



HM Government
G-Cloud

G-Cloud 15

Service Definition Document

Honeywell/Lenel OnGuard Cloud Access Control Solution *provided by Reliance*

*Serious about
technology,
passionate
about people*

Contents

1.0	About Reliance.....	3
1.1	Partnership Ethos and Customer-Centric Delivery	3
1.2	A Technology-Led Business with Strategic Depth.....	3
1.3	From Systems to Outcomes	4
1.4	Commitment to Quality and Assurance.....	4
1.5	Trusted in High-Governance and High-Compliance Environments	5
1.6	Organisational Capability and Service Structure	5
1.7	Serious About Technology. Passionate About People.	5
1.7	Resilient end-to-end solutions.....	6
2.0	Service Definition	7
2.1	Overview	7
2.2	Infrastructure and Architecture	7
2.3	Technical Solution.....	7
2.3.1	Centralised Access Control Management.....	7
2.3.2	Door Control, Alarms and Event Monitoring	7
2.3.3	Role-Based Access Control and Governance.....	8
2.3.4	Audit Trails and Reporting	8
2.3.5	Multi-site Standardisation.....	8
2.3.6	Cybersecurity	8
2.3.7	Resilience and Business Continuity.....	8
2.3.8	Integration and Expansion.....	8
2.4	Pricing Structure.....	8

VERSION CONTROL

Date	Version	Changes
26/1/26	1	G-Cloud 15 submission

RELIANCE HIGH-TECH CONTACT

James Smith

Sales and Marketing Director

E: james.smith@reliancehightech.co.uk

T: 0845 121 0802

1.0 About Reliance



Reliance is an independent UK security systems integrator, trusted by organisations operating in high-compliance, high-risk and mission-critical environments - where quality cannot be compromised. With decades of experience, we deliver high-performing, IT-aligned security solutions that reduce risk, strengthen resilience and provide long-term value.

For clients, this means more than system uptime. It means creating safer, better-managed environments through reliable core security, clear operational visibility and, where appropriate, analytics and alerting that help teams identify issues earlier and respond with confidence. By improving situational awareness and reducing avoidable incidents, we help organisations protect people, assets and reputations - while enabling day-to-day operations to run smoothly.

Quality, reliability and integrity sit at the heart of how we design, deliver and support every solution.

1.1 Partnership Ethos and Customer-Centric Delivery



Our mission is to protect people, assets, and reputations - but how we do it is just as important. We believe great partnerships are built on trust, shared goals, and strong personal relationships. That's why we take the time to understand what matters most to you - not just in terms of technical requirements, but the wider priorities, pressures, and aspirations that shape your environment. This approach allows us to deliver solutions that are truly aligned with your objectives. We also invest heavily in our own people - from structured training and mentoring to wellbeing and professional development - ensuring they bring not only expertise, but empathy and care to every engagement. Our clients know us not just for what we deliver, but for how we work - consistently collaborative, dependable, and easy to do business with. We grow with our clients, adapting as their needs evolve and working as an extension of their team.

1.2 A Technology-Led Business with Strategic Depth

While our roots are in security, our capabilities span much further. We are a technology-led business that blends physical security with IT, cloud, analytics, and IoT. This enables us to bring a strategic, joined-up perspective to system design and service delivery, helping clients navigate legacy challenges, embrace cutting-edge platforms, and plan confidently for the future. We work closely

across stakeholder groups - from IT and cyber teams to estates, compliance, and health and safety - taking time to understand their individual needs and turning them into actionable, aligned solutions that deliver meaningful outcomes across the wider organisation.

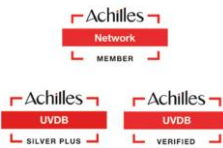
1.3 From Systems to Outcomes

We deliver more than systems - we deliver outcomes. Through data integration, asset lifecycle management, and remote monitoring, we help clients make smarter decisions, reduce total cost of ownership, and unlock operational efficiencies. Our managed services offering ensures performance is not just achieved, but sustained. These principles of continuous improvement, value creation, and operational excellence are embedded in our culture and backed by rigorous, externally verified standards.

1.4 Commitment to Quality and Assurance

We hold key certifications that reflect the breadth and depth of our commitment to quality, resilience, and cybersecurity - including ISO 27001 (Information Security), ISO 27017 (Cloud Security), ISO 22301 (Business Continuity), and ISO 9001 (Quality Management). We are also certified to Cyber Essentials Plus and are proud to be recognised as being in the top 6% of suppliers to the NHS Data Security and Protection Toolkit, with the rating of "Expectations Exceeded" - an accolade we have held for four consecutive years.

