



## Business Continuity and Disaster Recovery Plan

e: [info@redactxpert.ai](mailto:info@redactxpert.ai)

w: <https://www.redactxpert.ai>

Powered by Simpson Associates



Contents

1. Introduction..... 3

1.1 Purpose ..... 3

1.2 Scope ..... 3

2. Business Context & Criticality..... 3

3. Recovery Objectives ..... 4

3.1 Recovery Time Objective (RTO) & Recovery Point Objective (RPO) ..... 4

3.2 Azure Infrastructure SLAs..... 4

4. Resiliency ..... 5

4.1 Azure Regions..... 5

4.2 Availability Zones & Zone Redundancy ..... 5

4.3 Geo-Redundancy..... 5

4.4 Distributed Denial of Service (DDoS) ..... 5

5. Scalability ..... 5

6. Data Protection & Backup Strategy ..... 6

6.1 Tenant Database ..... 6

6.2 Global Database ..... 6

6.3 Storage Accounts ..... 6

6.4 Metrics, Logs & Audit Data ..... 6

6.5 Azure DevOps..... 6

7. Disaster Recovery Strategy..... 7

7.1 Azure regional outage ..... 7

7.2 Loss of a critical PaaS service ..... 7

7.3 Data corruption or accidental deletion..... 7

7.4 AI service unavailability or throttling..... 8

7.5 Deployment-related outage..... 8

## 1. Introduction

### 1.1 Purpose

The purpose of this Business Continuity and Disaster Recovery (BCDR) Plan is to define the approach and procedures used to ensure the continued operation and timely recovery of RedactXpert in the event of a disruptive incident.

The BCDR Plan aligns with the organisation's broader information security, risk management, and operational resilience objectives, and reflects the use of Microsoft Azure platform-as-a-service (PaaS) components and associated cloud-native recovery capabilities.

### 1.2 Scope

#### In Scope

The scope of this document covers the RedactXpert SaaS production environment only, including:

- RedactXpert Microsoft Entra Tenant.
- RedactXpert Azure Services and Resources.
- RedactXpert DNS Hosting.

#### Out of Scope

- Any non-production environments.
- Any resources or environments hosted within a customer's own Azure tenancy.
- Third-party authentication services e.g., a customer's own Microsoft Entra tenant.
- Networking and connectivity services for customers to access the RedactXpert SaaS application (e.g., a customer's own DNS servers, VPNs etc.).

## 2. Business Context & Criticality

RedactXpert is an AI powered SaaS based application which enables users to automate the process of redacting Personally Identifiable Information (PII) from a variety of document types.

Customers rely on this service to greatly improve the speed, accuracy and security of the document redaction process. If the service is unavailable, the only alternative available to most customers is to fallback to manually redacting documents.

This approach is both slower, impacting departments SLAs and with a greater possibility for missed PII or leakage of personal information, potentially leading to breaches of GDPR and/or the Data Protection Act.

## 3. Recovery Objectives

### 3.1 Recovery Time Objective (RTO) & Recovery Point Objective (RPO)

- Recovery Time Objective (RTO) for the application is 2 Business Days.
- Recovery Point Objective (RPO) for the application is 6 Business Hours.

### 3.2 Azure Infrastructure SLAs

The following Azure services are used in the RedactXpert application (along with SLAs):

- Application Gateway (99.95%)
- App Services (99.95%)
- SQL Database (99.99%)
- Storage Account (99.999%)
- Container Apps (99.95%)
- Azure AI Services (99.9%)

The composite SLA based on the underlying Azure Infrastructure in use is 99.59%.

## 4. Resiliency

RedactXpert has resilience built in at different layers in the platform and is designed to continue being operational in the event of a major outage or disaster.

### 4.1 Azure Regions

RedactXpert utilises a primary and secondary [Azure region](#). The primary and secondary region are contained within the same data residency boundary (e.g. the UK) but are geographically separated.

The primary region for RedactXpert is UK South, with the secondary region being UK West. These are also [region pairs](#) within Azure.

Alternative regions can be discussed on a case-by-case basis at Enterprise customers' request.

### 4.2 Availability Zones & Zone Redundancy

The primary region utilises [availability zones](#), which are separated groups of datacentres within a single region. Each availability zone has independent power, cooling, and networking infrastructure. If one zone within a region experiences an outage, then the relevant components would continue operating via the remaining availability zones as part of zone-redundancy.

### 4.3 Geo-Redundancy

Geo-Redundancy is utilised to provide failover as part of a region-wide outage. In the rare event of an entire region failure in the primary Azure region, then components can continue to operate via the secondary region.

### 4.4 Distributed Denial of Service (DDoS)

The RedactXpert platform protects against DDoS attacks using DDoS protection as part of the Azure Application Gateway.

## 5. Scalability

- The RedactXpert application uses a Container based approach to document processing. This enables horizontal scaling (scale-out) by adding additional container instances as demand increases, and scale-in when demand decreases.
- The application uses queue-based decoupling to smooth bursts of incoming workload and provide load levelling across processing components.
- RedactXpert uses a tenant isolation model in the data tier:
  - Each tenant has a dedicated database.
  - Each enterprise customer has a dedicated SQL Server instance.

