G-Cloud 15 (RM1557.15) Excelsior Solutions Ltd

End point and device protection

Service Definition

January 2025

1 Introduction

1.1 Document structure

This Service Definition document provides information about the services offered by Excelsior Solutions Limited under the Crown Commercial Service (CCS) G-Cloud 15 Framework. It is intended to support public sector buyers by clearly explaining the scope, functionality, security, pricing approach, and service management arrangements associated with our offerings, and by outlining how buyers can engage with us through the framework.

The document is structured into three core sections:

- **Service description:** Provides an overview of Excelsior Solutions Limited's digital and professional services, including key features, benefits, delivery approach, and assurance measures such as security, data protection, and compliance with relevant standards
- **Operational delivery and framework alignment:** Describes how services are delivered under the G-Cloud 15 framework, including onboarding, service management, change control, service levels, and alignment with G-Cloud contractual and operational requirements
- **Supplier information:** Summarises Excelsior Solutions Limited's organisational background, mission and values, relevant public sector experience, and clear guidance on how buyers can procure our services via the G-Cloud Digital Marketplace

Each section is designed to enable buyers to quickly locate information relevant to their stage of the procurement lifecycle, from initial service evaluation through to contract award and service delivery.

1.2 How to use this document

This document is intended to support public sector buyers throughout the full G-Cloud procurement lifecycle, from early service evaluation through to contract award and ongoing service delivery. It is structured to provide clear, accessible information that enables informed decision-making at each stage of the process.

For initial assessment and early-stage evaluation, Section 2 (Service description) outlines the scope of services offered by Excelsior Solutions Limited, including our delivery approach, methodology, and the key benefits provided. This section is designed to help buyers determine how well our services align with their organisational needs and objectives.

For due diligence and contract preparation, Section 3 (G-Cloud alignment information) provides detailed information on how our services are delivered in accordance with G-Cloud 15 requirements. This includes onboarding arrangements, service management and support processes, service levels, change control mechanisms, and exit procedures.

To support assurance around security, data protection, and regulatory compliance, Section 4 (Security and data governance) describes our information security framework, data handling and protection standards, and business continuity and resilience measures.

For supplier verification and procurement purposes, Section 5 (Supplier information) provides background information on Excelsior Solutions Limited, including relevant experience and accreditations, and explains how buyers can procure our services through the G-Cloud Digital Marketplace.

2 Service description

2.1 About our service

Excelsior Solutions Ltd provides endpoint and device protection software through G-Cloud 15 as a Lot 2a reseller, supported by advisory and consulting services. Our service helps public sector buyers evaluate requirements, understand vendor capabilities, and plan adoption of endpoint security controls across on-premises, hybrid, and cloud environments.

Our consulting support is recommendation-led and focused on governance, assurance, and adoption planning. Customers and/or their appointed delivery partners retain responsibility for all technical implementation, configuration, integration, deployment, and operational administration of the platform(s).

Our service includes:

- Licensing and subscription supply (where applicable)
- Onboarding coordination and vendor engagement support
- Zero Trust endpoint security recommendations and policy guidance
- High-level architecture and design recommendations
- Decision-support artefacts (e.g., options papers, high-level designs, and governance documentation)

Periodic service reviews may be provided to support adoption and value realisation. These reviews are advisory only and do not include hands-on platform administration or technical delivery.

2.2 Delivery framework

Our service supports buyers in adopting endpoint- and device-centric security controls aligned to Zero Trust principles, including identity-aware access, least-privilege enforcement, device protection, and visibility of endpoint posture and threat activity.

Designed to meet public sector expectations around transparency, assurance, value for money, and risk management, Excelsior Solutions Ltd provides a structured approach combining commercial supply and advisory support.

We support customers by:

- Managing licensing and subscriptions (where applicable)
- Coordinating onboarding with original equipment manufacturers (OEMs)
- Providing guidance on reference architectures and deployment options
- Supporting governance, assurance, and adoption planning

We do not perform technical delivery activities, including agent deployment, endpoint configuration, policy implementation, integration with customer systems, SOC tooling integration, or managed service operation. These activities remain the responsibility of the buyer, OEM, and/or a separately contracted implementation partner.

2.3 Service features / benefits

Showcasing the strength of our solutions, clients who procure our vendor software benefit from:

Feature	Benefit
Endpoint Detection and Response (EDR)	Detecting and responding to endpoint threats faster
Extended Detection and Response (XDR)	Reduced risk from compromised credentials and privileged accounts
Cloud access security and Zero Trust enforcement	Secured remote and hybrid working environments
Privileged access security and session monitoring	Improved visibility across devices, users, and cloud services
Strong authentication and hardware-based multi-factor authentication	Automated routine security investigations and responses
Real-time threat detection and alerting	Strengthened compliance and audit readiness
Automated investigation and response	Reduced operational overhead for security teams
Centralised cloud-based management	Improved resilience against ransomware and advanced threats
Policy-based access and device control	Supported Zero Trust security models
Reporting, audit, and compliance support	Enabled consistent security policies across diverse environments

2.4 Service scope

OEM platforms supplied under this service can integrate with existing identity stores, endpoint estates, applications, infrastructure and cloud services.

2.4.1 Add-ons and extensions

Is this service an add-on or extension to other software services?

Yes. This solution integrates with Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Identity and Access Management (IAM), and network security platforms.

What software services is it an extension to?