As part of our work with NHS organisations, we are delivering significant volumes of custom development at API and Webhook level - providing tight integration with third-party systems as part of a highly tailored security solution. This is a direct testament to the strength of our in-house development team and our proven ability to deliver secure, scalable, and standards-compliant integrations. Our broader experience spans multiple platforms, and our deep familiarity with Genetec and other enterprise-grade technologies means we can support complex development and testing requirements at an unrivalled level - bringing together security, IT, and application integration in a seamless and robust way.

 Verify at ssaib.org	 Verify at ssaib.org	
		

1.5 Trusted in High-Governance and High-Compliance Environments

Reliance supports organisations where security, resilience and accountability are non-negotiable. We work across high-governance, highly regulated environments - delivering and maintaining integrated security solutions for complex estates, critical operations and busy public settings. Our experience spans Central Government, CNI and defence-aligned supply chains; energy and utilities (power distribution and generation, water and gas); police and custodial environments; research organisations, governing bodies, large trusts and healthcare; financial and FTSE environments; bio/pharma; data centres and communications; transport and logistics; and higher education, including multi-building campus and university estates.

Across these markets, clients rely on us to operate safely, securely and with minimal disruption - combining strong technical capability with disciplined delivery, clear reporting and a long-term service mindset.

1.6 Organisational Capability and Service Structure

Our c.180-strong team includes expert engineers, project managers, developers, and cybersecurity professionals - backed by robust internal systems, including our centralised Service Management Platform and in-house pre-staging capability. These aren't just people with skills; they are people who care - committed to doing the right thing, taking pride in their work, and delivering consistent quality across every touchpoint. This investment in our people, combined with rigorous internal standards and industry-leading certifications, translates directly into the experience we offer and the outcomes we deliver.

1.7 Serious About Technology. Passionate About People.

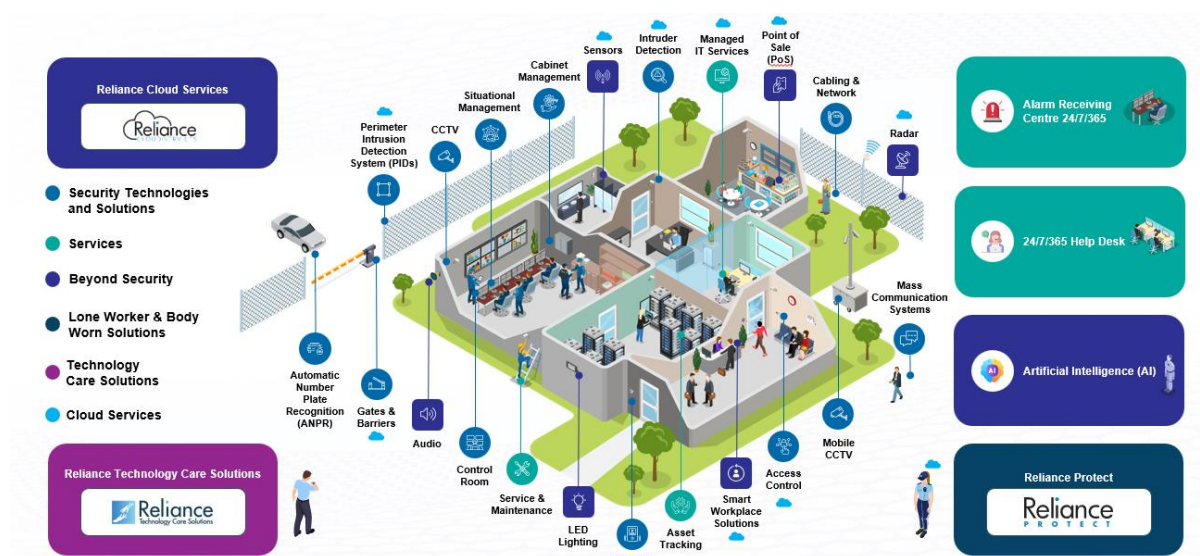
Technology is at the core of our approach, but it's the quality of our people that truly sets us apart. All of our engineers are security cleared, and all are trained to operate to the highest technical and ethical standards. We invest heavily in training, development, and wellbeing to ensure our teams not only stay ahead of technology - but consistently deliver with care, professionalism, and integrity. These are people who take pride in what they do and represent our values in every interaction - helping you protect what matters most.



At Reliance, we're Serious about Technology, Passionate about People. That ethos is at the heart of everything we do - driving innovation, building trust, and ensuring that the solutions we deliver truly make a difference.

1.7 Resilient end-to-end solutions

Reliance delivers resilient, end-to-end security solutions that cover the full lifecycle - from design and systems integration through IT enablement, ongoing maintenance, and specialist services such as lone worker protection and monitoring. Clients benefit from one accountable partner who can supply, install, integrate, host, support and continually optimise their solution, ensuring it remains secure, available and fit for purpose as requirements evolve. Whether you need a single capability or a fully integrated estate-wide approach, we bring the people, processes and infrastructure to deliver it reliably at scale.



