physical security which include 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 in order to achieve geo-redundancy.

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

Data center compliance
ISO27001 compliance and/or ISAE assurance reports.

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 have processes and infrastructure in place to meet the requirements detailed as part of the GDPR. Benify have an information security & data protection team that continuously work to improve policies and processes for data protection.

Storage location

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

Personal data retention

To ensure that personal data processing is limited to what is necessary Benify have a personal data retention policy implemented in the Benify application.
The purpose of this policy is 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