Our service extends and integrates with existing endpoint, cloud, and security platforms, enabling enhanced endpoint and device protection without replacing customers' current systems. It integrates with, but is not limited to:

- Cloud platforms and services (AWS, Microsoft Azure, Google Cloud Platform)
- Endpoint operating systems and device types (Windows, macOS, Linux, iOS, Android)
- Virtual, server, and workload environments, including cloud-hosted compute
- SaaS and line-of-business applications accessed from managed or unmanaged devices
- Identity providers and directory services (Microsoft Entra ID (Azure AD), Active Directory, LDAP)
- Endpoint agents, APIs, and standard authentication and authorisation protocols

The service integrates with existing security and operations tooling, including:

- Identity and Access Management (IAM) platforms
- Security Information and Event Management (SIEM) systems
- Security Orchestration, Automation and Response (SOAR) platforms
- IT Service Management (ITSM) tools
- Zero Trust-aligned endpoint, identity, and security architectures

This approach enables endpoint-centric security controls, policy enforcement, and continuous visibility to be applied consistently across existing environments, without imposing proprietary hosting models or requiring wholesale replacement of incumbent technologies. By layering Zero Trust-aligned endpoint and device controls over the existing technology stack, public sector organisations can improve protection against malware and ransomware, reduce the risk of credential compromise and lateral movement, and strengthen assurance and compliance while retaining control over their operating models.

2.4.2 Cloud deployment model

Meeting the UK public sector's varying security, operational, and compliance requirements, our network and environment security systems support multiple deployment models. To achieve this, our service can be deployed using Public and Hybrid Cloud models. The selected deployment model will be agreed during onboarding and documented as part of the service design.

The UK service is hosted in the UK. All environments are designed and operated in line with recognised industry best practices and public sector security expectations.

Customer data, including identity information, access logs, audit records, and privileged session data, is stored and processed within the United Kingdom unless otherwise agreed in writing. Complying with UK GDPR and the Data Protection Act 2018, our data residency controls prevent customer data from being transferred outside the UK without explicit approval.

Where Hybrid deployments are used, we apply consistent data residency and security controls across all components of the service.

2.4.3 Service constraints

Excelsior Solutions Ltd provides onboarding coordination and advisory support primarily on a remote basis. We do not provide technical configuration, deployment, integration, or managed service operations. OEMs provide product maintenance and platform updates in line with their published service terms.

2.4.4 System requirements

Administrative and user access to this service is provided through:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Safari

Use of unsupported or end-of-life browser versions may result in reduced functionality or security controls.

The service supports integration with workloads, endpoints, and identity sources running on supported operating systems:

- Windows Server
- Windows Desktop
- Linux distributions
- MacOS
- iOS
- Android
- Cloud platforms
- SaaS services

Where endpoint agents or connectors are required, they must be deployed on supported operating system versions only. End-of-life operating systems are not supported.

For cloud integration, the service requires access to Azure/Amazon Web Services, and appropriate network connectivity to allow secure communication between the service and customer systems. Customers must ensure that required ports, protocols, and firewall rules are permitted in line with the service's technical documentation.

The service integrates with standard identity protocols and interfaces, including:

- SAML 2.0
- OpenID Connect
- OAuth 2.0
- LDAP
- SCIM

The service may require compatible directory services such as:

- Microsoft Entra ID
- Active Directory
- LDAP-based directories

Use of the service requires valid licences for the data security platform itself and, where applicable, licences for any underlying cloud services, operating systems, or third-party software used as part of the deployment. Customers are responsible for maintaining appropriate licences for any third-party software.

No specialist hardware is required to access the service. Where optional components such as connectors, gateways, or session recording services are deployed, we will confirm minimum compute, memory, and storage requirements during onboarding based on the customer's scale and usage requirements.

2.5 Reselling

This service includes third-party cloud software and subscription services delivered by original equipment manufacturers (OEMs). Where applicable, Excelsior Solutions Ltd supplies access to services from Zymperium, Glacier, Netskope, CrowdStrike, CyberArk, and Yubico as part of a G-Cloud 15 Lot 2a reseller offering.

In this context, Excelsior Solutions Ltd acts as a reseller and commercial supplier, providing:

- Licence and subscription procurement
- Order processing, renewals, and subscription management
- Commercial coordination between the buyer and the OEM
- Access to OEM documentation and OEM support routes
- Billing and invoicing for the resold service (where applicable)

To help buyers understand product capabilities, align requirements, and develop adoption recommendations, Excelsior Solutions Ltd also provides advisory and consulting support. This may include high-level architecture guidance, options analysis, and assurance documentation.

Excelsior Solutions Ltd does not provide technical implementation, configuration, integration, platform administration, or managed service operations under this service definition. The OEM remains responsible for platform delivery, availability, maintenance, and product-specific support under their published service terms and service levels.

2.6 User support

Delivering timely, effective assistance throughout the delivery and operation of the service, our support model is clear, accessible and proportionate. Working reliably and transparently, we use defined support channels, response targets and escalation routes, to manage and resolve enquiries in line with agreed timescales.

Reflecting buyers' unique needs, we tailor our support arrangements to the nature and criticality of each project during onboarding. This ensures buyers understand how to access support, what levels of service are available, and how issues are escalated where required. Where appropriate, we will allocate a named point of contact.

2.6.1 Support details

Do you provide email support?

Yes. We commit to respond to priority requests within 1 hour, and standard queries within 4 hours. Vendors may offer this for product-specific support in line with their own service level agreements.

Do you provide online ticketing support?

No, though our vendors may offer this for product-specific support in line with their own service level agreements.

Do you provide phone support?

Yes. We commit to respond to priority calls within 1 hour, and standard queries within 4 hours. Vendors may offer this for product-specific support in line with their own service level agreements.

Do you provide web chat support?

No, though our vendors may offer this for product-specific support in line with their own service level agreements.

Do you provide AI-driven self-service tools (BOT)?

No, though our vendors may offer this for product-specific support in line with their own service level agreements.

When can users get phone support?

Monday-Friday 09:00-17:00, extended hours available by agreement. Our vendors may offer this for product-specific support in line with their own service level agreements.

When can users get web chat support?

We do not offer this. Our vendors may offer this for product-specific support in line with their own service level agreements.

When can users get ticketing support?

We do not offer this. Our vendors may offer this for product-specific support in line with their own service level agreements.

When is each support channel available?

Monday-Friday 09:00-17:00, extended hours available by agreement. Our vendors offer product-specific support in line with their own service level agreements.

How quickly do you respond to questions?

