# Company, Application, Data Security and Privacy

## LUCYs Security & Privacy Policies

### Organization of Risk & Information Security

| Questions | Response | Comments |
|---|---|---|
| Is there a comprehensive, documented information security & privacy policy in place? | yes | Yes, "Management-Handbook-Security-Policy" and a GDPR Code of Conduct for LUCY Employees |
| Are the policies communicated to all individuals with access to IT systems or access to tenants data? | yes | Personal information, part of the employee contract, availability for everybody |
| Is there a comprehensive, documented information security concept including access management for your service in place? | yes | Tenant Model, Role Model and ACL in Place (Access control list) |
| Is a risk management process implemented dealing with the periodical identification, valuation of risks and the implementation of mitigation controls? | yes | It's in Management Handbook Security Policy. Each employee is encouraged to report risks. This applies in particular to IT and Cyber risks. A risk catalog is kept. At least once a year a risk assessment is carried out. The obligation is with the DPO / Chief Security and Risk Officer. |
| Is a periodic assessment conducted of how well the security policies and procedures are respected within the company? | partially | We have two roles DPO & CSRO (chief sec and risk officer). There's a regularity done by the CSRO himself. . |

### Allocation of information security responsibilities

| Questions | Response | Comments |
|---|---|---|
| Do you have a dedicated person or team that is formally chartered with responsibility for information security? | yes | dpo at lucysecurity dot com |

### Allocation of IT risk management responsibilities

| Questions | Response | Comments |
|---|---|---|
| Do you have a dedicated person or team that is formally chartered with responsibility for IT risk management? | yes | dpo at lucysecurity dot com |

### Security Audits

| Questions | Response | Comments |
|---|---|---|
| Do you regularly conduct internal/external audits? | Annually | Internal Audit |

# Providers & external Suppliers

## Physical Protection

### Physical entry controls

| Questions | Response | Comments |
|---|---|---|
| Is physical access to buildings that house critical IT facilities restricted to authorized individuals? | yes | Access to the building is possible with a fingerprint in addition to an RFID key card. Without it no access is not possible. |

### Policy for DC and IT System access

| Questions | Response | Comments |
|---|---|---|
| Are policies and procedures implemented to specify proper use of and access to IT systems and network components. | yes | Access to Routers / Network components is only possible through a separate VPN network. Authentication on Firewalls / Routers is only possible through SSH-Key. All Logs are stored on a separate logging device, all configuration changes are monitored, saved and alerted. Physical Access is only possible for certified network admins. |

### Secure disposal or re-use of IT equipment

| Questions | Response | Comments |
|---|---|---|
| Is a secure decommissioning process in place? (E.g. wiping data from old hard drives, secure deletion of network configurations from routers.) | yes | We don't apply secure deletion. When applying dedicated deletion orders it is done with an overwrite routine using shred (Linux Software). |

## Human Resources Security

### Roles and responsibilities

| Questions | Response | Comments |
|---|---|---|
| Are security roles and responsibilities of employees defined and documented? | yes | A member of the top management. |

### Security awareness of LUCY staff

| Questions | Response | Comments |
|---|---|---|
| Is staff made aware of the key elements of information security and why it is needed (i.e. segregation of duties, need to know)? | yes | All staff that has any relation to the software code and our infrastructure (software engineers, QA engineers, support engineers, system admins, etc) pass internal information security courses. |

| Questions | Response | Comments |
|---|---|---|
| Are service administrators properly educated on their responsibilities with regard to security? | yes | All employees are getting an internal lesson on cybersecurity and passing security courses that include basic vulnerabilities overview, penetration technologies, mitigation methods, etc. It is an internal training based on the one-to-one introduction and a combination of Webinars / Practical Laboratory courses using Kali Linux. |

# Identity and Access Management

## Authentication

| Questions | Response | Comments |
|---|---|---|
| Which method is used to authenticate a user against the provided service (user ID/password, OTP, SMS, etc.). | yes | Username & Password and we use SMS-based one-time passwords. |

## Access control policy

| Questions | Response | Comments |
|---|---|---|
| Is the access to the service and data restricted to authorized individuals and based on an established access control policy? | yes | Physical access is protected with a fingerprint in addition to an RFID key card and the keys of the rack. "Virtual" access via SSH-Keys. No written policy for that and not mandatory for a company of this size. |
| Do access control arrangements restrict access to only approved system capabilities? | yes | Physical access is protected with a fingerprint in addition to an RFID key card and the keys of the rack. "Virtual" access via SSH-Keys. No written policy for that and not mandatory for a company of this size. |

## Data access

| Questions | Response | Comments |
|---|---|---|
| Is a Data Loss Prevention System in use? Who has the ability to accesses tenant data? | no | NO DLP System is in place and no alerting system is used at LUCYs promises |

