



# Security and cloud infrastructure

Secure and reliable platform hosted in Australia in the Microsoft Azure cloud

## Secure cloud hosting safeguarding your data with rigorous privacy and encryption standards.

LogiQC is an online platform used by hundreds of healthcare and community services sectors across Australia and New Zealand to manage safety, quality and risk.

LogiQC is designed to support organisations operating in complex regulatory environments to meet the requirements of standards such as ISO 9001, ISO 3100, NSQHS, NDIS Practice Standards, any many more.

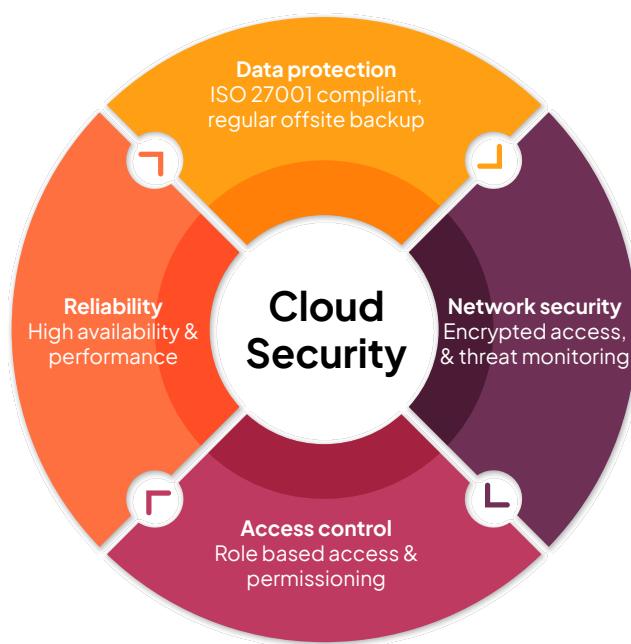
Since its release in 2010, LogiQC has become the system of choice for more than 250 organisations throughout the region.

Our web-based platform, delivered via Software-as-a-Service (SaaS), ensures accessibility and efficiency for our users.

### Trusted cloud partner

At LogiQC, safeguarding the security of your data is our top priority. We have implemented a range of industry-leading best practices aimed at fostering trust in our information and security management processes.

With LogiQC, you can trust that your data is in safe hands, allowing you to focus on what matters most delivering quality care and service to your clients.



### Key points

- ✓ All data stored in Australia
- ✓ 99.95% uptime
- ✓ Managed in accordance with ISO 9001 and ISO 27001 requirements
- ✓ Regular pen testing
- ✓ Data encrypted in transit using TLS version 1.2 with a 2048-bit signatory key
- ✓ Four hour RPO and six hour RTO





Security and cloud infrastructure

# Information & Data Security

## Deployment

The Logiqc system is a web-based application, functioning as a hosted service, thus eliminating the necessity for local application installations and mitigating security risks. It operates smoothly across a range of internet-enabled devices, including desktops, laptops, tablets, and smartphones. Logiqc seamlessly integrates with leading browsers such as Google Chrome, Microsoft Edge, Mozilla Firefox, and Safari.

## Infrastructure

In pursuit of maximum availability, security and resilience, customer data is hosted on the Microsoft Azure cloud platform. Renowned for its excellence in security and availability, Azure offers a robust infrastructure spread across multiple regions throughout Australia, anchored by its primary data centre in Sydney. Backed by Microsoft's assurance of 99.95% service availability, our service stands poised to deliver uninterrupted performance and reliability to our valued users.

## Data Centre Security

Microsoft plans, constructs, and manages data centres to tightly regulate physical access to the spaces housing your data. Employing stringent security protocols including onsite personnel, rigorous site access authorisation procedures, round-the-clock video surveillance, and single-entry points, Microsoft ensures optimal measures are in place to safeguard your data with the highest level of security and reliability.

## Compliance

Logiqc holds ISO 9001 certification, underscoring our commitment to quality management practices. In line with this, we have implemented various in-house policies to uphold security as a foundational aspect of our operations. Additionally, Microsoft boasts certifications in additional security-related standards, including ISO/IEC 27001:2013 and NIST SP 800-53, further

validating their dedication to robust security measures. The business continuity and disaster recovery plans for the Azure services have been independently validated as part of their SOC 2 Type 2 report and ISO 27001 certification. These certification documents can be viewed at <https://servicetrust.microsoft.com/viewpage/ISOIEC>.

## Penetration Testing & Auditing

Each year, an independent, reputable security company conducts annual application penetration testing using a combination of manual and automated methods. Furthermore, we are regularly partnered with companies specialising in security consulting and auditing, leveraging their in-depth understanding of our internal security mechanisms and architecture.