We commit to respond to priority calls within 1 hour, and standard queries within 4 hours. Our vendors will respond in line with their own service level agreements.

Are response times different at weekends?

We do not offer weekend support. Our vendors may offer this for product-specific support in line with their own service level agreements.

What accessibility standards does your online ticketing meet?

Vendor support is aligned to WCAG 2.2 A/AA/AAA principles.

What accessibility standards does your web chat meet?

Vendor support is aligned to WCAG 2.2 A/AA/AAA principles.

Can third-party contractors access support?

Yes.

Describe your support levels

These are dependent on the level of subscription purchased from the original equipment manufacturer.

Do you provide a technical account manager?

Together, the delivery lead, Customer Engagement Manager, and technical specialists ensure that customers have dedicated, accountable oversight, clear reporting, and access to expert advice throughout the programme lifecycle, aligning delivery to objectives, mitigating risk, and improving overall outcomes.

This approach provides a similar level of support to a Technical Account Manager or Cloud Support Engineer, tailored to programme delivery rather than platform operations.

Our vendors offer this for product-specific support in line with their own service level agreements.

2.6.2 Accessibility and usability

What accessibility standards does your service interface meet?

As a product reseller, this does not apply to our service. Where our vendors' solutions include user-facing interfaces, these have been designed following WCAG 2.2 A/AA/AAA principles. This ensures the service is perceivable, operable, understandable and robust for users with a wide range of access needs. Delivering one consistent standard, we select any third-party platforms used as part of the service based on their ability to meet the same or equivalent accessibility standards.

Describe how your service is accessible

Accessible to users with disabilities and those using assistive technologies, our vendors' interfaces support keyboard-only navigation, screen readers, adjustable text size and contrast settings, and clear, consistent layouts. Structured to support ease of navigation, our content is written in plain English, avoiding unnecessary jargon. Where digital interfaces are not suitable, our vendors offer alternative support channels such as telephone to ensure all users can access our service effectively.

Describe any interface testing with assistive technology

Inbuilding accessibility, our vendors consider usability throughout the service lifecycle. To identify and overcome potential barriers, our vendors conduct interface testing. Supporting ongoing service improvement and maintenance, any issues identified are logged, prioritised and addressed in line with original equipment manufacturer service level agreements.

What accessibility standards does your online ticketing/web chat support meet?

Where our vendors' service includes online/web chat support, they have designed these to follow WCAG 2.2 A/AA/AAA principles. This ensures the service is perceivable, operable, understandable and robust for users with a wide range of access needs. Delivering one consistent standard, we select any third-party platforms used as part of the service based on their ability to meet the same or equivalent accessibility standards.

How is your documentation accessible?

Accessible and usable by a wide range of users, our vendors write all documentation in plain English. Preventing confusion or reduced service quality, our vendors use clear headings and logical layouts. Adjusting the service to reflect individual user requirements, vendors provide reasonable adjustments or alternative formats on request.

Documentation formats

Supporting assistive technologies and readability across different devices, vendors provide documentation in HTML, accessible PDF and Microsoft Word.

2.7 How users work with our service

2.7.1 Browsers

To use this service, users will require access to one of the following:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Safari

2.7.2 Desktop application

Yes. Depending on the solution and required functionality, the service may require the installation of lightweight agents, scanners or connectors on applications, workloads or development and runtime environments. These components enable security visibility, policy enforcement and integration with existing platforms.

Administrative and management functions are accessed through web-based management consoles using supported browsers. No standalone desktop client is required for day-to-day administration unless specific use cases or integrations require it.

2.7.3 Mobile

Maximising functionality and convenience, our secure access controls extend to mobile devices and remote users. Access is provided on iOS/Android subject to platform capability.

Ensuring consistent policy enforcement across locations, secure access controls extend to mobile users through:

- Multi-Factor Authentication (MFA)
- Public key authentication (including by TLS client certificate)
- Identity federation with existing provider (for example Google apps)
- Limited access over government network (for example PSN)
- Dedicated link (for example VPN or bonded fibre)

Functionality available on mobile devices may vary depending on platform, device type, or user role.

2.7.4 Service interface

Accessible through the public cloud and Hybrid deployments, our vendors have designed service interfaces to provide secure and intuitive user interaction. The primary interface is accessible through supported browsers on supported operating systems.

Allowing different user roles to access appropriate features and views, original equipment manufacturer interfaces support role-based access control. Offering real-time visibility and policy management capabilities, vendor-software key functions include configuration, monitoring, reporting.

Enabling interoperability within existing IT environments, vendor service interfaces integrate with existing systems and third-party platforms using APIs.

2.7.5 API

Our vendor-provided services expose secure, standards-based APIs that enable users to integrate the end point protection service with existing identity, policy, monitoring, and orchestration platforms.

These APIs and interfaces support integration across hybrid, cloud, and SaaS environments, allowing authorised users and systems to interact with the service in a controlled and auditable manner. Through the available APIs and management interfaces, users can perform a range of administrative and operational functions, including:

- Service onboarding, configuration, and lifecycle management
- Identity, access, and policy enforcement
- User, role, and privileged-access management
- Application-level access controls, including software-defined perimeter and proxy-based access
- Retrieval of monitoring, telemetry, audit, and alerting data
- Integration with SIEM, SOAR, IAM, and IT service management platforms

The APIs also support automation and orchestration, enabling infrastructure-as-code workflows, CI/CD integration, and event-driven responses, subject to appropriate permissions and security controls.

To prevent unauthorised access, original equipment manufacturers protect API interactions using strong authentication, role-based access control, and encrypted communications. Access is restricted to authorised identities and governed centrally in line with customer security policies.

Offering a robust paper trail, vendors provide comprehensive API documentation in PDF formats. Working transparently, vendor documentation includes:

- Endpoint definitions
- Authentication requirements
- Request and response examples
- Error handling guidance to support development and integration activities

Where supported by the original equipment manufacturer, non-production or sandbox environments are available to allow customers to develop, test, and validate integrations without impacting live service data or operations. Access to these environments is typically provided during onboarding or upon request.