This isolation supports:

- Independent scaling and performance tuning per tenant/enterprise customer.
- Reduced blast radius for data-tier incidents.
- Tenant-specific maintenance and recovery operations without affecting other tenants.

## 6. Data Protection & Backup Strategy

### 6.1 Tenant Database

- Point-in-Time Restore (PITR): PITR is enabled for a short operational recovery window (e.g., 7 days) to support recovery from:
  - Accidental data changes.
  - Application defects causing data issues.
  - Short-term operational incidents requiring rollback.
- Long-Term Retention (LTR) for a short period (e.g., 7 days) to cover scenarios where PITR may be insufficient, particularly around accidental tenant deletion / deprovisioning.

### 6.2 Global Database

- Long-term retention enabled to support:
  - Audit and historical recovery needs.
  - Recovery from low-frequency, high-impact events.
- Redundancy: Backups are stored using geo-zone redundant storage (GZRS) to improve resilience against zonal and regional failures.

### 6.3 Storage Accounts

Data in storage accounts is by design ephemeral and not designed to be persisted long term.

- Storage uses GZRS to support resilience against zonal failures and to enable regional failover capabilities where supported.
  - Geo-redundancy protects against infrastructure loss, but does not inherently protect against logical corruption, accidental overwrite, or deletion that replicates.

### 6.4 Metrics, Logs & Audit Data

- Audit/metrics evidence is written to immutable/WORM-enabled storage to prevent alteration.
- Data is protected via geo-redundant storage configuration (GZRS).
- Evidence repositories are backed up and/or replicated in accordance with compliance requirements to ensure audit continuity even during incidents.

### 6.5 Azure DevOps

All application code and IaC are stored in Azure DevOps repositories and as such are treated as a Microsoft-managed SaaS dependency, relying on Microsoft's documented SLA, replication and retention windows.

Recovery from user-initiated deletions is governed by the recycle-bin/retention behaviour.

## 7. Disaster Recovery Strategy

### 7.1 Azure regional outage

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description of Impact | A regional outage will affect all customers in that region. This will prevent users from using the application and will be a critical incident.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Recovery Approach     | <p>Recovering from a regional outage will be done as follows:</p> <ol style="list-style-type: none"> <li>1. Assess the expected outage time; if the outage is expected to last longer than 1 day, start recovery; if the outage has continued for 1 day, start recovery.</li> <li>2. Create regional resources in the new region.</li> <li>3. Validate new regional setup.</li> <li>4. Restore customer databases from global backups</li> <li>5. DNS failover</li> <li>6. Notify customers of recovery</li> </ol> <p>Once the primary region is restored, failing back will be completed as follows:</p> <ol style="list-style-type: none"> <li>1. Secondary region will be turned off</li> <li>2. Data objects will be restored in the primary region</li> <li>3. DNS failback</li> <li>4. Delete secondary region deployment</li> </ol> |
| Notes                 | Customers will only be failed over to a new region if it meets the required data residency and other compliance requirements, i.e., if governed via GDPR, Europe and the UK West would be the only considerations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

### 7.2 Loss of a critical PaaS service

|                       |                                                                                                                                                                                                            |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description of Impact | Depending on the PaaS service that is impacted, the app will either partially function or experience a complete outage. The level of the outage and the function affected will dictate the incident level. |
| Recovery Approach     | Recovery from a PaaS service outage will be completed in line with the Azure Regional Outage; however, only the affected resources will be restored.                                                       |

### 7.3 Data corruption or accidental deletion

|                       |                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description of Impact | Data within the system is split between ephemeral and persistent data. Ephemeral data such as redactions, documents being redacted etc. will be recovered on a best effort basis. Persistent data will follow the following recovery approach.                                                                                                               |
| Recovery Approach     | <p>Both point-in-time backups and longer-term retention backups will be used to restore persistent data that has been deleted or corrupted.</p> <p>In the event of a full data resource being lost a full restore will be conducted.</p> <p>In the event of a partial corruption or deletion data will be copied back to the data resource from backups.</p> |
| Notes                 | <p>Persistent data includes:</p> <ul style="list-style-type: none"> <li>• Users</li> <li>• Tenant login configurations</li> <li>• Audits</li> </ul> <p>Metrics</p>                                                                                                                                                                                           |

#### 7.4 AI service unavailability or throttling

|                       |                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description of Impact | AI service unavailability will prevent new documents from being processed in the system. This will cause delays; however, in-progress redactions can be completed, and uploads will be processed once the system is restored. |
| Recovery Approach     | Follow the plan for the Loss of a critical PaaS service.                                                                                                                                                                      |

#### 7.5 Deployment-related outage

|                       |                                                                                                                                                                                                                                    |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description of Impact | Deployment outages are caused by misconfigurations or code deployments with unintended side effects. Other possible issues caused by deployment, such as data loss, will be covered under their recovery plan.                     |
| Recovery Approach     | Deployments are released using a fix-forward approach, meaning a reasonable effort is made to remediate issues. However, if they cannot be remediated, the system is rolled back to the last working version, which is redeployed. |