INFORMATION SECURITY POLICY OF SHOWELL

High level of security is one of Showell's primary focus areas in everything from our daily operations to product development.

Summary
ISO27001 certified cloud with 99.99% availability
Third party security audited Service (by cyber security company F-Secure Plc)
Operational security policies meets Finland's Ministry of Defence's (DSA*) Katakri security criterias

Data Center / Cloud Security
Comprehensive description of Service's Data Center Security: https://aws.amazon.com/security/
ISO27001 certified cloud service
24/7 security expert monitored data center
Perimeter layer: e.g. security guards, fencing, security feeds, intrusion detection technology and more
Infrastructure layer: e.g. back-up power equipment, the HVAC system, and fire suppression equipment
Data layer: e.g. restricted access, privilege separation, threat detection devices, video surveillance and system protocols
Environmental Layer: data center located in very low risk area (flooding, extreme weather, and seismic activity)
PCI DSS 3.2 Level 1 Service Provider (the highest level of assessment available)
High-performance redundant multi-path connection to backbone network.
High performance firewalls for incoming/outgoing traffic
Data at transit: all data encrypted. Data at rest (user data, file metadata): encrypted (with AWS S3 also files are stored encrypted)

*designated Security Authority

Software Security
Third party security audited Service (by cyber security company F-Secure Plc)
User authentication & access permissions settings (for Showell App & Showell Admin)
All connections are secure (HTTPS)
Strongly encrypted passwords
Separated accounts with account identifiers for all database queries
Continuous updates and security fixes
Automated software testing
Peer review practices for the code or documentation
Dedicated testing environment and process for software testing (testing - staging - production)
Comprehensive third-party application store review process for all new versions

Data Protection
Comprehensive description of Supplier´s Processing of Personal Data and compliance with Data Protection Law, “Client Global Data Processing Addendum”
Supplier´s personnel are regularly trained to follow security criterias and best practices
Only Supplier’s selected personnel are allowed to access the data on the servers
Supplier’s support personnel can access Client’s data only with a Client’s permission
Third parties don’t have access to Client’s data without a written permission from Client
Only VPN/SSH connections to servers, root-level access only available for selected employees.
Client’s Showell adminitrators can access all account data, e.g. files and users and set permissions.
Client’ Showell users can only access data based on group-level permissions
Data recovery availability levels: 1) system recovery, 2) database recovery and 3) transaction recovery
System level data backups (yearly, monthly, weekly and daily), database level backups (daily) and transaction logs (continuous)
Maximum time for data recovery is within 24 hours
Client may request full backup of files (secured download link) or removal of all data

Operational Security
Operational security policies for Supplier´s personnel, facilities, tools and work practices meets or exceeds Finland´s Ministry of Defence’s (DSA*) Katakri security criterias. *designated Security Authority.
Supplier´s offices have 24/7 surveillance, electronic access control and automatic security personnel alarm system
Supplier´s personnel are regularly trained to follow security criterias and best practices
The Suppliers’s development team is trained to understand and prevent common security flaws. OWASP Secure Coding Practices is used as one of the reference guides for secure software development