All interfaces are designed to support encrypted traffic, least-privilege access, and centralised governance, ensuring secure and consistent operation across customer environments.

2.7.6 Accessibility and usability

Enabling users to manage network and environment security services effectively with minimal training, original equipment manufacturers design their interfaces to be intuitive, consistent, and accessible. Following WCAG 2.2 A/AA/AAA usability and accessibility best practices, vendor design prioritises clear navigation, logical workflows, and consistent layouts to support both technical and non-technical users performing administrative, operational, and reporting tasks.

In-building accessibility considerations, where supported by the underlying platform, our solution supports:

- Keyboard navigation
- Screen readers
- Adjustable text sizing
- Colour contrast
- Labelling
- Form controls to improve readability and reduce cognitive load

Supporting usability and reducing the likelihood of configuration errors, vendor interfaces provide role-based views and permissions. This ensures that users only see and interact with features relevant to their responsibilities.

Helping users to quickly understand system status, identify risks, and take appropriate action, we use dashboards, visual indicators, and reporting views that provide clear visibility of identity, access, and security posture.

Where required, original equipment manufacturers provide training and onboarding support.

2.7.7 Customisation

Offering a high level of configurability, original equipment manufacturer platforms support customers in tailoring the service across network, environment, and security controls. Customisable elements include:

- Network segmentation and access-control policies
- Identity, user, and privileged-access rules
- Encryption and security configuration settings
- Monitoring thresholds, alerts, and telemetry views
- Integrations with external identity, security, and service-management platforms
- Automation and policy-driven workflows

Enabling consistent, repeatable, and auditable configuration aligned to customer governance requirements, configuration activities are performed through secure management consoles, APIs, and infrastructure-as-code tools.

Streamlining configuration changes, the administrative user can complete customisation through the administrative interface. For more complex customisation, such as advanced integrations, custom reporting templates, or workflow automation beyond standard capabilities, vendors will implement these changes in collaboration with the customer to ensure compliance with security policies, governance standards, and operational requirements.

Allowing customers to independently manage day-to-day adjustments while retaining access to expert support for advanced or specialised customisation needs, original equipment manufacturers have designed all customisations to be non-disruptive to ongoing operations.

2.7.8 Service levels and availability (Reseller + Professional Services)

Metric	Target	Measurement and reporting
Excelsior service desk availability (reseller support)	09:00-17:00 UK time, Monday–Friday	Availability confirmed through service contact channels and response logs
Priority 1 request response (commercial/service coordination)	Within 1 hour	Time from request received to first response recorded via email log
Priority 2 request response (commercial/service coordination)	Within 4 hours	Time from request received to first response recorded via email log
Request resolution / fulfilment time	Dependent on request type and OEM response times	Tracked through customer updates and vendor case references
OEM incident escalation (where applicable)	Same business day escalation	Logged and evidenced through OEM case creation and escalation emails
Service review reporting (governance)	Monthly (or as agreed)	Meeting notes and action tracker issued following each review
Licence usage / subscription reporting	Within 5 business days of request	Provided using vendor-provided reporting outputs and commercial records
Outage / vendor notice forwarding	Within 1 business day of OEM notification	Email notice forwarding and service communications log

Delivering predictable service coordination, transparent reporting, and clear escalation routes, Excelsior Solutions Ltd provides defined service levels that are proportionate to our role as a reseller and professional services provider. We do not operate, monitor, configure, or manage customer environments. Technical service availability, platform uptime, patching, and product-level incident resolution are delivered by the original equipment manufacturer (OEM) under their published service terms.

Excelsior provides responsive support for licensing, subscription management, commercial coordination, and governance activities. Where service issues are raised, we log the request, provide an initial response within the agreed target, and coordinate escalation to the OEM support route where required. We support buyers through structured service reviews, action tracking, and programme governance reporting to ensure clear oversight, risk management, and delivery assurance throughout the contract term.

3 G-Cloud alignment information

3.1 Section introduction

Designed for use in public sector environments, we deliver this service using a structured, lifecycle-based delivery model. A key competitive differentiator, our delivery philosophy prioritises secure-by-design implementation, clear accountability, and predictable service outcomes, while remaining flexible enough to adapt to each buyer's operational and security requirements.

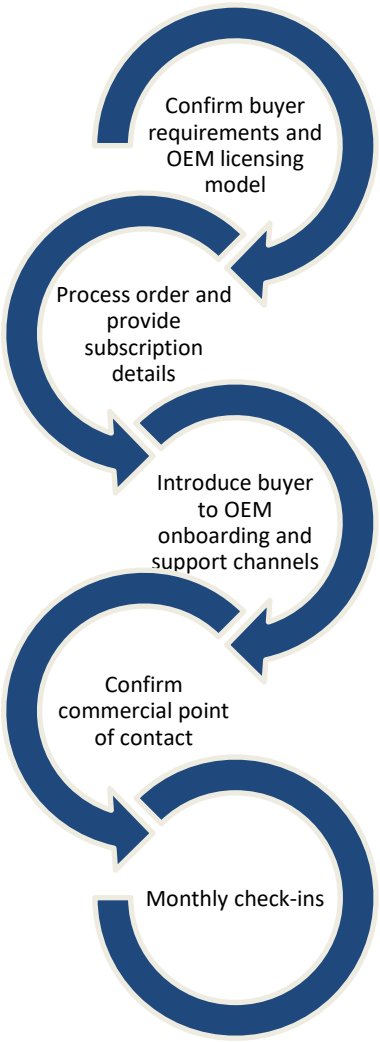
Centred on advisory-led enablement rather than managed service lock-in, we work alongside our customer teams to coordinate onboarding, integrate original equipment manufacturer platforms, manage licensing, and provide architectural and operational guidance. Support, incident management, and service performance are managed through defined SLAs, prioritisation, and escalation processes.

Remaining resilient, compliant, and aligned to evolving public sector security, governance, and operational needs, we maintain our service through ongoing monitoring, monthly (or as required) service reviews, and continuous improvement activities.

