DESKBRIDGE

Controlled workspaces for accountable digital work

Managed access, support records, data-handling boundaries and evidence for teams that need control.

Controlled access

Governed workspaces

Operational evidence

2026

The risk is not lack of software. It is lack of operated proof.

Most organisations already have tools. What breaks down is authority, supportability and evidence.

Hidden exposure

Unmanaged laptops and local data

Shared accounts and informal access

Contractors without clear expiry

Support changes without a durable record

What clients need

Named access and role ownership

Workspace boundaries that can be supported

Offboarding and revocation evidence

Clear proof when challenged

DeskBridge provides the managed layer around work

One accountable service boundary around people, devices, access, support, data and evidence.

Managed controls

Identity, MFA, roles, expiry and revocation

Approved applications and controlled sessions

Clipboard, file, print and AI handling by policy

Evidence outputs

Ticketed changes and traceable actions

Access, support, change and backup review packs

Client-safe records for audits, insurers and boards

Client-safe summary. Final commitments require signed scope and service design.

Where DeskBridge is strongest

Best fit is where access, support and evidence matter as much as the desktop itself.

Strong fit

Professional services handling client material

Contractor-heavy teams with access expiry risk

Sensitive data workflows adopting AI cautiously

Less suitable without redesign

Uncontrolled BYOD as the primary model

Informal shared-account working

Projects needing unsupported sovereignty claims

Client-safe summary. Final commitments require signed scope and service design.

Key custody models and the trade-offs

Data residency answers where data is stored. Key custody answers who can decrypt protected data.

DeskBridge Managed Keys

Best for normal managed-service support.

Caveat: DeskBridge may technically access protected service data for authorised support, recovery or lawful operation.

Customer-Controlled Keys

Best where clients approve protected data access.

Caveat: restore, migration, search and incident response may require client key release.

Customer-Held / Zero-Knowledge Keys

Best for the strongest custody boundary.

Caveat: lost keys may mean unrecoverable data; some server-side features may be unavailable.

Client-safe summary. Final commitments require signed scope and service design.

The human workspace is the control point

DeskBridge can wrap AI and sensitive-data workflows with access control, approvals, support records and evidence.

Controls

User and contractor access to governed workflows

Approved tool and data-handling records

Role, expiry and exception evidence

Client-controlled key options where required

Boundary

No implied partnership or endorsement

No unsupported sovereignty or compliance claims

Final scope depends on signed service design

Unsafe shortcuts are refused and recorded

Client-safe summary. Final commitments require signed scope and service design.

What a client receives

The service is designed to leave management evidence, not just a working login.

Onboarding scope

Users, roles, applications, data, devices and key custody decisions.

Controlled access

Named users, roles, approvals, MFA direction and expiry.

Support record

Ticketed requests, change notes, outcomes and escalation evidence.

Monthly evidence

Access review, contractor expiry, backup/restore and risk summary.

Client-safe summary. Final commitments require signed scope and service design.

Start with a scoped workspace review

DeskBridge confirms fit before deployment: users, access risk, applications, data handling, support needs and evidence expectations.

Review sequence

Confirm operating scope and client responsibilities

Select the data access assurance model

Map applications, users, suppliers and support routes

Produce a controlled proposal with caveats and evidence plan

Output

Commercially clear proposal

Confirmed caveats and exclusions

Evidence plan before deployment

Supportable operating boundary