

CIRRO

Virtual Desktop Infrastructure



Virtual Desktop Infrastructure (VDI) Service Description 3
Service Scope 3
Security & Access Management 3
Availability & Resilience 3
Service Management & Support 4
Exit & Data Handling 4

Virtual Desktop Infrastructure (VDI) Service Description

The Virtual Desktop Infrastructure (VDI) service provides centrally hosted, securely managed virtual desktops that are delivered to end users over a network as a managed service. The service enables users to access a consistent desktop environment from approved devices and locations, while maintaining strong security controls, high availability, and operational efficiency.

The VDI service is designed to support a range of business use cases, including office productivity, remote and hybrid working, regulated environments, and role-based desktop delivery. Virtual desktops may be provided as persistent or non-persistent instances depending on user requirements and service design.

Service Scope

The VDI service includes the design, provisioning, operation, and ongoing support of the virtual desktop platform, including:

- Hosting and management of virtual desktop infrastructure
- Creation and maintenance of standardised desktop images and operating systems
- Secure user access to virtual desktops via approved client software or browser-based access
- Centralised management of user profiles and user data
- Integration with customer identity and directory services for authentication and authorisation
- Continuous monitoring, maintenance, and operational support of the VDI platform
- End-user devices, local peripherals, and bespoke application development are excluded unless explicitly agreed.

Security & Access Management

Security is integral to the VDI service design. User access is controlled through integration with enterprise identity services and supports multi-factor authentication where required. Role-based access controls and least-privilege principles are applied to both users and administrators.

Virtual desktops operate within segmented network environments, and data is retained within the controlled VDI platform rather than on endpoint devices. Regular operating system and platform patching, vulnerability management, and configuration hardening are applied in accordance with defined security policies. Security events are monitored and managed through established incident response processes.

Availability & Resilience

The VDI service is architected to provide high availability and resilience. Core platform components are deployed with redundancy to minimise single points of failure, and capacity is actively managed to support peak usage periods. The service includes routine backup of user data and configuration in line with agreed retention policies.

Documented recovery procedures are maintained and periodically tested to support service continuity in the event of infrastructure or service failures. Planned maintenance activities are scheduled and communicated in advance to minimise user impact.

Service Management & Support

The VDI service is delivered in accordance with recognised service management practices. This includes incident management, service request fulfilment (such as user onboarding, desktop provisioning, and changes), change management, and problem management.

Service performance is measured and reported using defined metrics, which may include service availability, desktop login times, session stability, and incident response and resolution times. Service desk support is provided during agreed service hours, with priority-based escalation paths.

Exit & Data Handling

At contract termination, customer-owned data can be securely extracted and returned in agreed, industry-standard formats. Following confirmation of successful data handover, customer data is securely deleted from the VDI platform in accordance with data protection and retention policies.

The VDI service enables organisations to deliver secure, resilient, and scalable desktop environments while reducing operational complexity, improving control, and enhancing user experience.