3.2 Onboarding and offboarding processes

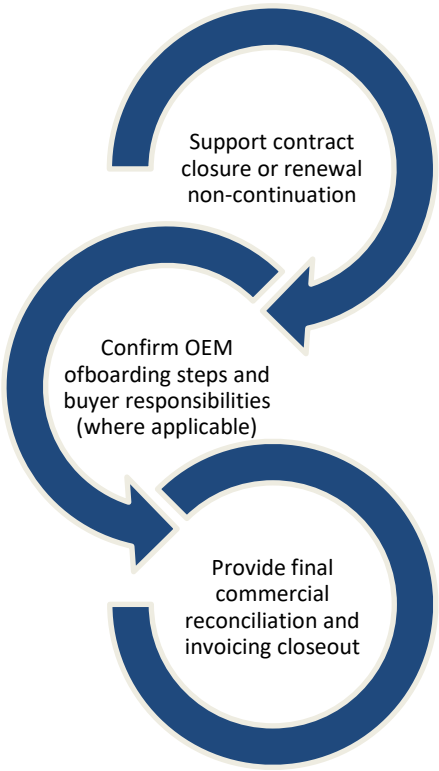
3.2.1 Onboarding

Completed within 24 hours of purchase, our structured onboarding process is outlined below:



3.2.2 Offboarding

Supporting a straightforward and secure exit process, our offboarding processes ensure users can leave the service at the end of the contract term or upon termination, without vendor lock-in or hidden costs.



3.3 Data

3.3.1 Data importing and exporting

Making both importing and exporting data straightforward, flexible, and secure, our vendors' tried-and-tested procedures allow users full control over their information.

Data importing and exporting

Data importing and exporting for the security platforms supported through this reseller service are provided by the original equipment manufacturers (OEMs). OEM solutions are designed to make data transfer straightforward, flexible and secure, while ensuring customers retain full control over their operational and security data.

OEM platforms allow customers to import data using a range of supported and documented formats. Data can be uploaded using OEM-provided interfaces, tools or APIs to support efficient onboarding and migration from existing systems.

During import, OEM systems perform validation and integrity checks to ensure data accuracy, consistency and compliance with required schemas. OEMs provide templates, documentation and automation options to support the import of large or complex datasets.

Customers can export their data from OEM platforms at any time using open, non-proprietary formats where supported. Additional export formats may be made available by the OEM on request.

Exports may be completed on an ad-hoc or scheduled basis through OEM service portals or API-based automation tools. At the end of a contract, OEMs provide all customer operational data in a mutually agreed format to support service exit or transition.

Excelsior Solutions does not host, access, store or process customer production environments, security logs, network telemetry, identity data, privileged session information, or other operational security data. Technical service delivery, platform operation, hosting and data processing for these datasets are performed by the OEMs under their own service terms.

Open formats and lock-in

OEM platforms prioritise open and widely supported data formats to support interoperability and minimise vendor lock-in. Where proprietary formats are used internally, OEMs provide documentation and conversion options to enable customers to migrate their data to alternative platforms or services.

Security and compliance

All operational data transfers performed by OEM platforms are encrypted in transit and at rest, and OEMs maintain audit logs to support security monitoring and compliance requirements.

Excelsior Solutions Limited is headquartered in the United States and hosts limited customer business contact information required to deliver the reseller service. This may include names, business email addresses, job titles, organisation details, postal addresses, order references and licensing information. Excelsior does not store or process customer operational, identity, access or security telemetry data.

3.3.2 Analytics

Excelsior Solutions Ltd provides analytics and reporting to support service governance, commercial oversight, and programme delivery assurance. As a reseller, we do not operate the underlying software platforms, generate technical security telemetry, or access customer operational security data (for example logs, alerts, endpoint events, or network traffic). Product-level analytics, dashboards, and technical reporting are provided directly by the original equipment manufacturer (OEM) platforms within the buyer's tenancy and subject to OEM capabilities.

Where requested, Excelsior supports buyers by consolidating and summarising OEM-provided outputs into non-technical governance reporting. This may include licence utilisation summaries, subscription and renewal timelines, support case trends, RAID logs, delivery milestones, and agreed KPIs. Reporting is provided monthly or on request and is used to track progress, manage risks and dependencies, and support stakeholder communication throughout the contract term.

3.3.3 Data-in-transit protection

Excelsior Solutions does not store or process customer operational data. Data exchanged between customer environments and supported platforms is protected by original equipment manufacturer (OEM) services designed around a Zero Trust, encryption-first security architecture.

Connectivity between the customer environment and OEM platforms is established using identity-bound, session-based access controls rather than flat or persistent network trust models. This removes inbound network exposure and ensures access is granted only for the specific user, device, application and duration required.

OEM platforms protect data in transit using strong, industry-standard encryption protocols, including TLS 1.2 and TLS 1.3 or IPsec, both between the customer network and the platform and within OEM-managed environments. Network security controls such as stateful firewalls, segmentation and traffic inspection are used to restrict, monitor and protect communications between services. Internal service-to-service communications are similarly encrypted to prevent unauthorised interception or access.
Access to platforms and management interfaces is governed by multi-factor authentication (MFA), role-based and attribute-based access controls (RBAC/ABAC), and, where supported, device posture and contextual access checks to enforce least-privilege access.

Customer data within OEM platforms remains encrypted, logically isolated and under customer ownership at all times. Where supported by the OEM, data is protected by secure, encrypted cloud backup and recovery mechanisms to support resilience and service continuity.

3.3.4 Asset protection

Our service provides robust protection for user data at rest and ensures that physical and digital assets are managed securely throughout their lifecycle.

User data is stored and processed in the UK. Vendor data centres comply with industry-recognised standards, including ISO 27001, and provide physical and logical security controls including:

- Controlled access
- CCTV monitoring
- Redundant power and cooling
- Continuous environmental monitoring

All user data at rest is encrypted with keys managing securely according to best practices. Access is restricted to authorised personnel, and activity is monitored and logged for auditing and compliance purposes.

