

Business Continuity & Disaster Recovery - Content Hub

Version 1

Last modified 5-August-2026

Classification: Internal

Prepared for: Mindtools Kineo

Prepared by: IMS Governance Team Stakeholders

Version: 1 **Title:** Business Continuity & Disaster Recovery - Content Hub
Official/Internal

Document revision history

Version	Changed by	Summary of change	Approval date
1.0	DevOps Engineer	Initial Release	03 August 2026

Approval

Date effective	Superseding	Policy review date	Approver
05 August 2026	NA	At least once a year or when material changes	DevOps Engineer and IMS Owner

Introduction

Mindtools Kineo offers a range of business support services that become a part of the operations of our clients.

We recognise that in providing these services, we are committed to delivering a continuity of service that allows our clients to maintain the continuity of their operations.

This BCDR plan outlines the procedures and actions to be taken to ensure the continuity of business operations and the rapid recovery of services for the Content Hub.

The hosting is provided through Amazon Web Services (AWS). A Global AWS Region supports tenant discovery and routing. Satellite AWS Regions in Europe, Oceania and America host authenticated application workloads. Generic content data is held within the AWS London (UK) region. User data is stored in the appropriate AWS regulatory region to meet data compliance requirements (captured during client onboarding).

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- Ensure the availability and resilience of Content Hub services.
- Minimise downtime and data loss in the event of a disaster.
- Maintain customer trust and compliance with regulatory requirements.
- Provide a clear framework for response and recovery actions.

Hosting Infrastructure

Mindtools Kineo has partnered with Amazon Web Services (AWS) to host and deploy the Content Hub application as a serverless, multi-region architecture. AWS provides scalable computing capacity in the AWS cloud.

AWS enables Mindtools Kineo to configure security and networking, manage storage and scale services up or down to handle changes in forecast traffic. The platform is defined using Infrastructure as Code to allow redeployment into an alternate available AWS region when required.

Importantly, AWS meets and exceeds security and compliance requirements ensuring Mindtools Kineo maintains data protection for its clients. You can read about AWS compliance via the following [AWS compliance documentation](#) from Amazon.

The Content Hub environment is designed for secure, scalable and efficient operation in AWS cloud infrastructure.

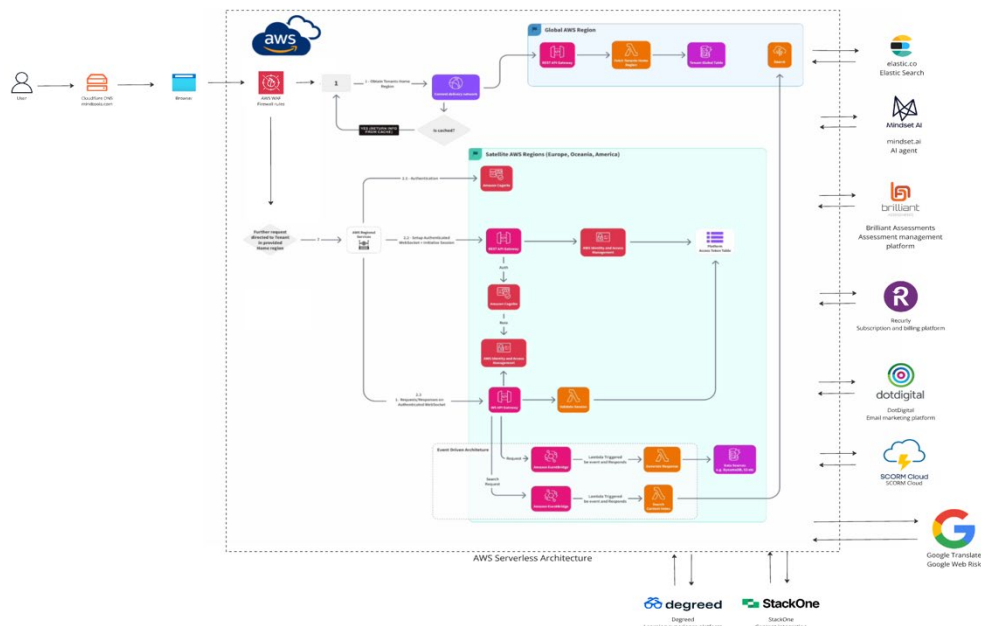


Figure 1 Content Hub AWS Serverless Architecture Overview

The following is a breakdown of key components and their functionality.

Key Components

- **AWS Regions:** A Global AWS Region for tenant discovery, plus Satellite AWS Regions for Europe, Oceania and America for authenticated application workloads, with cross-region and cross-account backup replication for disaster recovery.
- **Data Backup:** Managed backups using AWS native services (AWS Backup, DynamoDB PITR, S3 Cross-Region Replication, RDS automated snapshots), replicated across regions and accounts.
- **Monitoring and Alerts:** Real-time monitoring and alerts via AWS CloudWatch and Datadog.

