BeesApps Security Policy

INFRASTRUCTURE - HOSTING

Data Center

- Biometric identification and RFID badges
- 24/7 physical security staff
- Internal and external security camera with full coverage of the site
- 24/7 monitored alarms
- Smoke detector
- Secure racks
- Firewall
- DDOS and DOS protection via Cloudflare & Arbor Peakflow
- Tier III certified
- ISO 50001 certified
- Service availability rate : 99.982
- BeesApps physical servers, no cloud offer

BeesApps Premises

- Secure access by badge
- Security camera on each floor

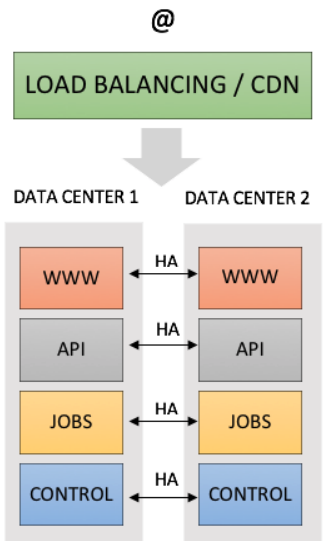
SERVICE AVAILABILITY

Dynamic

- Several different datacenters connected by secure lines
- 4 redundant logical layers
- Load balancing web service
- High availability clustering - 3 second failover time
- Files Servers
- Database Servers

Static

- Content Delivery Network



DATA AVAILABILITY

Availability	Backup
• Total export with attachments of data (in accordance with the GDPR) • Offline data availability (iPhone, iPad) • High availability clustering database architecture (HA) • Proxy database • Soft deletion management - permanent possibility of backtracking (except under request of deletion)	• Incremental backup per hour • Full backup per day on storage servers • Servers equipped with RAID5 • Encrypted backup with keys

AUTHENTICATION

Authentication
• Complex password policy (minimum 8 characters: 1 lowercase, 1 uppercase, 1 digit/special character) • Rules of automatic banishment both admin and users against attacks (Brute Force, Errors generations...) • No password backup in the database • SSH remote access using a 2048-bit private key • HTTPS with double certification • Authentication via Oauth 2.0 on Iphone/iPad • SSL via GlobalSign 2048-bit • SHA-256 encryption •1 unique identifier per account

VALIDITY TESTS

At each major update of the solution, automated security tests are set up verifying the known attacks or undergone

Application	Network
• XSS • CSRF • SQL Injection	• DDOS protection • Fail to ban exponential against: port scanning • Version Identification Vulnerability Scan

AUTHORIZATION

Authorization
• No usurpation of rights/account even in admin • Possibility of additional rights granted by a Beesy admin when creating an account • Users manage their rights when sharing • Feature to totally block a contact • Data access locks • Revocation of account

MONITORING & LOGS

Monitoring & Logs
• System and web log centralization platform (Graylog) 1-year data retention • Logs on any changes in Beesy - 1 month data conversation • Management of equipment access logs • Alarm when creating Admin accounts • Alarm for the security rules of automatic ban • Alarm during intrusion attempts • Monitoring and alarm system on the servers • SLA 99.982% on servers • Intervention on the site on 1h • Restoration procedure