VICTORIA POLYTECHNIC
TAFE DIVISION OF VICTORIA UNIVERSITY

Appendix 1 – Initial Sign-Off Form

SERVER INFRASTRUCTURE CYBER SECURITY PROJECT

Team Name: SecureNET

TEAM MEMBERS (Name and Student Number):

		Hettige Jayatissa	Project Owner
S3113490	-	Giuseppe Raciti	Project Manager
S8061631	-	Shaun Heywood	Cyber Security Specialist
S8063543	-	Mark Byrne	Cloud Architect / Engineer
S8062754	-	Mauricio Guerra	Server Administrator

Project Plan Details

This project plan outlines the steps and activities required to secure OzCazual's cloud infrastructure and enable a safe and secure migration from their existing local server. The objective is to address the sudden increase in online sales, scale the infrastructure to meet business demands, and ensure the confidentiality, integrity, and availability of the systems and customer data. Our team of Cyber Security specialists will be responsible for implementing robust security measures in the cloud environment.

Securing Servers – The following tools will be used to secure the server:

On the Windows 2022 Server, we intend to install the following security and monitoring software:

- **Firewall –** pfSense and/or Windows Defender
- **IPD/IDS –** Snort
- **Anti-virus/malware –** Sophos – (backup ClamAV)
- **Log Monitoring and Analysis –** Splunk
- **Real-time Monitoring –** Wireshark

On the Linux Web server,

- **Firewall –** Sophos
- **IPD/IDS –** Snort
- **Anti-virus/malware –** Sophos Intercept X
- **Log Monitoring and Analysis –** Splunk
- **Real-time Monitoring –** Wireshark

As part of the process of securing the network infrastructure, our cyber experts will run external scans of the Windows and webserver, using a free open-source program called Infection Monkey, we intend to run automatic attack simulations that scan for vulnerabilities such as credential theft, misconfiguration, compromised assets, etc

During the final phase of the project, we will conduct red team / blue team exercises, to expose vulnerabilities on the Windows and Webserver systems.

We are considering using the following attack methods to test the security of the AWS environment:

1. Denial of Service attack (DDoS)
2. Brute force Attack (SSH)
3. Virus/Malware Protection

By completing all the above, SecureNET can ensure that the cloud infrastructure is secure and ready for release. Before the project is handed over to OzCazual, SecureNET will assure that all technical documents are signed off and handed over to the owner upon releasing the project.

Proposed project plan is hereby accepted by the Project Owner

Name: ___________________________________

Signature: ________________________________ Date: ____________________________________