Functionality

End User Access:

HTTPS Connections: Users securely access the Content Hub application via HTTPS from a modern browser.

Cloudflare Layer: DNS services are provided by Cloudflare as the first external security and routing layer for internet traffic.

CloudFront: Amazon CloudFront provides content delivery and an additional layer of performance and protection for user-facing traffic.

Security Tier:

AWS WAF: Requests entering AWS are protected by AWS WAF and firewall rules before reaching application endpoints.

VPC: Application resources run within Amazon Virtual Private Clouds (VPCs), providing network isolation and controlled access between tiers.

DDoS Protection: Denial of Service (DOS) and Distributed Denial of Service (DDOS) protection are provided by AWS CloudFront and AWS API Gateway, complemented by Cloudflare edge protection.

Web/Application Tier:

Application Services: This tier houses the Content Hub application, which users interact with. Workloads run across Satellite AWS Regions in Europe, Oceania and America, with a Global AWS Region used for tenant discovery and routing. Traffic between application services and data stores is managed securely through encrypted AWS service protocols.

Network Security: Further secured by security groups for controlled access between tiers.

Database/Data Tier:

Database and Data Services: This tier contains the primary data stores that support the Content Hub application, including Amazon DynamoDB for application data, Amazon Cognito for user identity, Amazon S3 for content assets and Amazon RDS for reporting.

Encrypted Data Transmission: Data transmitted between the application and data stores is encrypted in transit and at rest.

Search/Index Tier:

Search Services: Search indexing supports Content Hub content discovery and can be restored from backup or rebuilt from source data in a disaster recovery event.

DevOps Access:

Content Hub DevOps Access: Secure administrative access to the environment for

monitoring, maintenance and updates is restricted to authorised personnel using multi-factor authentication (MFA).

Customer Integrations:

Customer Integrations: Customers can securely connect via Single Sign-On (SSO) and approved third-party integrations. All communication with external systems is encrypted to ensure data protection.

Logging, Monitoring and Backup:

Log Workspace: Activities within the architecture are logged and stored using AWS CloudWatch and CloudTrail, allowing for auditing and troubleshooting. Access to audit logs is restricted to authorised personnel.

Object Storage: Secure storage for encrypted backups and diagnostics in Amazon S3, with versioning and cross-region/cross-account replication for critical buckets.

Monitoring: Continuous monitoring of infrastructure, performance and security events is conducted via AWS CloudWatch and Datadog, enabling proactive management of the system.

Security Features:

- **HTTPS:** End-to-end encryption for all user-facing traffic.
- **Encrypted Backups/Data at Rest:** Data is encrypted at rest using AWS KMS (FIPS 140-2 validated HSMs) and in transit using TLS 1.2.
- **Cloudflare and AWS WAF:** Applied at the edge and within AWS to ensure granular control over traffic flow and access to resources.
- **Managed Service Encryption:** Communication with DynamoDB, S3, Cognito, API Gateway and RDS uses encrypted channels to maintain the integrity of sensitive data.

Regional Data Storage

All data collected by the application is stored within the Client's selected/applicable geographic region for user data. Generic content data is held in the UK (AWS London). This architecture is designed with scalability, security and resilience at the forefront, ensuring compliance with industry standards and delivering a robust learning content platform for customers.

Password security

- User authentication is managed via Amazon Cognito, with Single Sign-On (SSO) available for enterprise customers.
- Passwords and credentials managed by Cognito are stored using Cognito's secure credential storage mechanisms.
- Administrative access to AWS, GitLab and Microsoft 365 requires multi-factor authentication (MFA).

Backups

Backup is an important aspect of the Content Hub. The Disaster Recovery strategy utilises data replication techniques available in AWS. Backups are taken from primary production data sources, then stored in a separate AWS account and service region to protect against account-level and regional issues (cross-account and cross-region).

Backups include the following elements:

- Application data stored in Amazon DynamoDB
- User identity data managed by Amazon Cognito
- Content assets and files stored in Amazon S3
- Reporting databases on Amazon RDS
- Search indexes (Elastic Cloud snapshots and/or re-index from source)
- Messaging/event-driven operational data
- Source code stored centrally in GitLab
- Infrastructure configuration defined as Infrastructure as Code

Backups are encrypted at rest and replicated across AWS regions and accounts. Retention is managed in accordance with Mindtools Kineo backup policy.

Testing and Maintenance

- Conduct bi-annual BCDR plan reviews and updates.
- Perform service-level DR testing drills throughout the year against a quarterly schedule, with each quarter targeting a different storage system.
- Document lessons learned from each test and update the BCDR plan accordingly.

Disaster Recovery

In the unlikely case of a disaster, Mindtools Kineo has implemented a comprehensive disaster recovery process.

