| **QUALITY MANAGEMENT PLAN** | | | | | |
| --- | --- | --- | --- | --- | --- |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | | **18th of June, 2023** |
|  |  |  |  | |  |
| Prepared By: | **Shaun Heywood** |  | Project Sponsor: | **OzCazual** | |

| **Quality Standards** | | | | | |
| --- | --- | --- | --- | --- | --- |
| Setting quality standards establishes benchmarks or requirements that specify the level of excellence or suitability expected for the project. For the SecureNET AWS CyberShift Initiative project, the following quality standards apply: | | | | | |

### **Security Standards:**

To guarantee the privacy, accuracy, and accessibility of data and systems, compliance with relevant security frameworks is required, such as the ISO 27001 standard and the SANS Cybersecurity Framework.

SecureNET will also look at the implementation of secure network settings, encryption techniques, and access control measures, while placing an emphasis on the adherence to industry best practices for detecting and reducing security risks and vulnerabilities.

### **Compliance Standards:**

### SecureNET will implement compliance with relevant legal and regulatory standards, including industry-specific rules and regulations and data protection laws (such as GDPR and CCPA). Additionally, the project will adhere to relevant compliance frameworks, such as PCI-DSS for e-commerce environments' payment card data security.

### **Performance Standards:**

### SecureNET will ensure the system meets the expected performance levels, including response times, throughput, and scalability, to handle the increased online sales and staff.

### The project will adhere to a service level agreement (SLA) for uptime, availability, and reliability of the AWS cloud infrastructure.

| **Usability and User Experience Standards for Data Migration to the Cloud** | | | | | |
| --- | --- | --- | --- | --- | --- |

**User-friendly Interfaces:**

Designing user-friendly and simple interfaces will be an important step to improve the user experience while moving servers and data to the cloud. These user interfaces will make it simple for users to move around as they carry out necessary tasks. To ensure a smooth and user-friendly experience during the migration process, clear and simple instructions will be available to required users.  
  
**Consistent Branding and Design:**

Maintaining similar branding components, such as logos, colours, and typography, across the cloud-based server and data management interfaces is crucial to establishing a unified and recognisable brand identity during the transfer of servers and data to the cloud.   
  
By using a visually cohesive design that complements the on-premises systems' current branding, users may readily recognise and relate to the well-known brand identity encouraging a feeling of familiarity and trust.

| **Cross-Device and Cross-Browser Compatibility** | | | | | |
| --- | --- | --- | --- | --- | --- |

SecureNET will optimize the AWS cloud-based management interfaces to work seamlessly across different devices, such as desktops, laptops, tablets, and mobile phones, whilst also ensuring compatibility with various web browsers, including popular ones like Chrome, Firefox, Safari, and Edge.

Furthermore, SecureNET will conduct thorough testing on different devices and browsers to ensure consistent functionality and user experience.

| **Data Integrity and Accuracy Standards** | | | | | |
| --- | --- | --- | --- | --- | --- |

SecureNET will make sure that data is accurately and reliably transferred, stored, and processed throughout the migration process, by putting in place suitable error management and data validation systems, and preserving data consistency and integrity throughout the cloud environment.

| **Testing and Quality Assurance Standards** | | | | | |
| --- | --- | --- | --- | --- | --- |

SecureNET will adhere to best practices for testing, such as those set forth by the ISTQB (International Software Testing Qualifications Board).

We will be putting into practise solid test strategies, test procedures, and test scripts to validate the performance, security, and functionality of cloud infrastructure and apps, whilst also testing effectiveness and efficiency through the use of automated testing tools and procedures, and conducting red team, blue team penetration testing.

| **Documentation Standards** | | | | | |
| --- | --- | --- | --- | --- | --- |

SecureNET will provide clear and concise documentation of design requirements, configuration information, test schedules, and incident response processes. Processes for managing change will be well-documented, such as records of change requests, impact analyses, and implementation.

Additionally, SecureNET will provide documentation that demonstrates compliance, such as data processing agreements, permission papers, and privacy policies

By adhering to these usability and user experience standards, the migration process from on-premises servers to the cloud ensures that users can easily navigate the interfaces, experience consistent branding, and access the systems across different devices and browsers. Additionally, these quality standards offer a framework to make sure that the project deliverables and procedures adhere to industry best practices, satisfy the needs and expectations of the stakeholders, and are of the intended level of quality. Following these guidelines promotes reliability, confidence, and trust in the cloud migration effort.

| **Data Integrity and Accuracy Standards:** | | | | | |
| --- | --- | --- | --- | --- | --- |

### SecureNET will ensure the accurate and reliable transfer, storage, and processing of data during the migration process, as well as implement appropriate data validation mechanisms and error handling procedures.

