Kineo Learning Platforms
Business Continuity & Disaster Recovery – EMEA & US Regions

Version 1.1
Last modified 28-April-2025
Classification: Public

Prepared for: Learning Platforms infrastructure
Prepared by: Global Product Manager – Learning Platforms
Approved by: Global Product Manager Learning Platforms & Legal and Compliance Officer

Document revision history

Version	Changed by	Summary of change	Approval date
1	Learning Platforms	Create & release	10 October 2024
1.1	Legal & Compliance Officer	Update product name	19 March 2025

Approval

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 October 2026	Legal and Compliance Officer

Contents

Introduction **3**

Policy Statement **3**

Objectives **3**

Hosting Infrastructure **4**

Key Components **4**

Functionality **5**

- End User Access: 5
- Security Tier: 5
- Web/Application Tier: 5
- Database Tier: 5
- Replica Database Tier (Optional): 5
- DevOps Access: 5
- Customer Integrations: 6
- Logging, Monitoring, and Backup: 6
- Security Features: 6
- Regional Data Storage 6
- Password security 6

Backups **7**

Testing and Maintenance **7**

Disaster Recovery **7**

- Kineo Disaster Recovery Process: 8
- Immediate Assessment: 8
- Action Plan and Estimate: 8
- Rectification Process: 8
- Ongoing Communication: 8
- Domain Re-Delegation Delay: 9
- Recovery Time Objective (RTO): 9

Recovery Tests & Validation **9**

- Failover and Redundancy 9

Cybersecurity Measures **9**

Communication Plan **10**

- Internal Communication 10
- External Communication 10

Roles and Responsibilities **10**

Conclusion **10**

Introduction

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 Totara LMS managed services in the EMEA and US regions.

The hosting is provided through Azure regions within the United Kingdom for EMEA clients and within the US for our US clients (unless explicitly requested otherwise by our clients).

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 Totara LMS 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.

Hosting Infrastructure

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

Azure enables 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.

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

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

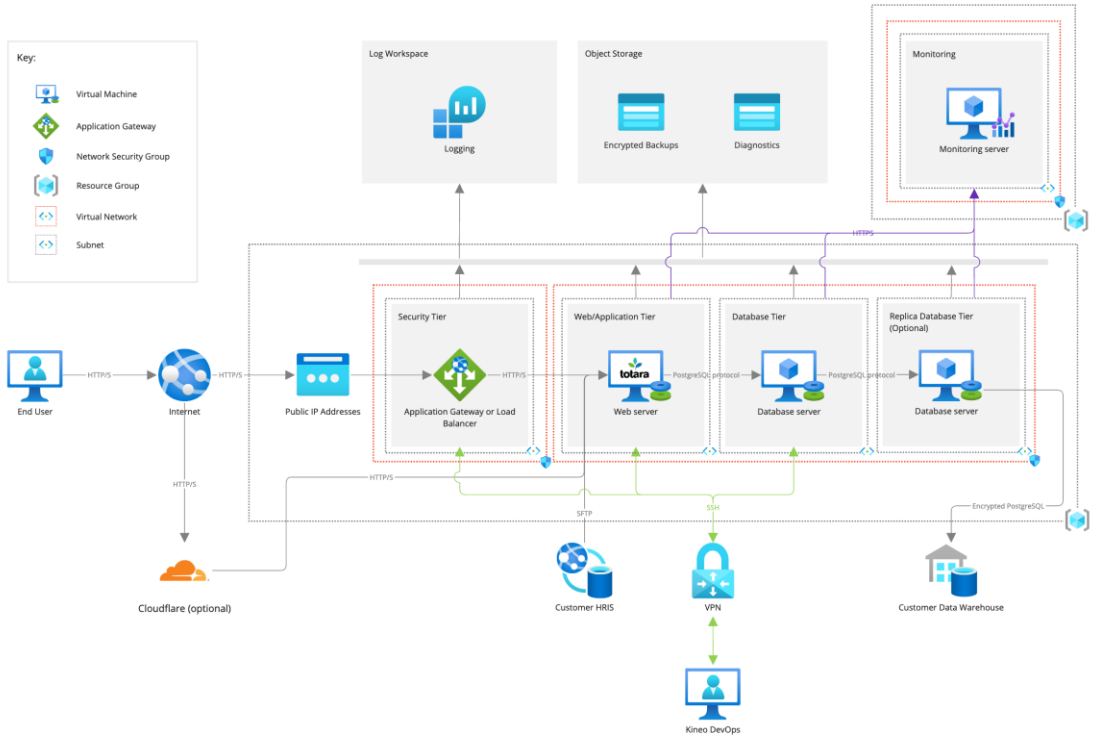

Figure 1 Totara LMS Azure MCE Architecture Overview

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

Key Components

- **Azure Regions**: Primary and secondary data centres within the UK or US.
- **Data Backup**: Regular backups to Azure Blob Storage with geo-redundancy.
- **Monitoring and Alerts**: For real-time monitoring and alerts.

