Service Definition Document

iSaaS Systems Security Services

Rosebud Cloud Solutions
G-Cloud 15 – Lot 2a: Infrastructure Software as a Service (iSaaS)

1. Overview

Rosebud Cloud Solutions' *iSaaS Systems Security Services* deliver cloud-native protection across applications, endpoints, identities, and networks. The service includes privileged access controls, identity and access management, endpoint security, network segmentation, trusted access enforcement, and active threat detection. Integrated analytics and governance tooling support risk management, compliance, and secure operations across public sector environments.

2. Service Summary

Service Name

iSaaS Systems Security Services

Service Type

Lot 2a – Infrastructure Software as a Service (iSaaS)

Service Description

Rosebud's Security service delivers cloud-native protection across applications, endpoints, and networks. It includes identity and access management, privilege controls, active threat detection, and trusted network access. Integrated analytics and governance tools support risk management and compliance, ensuring secure, scalable infrastructure tailored to public sector environments and operational needs.

Service Categories

- Security
- Cloud-Native Application Protection Platform
- Identity and Access Management
- Privileged Access
- Endpoint Security
- Network Security

- Trusted Network Access and Protection
- Active Application Security
- Security Analytics
- Governance, Risk, and Compliance

Multi-Cloud Support

Yes – supports public, private, and hybrid cloud deployments.

3. Service Features and Benefits

3.1 Features

- Privileged access control
- Cloud-native application protection platform
- Identity and access management tools
- Endpoint security configuration
- Network segmentation and firewall policies
- Trusted network access enforcement
- Active threat detection and response
- Security analytics and reporting
- Governance, risk, and compliance tooling
- Role-based policy automation

3.2 Benefits

- Enhanced protection across cloud and hybrid environments
- Reduced risk of unauthorised access
- Improved visibility into user activity
- Faster threat detection and response
- Simplified compliance tracking
- Scalable security for growing infrastructure
- Lower operational security overhead
- Stronger endpoint and data protection

- Automated enforcement of security policies
- Confidence in public sector governance alignment

4. Service Scope

4.1 Included

- Identity and access management configuration
- Privileged access and policy enforcement
- Endpoint and network security tooling
- Threat detection and response capabilities
- Security analytics and reporting
- Governance, risk, and compliance support
- Trusted network access configuration
- Standard onboarding and documentation

4.2 Not Included

- Custom development or bespoke integrations
- Third-party licensing costs
- Onsite support (available at extra cost)
- Extended support packages (quoted separately)

5. Service Constraints

- Relies on Microsoft Azure infrastructure and SLAs.
- Service is not ISO/IEC 27001 certified.
- Buyers must configure identity, access, and policy settings correctly.
- Security analytics depend on buyer-enabled telemetry and logging.
- Some advanced features or integrations may require additional scoping or licensing.
- Onsite training and support for unmanaged environments may incur extra cost.
- Data residency must be configured by the buyer.
- Buyer-led changes outside agreed parameters may affect service integrity.

- All constraints are reviewed and documented during onboarding.

6. System Requirements

- Role-based access control configured
- Endpoint agents installed and updated
- Network segmentation and firewall rules defined
- Logging and telemetry enabled
- API access for integration
- Stable internet connection and bandwidth

7. Reselling Information

Supplier Type

Reseller providing additional features and support not available from the original supplier.

Original Supplier

Microsoft

8. User Support

8.1 Support Channels

- Email or online ticketing: **Yes, at extra cost**
- Phone support: **No**
- Web chat support: **No**
- Onsite support: **Yes, at extra cost**

8.2 Support Response Times

- 1-hour initial response
- 2-day fix target
- 12-hour weekend response time (unless otherwise agreed)

8.3 Support Levels

- Standard support level (cost provided at discovery/quote stage)
- Dedicated technical account manager (qualified cloud engineer)

8.4 Support for Third Parties

Yes – support available to authorised third-party partners or managed service providers.

8.5 Accessibility

Compliant with EN 301 549.

9. How Users Access the Service

- Web browser interface: **No**
- Application installation: **No**
- Mobile-optimised interface: **No**
- Service interface: **No**
- API availability: **No**
- Customisation: **No**

10. Pricing

Pricing is provided during discovery and quotation, based on:

- Security tooling and capabilities required
- Number of systems and environments in scope
- Required support levels
- Optional onsite or extended support services

11. Onboarding and Offboarding

11.1 Onboarding

- Requirements and environment assessment
- Access and permissions setup
- Identity, endpoint, and network security configuration
- Threat detection and analytics setup
- Governance and reporting structure definition

11.2 Offboarding

- Removal of access permissions

- Export of logs, configurations, and monitoring data (where applicable)
- Decommissioning of service components
- Optional transition to Managed Cloud Support Services

12. Security and Compliance

- Delivered using secure, approved cloud environments
- Supports governance, risk management, and compliance frameworks
- Reinforces secure-by-design principles
- Data residency aligned with buyer-selected Azure regions

13. Service Management

Rosebud provides ITIL-aligned service management, including:

- Incident management
- Change management
- Problem management
- Capacity and performance monitoring
- Governance reporting

14. Technical Roadmap

Rosebud continues to enhance the service through:

- Expanded threat detection and analytics capabilities
- Enhanced automation for identity and access management
- Additional hybrid cloud security integrations
- Improved reporting and compliance tooling