| **Quality Objectives** | | | | | |
| --- | --- | --- | --- | --- | --- |
| These measures help evaluate the achievement of the corresponding quality objectives and provide quantifiable data or assessments to determine the effectiveness and success of the project in meeting these objectives. | | | | | |

| **Metric or Specification** | **Measure** |
| --- | --- |
| **1.Design & Implementation** | **1.** Evaluate the design documents, configuration specifications, and migration plan to confirm their accuracy, and adherence to industry best practices and standards. |
| **2. Robust Security Measures** | **2.** Perform security assessments, including red team blue team penetration testing, vulnerability scanning, and risk assessments, in order to identify, mitigate and rectify any security vulnerabilities or weaknesses in the cloud environment.   This measure will also cover monitoring access controls, encryption mechanisms, authentication, and authorization mechanisms for their effectiveness and compliance with security standards. |
| **3.Seamless migration** | **3.** SecureNET will prioritise minimising downtime and disruption to normal business operations during the migration process. The metric can be measured by keeping note of how long the migration took, how many problems or disruptions occurred, and how satisfied users were with the migration process. |
| **4.Compliance** | **4.** During the AWS cyberShift Initiative, SecureNET will provide regular audits and assessments to verify adherence to relevant compliance regulations and industry standards.   As part of this, compliance procedures must be documented, internal and external audits must be carried out, and any compliance gaps must be addressed and rectified. |
| **5. Data Confidentiality, Integrity, and Availability** | **5.** To maintain the privacy, availability, and integrity of data, regular monitoring of data access logs, encryption methods, and backup and recovery procedures are necessary.   Verifying the accuracy of data backups, recording incidents linked to data breaches or unauthorised access, and evaluating the system's capacity to recover data in the event of a failure or disaster are measures that SecureNET will have in place. |

| **Quality Roles and Responsibilities** | | | | | |
| --- | --- | --- | --- | --- | --- |

| **Roles** | **Responsibilities** |
| --- | --- |
| **Project Owner** -  Hettige Jayatissa | * Defines the project objectives * Provide project direction and guidance * Manage project stakeholders * Approve project deliverables * Make decisions and resolve issues * Manage project constraints * Ensure project success * Participate in project governance * Act as a liaison between the project team and senior management |
| **Project Manager** -  Giuseppe Raciti | * Overall project coordination and management * Plan, organize, and control project activities * Ensures project deliverables are completed on time and within budget * Risk management and mitigation * Stakeholder Communication and Reporting |
| **Cyber Security Specialist** -  Shaun Heywood | * Conduct assessments of the existing infrastructure * Design and implement security measures for the cloud infrastructure * Configure and manage firewalls, IPS/IDS systems, and antivirus/malware protection * Oversee testing and incident response * Monitor and analyze logs for potential security threats or breaches * Provide guidance on security best practices * Collaborate with the project team to address security vulnerabilities and risks |
| **Cloud Architect / Engineer** -  Mark Byrne | * Designing and configuring the cloud infrastructure on Amazon AWS * Setting up network connectivity with on-site systems * Ensuring scalability and high availability of the cloud environment * Collaborating with the Cyber Security Specialist to implement security measures * Monitoring and optimizing cloud infrastructure performance * Providing technical expertise on cloud architecture and services |
| **Server Administrator** - Mauricio Guerra | * Collaborating with the project team to ensure a secure transition to AWS * Assisting in the migration of systems and data to the cloud environment * Configuring and managing the Windows Server 2019 Active Directory server * Supporting the setup and configuration of the Amazon Linux 2 web server * Providing technical assistance during the transition phase * Ensuring the smooth operation of the server infrastructure in the cloud environment |

| **Deliverables and Processes Subject to Quality Review** | | | | | |
| --- | --- | --- | --- | --- | --- |

The following deliverables undergo a quality review to ensure they meet the specified quality standards and requirements. In the context of the SecureNET AWS CyberShift Initiative project, the following deliverables and processes are subject to quality review:

| **Deliverables** | **Processes** |
| --- | --- |
| **Design and Implementation Documentation** | * Documents used in the creation of the safe Amazon AWS cloud environment * Configuration guidelines for servers, network infrastructure, and security measures. * A thorough migration plan outlining the procedures and due dates for moving Active Directory and the online store. |
| **Security Measures and Controls:** | * Configure protocols for user authentication and authorisation * Provide mechanisms for both data in transit and data at rest being encrypted. * Implement Firewalls and intrusion detection and prevention systems (IDPS). * Create procedures for handling security incidents. |
| **Testing and Validation:** | * Test and validate the AWS cloud infrastructure for functionality, performance and security. * Gather results from vulnerability testing and penetration testing * Validate data migration and data integrity |
| **Compliance:** | * Provide documentation to demonstrate compliance with relevant regulations and data protection and privacy laws * Document adherence to industry standards such as Iso 27001 – