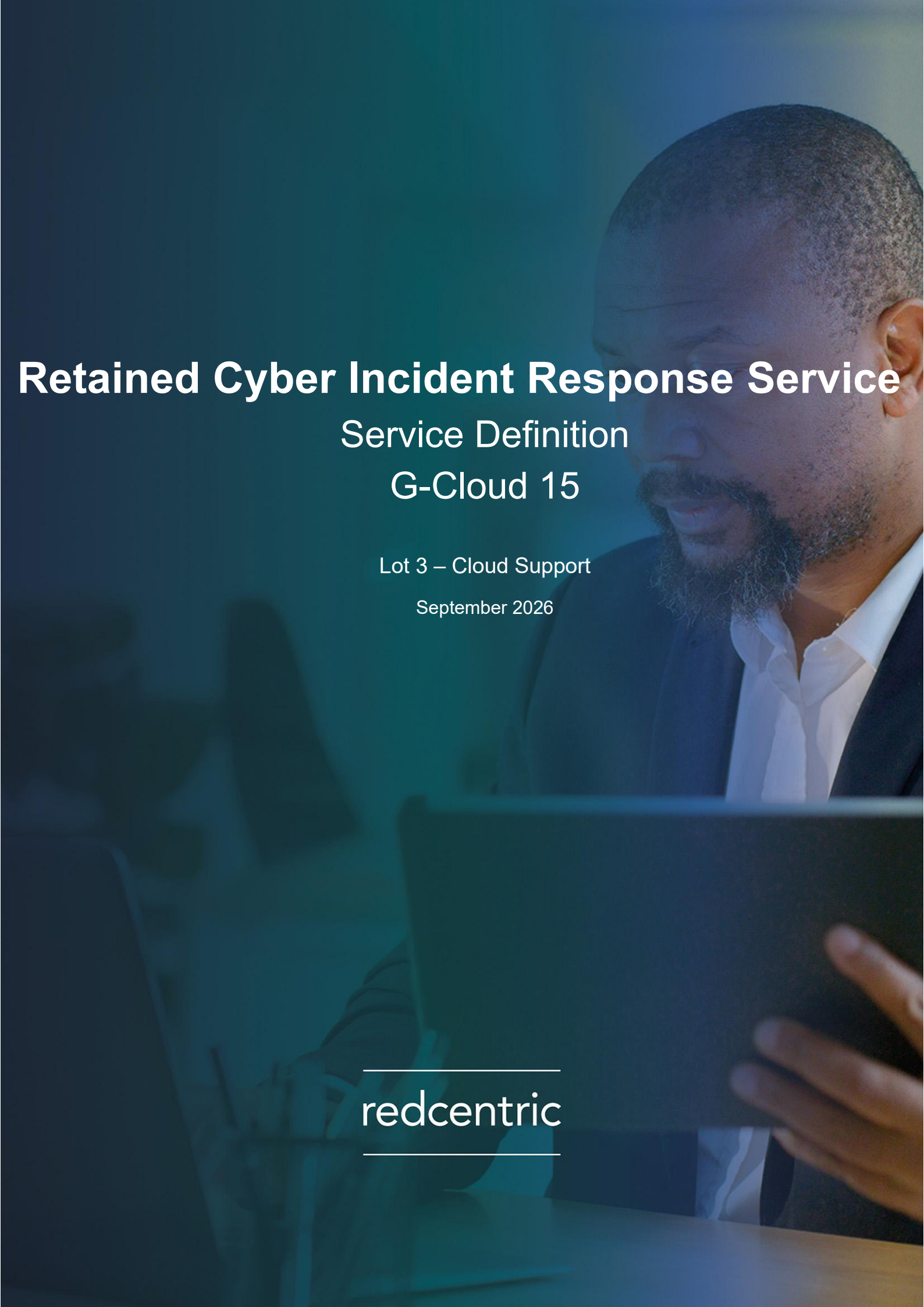


# Retained Cyber Incident Response Service

## Service Definition

## G-Cloud 15

Lot 3 – Cloud Support

September 2026

redcentric

# Contents

# 1. Service Definition

In today's digital world, businesses increasingly face cyber threats that can cause significant business disruption, data breaches, and reputational damage. At Redcentric we recognise the value of comprehensive cyber security that includes not only protective and detective measures, but also responsive strategies to swiftly address and recover from such incidents. We recommend that all organisations reserve the right to call on expert Cyber Incident Response services to mitigate the impact of a cyber-attack and avoid full-scale compromise when defences are breached. We provide the following services to enable effective cyber incident response:

**Cyber Incident Response Retainer** – Guaranteed response support when you need it most, with rates tied to response times and service levels.

**Cyber Incident Readiness Services** – Prepare your internal teams by implementing effective processes and plans and rehearsing them in a realistic environment, to improve your response to a major cyber crisis.

Our Retained Cyber Incident Response service provides clients with on-demand access to Incident Response specialists in the event of a major cyber security incident to contain and eradicate live security threats affecting your network and business operations.

The retainer can be invoked by a customer in the event of a suspected or confirmed Cyber Security Incident. When activated, our partner will deploy suitably qualified and experienced Cyber Incident Responders to triage, investigate, contain, and eradicate the threat from the customer's network.

Depending upon the extent and severity of the incident, either our partner or in some circumstances Redcentric can also provide support to enable the customer to rebuild and recover from the incident and facilitate the restoration of normal business operations.

### 1.1. Key Features

- A market leading SLA. Our partner will rapidly respond to cyber security incidents, providing you with the best chance of avoiding serious damage or disruption.
- 24/7/365 support. Retained clients have access and flexible support to specialists that suits their needs and budgets.
- Technical Onboarding. Onboarding enables data gathering and accelerates incident intake focusing on the customers technology and data stack, key people and contacts and agreed escalation processes.
- Preferential Rates. Our partners retainer has an associated preferential rate with savings starting from 25% and increasing as the investment grows.

### 1.2 Key Benefits and Outcomes

- Continuously accessible service and guaranteed support. Assets are deployed remotely to eliminate response delays and swiftly contain and remediate threats.
- Leverage powerful remote response capabilities to conduct incident response at-scale.
- Access to specialists in forensic investigations, threat actor engagement and crisis management.

### 1.3 Scope of Services

- SLA-backed service.  A one-hour response to a call being logged with the 24/7/365 service desk, with guaranteed resource availability.

### 1.4 Partners

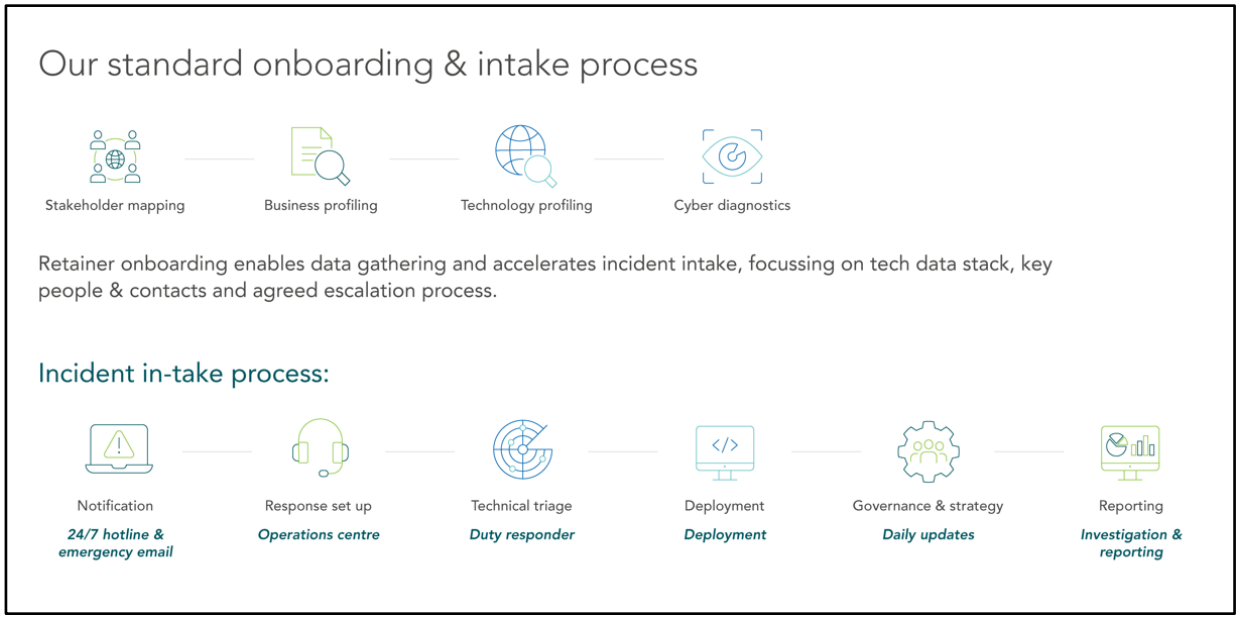
Our NCSC assured partner, S-RM, provides the incident response capability and guarantee's the retainer SLA.

- Our partner retains approximately 50 highly skilled and experienced incident response consultants with industry-leading credentials.
- Our partner has supported more than 140 clients worldwide, across several industry sectors.
- They are a member of the NCSC CIR scheme.
- A well-known partner of cyber insurance brokers and providers, meaning that any insurable costs may be covered by your provider.
- Experts in litigation support with Chain of Custody compliant processes and procedures.

# 2. Onboarding and Offboarding

## 2.1 Onboarding

Once authorised, customers will be scheduled for an on-boarding workshop with our partner. This will involve the capture of key information that will facilitate timely and effective incident response. It will also provide customers with an understanding of the service and how to engage it. The workshop will be held remotely with nominated customer personnel who will be responsible for managing the relationship and activating the retainer where required.




## 2.2 Retainer activation

First contact should always be made via the 24/7/365 partners Service Desk in an emergency to engage the service.

- The hotline number and alternative e-mail contact details will be provided during onboarding.
- Upon contacting the hotline your details will be captured, and a ticket will be raised and a call will be logged to engage the response team.
- Customers will be contacted within 1 hour of the initial call being recorded by the duty responder who will undertake a rapid technical triage of the situation with the client.

The customer's nominated personnel who are authorised to activate the service will be defined as part of the on-boarding process.

## 2.3 Resource assignment

Once a call is logged our partner will assign the incident to their on-call IR consultant.

### 2.3.1 Incident Responder credentials

Responders with appropriate skills, capabilities, and experience/seniority will be nominated for the incident based on the initial triage call. Additional responders may be allocated as the incident develops.

### 2.4 Triage

The nominated responder will contact the customer to appraise the incident. This usually takes the form of a triage call between the client and our partner to gauge the severity of the incident by understanding which systems and business processes are affected and establish a timeline of events to-date.

By the end of the triage call, our partner will be able to provide an initial risk assessment of the incident and recommend appropriate next steps. This will include whether further investigation and response activity is recommended and the estimated effort for the required works.

#### 2.4.1 Estimation of effort

Our partner will provide an estimation of the total cost of the response effort based on the nature of the incident as diagnosed during the triage call. This does not entail a final quote but is intended to support the customer in understanding the severity of the incident and evaluating whether to proceed with the incident response effort. The total effort will be calculated following completion of the incident and billed as consumed.

### 2.5 Tooling deployment

Remote response tooling will be deployed on a just-in-time basis where required. This will be required where no suitable tooling exists in the customer environment that can be accessed by the incident responders. Our partner uses primarily a combination of industry recognised incident response tools.

### 2.6 Digital Forensics and Chain of Custody

At the outset of the incident response process, our partner will establish whether the incident may result in a court case or involve law enforcement. If this is the case, then suitable evidence handling, and chain of custody procedures will be applied. Within the UK the foundations for this approach have been well documented by the Association of Chief Police Officers (ACPO) and serve to ensure that evidence handling, investigation practices, and supporting activity are carried out legally.

Where a ‘forensically sound’ approach is required, our partner can advise and co-ordinate the necessary response using forensically trained specialists. Due to the specialist nature and the requirement to use ‘competent’ individuals as part of such a deployment, our partner, in consultation with the client and potentially Redcentric would engage external professional resources as additional sub-contractors to ensure that this requirement is satisfactorily met.

### 2.7 Threat actor negotiation

Our partner has staff who can negotiate - with threat actors on the customers behalf in the case of an incident involving extortion (e.g. Ransomware).

# 3. Service Levels

## 3.1 SLA-backed model

A guaranteed response within one (1) hour of a call being logged with the 24/7/365 service desk, with guaranteed resource availability.

# 4. Responsibilities

### 4.1 CIR Partner Obligations

Our partner will be responsible for

- providing access to a 24/7/365 hotline and triage services.
- the configuration of the EDR platform to deliver the required system visibility for the Cyber Incident Response service.

