VE3 – Standard Service Definition G-Cloud 15 RM1557.15

1. Overview of Approach

VE3 delivers secure, scalable, cloud-based services aligned to the NIST Cloud Computing model, enabling Buyers to consume Infrastructure, Software, Platform, and Cloud Support Services on a fully managed, PAYG or subscription basis. Our approach focuses on reliability, scalability, automation, accessibility, and compliance with UK Government policies—including Technology Code of Practice, Cloud First Policy, Greening Government ICT, and all mandatory standards defined in Framework Schedule 1.

We combine AI-enabled operations, DevSecOps pipelines, automated monitoring, and a Shared Responsibility Model to ensure performance, resilience, and continuous service improvement. Our services operate through an accessible Supplier Portal that meets WCAG 2.2 AA guidance and is continuously improved in line with GOV.UK accessibility guidance.

2. Service Description

VE3 provides cloud-based services in accordance with the Lot specifications and Full Taxonomy of Services outlined in Framework Schedule 1. Our Service Catalogue supports:

a. Incident Reporting & Management

- 24×7 automated monitoring and logging
- Incident reporting via email (prime@ve3.global), web portal, or API
- Unique ticket IDs, status tracking, and Buyer notification workflows
- Classification by impact and urgency to match agreed SLTs

b. Service Level Targets (SLTs)

- SLTs aligned to severity levels (Critical, High, Medium, Low)
- Response, update, and resolution commitments
- Support for FOCUS (FinOps) reporting where applicable
- Service availability reporting via dashboards and monthly MI

c. Escalation Process

- Level 1 – VE3 Support Team
- Level 2 – Named VE3 Account Manager (Buyer's single point of contact per Schedule 1)
- Level 3 – VE3 Service Director

d. Shared Responsibility Model

VE3 adopts a model aligned with NCSC cloud security guidance. Responsibilities are clearly allocated for:
- Infrastructure security and resilience
- Data protection and access control
- Backup and recovery

- Log retention
- Vulnerability and patch management
- Buyer configuration responsibilities

3. Scope of Service Support and Exclusions

Hours of Support

- Standard support: 09:00–17:00, Monday–Friday (UK time)
- Extended/24×7 support available via optional enhanced SLAs on request
- Marketplace-based services (Lot 1a) follow the underlying provider's SLA where applicable

Out-of-Hours Support

- Priority incidents (Critical) supported 24×7 by default
- Escalation coverage maintained for all production services

Service Exclusions (Framework-mandated)

VE3 will not provide through G-Cloud:
- Hardware procurement not linked to IaaS/PaaS services
- Co-location services
- Contingent labour / IR35 resources
- Bespoke development for Lot 3 (Cloud Support Only)
- Any service outside the NIST cloud definition

4. Responsibilities

4a. Customer Responsibilities

- Provide accurate incident information (impact, system, logs, screenshots)
- Maintain list of authorised Buyer contacts
- Perform basic preliminary checks (as per VE3 guidance)
- Ensure user-level configuration within their responsibility scope
- Confirm closure of incidents on resolution
- Manage internal policies for user behaviour, access, and data governance

4b. VE3 Responsibilities

- Provide a named Supplier Framework Manager and a Contract Manager
- Maintain a secure, accessible Supplier Portal
- Ensure availability of support channels (email, portal, API)

• Provide timely MI, KPIs, FPMs and FOCUS reports
• Deliver services in accordance with NIST cloud characteristics
• Provide onboarding/offboarding processes and Exit Plans
• Maintain all mandatory certifications (Cyber Essentials Plus, ISO 27001, ISO 9001, ISO 14001, ISO 20000-1)
• Maintain carbon reduction plans aligned to PPN 06/21

---

5. Problem Reporting and Incident Management

Incidents must be reported via prime@ve3.global, where they are automatically logged in the VE3 Service Desk with a unique ticket reference.

Process includes:

1. Ticket creation & confirmation
2. Initial triage and severity assignment
3. Root cause diagnostics
4. Fix, workaround, or escalation
5. Resolution confirmation
6. RCA report (for Sev 1/Sev 2 incidents)

Impact assessment follows G-Cloud-compliant thresholds:
• Critical – Total service loss
• High – Major degradation
• Medium – Partial loss
• Low – Minor/non-urgent issue

---

6. Incident Logging Requirements

To accelerate triage, VE3 requires:
• Time and date of issue
• Affected system/service ID
• Error codes/log snippets
• Screenshots
• Description of last known good state
• Steps to reproduce

VE3 stores this information securely and in line with data minimisation principles. No personal data is required or processed unless explicitly required under a Call-Off Contract.

---

7. Service Levels

Indicative SLTs (customisable per Call-Off)

Priority	Response	Update Frequency	Target Resolution
Critical	30 mins	Hourly	4 hours
High	1 hour	2 hours	1 business day
Medium	4 hours	1/day	3 business days
Low	1 business day	2/day	5 business days

Availability: 99.9%–99.99% depending on service type and SLA tier.

---

8. Escalation Process

Level 1: VE3 Support Team

Email: support@ve3.global
Include:
• Ticket ID
• Summary of issue
• Reason for escalation

Level 2: Named Account Manager

If Level 1 is unsatisfactory, escalations go to VE3's designated Contract Manager with authority to adjust resources and priorities.

Level 3: VE3 Service Director

For unresolved or high-impact cases (service outage, prolonged degradation).

---

9. Complaints Procedure

Step 1 – Contact Account Executive

Issues should first be raised with VE3's Account Executive for quick resolution.

Step 2 – Formal Complaint

Email: clientservice@ve3.global
Include:
• Full description of issue
• Steps taken so far
• Expected vs delivered service
• Any supporting documents

VE3 acknowledges all complaints within 2 working days and provides a final response within 10 working days.

10. Exit Management (Framework-compliant)

In line with Framework Schedule 1 requirements :

• VE3 provides a full Exit Plan within 3 months of Call-Off start.
• Minimum 90-day post-termination data access, unless otherwise defined.
• Buyer support for data migration, environment teardown, and knowledge transfer.
• Clear articulation of shared responsibilities during exit.
• If overspend triggers termination conditions (Lots 1a/1b), VE3 maintains access for the minimum required period.

---

11. Security & Compliance

VE3 complies with all mandatory standards for Lots 1a, 2a, 2b & 3, including:
• Cyber Essentials Plus
• ISO 27001
• ISO 20000-1
• ISO 9001
• ISO 14001
• Quantum-safe migration commitments (Lot 1a)
• NCSC Cloud Security Principles
• Government Security Classification guidance
• Sustainable technology strategy
• Accessibility (WCAG 2.2 AA)

No personal data is processed unless explicitly defined in a Buyer Call-Off.

12. Contact Information

T: +44 (0)20 4552 0840
E: prime@ve3.global
W: https://www.ve3.global