When data is no longer required, vendors follow securely erase and sanitise storage media, ensuring that information cannot be recovered.

Whilst hardware is not required for this service, we dispose of decommissioned equipment in line with regulatory and environmental requirements. Physical drives and other sensitive components are destroyed or wiped using approved methods before recycling or disposal.

3.4 Availability and resilience

3.4.1 Guaranteed availability

Our dedicated advisory support is available Monday to Friday from 09:00 to 17:00. While we do not operate or host customer systems, our guaranteed availability ensures that organisations have expert guidance whenever it is needed. This support helps customers make informed decisions, optimise configurations, and respond quickly to operational questions.

By providing reliable and accessible advisory services, we help organisations maximise the availability and resilience of their own systems. Our guidance ensures secure and effective configuration of network and access controls, supports integration across hybrid and multi-cloud environments, and enables customers to address issues promptly, reducing the risk of downtime. Where platform-specific issues arise, vendor support teams facilitate timely resolution in line with their own SLAs, providing customers confidence that their systems remain stable and continuously available.

3.5 Governance

Delivering consistency, accountability, and compliance with recognised industry standards, Babatunde Ademiju, CEO, oversees our integrated management system, aligned to:

- ISO 27001
- ISO 9001
- ITIL

Working at the forefront of industry best practice, we will continuously hold the Cyber Essentials accreditation throughout the framework lifetime.

Babatunde reviews our governance policies and procedures annually to ensure that our controls remain effective and compliant.

To verify our adherence to standards, regulations, and contractual obligations, we conduct internal audits. Working transparently, we address audit outcomes through corrective actions. Where process changes are required, our teams apply ITIL-based service management principles to manage incidents, changes, and continual improvement. For consistent delivery and accountability, we clearly define roles, responsibilities, and escalation paths.

3.6 Security

Maintaining accountability and clear decision-making, we maintain comprehensive information security policies covering data protection, access control, incident management, and operational security. All policies are centrally controlled, enforced, and regularly reviewed to ensure ongoing compliance with ISO 27001, NIST CSF, ITIL security management practices, and our Software Security Code of Practice.

All controls and processes are subject to regular internal and external audits in line with:

- Zero Trust Architecture principles
- NIST Cybersecurity Framework alignment
- ISO/IEC 27001-aligned controls
- ITIL v4-aligned service management
- Agile onboarding and enablement practices

3.6.1 Operational security

Embedding security into all operational processes, we embed security considerations through a formal ITIL-aligned change management process. This ensures that modifications are assessed for risk, proved, tested, and implemented in a controlled manner to maintain service stability and security.

Our internal operational security controls (completed by Microsoft, our contracted delivery partner) include:

- Continuous identification and assessment of vulnerabilities across software, infrastructure, and integrated components
- Timely application of patches and updates based on severity, exploitability, and risk
- Secure configuration and lifecycle management of service components
- Ongoing monitoring of networks, applications, and endpoints to detect anomalies, security events, or suspicious activity

Access to Excelsior systems and data is strictly controlled through unique user identities, multi-factor authentication (MFA), and least-privilege access principles. Policies define acceptable use of corporate devices, cloud services, and remote access mechanisms to maintain secure operations.

Security incidents are logged, assessed, and managed according to defined incident-response procedures. Containment, remediation, and recovery actions are applied proportionally, and lessons learned from incidents and near-misses are reviewed and incorporated into internal processes to drive continuous improvement.

Where applicable, internal systems are designed to support evolving security standards, including modern encryption practices, to protect sensitive information throughout its lifecycle and maintain organisational resilience.

3.6.2 Staff security

We maintain robust staff security procedures to ensure that all personnel with access to our systems and customer data are properly vetted, authorised, and continuously monitored. Access is granted strictly on a need-to-know basis, and only employees who meet our security requirements are permitted to interact with production systems or sensitive data.

All staff undergo background checks prior to access being granted. To ensure suitability for working in secure environments, our screening process includes verifying:

- Identity
- Employment history
- Criminal record checks

To maintain staff competency and security, we control access to strict role-based permissions and duties.

3.7 Auditing

Supporting governance, compliance, and operational oversight, we follow Cyber Essential best practice for auditing and logging processes. Key activities performed on internal systems are logged to provide a record of user actions and administrative changes.

Access to internal audit logs is restricted to authorised personnel, and logs are stored securely to prevent unauthorised access or tampering. Logs are reviewed periodically to support operational monitoring and identify any unusual or suspicious activity.

Audit records are retained for a defined period in accordance with internal policy and Cyber Essentials guidance, ensuring they are available for compliance, accountability, and operational review purposes.

3.7.1 Compliance and quality management

Operating under a structured compliance and quality management framework, we align our service delivery to the best practice standards set by:

- ISO 27001
- ISO 9001
- ITIL
- Cyber Essentials

Babatunde Ademiju, CEO, oversees all aspects of the service using clearly defined processes, roles, and responsibilities. To verify that our processes, controls, and operations meet both regulatory and contractual requirements, we complete external audits for independent review. Demonstrating our compliance, we address findings through structured corrective actions.

3.8 Backup, restore & disaster recovery

To identify potential threats and evaluate their impact on operations, we use our annually updated Business Continuity and Disaster Recovery framework to activate recovery protocols, coordinates communications, and oversees restoration.

Aligned to ISO 27001, our approach focuses on protecting critical business information, such as customer contact details, licensing information, and internal documentation.

All internal data is backed up to the Microsoft Cloud, using Microsoft-managed services. Backups are performed incrementally on a daily basis, automatically encrypted both in transit and at rest, and managed entirely by Microsoft as part of their secure, certified cloud environment. This ensures that internal business data is consistently protected without manual intervention and adheres to strong encryption and access controls.

Recovery procedures are tested periodically to confirm that critical data can be restored reliably and efficiently. In the event of a disruption, our internal processes ensure that essential business information can be recovered quickly, supporting continuity of advisory services to customers.

