

APAC Business Continuity & Disaster Recovery

UPDATED MARCH 2025 - VERSION 1.2



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.



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.



Intended Audience

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

Kineo staff seeking guidance on business continuity

Clients and prospective clients evaluating Kineo as a service provider, and

Clients raising a specific issue in relation to Kineo's business continuity.





Definitions

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

Hosted Learning Platforms
which consists of the
following core applications:

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

These services are referred to as the Hosted Learning Platforms.



Policy Statement

Corporate management has approved the following policy statement:

The company shall develop a comprehensive IT 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:

The need to ensure that all employees fully understand their duties in implementing such a plan.

The need to ensure that operational policies are adhered to within all planned activities. The need

to ensure that proposed contingency arrangements are cost-effective.

The need to consider implications on other company sites.

Disaster recovery capabilities as applicable to key customers, vendors and others.



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 links:

[Azure compliance documentation](#)

[Microsoft Azure Compliance and Australian Security and Privacy](#)

[Requirements Microsoft Azure Compliance in the context of New Zealand](#)



Regions and Availability Zones

Microsoft Azure offer hosting in multiple locations world-wide, known as regions. To date, Kineo has deployed its hosted Learning Platforms in just one region across Australia and New Zealand but is able to offer hosting in any supported region. All data collected and processed from the Kineo application is retained within the Australian region selected for deployment.

Each Microsoft Azure region is completely isolated from other Microsoft Azure regions, and within each Azure region there are multiple, isolated locations known as **Availability Zones**.

Microsoft Azure provides Kineo with the ability to place resources, such as instances (servers), and data in multiple locations within that region ensuring the highest level of fail over and redundancy in the situation of a disaster.

The **Availability Zones** in each region are connected through low-latency links. Kineo is able to use both the separation of Regions and **Availability Zones** within Azure regions to maintain data protection, and implement both disaster recovery and backup.



Instances

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



Horizontal Scaling

Horizontal scaling is the process of adding more nodes to a system, such as adding a new server to a distributed software application. Kineo uses horizontal scaling to extend its platform by adding additional instances across regions where required to meet its business requirements, but important to meet usage demands.



Vertical Scaling

Vertical scaling means to add more resources to a single node within a system, such as increasing the CPU or memory requirements for a single server. Vertical scaling is used by Kineo to increase performance to align with forecast user traffic, and manage performance of its application when under load.

Vertical scaling is the process of increasing the instance type (hardware performance) for each instance on Azure. Kineo uses a variety of instance types depending on the purpose and requirements for the application or software that is run on the instance.



Kineo Learning Platforms

Hosted Learning Platforms consists of the following virtualised servers:

- Production
- Sandbox
- Backup
- Monitoring



Production

This is the cluster of production servers which host the application, files and database. All user traffic is directed to the platform hosted on these servers.

The production cluster is divided into four tiers:

Front End Web Servers	Front end web servers deliver the Totara Learn application to the user.
Database	Platform uses Azure managed database platform to host the database, which provides scalability, redundancy and to-the-minute backups. All database data is encrypted at rest.
Sandbox	This instance is accessible to Kineo clients to conduct functional and integration development and testing, which is separate from their production (live) environment.
Recovery Services Vault	Front end web servers deliver the Totara Learn application to the user. The recovery services vault is responsible for coordinating and storing all backups for the application, files and database and synchronously maintains three locally redundant storage (LRS) copies of the data within a single physical location in the primary region. The Recovery Services Vault is hosted in a separate Availability Zone to Kineo Learning Platforms servers to ensure that the backups of customer data are logically and physically separate from production data and can be accessed in the case of a disaster in another Availability Zone.



Monitoring

This instance is used by Kineo to host our internal monitoring and logging systems. Metrics logged include:

Application access logs

Application uptime, and

Platform performance and utilisation statistics.



Application

This section details information about the following:

- Password security
- Encryption, and
- Data storage.

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.

Encryption

The application uses https (SSL) to encrypt all data between the application and the user's browser.