### 4.2 Customer Obligations

The Customer will be responsible for:

- updating the details of network ranges if there are any changes to the scope during the period of the contract.
- the creation of service accounts as required.
- network configuration allowing access from the Incident Responder's and sub-contractor's devices to all in scope systems.
- gaining the appropriate approval from any third-party hosting / support services as required.

# 5. Associated Services

The table below provides details of other compatible services available from Redcentric on G-Cloud 15.

| Service Name | Service Summary |
|---|---|
| Cyber Security Professional Services | **Cyber Security Professional Services** Redcentric offers a wide range of Cyber Security Professional Services from strategy to implementation. Aligned to the NIST Cyber Security Framework, our qualified industry professionals will support you in overcoming your cyber security challenges around governance, InfoSec compliance, security testing, vulnerability management, business continuity, disaster recovery, data breach and Incident Response. |
| Managed Vulnerability Scanning | **Managed Vulnerability Scanning** enables organisations to identify, prioritise, and remediate software vulnerabilities affecting their digital infrastructure, applications, and services that can be exploited by a cyber attacker to cause harm to their business. We will perform regular vulnerability scanning of your internal and external (internet-facing) assets. |

# 6. Business Continuity and Disaster Recovery

## 6.1 Business Continuity

Redcentric under its ISO22301:2019 Business Continuity certification, operates and maintains a robust Business Continuity Management System (BCMS). The BCMS scope includes;

- Data Centres
- Managed Services
- ICT technologies and systems
- Staff and business functions

and is externally assessed by the BSI annually to ensure continued effectiveness in line with BSI published standards.

Our Business Continuity Policy Plan (BCP) is fully supported by the Board and is designed to enable a return to normal operations in the shortest practical time, with minimum disruption. The primary objective is to restore and deliver continuity of key services in the event of a critical incident.

Our overall Business Continuity strategy is to provide resilience for all systems that support critical processes, by having data backed up to alternative Data Centers, or dual site services configured as active-active.

We use the same cloud backup service (Acronis BaaS) for our own IT and services as we do for our customers, ensuring fully secure, encrypted data is available off-site when needed. Departments and services are required to test backup and restore annually.

### Testing

Our BCP is routinely tested annually, and as Redcentric is a provider of critical services to the NHS (Peering Exchange and Consumer Network Service Provider), is independently witnessed by a member of NHS England.

Disaster Recovery plans underpinning the BCP have been developed for each Department and Service, and these are externally audited and tested annually.

### Network Resilience

Our network is designed and engineered to deliver highly available, stable connectivity to maintain business access to critical applications. To maximise resilience, multiple carriers provide core connectivity and routing, and switching devices are from market leaders Cisco Systems. The network design and build are geographically resilient providing a minimum of 99.99% availability (to resilient end points).

The Redcentric highly resilient, high-capacity core has connections to several carriers providing multiple options for our internal business operations and critical services, and customers wishing to access cloud services, applications, and data:

- Geographically resilient connectivity to multiple Tier-1 Internet transit providers and Internet exchanges.
- Geographically resilient connectivity directly into the inner core of the HSCN network.

- Core network engineered to withstand multiple concurrent failures and to re-route around a failed transit path in under a second.

### 6.2 Disaster Recovery

No disaster recovery plan is provided as part of these Services.

# 7. Data Management

### 7.1 Data Processing

Note that in completion of this Statement, the CCS Customer is the Controller and Redcentric is the Processor unless otherwise stated.

### 7.2 Subject matter of the processing

Redcentric delivers a wide range of cyber security professional services from strategy to implementation. Aligned to the NIST Cyber Security Framework, our qualified industry professionals will support you in overcoming your cyber security challenges around governance, InfoSec compliance, security testing, vulnerability management, BC, DR, data breach and Incident Response.

### 7.3 Nature and purposes of the processing

All personal data is stored in UK Data Centres unless otherwise stated. Some personal data may be accessed by our Support operation in Hyderabad, India. This access is to authenticate CCS Customer users following a support request or to troubleshoot incidents and is required to satisfy obligations under the Contract. This is subject to controlled remote access using Redcentric owned devices only and is operated under an International Data Transfer Agreement between Redcentric Solutions Limited and Redcentric India.

### 7.4 Duration of the processing

From the start date of the contract until seven years after the expiry or termination date. It may be necessary to retain data beyond this time according to UK Law.

