We work hard in making LUCY a secure product. Here is a quick overview of the most important security topics:

- **Restricted network-based access to LUCY**: Firewall
- **Secure the user access**: Password Policy
- **2-Factor Authentication**: 2FA
- **Restrict the user access**: Administrative Users
- **Secure Setup of LUCY in DMZ**: Master & Slave
- **Secure (and anonymous) storage of data**: Confidentiality of Data
- **Delete sensitive data:** Data clean-up
- **Secure communication channels**: Trusted ADMIN Certificate Generation with LUCY
- **Transparent network communication**: Network Communication
- **Secure support**: SSH in LUCY
- **Updates of the application**: Lucy Update
- **OS, Patches & Software**: Technical Information
- **Custom Admin URL creation**: Admin Path
- **Ability to monitor all system activities**: System Logs
- **Ability to monitor the system in real-time**: System Monitoring
- **Data Security, Processes Privacy (GDPR)**: Company, Application, Data Security and Privacy
- **Ability to store key on HSM:** HSM Database encryption
- **Block access to campaigns based on IP-ranges and browser types**: Filters
- **VPS Hardening info:** VPS Hardening
- **Optional protection system:** IPS/IDS

Additionally we perform regular external (anonymous) penetration tests according to the OWASP testing categories (https://www.owasp.org/). If you still should experience a security issue, please contact us under support@lucysecurity.com.

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=security_considerations

Last update: **2021/12/13 15:13**