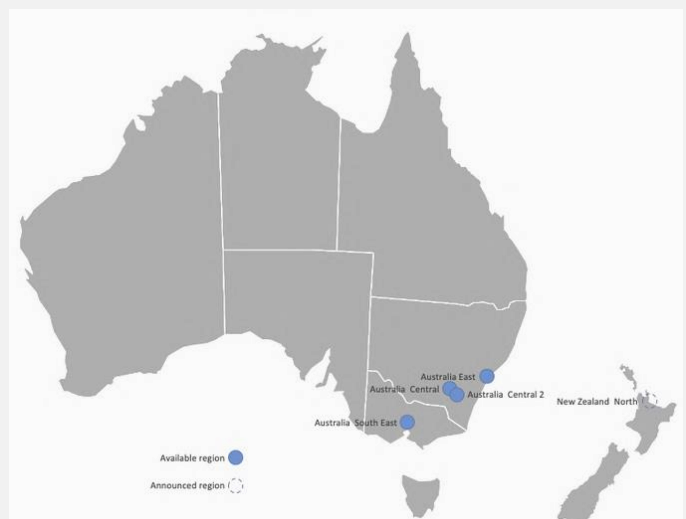
Data Storage

All data collected by the application is stored within each geographic region, as indicated in the agreement.

- For Australia, this is Microsoft's Australia Azure East region
 - Kineo will extend storage to New Zealand North once available
-

All databases and database backups are encrypted at rest.

To provide a range of restore point options, backups are retained for 30 days.





APAC Hosted Kineo Platforms

All clients and users located within Australasia, particularly in Australia and New Zealand are serviced from Microsoft's Australia Azure East region and uses availability zones in this region. The Azure East region hosts all Kineo Learning Platforms and provides storage for backups.

Hosting will also be offered from New Zealand North once made available.

On request Kineo can host and store client data in any Microsoft Azure supported region.



Backup

Backup is an important aspect of Kineo's Hosted Learning Platforms, and Kineo have implemented a multi-facet backup solution.

Full backups

Full backups of each instance are taken once each week.

Incremental backups

Incremental backups of each instance are taken twice each day.
Backups include the following elements:

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

Transaction log backups

A transaction log backup is taken every five minutes. Backups are encrypted at rest and retained for 30 days.



Disaster Recovery

In the unlikely case of a disaster Kineo has implemented a multi staged disaster recovery process.

Using backups created each day / week 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 up to 2 hours for Web VM.
- The expected recovery time objective (RTO) is up to 20 hours for Database.

Stage 1

- 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.

Stage 2 (needs to be costed)

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.

- The expected recovery time objective (RTO) is up to 2 hours for Web VM.
- The expected recovery time objective (RTO) is up to 20 hours 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.



Disaster Recovery Process

In the event of a significant server failure, Kineo will take the following steps to address the issue:

Conduct an immediate assessment of the problem

Identify an action plan and develop initial estimate for the rectification

Send communication and an estimated time of rectification to affected client contacts

Implement the action plan. Depending on the circumstance this could include:

- Creating a new server from the most recent **full backup** of the server that has failed
 - Overlay the most recent **incremental backup** to provide a RPO of 12 hours
 - Undertake system testing using random user accounts with differing user permissions and completing common operational procedures
 - Re-delegate domains
-

When there is a change to the circumstances, Kineo will provide communication update to the client contacts detailing the change.

Where domain re-delegation is required, there may be a 12 to 24-hour delay between restoration of system functionality and the system becoming available via the Internet, due to the delay in DNS.



Disaster Recovery Testing & Validation

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

Daily

Monitor and review the backup log for any failures

Quarterly

Stage 1 disaster recovery is tested. The recovery process is tested by:

- 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
-

Yearly

Stage 2 disaster recovery is tested. The recovery process is tested by:

- A new simulated Production instance of the application is built from backup in order to test the processes and procedures that is required to rebuild the application and infrastructure in case of a disaster
-