

Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)

Version: 2.0

Last modified: 25-September-2026

Public

Prepared for: Learning Platforms infrastructure

Prepared by: Global Product Manager – Learning Platforms

Approved by: Global Product Manager Learning Platforms & Legal and Compliance
Officer

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)

Public

Document revision history

Version	Changed by	Summary of change	Date
1	Learning Platforms	Create & release	10 October 2024
1.1	Legal & Compliance Officer	Update product name	19 March 2025
2.0	Learning Platforms	Merged the EMEA & US (v1.1) and APAC (v1.2) plans into a single global plan covering all Hosted Learning Platforms.	21 September 2026

Approval history

Date effective	Superseding	Policy review date	Approver
10 October 2024	NA – first release	10 October 2026	Global Product Manager Learning Platforms & Legal and Compliance Officer
19 March 2025	V.1	10 September 2026	Legal and Compliance Officer
25 September 2026	EMEA & US v1.1 and APAC v1.2	March 2027	Global Product Manager Learning Platforms & Legal and Compliance Officer

Contents

Document revision history	2
1. Introduction	5
2. Document Purpose	5
3. Intended Audience	5
4. Definitions	5
5. Policy Statement	6
6. Objectives	6
7. Hosting Infrastructure	6
7.1. Regions and Availability Zones	7
7.2. Architecture Overview	7
7.3. Key Components	8
7.4. Instances and Scaling	8
7.5. Hosted Learning Platform Environments	9
8. Functionality	9
8.1. End User Access	9
8.2. Security Tier	9
8.3. Web/Application Tier	9
8.4. Database Tier	9
8.5. Replica Database Tier (Optional)	10
8.6. DevOps Access	10
8.7. Customer Integrations	10
8.8. Logging, Monitoring, and Backup	10
8.9. Security Features	10
8.10. Regional Data Storage	11
8.11. Password security	11

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)**Public**

9. Backups	11
10. Testing and Maintenance	12
11. Disaster Recovery	12
11.1. Mindtools Kineo Disaster Recovery Process	13
11.2. Immediate Assessment	13
11.3. Action Plan and Estimate	13
11.4. Rectification Process	13
11.5. Ongoing Communication	13
11.6. Domain Re-Delegation Delay	14
11.7. Recovery Time Objective (RTO)	14
12. Recovery Tests & Validation	14
13. Cybersecurity Measures	14
14. Communication Plan	14
14.1. Internal Communication	14
14.2. External Communication	15
15. Roles and Responsibilities	15
16. Conclusion	15

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)
Public

1. 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 Mindtools Kineo Hosted Learning Platforms managed services in the EMEA, US and APAC regions.

Hosting is provided through Microsoft Azure regions within the United Kingdom for EMEA clients, within the US for our US clients, and within Australia for our APAC clients (unless explicitly requested otherwise by our clients).

2. Document Purpose

The purpose of this document is to explain the:

- Measures we take to mitigate risks to our business
- Technical measures we take to protect our data, and
- Technical and administrative measures we take to recover from a disaster.

3. Intended Audience

This document is intended for the following groups with the purpose of:

- Mindtools Kineo staff seeking guidance on business continuity
- Clients and prospective clients evaluating Mindtools Kineo as a service provider, and
- Clients raising a specific issue in relation to Mindtools Kineo's business continuity.

4. Definitions

Hosted platform: The primary services offered by Mindtools Kineo Learning Platforms are:

- Totara LMS
- Totara Perform
- Moodle (Scaffold LMS / Track)
- Mindtools Kineo Analytics

These services are referred to as the Hosted Learning Platforms.

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)
Public

5. 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.

6. 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 the Hosted Learning Platforms managed 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.
- Ensure that all employees fully understand their duties in implementing the plan.
- Ensure that operational policies are adhered to within all planned activities.
- Ensure that proposed contingency arrangements are cost-effective.
- Consider implications on other company sites.
- Provide disaster recovery capabilities as applicable to key customers, vendors and others.

7. Hosting Infrastructure

Mindtools Kineo has partnered with Microsoft Azure to host and deploy its application. Microsoft Azure provides scalable computing capacity in the Azure cloud.

