# Assignment 3: Disaster Recovery Plan for Unicorn Universal Software

INFOSYS 727 Group Member: Long Liang, Jiangbo Yan.

## ****1 Authorization****

### ****Policies and Administrative Regulation****

### This plan is formulated in accordance with New Zealand's Privacy Act 2020, with the aim of ensuring that customer data can also be recovered and protected after cyber attacks.

### 1.2 Objectives

### The objective of this plan is to ensure that UUS's software development process can be quickly restored in the event of data leakage or other major cyber attacks, that customer data can be securely protected, that customer trust can be maintained, and that legal risks and economic losses can be reduced

## ****2 Services and Their Priorities****

### ****2.1 Services List****

### Azure DevOps: Managing software development processes.

### Azure Database: Storing customer data.

### VPN and Firewall: Protecting internal networks.

### Microsoft Sentinel: Basic monitoring and notification.

### Microsoft Purview: Data classification and protection.

### Azure Backup: Data backup and recovery.

### ****2.2 Assess Impact of Service Outage****

### • DevOps unavailable: Affects project development progress.

### • Database lost connection: Official website and customer operations cannot be carried out.

### • VPN/Firewall failed: Internal data is at risk.

### ****2.3 Assess Risks**** • Azure configuration error.

### • Third-party server vulnerability.

### • Sentinel not configured correctly, unable to perform quick notifications.

### • Microsoft Purview configuration error, leading to failure in data classification and protection of sensitive client data.

### ****2.4 Prioritize****

Priority division is based on RTO/RPO values:

• Prio 1: Network protection and database.

• Prio 2: DevOps and development tools.

• Prio 3: Monitoring and post-processing services.

### ****2.5 Set Scope****

This plan basically includes, in accordance with priorities:

• Azure SQL Database

• VPN/ Firewall

• DevOps

## ****3 Facility and Infrastructure Plan****

### ****3.1 Determining technical approach for each service****

• Azure Database: Establish geo-redundant backup + read replica.

• DevOps: Equip backup resources and scripts to restore projects.

• VPN/ Firewall: Establish backup configuration + separate network cache charging.

### ****3.2 Facility Plan****

It is recommended to choose an Azure area that is geographically separated from the main data center and is equipped with an environment that has sufficient power, network, and security.

### ****3.3 Infrastructure Plan****

The infrastructure of UUS includes network, storage, access control and remote connection services.

• Azure Availability Zones: To ensure high availability and fault tolerance, the infrastructure will utilize Azure Availability Zones. By distributing resources across multiple physically separate zones within a region, the system can withstand data center-level failures without service interruption.

• Local Network (LAN) : Pre-configure switches and core routing devices in the standby data center, and use automated scripts to complete IP allocation and network policy deployment.

• Wide Area Network (WAN) : Establish alternative links with alternative ISPs and achieve automatic failover through BGP or VPN.

• Servers and Storage: All critical services (such as DevOps platforms and databases) are set up in a mirror environment in the cloud, and data is regularly synchronized from the master node.

• Remote access and security devices: The backup VPN gateway and firewall rules are predefined and can be automatically switched within one hour after the primary service fails.

• Fault Monitoring: With the help of Microsoft Sentinel, monitor the logs and recovery process, and report anomalies through the alarm system.