whistlelink

# Whistlelink – SaaS Fact sheet

## ISO 27001 Certification

| | |
|---|---|
| Certificator | RISE |
| Process for risk analysis | Yes |
| Process for deviations | Yes |
| Process for incidents | Yes |
| Education of staff | Yes |

## Functionality in Whistlelink

**Password**

| | |
|---|---|
| Length | Min 8 |
| Characters | Min 1 uppercase letter<br>Min 1 lowercase letter<br>Min 1 number<br>Min 1 symbol |
| Nr of attempts, then blocked | 5 |
| 2FA log in available | Yes, TOTP/SMS |
| Time out after inactivity | 30 minutes |

User Management

| | |
|---|---|
| Roles available | Owner<br>Administrator<br>Case handler<br>Viewer |

Logs

| | |
|---|---|
| Logs available | Login, views, Actions as assignments, notes, updates of summary, sent messages etc. |

Data retention

| | |
|---|---|
| Defined by customer | 8 hours - 10 years |
| Backup retention | 14 days |

## Support

| | |
|---|---|
| Online support | 8-17 CET |
| Languages | English, German, French, Italian, Polish, Swedish |

## SLA

| | |
|---|---|
| Service time | Business days: 8-17 CET |
| Support tickets | One business day |
| Tech issues, setting time | One hour, business time |
| Guaranteed uptime | 99,9% |

## Technical security

| | |
|---|---|
| Separate production environment | Yes |
| Backups | Daily |
| Geo redundant backups | Yes |
| Encryption | Bhash |
| Firewall model | pfSense |
| Patch management process | Yes |
| Logging | Yes |
| IDS | Yes |
| IPS | Yes |

| | |
|---|---|
| Incident response plan | Yes |
| Business continuity plan | Yes |
| Access principal | Principle of least privilege |
| Separate of duties | Yes |

## Tests

| | |
|---|---|
| External penetration tests | Yes. Annual. |
| Vulnerability tests | SonarQube and Detectify |

## Hosting provider

| | |
|---|---|
| Company | Glesys, glesys.com |
| Location | Sweden |
| Building year | 2020 |
| Temperature | 20-30 C |
| Humidity | 40-60% |
| Redundancy | N+1 |
| Utility connection redundancy | N+1 |
| Backup Power Type | Generator |
| Backup Power Redundancy | N |
| CCTV | Yes |
| Burglar Resistance | Class 3 |
| Authentication Factor | Access card, PIN |
| Fire Suppression | Aspirating Smoke Detector 3M Novec 1230 |
| Destruction of used discs | Yes |
| Certificates | ISO9001 ISO14001 ISO27001 |

## GDPR

| | |
|---|---|
| Transfer to third country | No |
| Data breach procedure guideline | Yes |
| Data Protection Impact Assessm. | Yes |

## Staff

| | |
|---|---|
| Background check | Yes |
| Onboarding process | Yes |
| Offboarding process | Yes |

## Encryption and hashing

For secure communication between clients and server we use TLS for data in transit encryption. We support TLS version 1.2 and 1.3.

All sensitive data falling under GDPR is encrypted in rest using AES256 algorithm. The encryption keys used are handled by a Key Management System and by that stored safely. Furthermore, our KMS supports key rotations. Keys are never shared between customers. Each customer has their own unique set of keys. For one customer a set of keys is used to encrypt different types of data. That means for example that case data use one key and attached files are encrypt with another key.

Passwords have an extra security layer. We never store passwords as entered by user. All passwords are hashed using salt before they are encrypted and stored in the database.