cognia

Platform security

Security highlights

Certification	**Information Security Management System (ISMS)** is certified to ISO 27001:2013. **Compliant to PCI-DSS version 3.1**
Staff and third-party security	**Security checks and training** are integral to staff and contractor recruitment polices. **System access policies** ensure data and services exposed on a strict needs-only basis.
Systems security	**System design and development**: All aspects of system design, service development, code release and change management are subject to defined security impact and risk assessments and approval policies. **Data security and encryption**: All media is tagged at a fundamental level against account and device and then stored anonymously with dual encryption keys. **Penetration testing**: Internal and external penetration testing is undertaken at least every six months. **OS and server management**: All operating systems and servers are operated to minimal config with only the necessary services active. All applications are updated with the latest patch releases.
Monitoring	**Automated monitoring** for security information and event management, backed up by 24/7 support. **All incidents are logged and reviewed** for root causes, and preventative and corrective actions tracked. **Emerging threats and vulnerabilities are monitored** and action taken accordingly.
Data centre security	Data centres operated to **ISO 27001, PCI DSS v3.1, SOC 1, SOC 2 reports audited from SSAE 16/ ISAE 3402, and HIPAA.**

Built to protect your data

Protecting the confidentiality and integrity of our customers' data, and ensuring service availability, is of the utmost importance to us.

Operating in sectors where security is a key factor since launch, we have engineered a unique architecture backed up by robust measures to ensure the integrity and security of our platform and protect customer data.

From access controls, to regular audits and penetration tests, from application and storage design, to network security measures, we have taken steps meeting or exceeding industry best practice to protect our platform — your data — at every level.

Inbuilt security measures combine with customizable security rules controlling staff access to the administration and playback Console, letting organizations align their Cognia Cloud services to company policy.

This information sheet provides a summary of the security controls, policies and systems we employ, and provides the answers to the more common questions we receive about platform security.

To read more about the measures in place to protect the Cognia Cloud, please get in touch to request the *Cognia Cloud security paper*.

Information Sheet