Azure enables Mindtools Kineo to launch as many or as few virtual servers as required, configure security and networking, manage storage, and scale up or down to handle changes in forecast traffic.

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)
Public

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

7.1. Regions and Availability Zones

Microsoft Azure offers hosting in multiple locations worldwide, known as regions. Each Azure region is completely isolated from other Azure regions, and within each region there are multiple isolated locations known as Availability Zones, connected through low-latency links.

Azure provides Mindtools Kineo with the ability to place resources, such as instances (servers) and data, in multiple locations within a region. Mindtools Kineo uses both the separation of regions and the Availability Zones within regions to maintain data protection and to implement disaster recovery and backup.

Mindtools Kineo is able to offer hosting in any supported Azure region on request. By default, client data is hosted as follows:

Region	Default Azure hosting
EMEA	Azure regions within the United Kingdom
US	Azure regions within the United States
APAC	Australia East, using the Availability Zones within the region

7.2. Architecture Overview

The Totara LMS environment is designed for secure, scalable, and efficient operation in Azure cloud infrastructure.

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)
Public

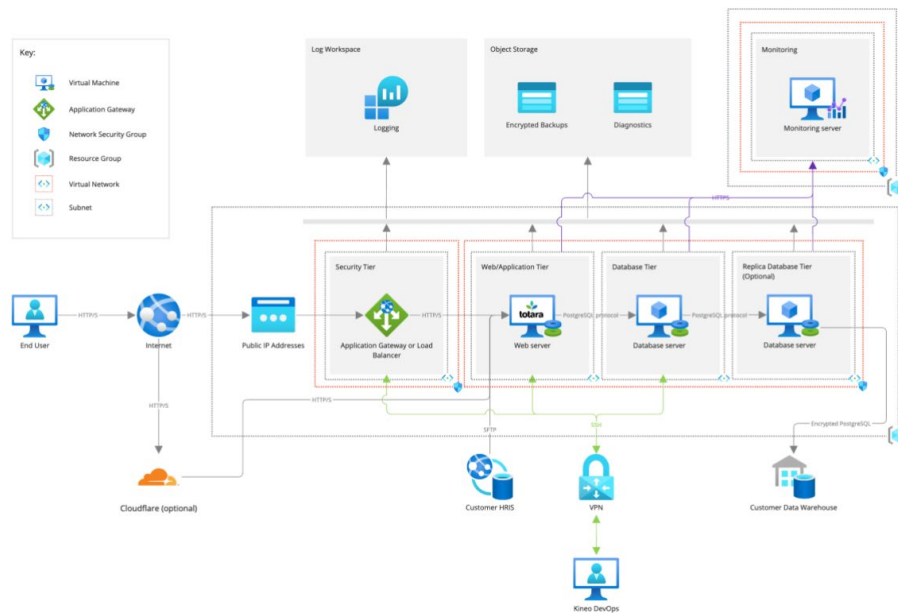


Figure 1 Totara LMS Azure MCE Architecture Overview

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

7.3. Key Components

- **Azure Regions:** Mindtools Kineo Hosted Learning Platforms are deployed in Azure regions in the UK, the US and Australia.
- **Data Backup:** Daily encrypted backups held in dedicated backup storage (see Section 9).
- **Monitoring and Alerts:** For real-time monitoring and alerts.

7.4. Instances and Scaling

Azure enables Mindtools Kineo to deploy multiple instances (servers) to meet its business requirements and platform needs, and to scale both horizontally and vertically to support performance, disaster recovery and backup requirements.

Horizontal scaling is the process of adding more nodes to a system, such as adding a new server to a distributed software application. Mindtools Kineo uses horizontal scaling to extend its platform by adding instances where required to meet usage demand.

Vertical scaling means adding more resources to a single node, such as increasing the CPU or memory of a server (the instance type). Mindtools Kineo uses vertical scaling to align performance with forecast user traffic and to manage performance under load, choosing instance types according to the purpose and requirements of each workload.