### 7.5 Categories of Data Subject International Transfers

It may be necessary for our Support operation in Hyderabad to access personal data to authenticate CCS Customer users following a support request or to troubleshoot incidents. The personal data may include first name, last name, role title, telephone number, which may be checked against a pre-approved list.

### 7.6 Sub Processors engaged by Redcentric (sub-contractors)

All Redcentric suppliers (sub-processors) are checked for compliance with UK GDPR as part of onboarding and regularly reviewed.

### 7.7 Types of Personal Data Processed

During Cyber Security Professional Services work the following elements of Personal Data may be processed: first name, last name, telephone number, role title, DDI number, work email address, IP address. The Personal Data to be processed do not include sensitive personal data, or any data the processing of which is restricted (e.g. data relating to criminal offences or convictions)

### 7.8 Special Category Data

The Personal Data to be processed do not include racial or ethnic origin, genetic data, biometric data, health data, political views, religious beliefs, or trade union membership.

### 7.9 Data Processing Location

Redcentric Cyber Security Professional Services staff are all UK based, and all personal data is stored in UK Data Centres unless otherwise stated.

# 8. Information Assurance

### Certifications

Redcentric are ISO 20000-1 certified, demonstrating that we adhere to ITSM (IT Service Management) best practice, and ITIL (Information Technology Infrastructure Library) provides advice on ITSM best practice.

ITIL v4 is at the heart of Redcentric managed service operation and support. Redcentric believes that to deliver a high quality, professional service it is necessary to invest in training people, empowering them to be strong ambassadors of our service model.

Redcentric has provided managed services to the UK public and private sector for over 30 years. As a highly accredited business, we are proud of the standards and processes for which we are certified.

Our data centres and all supporting operations are fully UK Sovereign and are congruent with;

- The Government's Security Classification Policy ('Official-Sensitive')
- The Government's previous Protected Marking Scheme classification (BIL4 - Confidential)

**Note** – Redcentric can also support information and assets classified above the GSCP level of 'Official-Sensitive'.

### ISO

- ISO 27001:2022 Information Security Certified
- ISO/IEC 27017:2015 Cloud Security Certified
- ISO/IEC 27018:2019 Personally Identifiable Information (PII)
- ISO 9001:2015 Quality Management Certified
- ISO22301:2019 Business Continuity Management
- ISO 14001:2015 Environmental Management System Certified
- ISO 20000-1: 2018 IT Service Management System Certified

### NHS standards

- Registered HSCN CNSP (Health and Social Care Network, Consumer Network Service Provider)
- DSPT (Data Security and Protection Toolkit) assessed as exceeding standards
- NHS Certified Commercial Aggregator
- NHS Business Partner
- Authorised to transmit, process and store Person Identifiable Data (PID)
- NHS England IGSoC Compliant Commercial Third Party (NACS code: YGMAP)
- NHS England accredited Service Provider (Network Access Agreement number: 0740).

### HMG / other standards

- PCI-DSS Compliant for physical hosting and managed firewall services within our data centre locations
- Cyber Essentials Plus Certified
- Data Centres are externally certified to attest they have the necessary physical security measures to process HM Government 'Official-Sensitive' classified data
- Main data centres are certified as Police Assured Secure Facilities
- Full alignment with the Security Policy Framework
- All services are designed, built, implemented and supported using all relevant and appropriate NCSC GPGs, Cabinet Office and NHS England standards

### Networks Connectivity

- The Public Internet via Private or Public IP VPN
- The HSCN Peering Exchange
- PSTN
- PSN (Public Sector Network) certified as one of the few DNSPs (Direct Network Service Provider)
- PSN Gateway Access for both PSN-Assured and PSN-Protected
- JANET (Joint Academic Network)

Further information with regards to the Redcentric assurance and governance framework can be found within the Redcentric customer security pack which consist of the following documents:

- Cloud Security Principles (aligned with the NCSC 14 principles)
- Security Management Plan
- Security Statement
- Accreditations and Mappings (lists all business accreditations and relevant controls and standards utilised for Redcentric G-Cloud services)
- Security Control Framework

Copies are available under NDA upon request

## Head Office

Central House
Beckwith Knowle
Harrogate
HG3 1UG

**T** 0800 983 2522
**E** sayhello@redcentricplc.com
**W** www.redcentricplc.com

redcentric