## Data integrity

| Questions | Response | Comments |
|---|---|---|
| Are controls implemented to confirm that customer data has not been improperly altered or destroyed | yes | NO DLP System is in place and no alerting system is used at LUCYs promises |

## Password policy

| Questions | Response | Comments |
|---|---|---|
| Will the allocation of passwords be controlled through a formal password policy process? | partially | When choosing passwords they need to have more than 8 characters and they must be a mix of capital/lower letters, numbers and special characters. If there is a possibility for two-factor authentication (2FA), then 2FA should be applied. |

### User registration & management

| Questions | Response | Comments |
|---|---|---|
| Is there a formal user registration and de-registration procedure in place for granting and revoking access to all systems and services and to tenants data? | yes | An engineer may obtain access to a single tenants data only in case there is a need for maintenance, based on tenants request. An engineer sends a request to the systems admin or to the tenants responsible person (there is an option to grant access from the tenant's side). The permission is immediately revoked after the maintenance is finished. The permissions are granted and revoked within a few minutes. |
| Is a user management process in place (creation, revocation, provisioning, and termination of rights, etc.)? | yes | After contract termination the LUCY Server Instance is safely reset. This is a built-in and secure feature in LUCY Server. https://www.lucysecurity.com/PS/doc/dokuwiki/doku.php?id=factory_reset |

### Session time-out

| Questions | Response | Comments |
|---|---|---|
| Do inactive end-user sessions shut down after a defined period of inactivity? | yes | The end-user session terminates after 1 hour of inactivity |

## Vulnerability Reporting and Management

### Alerting

| Questions | Response | Comments |
|---|---|---|
| Do you have an easy way for externals to report security vulnerabilities in your systems? | yes | Write a mail to support@lucysecurity.com or dpo@lucysecurity.com . Every employee needs to react as stated in the GDPR code of contact |

### Information about inappropriate access

| Questions | Response | Comments |
|---|---|---|
| Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data? | yes | With a dedicated form, within 72 hours after discovery |

### Notification of customers

| Questions | Response | Comments |
|---|---|---|
| Do you inform your customers about vulnerabilities in your products once you had a chance to address them, regardless of whether they were discovered internally, or reported to you? | yes | with a dedicated form and a direct mailing put in place already |

## Operations Management and Security Controls

### Separation of development, test and operational facilities

| Questions | Response | Comments |
|---|---|---|
| Are development, test and operational facilities separated from each other to reduce the risk of unauthorized access or change to the operational environment. | yes | Operational facilities are completely separated. |

### Network hardening

| Questions | Response | Comments |
|---|---|---|
| Is hardening for Firewalls and Routers performed? | yes | On all routers and firewalls, management access is only possible via VPN. There are separate users for monitoring and configuration. All configuration changes are automatically reported and saved. In general, all firewalls and routers only run SSH for management access and otherwise only the necessary routing processes such as BGP, OSPF or just the firewall software. |

### Operating system hardening

| Questions | Response | Comments |
|---|---|---|
| Is an operating system hardening performed for all systems involved? | yes | OS is protected by internal firewall (iptables), SSH access keys are randomly generated, removed USB/firewire drivers, the app runs under a limited user account, etc. |

### Application Server hardening

| Questions | Response | Comments |
|---|---|---|
| Is hardening performed for all relevant application server? | yes | App servers are hardened using common approaches: proper file permissions, non-privileged account, removed version banner, disabled directory indexes, disabled ETags, secure cookie flags, etc. The system partially conforms to "CIS Debian 8" checklist (50% conformance), we can provide a detailed list of non-conforming items upon request. |

## Database hardening

| Questions | Response | Comments |
|---|---|---|
| Is hardening performed for all relevant database management systems? | yes | Only local connections are allowed and the system partially conforms to "CIS PostgreSQL 9.5" checklist (50% conformance), we can provide a detailed list of non-conforming items upon request. |

## Security Updates

| Questions | Response | Comments |
|---|---|---|
| Is a process in place to install emergency patches outside of the regular patching schedule for security updates that address high-risk vulnerabilities? | yes | Critical and high-risk patches are issued within 24 hours, medium - up to 1 week, low-risk - up to 1 month |