Functionality

End User Access:

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

Optional Cloudflare Layer: Provides an additional layer of security and performance optimization through Cloudflare, acting as an optional intermediary for external traffic.

Security Tier:

Application Gateway or Load Balancer: The first layer of the architecture, which ensures secure and balanced traffic distribution across the application.

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

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.

Database Tier:

Database Servers: This tier contains the primary database that supports the Totara application. It 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.

Replica Database Tier (Optional):

Replica Servers: Optional replication servers provide high availability and data redundancy for critical services, ensuring business continuity in the case of a primary database failure.

DevOps Access:

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.

Customer Integrations:

Customer HRIS and Data Warehouse Integrations: Customers can securely connect their HRIS systems or data warehouses via VPN for data exchange. All communication with external systems is encrypted, ensuring data protection.

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 Server: Continuous monitoring of the infrastructure, performance, and security events is conducted via a dedicated monitoring server, enabling proactive management of the system.

Security Features:

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

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.

Regional Data Storage

All data collected by the application is stored within Client's selected geographic region.

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.

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 as *, -, or #.

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

Backups

Backup is an important aspect of Kineo's Hosted Learning Platform. Backups are incremental and include the following elements:

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

Backups are encrypted at rest and retained for 30 days.

Testing and Maintenance

- Conduct bi-annual BCDR plan reviews and updates.
- Perform Quarterly Periodic Fai lover Tests and Annual Full-scale Disaster Recovery Drills.
- Document lessons learned from each test and update the BCDR plan accordingly.

Disaster Recovery

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

Using backups created each day 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 case, that a disaster has impacted the entire Azure Region, Kineo are able to execute an action plan to restore the service from a backup that has been created in another region.

Kineo Disaster Recovery Process:

In the event of a significant server failure, 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 Kineo technical team to determine the root cause and potential impacts on the system.

Action Plan and Estimate:

Based on the initial findings, 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:

Server Rebuild from Backup:

Kineo will initiate the creation of a new server using the most recent full backup of the failed server.

RPO and Incremental Backup Overlay:

The most recent incremental backup will be overlaid, providing 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.

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):

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 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 log for any failures
- Schedule daily backups of all databases and configuration files.
- Store backups in a geo-redundant Azure Blob Storage.
- Perform quarterly recovery drills to test backup integrity and restoration processes.
    - Restoring backups from a production server to a simulated production server
    - Undertaking system testing using random user accounts with differing user permissions and completing common operational procedures

Failover and Redundancy

- Set up Azure Site Recovery to replicate services to a secondary Azure region.
- Ensure automatic failover capabilities with minimal manual intervention.
- Test failover procedures quarterly to ensure smooth transitions during an actual disaster.

Cybersecurity Measures

- Implement Azure Security Center recommendations to protect against cyber threats.
- Regularly update and patch all systems.
- Conduct annual security audits (CE+ & ISO27001) and penetration 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 the 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.

Roles and Responsibilities

- **Crisis Management Team**: Lead by the Head of IT, includes representatives from IT, IS&DP, Customer Success, and Compliance.
- **Learning Platforms DevOps**: Responsible for technical recovery actions, system monitoring, and backups.
- **Customer Support Team**: Handle customer communications and support during disruptions.
- **Compliance Officer**: Ensure adherence to regulatory requirements and documentation.

Conclusion

This BCDR plan is designed to ensure the resilience and quick recovery of Totara LMS managed services in the EMEA region. Regular testing, clear communication, and robust cybersecurity measures are critical components to achieving these goals

Discover how we're shaping the future of learning

Everything we do at Kineo stems from a simple idea – if we design a better learning experience, together we'll get better results.

Kineo helps the world's leading businesses improve performance through learning and technology. We're proud of our reputation for being flexible and innovative, and of our award-winning work with clients across the world

Whatever your business challenge, we will partner with you every step of the way to find the learning solution that fits best – and delivers results.

So, how can we help you?
Get in touch about your digital learning challenges

Kineo UK
info@kineo.com
+44 (0)1 273 764 070

Kineo USA
usinfo@kineo.com
+1-312-846-6656

Kineo APAC
hello@kineo.com.au
1300 303 318

www.kineo.com