Key principles of our backup and recovery processes include:

- Daily incremental backups to capture changes to internal business data.
- Automatic encryption of all backup data, ensuring confidentiality and integrity.
- Microsoft-managed storage and replication, providing secure, geographically resilient storage.
- Periodic restoration testing to verify recoverability and readiness.
- Post-event review of any incidents or recovery exercises to identify improvements and incorporate lessons learned into internal processes.

These internal measures ensure that we can continue to provide advisory support reliably, maintain operational continuity, and protect critical business information even in the event of system or service disruption.

3.9 Training

Ensuring users are confident, capable, and able to realise full value from our solution, original equipment manufacturers deliver training and knowledge transfer as a core component of the service. Supporting effective adoption, long-term usability, and operational continuity, training reflects the user's environment, role, and operational context. Providing training that is relevant to their responsibilities and level of service interaction, programmes support different audiences, including end users, administrators, and support teams.

Allowing users to choose delivery methods that best suit their workforce, schedules, and learning preferences, original equipment manufacturers deliver training through a range of formats, including instructor-led sessions, virtual workshops, and self-paced learning materials.

In addition to direct user training, vendors support knowledge transfer through train-the-trainer approaches and administrative enablement, allowing customers to build internal capability and reduce reliance on external support. This ensures sustainability beyond initial implementation.

Vendors reinforce training with supporting documentation such as user guides, configuration notes, and quick-reference materials. Vendors provide materials in accessible digital formats and update these as the service evolves.

To refine content and improve user engagement, vendors review training feedback through feedback, completion tracking, and post-training evaluation.

3.10 Service pricing

We price our service transparently under the G-Cloud framework, with full pricing details published in the separate Pricing Document. Pricing is structured to provide flexibility and alignment with public sector procurement and budgetary requirements.

Professional services are charged on an hourly basis, with rates determined by the service type and skill level required, in accordance with our SFIA-aligned rate card. Where appropriate, discounted rates may be offered for bundled services or longer-term engagements.

Pricing for cyber security products is dependent on the selected vendor, solution scope, and customer requirements. We work closely with original equipment manufacturers, distributors, system integrators, and customers to structure pricing in a way that aligns with public sector procurement models. This includes mapping OEM Stock Keeping Units (SKUs) to government Contract Line-Item Numbers (CLINs) and bundling products where required. In some cases, costs can be profiled across the contract term to align with government budget cycles.

All pricing is tailored to customer needs and confirmed during contract negotiations and onboarding. We offer free trials and discounts for educational organisations as detailed in the Pricing Document.

3.11 Invoicing process

We issue invoices monthly in arrears, providing clear visibility of charges incurred during the billing period:

- **Payment terms:** 30 days, in line with standard UK government payment requirements
- **Billing method:** Invoices are issued against an agreed purchase order
- **Accepted payment methods:** BACS and other standard government payment mechanisms

3.12 Termination terms

Contracts may be terminated at the end of their natural term or earlier in accordance with standard contractual provisions:

- **Minimum contract term:** None, unless otherwise specified in the Order Form
- **Standard termination notice period:** One month
- **Early termination:** Material breach provisions apply, in line with G-Cloud Call-Off Terms

On termination, we conclude services in an orderly manner, and invoice any outstanding charges incurred up to the termination date in accordance with the agreed pricing and invoicing terms.

4 Security and data governance

4.1 Data protection and encryption

We do not host, access, store, or process customer production environments, security logs, network telemetry, identity data, or privileged session information. Technical service delivery, platform operation, hosting, and data processing are provided directly by the original equipment manufacturer (OEM) under their own service terms and security controls.

Where limited customer information is required to deliver the reseller service (such as named contacts, business email addresses, order references, licensing details, and support case identifiers), we process this data securely and solely for the purposes of licensing administration, contract management, and support coordination. Access to this information is restricted to authorised personnel using role-based access controls, least-privilege principles, and multi-factor authentication.

All customer data handled by Excelsior Solutions Limited is protected using encryption in transit and at rest. Data in transit is secured using TLS version 1.2 or higher, and stored data is encrypted using industry-standard algorithms such as AES-256 or equivalent protections provided by the underlying hosting platform. Network access to reseller systems is protected by firewalls and secure gateways enforcing traffic filtering, protocol validation, and access control policies.

Our internal environments are designed to minimise attack surface and reduce the risk of unauthorised access through network segmentation, secure access mechanisms, and continuous monitoring. Security events related to access and data handling are logged and reviewed as part of ongoing security operations. Any transfers of personal data are managed in accordance with UK GDPR and the Data Protection Act 2018. Where applicable, we use appropriate contractual safeguards, including the UK International Data Transfer Agreement (IDTA) or the UK Addendum to Standard Contractual Clauses. Customer data is retained only for as long as necessary to meet contractual, legal, and audit obligations and is securely deleted when no longer required.

Ensuring continued alignment with government policy and industry best practice, we review and update our security and encryption practices annually in line with evolving standards and regulatory requirements.

4.2 Data at rest, storage locations, and physical security

Storing, processing and protecting data in secure, UK-located environments, this service does not require data to be transferred or processed outside these locations unless explicitly agreed with the buyer.

Where supported by the underlying hosting platform, users may specify or agree the geographic location in which their data is stored and processed to meet data-sovereignty, regulatory, or organisational requirements.

The service operates from professionally managed data centres that meet internationally recognised security and resilience standards. These facilities are certified to standards such as:

- ISO/IEC 27001 for information security management
- SOC 2 Type II / ISAE 3402 / SSAE-18, where applicable
- Alignment with recognised cloud security frameworks such as CSA Cloud Controls Matrix (CCM)

These certifications provide independent assurance that security, availability, and operational controls are in place and subject to regular external audit.

All user data stored within the service is protected using strong encryption at rest, typically employing AES-256 or equivalent encryption mechanisms provided by the hosting platform or application layer. Original equipment manufacturers apply encryption consistently across structured and unstructured data, including databases, file storage, backups, and audit logs.