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)
Public

7.5. Hosted Learning Platform Environments

The Hosted Learning Platforms consist of the following environments and services:

- **Production:** the servers that host the application, files and database. All user traffic is directed to the platform hosted on these servers.
- **User Acceptance Testing (UAT):** an environment accessible to Mindtools Kineo clients for functional and integration testing, separate from their production (live) environment.
- **Backup:** dedicated backup storage for the application, files and database (see Section 9).
- **Monitoring:** Mindtools Kineo's internal monitoring and logging systems.

8. Functionality

8.1. End User Access

HTTPS Connections: Users securely access the Totara application via HTTPS, using public IP addresses routed through the internet.

Cloudflare Layer: Traffic is routed through Cloudflare, which provides an additional layer of security and performance optimisation. Cloudflare is being rolled out across all hosted sites and is not yet in place for every site.

8.2. Security Tier

Cloudflare Web Application Firewall (WAF): The first layer of protection, filtering malicious traffic before it reaches the platform. Cloudflare WAF protection is replacing the Azure Application Gateways and load balancers previously used in this tier, which are being retired.

Network Security Group (NSG): Controls inbound and outbound traffic based on defined security rules to protect the network at the perimeter level.

8.3. Web/Application Tier

Web Servers (Totara): This tier houses the Totara application, which users interact with. Traffic between the web servers and database tier is managed securely through PostgreSQL protocols.

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

8.4. Database Tier

Database Servers: This tier contains the primary database that supports the Totara application. Depending on the hosting environment, databases run either on dedicated

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)

Public

PostgreSQL servers or on Azure's managed PostgreSQL service. The database communicates with the web/application tier using encrypted PostgreSQL protocols.

Encrypted Data Transmission: Data transmitted between the application and database is encrypted to ensure security and privacy.

8.5. Replica Database Tier (Optional)

Replica Servers: Optional replica databases can be provided for client reporting access or to share reporting load. They are not used for high availability or data redundancy.

8.6. DevOps Access

Mindtools Kineo DevOps Access: Secure administrative access to the environment for monitoring, maintenance, and updates is provided through a VPN tunnel. SSH access is available for managing secure file transfers (SFTP) and other administrative tasks.

8.7. Customer Integrations

Customer HRIS and Data Warehouse Integrations: Customers can securely exchange data between their HRIS systems and the platform using SFTP. Customer data warehouses can connect to the replica database (see Replica Database Tier) over an encrypted PostgreSQL connection. All communication with external systems is encrypted, ensuring data protection.

8.8. Logging, Monitoring, and Backup

Log Workspace: All activities within the architecture are logged and stored in a central logging workspace, allowing for comprehensive auditing and troubleshooting.

Object Storage: Secure storage for encrypted backups and diagnostics, ensuring availability of data for recovery and performance monitoring.

Monitoring Servers: Continuous monitoring of the infrastructure, performance, and security events is conducted via dedicated monitoring servers, enabling proactive management of the system.

Metrics logged include:

- Application access logs
- Application uptime, and
- Platform performance and utilisation statistics.

8.9. Security Features

- HTTPS: End-to-end encryption for all user-facing traffic.

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)

Public

- **Encrypted Backups:** Data is encrypted both at rest and in transit, providing robust protection against unauthorised access.
- **Network Security Groups (NSGs):** Applied at all levels of the architecture to ensure granular control over traffic flow and access to resources.
- **PostgreSQL Encryption:** Communication between application and database is encrypted to maintain the integrity of sensitive data.
- **Databases at rest:** All databases and database backups are encrypted at rest.

8.10. Regional Data Storage

All data collected by the application is stored within the client's selected geographic region, as indicated in the agreement (see Regions and Availability Zones above).

This architecture is designed with scalability, security, and resilience at the forefront, ensuring compliance with industry standards and delivering a robust learning platform for customers.

8.11. Password security

All passwords stored by the application are salted and hashed using the per-user salted BCrypt hash algorithm.

Minimum password complexity rules for the application are:

- 8 characters in length.
- Must contain at least 1 digit(s), at least 1 lower case letter(s), at least 1 upper case letter(s), at least 1 non-alphanumeric character(s) such as *, -, or #.

These rules are configurable and can be increased in complexity by named site administrators.