Using backups and replication, Mindtools Kineo are able to execute an action plan to restore the service with the following recovery time and recovery point objectives:

- The expected recovery time objective (RTO) is **6 hours**.
- The expected recovery point objective (RPO) is **12 hours**.
- The estimated time of recovery depends on several factors including data volumes, the number of services being restored, network bandwidth and whether recovery is within-region or cross-region. Service recovery is targeted within the stated RTO.

In the unlikely case that a disaster has impacted an entire AWS Region, Mindtools Kineo are able to execute an action plan to restore the service from backups that have been replicated to another region and/or account and to re-provision the application environment in an alternate region.

Mindtools Kineo Disaster Recovery Process

In the event of a significant service failure, Mindtools Kineo will follow a defined Disaster Recovery (DR) process to ensure the quickest possible restoration of service. The specific steps are outlined below, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO) targets.

Immediate Assessment:

A rapid assessment of the failure is conducted by the Content Hub technical team to determine the root cause and potential impacts on the system.

Action Plan and Estimate:

Based on the initial findings, Mindtools Kineo will develop an action plan and provide an estimated timeline for rectification. Communication will be sent to all affected client contacts.

Rectification Process:

The rectification will depend on the nature of the failure. The following steps may be undertaken:

Restore/Redeploy from Backup:

Mindtools Kineo will initiate restoration of affected data services from the most recent available backups/replicas and re-provision application infrastructure in an available AWS region where required. Critical data required for service restoration is prioritised.

RPO and Backup Overlay:

Restoration will use the most recent viable backup/replica, providing a Recovery Point Objective (RPO) of 12 hours. This means that data changes within the last 12 hours prior to the failure could potentially be lost.

System Testing:

System testing will be conducted using random user accounts with differing user permissions to perform common operational procedures, ensuring the system is fully functional after restoration.

Re-delegation of Domains:

If applicable, domains may need to be re-delegated to point to the new service endpoints.

Ongoing Communication:

Clients will be kept informed throughout the process. Any changes to the initial rectification plan, including updated time estimates, will be communicated promptly to affected client contacts.

Domain Re-Delegation Delay:

Where domain re-delegation is required, a delay of 12 to 24 hours may occur between restoration of system functionality and system availability via the Internet due to DNS propagation times.

Recovery Time Objective (RTO):

Mindtools Kineo will aim to restore full system functionality within the agreed RTO of **6 hours**.

However, no RTO guarantee is provided where the Client manages their own DNS zone, as any necessary DNS Zone updates required to re-establish access to the service are outside of Mindtools Kineo's control.

Recovery Tests & Validation

The following activities are performed in order to test the disaster recovery process and validate the integrity of backups:

- Monitor and review the backup logs and CloudWatch alarms for any failures
- Maintain scheduled backups of DynamoDB, S3, RDS and Elastic Cloud according to defined schedules
- Store backups using cross-region and cross-account replication
- Perform quarterly recovery drills to test backup integrity and restoration processes (one data system per quarter)

Failover and Redundancy

- Maintain cross-region and cross-account backups for critical data services.
- Define all infrastructure and application components using Infrastructure as Code to allow redeployment into another available AWS region.
- Test recovery/failover procedures quarterly to ensure smooth transitions during an actual disaster.

Cybersecurity Measures

- Implement AWS security best practices and recommendations to protect against cyber threats.
- Regularly update and patch all systems.
- Conduct annual security audits (Cyber Essentials Plus & ISO 27001) and penetration testing/Continuous Security Testing.

Communication Plan

Internal Communication

- Establish a crisis management team with defined roles and responsibilities.
- Use email and Microsoft Teams for instant communication during an incident.
- Conduct regular training sessions and drills for all staff.

External Communication

- Notify customers promptly via email and Mindtools Kineo customer support channels in the event of a disruption.
- Provide regular updates on the status and expected resolution time.
- Designate a spokesperson for media inquiries.

Roles and Responsibilities

- **Incident Commander:** Ultimate decision authority during a DR event, including severity classification, maintenance page activation/deactivation, recovery strategy and authorisation of customer communications.
- **Technical Lead:** Responsible for technical implementation, solution execution and architecture decisions during recovery.
- **Head of Product & Product Manager:** Strategic communication, executive reporting and external stakeholder management.
- **DevOps Engineer:** Responsible for infrastructure recovery actions, system monitoring, deployments and backups.
- **CX Team Lead:** Crafts and delivers customer communications based on the Incident Commander's brief.
- **Legal & Compliance Manager:** Ensure adherence to regulatory requirements and documentation.
- **CEO:** Escalation point for critical business, legal, or strategic decisions only, as determined by the Incident Commander.

Conclusion

This BCDR plan is designed to ensure the resilience and quick recovery of Content Hub services in all regions. Regular testing, clear communication and robust cybersecurity measures are critical components to achieving these goals.