Additional data-at-rest protection measures include:

- Secure key management services with restricted access
- Logical separation of customer data in multi-tenant environments
- Controlled access to storage systems based on least-privilege principles
- Continuous monitoring and logging of access to stored data

Physical access to data-centre facilities is tightly controlled by the hosting provider and restricted to authorised personnel only. Physical security measures typically include:

- 24/7/365 on-site security personnel
- CCTV monitoring and recording
- Multi-factor physical access controls, such as key cards and biometrics
- Secure perimeters, mantraps, and monitored entry points
- Environmental controls to protect against fire, flooding, and power disruption

These controls ensure that infrastructure hosting user data is protected against unauthorised physical access, tampering, or theft.

4.3 Data sanitisation and disposal

As our reseller service is designed to avoid access to or storage of customer operational or production data, Excelsior Solutions Limited does not hold customer application data, system data, or service-generated content. Technical service delivery, hosting, and data processing are performed by the original equipment manufacturer (OEM) under their own data sanitisation and disposal controls.

Where we process limited customer information, we operate a defined and auditable processes. We securely delete customer data and safely dispose of equipment to ensure that data is permanently removed and cannot be recovered at the end of its lifecycle or following contract termination. These processes are aligned with recognised industry standards and UK government guidance.

Securely and irreversibly removing customer data, the formal data sanitisation process uses cryptographic erase methods where encryption is in use. This involves securely destructing encryption keys, rendering the underlying data permanently unreadable. Cryptographic erasure is aligned with National Cyber Security Centre guidance and is the primary method used for cloud-based and encrypted storage environments.

Where cryptographic erase is not applicable, alternative approved methods may include:

- Secure overwrite (secure erase) using industry-recognised techniques
- Physical destruction of storage media where required
- Degaussing, where appropriate for the media type

The sanitisation method selected is appropriate to the storage technology and risk profile and ensures that data cannot be reconstructed or retrieved.

Our service does not require customer-owned hardware. Any Excelsior Solutions Limited equipment that is decommissioned or reaches end of life is disposed of through controlled and auditable processes, either in accordance with recognised industry standards by the hosting provider or via approved third-party IT asset disposal partners. Third-party providers are selected based on compliance with recognised standards such as ISO 27001 and ISO 14001.

4.4 Information security management and certifications

Professionally managing and independently validating governance, risk management, and operational controls, our services comply with the best practice standards set by:

- ISO 27001
- ISO 20000-1
- ISO 9001
- Cyber Essentials

These certifications provide independent, third-party assurance that organisational policies, processes, and controls are effective, consistently applied, and regularly reviewed.

Maintained through a formal programme of annual audits and surveillance assessments by accredited bodies, Babatunde Ademiju, CEO, oversees all aspects of our information security management, risk assessment, and compliance.

4.5 Identity and access management

Allowing only authorised users to access our systems, we implement robust identity and access management (IAM) controls and tightly control privileged accounts. We restrict access to our systems to authorised personnel only and protect this using role-based access controls aligned to job function and responsibility. Privileged and administrative access is tightly controlled, segregated, and granted only where required to perform specific operational tasks.

Our operating model limits access to the minimum necessary and avoids access to customer production environments and underlying platforms, which are operated by the original equipment manufacturer (OEM).

All administrative and privileged accounts are protected using multi-factor authentication (MFA). Password policies, session controls, and account lockout mechanisms are enforced to reduce the risk of unauthorised access. Access rights are reviewed on a regular basis, and changes are logged for audit purposes. Access is promptly revoked when personnel no longer require it, including following role changes or staff departures.

Excelsior Solutions Limited does not manage user access to customer production systems or hosted service platforms. Authentication, authorisation, and access to the service itself are provided by the OEM under their own identity and access management controls. OEM platforms typically support secure authentication mechanisms, including Single Sign-On (SSO) and industry-standard protocols such as SAML 2.0 and OAuth 2.0, with multi-factor authentication applied to administrative and privileged accounts.

5 Supplier information

5.1 About us

Bringing 25 years' experience, we are a Woman-Owned Small Business team of 5 delivering application and workload services globally. Adding value to original equipment manufacturer software, we specialise in:

- Public sector expertise
- Security-first delivery
- Vendor-neutral advice
- Deep cloud and DevSocOps expertise

Our experience spans across government, local authorities, healthcare, education and critical infrastructure, where we have successfully delivered major enterprise-wide technology contracts to:

- VillageCareMax (VCM)
- U.S. Department of Veterans Affairs

Committed to professional governance, security, and industry-leading quality, our service is aligned to:

- ISO 27001
- ISO 20000-1
- ISO 9001

Working at the forefront of industry best practice, we will continuously hold the Cyber Essentials accreditation throughout the framework lifetime.

Our solutions are designed to meet rigorous public-sector standards and align with NIST, ITIL, and NHS Digital guidance as applicable.

Our mission is to empower organisations to thrive through secure, innovative, and tailored technology solutions and we achieve this by combining innovation, technical expertise, and a service-focused mindset. This commitment ensures that our clients receive tailored solutions, responsive support, and measurable outcomes that advance their strategic objectives.

5.2 How to buy

Excelsior Solutions Limited's services are available for direct purchase through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace.

Buyers can locate Excelsior Solutions Limited on the Digital Marketplace and select the appropriate service listing.

Following selection, the buyer and Excelsior Solutions Limited will:

1. Agree a Statement of Work (SoW) outlining the scope, deliverables, timelines, and pricing
2. Establish a Call-Off Contract in accordance with G-Cloud framework terms
3. Issue a Purchase Order (PO) to confirm commencement of services

All engagements are conducted in full compliance with public-sector procurement regulations and the conditions of the G-Cloud framework, ensuring transparency and governance throughout.

For enquiries or pre-contract discussions, please contact us via our central point of contact:

- Phone: 240-478-233
- Email: info@excelsortech.com