9. Backups

Backup is an important aspect of Mindtools Kineo's Hosted Learning Platforms. A complete, independently restorable backup point is created at least once every 24 hours for each hosted environment. Each backup point includes:

- The application and its database
- User and course records
- User uploaded files and assets
- Course content
- All logs including site logs
- Infrastructure instance configuration

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)

Public

Depending on the hosting environment, backups are taken as encrypted, deduplicated file-level backups or as Azure platform backup points. In either case, every backup point can be restored on its own.

Backups are:

- Encrypted at rest and in transit.
- Held in dedicated backup storage, independent of the production servers and their disks.
- Stored with at least three redundant copies within the hosting region. Zone-redundant or geo-redundant storage is used where available and is being extended across all environments.
- Retained for 30 days, providing a range of restore points.

10. Testing and Maintenance

- Conduct bi-annual BCDR plan reviews and updates.
- Monitor backups daily and perform quarterly restore drills (see Section 12).
- Document lessons learned from each test and update the BCDR plan accordingly.

11. Disaster Recovery

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

Using the most recent daily backup point, 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 within 1 business day for Web VM.
- The expected recovery time objective (RTO) is within 1 business day for Database.
- The estimated time of recovery depends on several factors including the database sizes, the transaction log size, the network bandwidth, and the total number of databases recovering in the same region at the same time. The recovery time is usually less than 12 hours.
- The expected recovery point objective (RPO) is 24 hours.

In the unlikely event that a disaster affects an entire Azure region, Mindtools Kineo will rebuild the affected services in an alternative Azure region from the most recent available backup. Where backups are already replicated to a secondary region, this capability is available today. Mindtools Kineo is extending cross-region backup replication to all hosting environments so that region-wide recovery is available globally.

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)
Public

Recovery time for a region-wide event depends on the scale of the incident and the availability of capacity in the alternative region, and may exceed the recovery time objectives above.

11.1. Mindtools Kineo Disaster Recovery Process

In the event of a significant server 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.

11.2. Immediate Assessment

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

11.3. 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.

11.4. Rectification Process

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

- **Restore from Backup:** Mindtools Kineo will restore the affected service to a new server or service instance from the most recent backup point.
- **Recovery Point:** Restoring from the most recent daily backup point provides a Recovery Point Objective (RPO) of 24 hours. This means that data changes within the last 24 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 server instance.

11.5. 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.

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)
Public

11.6. Domain Re-Delegation Delay

Where domain re-delegation is required, a delay of up to 24 hours may occur between restoration of system functionality and system availability via the Internet for some users, due to DNS propagation times. In many cases this delay will be significantly less.

11.7. Recovery Time Objective (RTO)

Mindtools Kineo will aim to restore full system functionality within the agreed RTO.

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.

12. Recovery Tests & Validation

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

Frequency	Activity
Daily	Monitor and review backup logs for any failures, confirming that a backup point has been created for every hosted environment.
Quarterly	Restore drill: restore backups from a production environment to a simulated production environment, then undertake system testing using random user accounts with differing user permissions, completing common operational procedures.

13. Cybersecurity Measures

- Use Tenable vulnerability management to identify, prioritise and remediate security vulnerabilities across the hosting estate.
- Regularly update and patch all systems.
- Conduct annual security audits (CE+ & ISO27001) and penetration testing.

14. Communication Plan

14.1. Internal Communication

- Establish a crisis management team with defined roles and responsibilities.
- Use email and Microsoft Teams for instant communication during an incident.

Version: 2.0 **Title:** Business Continuity & Disaster Recovery – Global (EMEA, US & APAC)

Public

- Conduct regular training sessions and drills for all staff.

14.2. External Communication

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

15. Roles and Responsibilities

- Crisis Management Team: Lead by the Legal and Compliance Manager, includes representatives from IT, Legal and Compliance Team, IMS Governance Team and Customer Success.
- Learning Platforms DevOps: Responsible for technical recovery actions, system monitoring, and backups.
- Customer Support Team: Handle customer communications and support during disruptions.
- Compliance Manager: Ensure adherence to regulatory requirements and documentation.

16. Conclusion

This BCDR plan is designed to ensure the resilience and quick recovery of Mindtools Kineo Hosted Learning Platforms managed services in the EMEA, US and APAC regions. Regular testing, clear communication, and robust cybersecurity measures are critical components to achieving these goals.