## Vulnerability management

| Questions | Response | Comments |
|---|---|---|
| Do you regularly perform penetration tests on all systems relevant to your service? | yes | We use various web application vulnerability scanners and OS security auditing tools (Burp Suite, OpenVAS, Lynis, Nessus). Even though we've done our own human-based penetration tests in the past we do not perform human-based penetration assessment on a regular basis. |
| How often are penetration tests done for the above scope (on average)? | yes | LUCY software is not a classic SaaS Plattform or Software. We do not perform penetration tests on client production instances. We release new Major updates of the software every 1-2 months, the software is mostly distributed as a virtual appliance (VMWare ESXi or Amazon image) and the process of automated penetration testing is tied to the release process - we perform such testing on the final stage of the release lifecycle. The set of application versions and software configurations of the version we are going to roll out exactly corresponds to the state of all systems after they migrate to the new version. For example, we are preparing version 5.0 for release and run penetration tests against it, within a virtual appliance. After all tests passed and all vulnerabilities are closed, we release the update, which is distributed over all existing software installations on different servers. All existing installations switch their state (install all required packages, remove old ones, change configuration, etc) to the state of the new version automatically, so all vulnerabilities closed on the pre-release stage will be closed on all tenants servers automatically. We never change anything on tenants servers directly. |

## Security incident detection and correlation

| Questions | Response | Comments |
|---|---|---|
| Does your infrastructure include a capability for security incident detection e.g. file integrity (host) and network intrusion detection (IDS) tools? | partially | These tools are used on infrastructure servers. Workstation installations do not have file integrity or IDS tools installed. |

## Protection of data storage media

| Questions | Response | Comments |
|---|---|---|
| Is tenets data held on data storage media (including magnetic tapes, disks, printed results, and stationery) protected against corruption, loss or disclosure? | yes | Tenants data is entirely stored on a disk on the server, and the only measure against data loss we perform _by default_ is a local daily database backup, which can help to prevent minor data loss. As an additional measure, we can set up RAID0 or RAID5 array, which can add an additional layer of protection against data loss or corruption. There is no access to other storage media from the server. The information in DB is encrypted using AES-256 (so it's stored int he encrypted form) and the key is built into the application, so there's minimal protection from data disclosure. |

## Malware/ Defacement

| Questions | Response | Comments |
|---|---|---|
| Are controls in place to protect the service and our tenants from malware? | yes | Infrastructure servers have anti-malware software installed. |

## Security gateways

| Questions | Response | Comments |
|---|---|---|
| Is network traffic routed through security gateways like web application firewalls or reverse proxies, prior to being allowed access to target service? | partially | WAFs and reverse proxies are used on infrastructure servers, though that is not the case on workstation installations. |

## Data encryption

| Questions | Response | Comments |
|---|---|---|
| Do you encrypt tenant data in storage and server side? | yes | Data is encrypted using AES-256. The application server gets data over HTTP/TLSv1.1+ connection and operates the data in cleartext form. The information is encrypted by the application before storing it into the DB, so the DB engine receives the information in an encrypted form (and therefore stores it to the storage media). The application decrypts the information from the DB before processing it. There are no other types of encryption beyond these. |

## Network encryption

| Questions | Response | Comments |
|---|---|---|
| Do you encrypt tenant data in transit (network - e.g. TLS)? | yes | The system uses TLSv1.1+ |

## Logging & Monitoring

| Questions | Response | Comments |
|---|---|---|
| Are a process and audit trails in place to monitor and record exceptions and other security-relevant events to assist in investigations and in access control monitoring? | yes | All actions are monitored and logged in order to help investigating any incidents. |

# Service Development

## Data input and output validation

| Questions | Response | Comments |
|---|---|---|
| Do you provide secure software development training to your engineers, that teaches them about common threats and countermeasures related to the software they are writing? | yes | Software engineers are trained to avoid OWASP top 10 vulnerabilities identify any existing vulnerabilities and mitigate them during the software development. |

## Use of productive Data for test purpose

| Questions | Response | Comments |
|---|---|---|
| Will you use tenant data for testing purposes? | no | |

## Data input and output validation

| Questions | Response | Comments |
|---|---|---|
| Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data? | yes | Built-in validations in the application |

# Business Continuity Management

## Plans and procedures

| Questions | Response | Comments |
|---|---|---|
| Has the provider a defined and documented method for coping with a business continuity situation? | no | The software has not mission criticality for the business |

## Plans and procedures

| Questions | Response | Comments |
|---|---|---|
| Has the provider implemented, tested and documented a set of procedures and actions for a contingency situation? | no | The software has not mission criticality for the business |

## Data and production recovery

| Questions | Response | Comments |
|---|---|---|
| Is the data security ensured by redundant systems? | no | The software has not mission criticality for the business |

## Crisis management

| Questions | Response | Comments |
|---|---|---|
| Does the provider have an emergency and crisis management with defined contact people? | yes | It's in LUCYs Management Handbook Security Policy. |

## GDPR Agreement

Please download our GDPR agreement

here

## Auftragsdatenverarbeitungsvertrag (German)

Please download our Auftragsdatenverarbeitungsvertrag

here