## Application Security

Recognizing the diverse needs of our users, Logiqc provides robust access control mechanisms tailored to your requirements. Our platform empowers you to define precise permissions and roles for each user, guaranteeing that only authorised individuals can access sensitive data. Whether you oversee a small team or a large enterprise, you retain complete control over access privileges within our platform. This ensures heightened security, minimising the likelihood of data breaches and unauthorised access from within, or external, to your own organisation.

Additionally, we offer Single Sign-On (SSO) to enhance security for both individual users and enterprises, fortifying their accounts against unauthorised access.

## Encryption

The Logiqc platform utilises SSL (Secure Sockets Layer) encryption for transporting data between the user's device and cloud hosted server, ensuring that your sensitive data remains safeguarded during its journey across the internet. The data is encrypted in transit using TLS version 1.2 with a 2048-bit signatory key. We also encrypt your data at rest within the database using AES-256 encryption, which ensures that in the unlikely event of a security breach, your data remains secure.

## Alerting and Monitoring

Logiqc not only completely automates its build processes but also prioritises substantial investments in automated monitoring, alerting, and response capabilities to proactively tackle potential issues. Our product infrastructure is equipped with instrumentation to promptly notify engineers and administrators of any anomalies. Specifically, fluctuations in error rates, instances of abuse, application attacks, and other irregularities prompt automatic responses or alerts to the relevant teams for swift investigation and resolution.

Moreover, numerous automated triggers are specifically designed to promptly address abnormal situations. Actions such as traffic blocking, file quarantining, process termination, and similar functions are activated when predefined thresholds are exceeded.

## Availability

Microsoft Azure guarantees high levels of service availability, ensuring redundancy to all power, network, and HVAC services. The business continuity and disaster recovery plans for the Azure services we utilise have been independently validated as part of their SOC 2 Type 2 report and ISO 27001 certification.



Security and cloud infrastructure

# Information & Data Security

## INCIDENT MANAGEMENT

LogiQC collaborates with its technical partners to address business disruptions from the initial response to a disaster until normal business operations are restored. Managed Service Provider Service Level Agreements (SLAs), which include incident management protocols, are established. Clients are promptly notified in case of incidents affecting the confidentiality, integrity, or availability of client information. Comprehensive incident detection and management policies are also implemented.

Within the hosted environment, crisis management is overseen by Microsoft, following local Azure Cloud protocols. Crisis coordination is jointly managed by LogiQC and relevant vendors on a 24/7 basis. Clients can report incidents by initiating support tickets with the LogiQC Support team.

## DATABASE BACKUP

Database transaction logs are backed up every four hours and distributed to an offsite regional data centre. Full database backups are taken nightly, and also distributed to an offsite data centre. We are committed to achieving a sub-four-hour recovery point objective should data corruption occur. Our target time to restoration should a disaster occur affecting all server infrastructure is less than six hours.

## FILE BACKUPS

Documents uploaded onto the LogiQC platform are securely stored within the Microsoft Azure cloud infrastructure. Upon initial upload, these documents are promptly replicated across various regional data centres for enhanced accessibility. Access to these files is restricted to authorised users solely through the LogiQC platform, ensuring utmost privacy and security.

## DATA RETENTION AND DATA DELETION

Customer data is retained for as long as you remain an active customer. Data created and stored within the platform remains the property of the client. Upon termination of subscription client data can be provided in a csv format. Former clients will have their data and backups removed from our production servers and following the termination of all customer agreements.

## DATA CLASSIFICATION

LogiQC QMS enables users to store data pertaining to their internal quality controls. According to our Terms of Service, clients bear the responsibility of ensuring that the data captured is relevant solely to their internal quality control procedures. The LogiQC QMS platform should not be utilised for collecting sensitive information, such as credit or debit card numbers, financial details, or health-related data.

## EMPLOYEE ACCESS TO CLIENT DATA

LogiQC support staff will access client systems only when necessary to address specific issues or provide assistance as requested by the client. All access is closely monitored and recorded to ensure transparency and accountability. Each interaction with client systems is logged, detailing the time, nature of the activity, and the staff member involved. These records serve as a comprehensive audit trail, enabling thorough oversight and review of support activities. Additionally, access permissions are strictly controlled, with staff granted only the minimum level of access required to fulfil their support duties. This meticulous approach to monitoring and recording ensures the security and integrity of client systems while maintaining the trust and confidence of our clients.

## EMPLOYEE ACCESS TO PRODUCTION INFRASTRUCTURE

Access to LogiQC's production infrastructure is rigorously managed and restricted to authorised employees and partners who possess the requisite security privileges. Additional layers of security are implemented, including multi-factor authentication and role-based access controls, to further regulate and safeguard access to sensitive systems and data.

## TERMS OF USE

LogiQC's Terms of Use is available at <https://knowledgebase.logiqc.com.au/logiqc-terms-of-use>

## PRIVACY POLICY

LogiQC's privacy policy is available at <https://logiqc.com.au/privacy-policy>