Systems Integration

- Access Control
- Closed Circuit Television
- Perimeter Security
- Network
- Information Management & Situational Awareness

Maintenance

- 24/7/365 Help Desk
- Nationwide Cover & LSP's in Europe
- Flexible & Tailored Plans
- Advance Call Handling and Tracking Software
- Web-based Service Report Module

Monitoring Services

- Dedicated Monitoring Centre
- 24/7/365 Security & Surveillance
- Systems Monitoring and Remote Diagnostics
- Reliance Protect – Lone Worker Monitoring

IT Capability

- In-house Expertise
- Fully Accredited – ISO27001 & Cyber Essentials Plus
- Support for all Security related IT Requirements
- High-availability Hosting and DR Solutions

Lone Worker Solutions

- ID Cards & Fobs with GPS and Audio
- Body Worn Cameras
- Slip/Trip/Fall and 'Man Down'
- Check-ins and Safety Timers
- Two-way Audio with Trained Operators

2.0 Service Definition

This section describes the proposed solution and the benefits it will realise for G-Cloud 15 Framework users.

2.1 Overview

Reliance offer a range of cloud and hybrid access control solutions designed for organisations operating in high-governance and high-compliance environments. This Service Definition provides details of **LenelS2 OnGuard Cloud**, a cloud-managed access control platform that supports secure identity management, door control, alarms and event monitoring across single sites and complex multi-site estates.

OnGuard Cloud enables centralised administration, consistent policy application and remote support, while maintaining robust on-site control of doors and readers. This helps organisations reduce operational risk, improve resilience and simplify lifecycle management, without compromising security or uptime.

2.2 Infrastructure and Architecture

A typical OnGuard Cloud deployment combines cloud management services with on-site access control hardware.

Core architectural elements include:

- **Cloud management layer:** central administration for users, credentials, access levels, schedules, reporting and audit trails.
- **On-site controllers and door hardware:** panels/controllers manage local door decisions and inputs/outputs, ensuring doors continue to operate safely even during internet interruptions (deployment dependent).
- **Credentials and identity:** support for common credential formats (e.g., card technologies and mobile credentials), configured to meet site policy and risk profile.
- **Secure connectivity:** encrypted communication between on-site equipment and the cloud environment, typically using outbound connectivity principles to reduce exposure.
- **Client access:** authorised operators and administrators access the platform via secure browser-based interfaces, subject to role-based permissions.
- **Scalability:** sites, doors and users can be added in a controlled manner, supporting estate growth and change programmes.

2.3 Technical Solution

The following section details key functionality, features and benefits.

2.3.1 Centralised Access Control Management

OnGuard Cloud supports central management of cardholders, credentials, access groups, schedules and door permissions. This improves consistency across sites, reduces manual effort and supports controlled change management.

2.3.2 Door Control, Alarms and Event Monitoring

The platform supports real-time door monitoring, alarm/event handling and the ability to manage cause-and-effect style responses (where applicable and within the agreed configuration). This enables security teams to respond faster and maintain control of operational risk.

2.3.3 Role-Based Access Control and Governance

Access to administrative and operational functions can be restricted through role-based permissions. This supports segregation of duties and helps ensure only authorised personnel can perform sensitive actions (e.g., adding users, changing access levels, exporting reports).

2.3.4 Audit Trails and Reporting

OnGuard Cloud provides audit records and reporting to support governance, investigations and compliance requirements. Typical outputs include access history, alarm activity, operator actions and system configuration changes (subject to configured retention policies).

2.3.5 Multi-site Standardisation

For organisations with distributed estates, OnGuard Cloud supports standardised access policies and templates, enabling consistent onboarding of new locations and repeatable operational processes.

2.3.6 Cybersecurity

OnGuard Cloud is designed to support secure access control operations, including:

- Encrypted communications between cloud services and on-site components
- Strong authentication options (including SSO/MFA where applicable to the deployment)
- Least-privilege access via roles and permissions
- Logging and auditability to support accountability and forensics
- A structured approach to updates and vulnerability management (deployment dependent)

2.3.7 Resilience and Business Continuity

The solution can be designed to maintain safe and secure access control operations during connectivity issues, with local controllers continuing to enforce door permissions and schedules (architecture dependent). This provides continuity for mission-critical environments where access control must remain available.

2.3.8 Integration and Expansion

OnGuard Cloud can be aligned with wider security and operational systems, such as CCTV, intercoms, intrusion detection, visitor management and reporting platforms. Reliance can scope and deliver integrations and phased migrations to support long-term modernisation programmes.

2.4 Pricing Structure

Guide pricing is provided in the separate pricing schedule. Please contact Reliance to confirm the required architecture, number of doors/readers, credential approach, reporting needs, hosting/resilience requirements and any integration scope, so we can provide a tailored quotation.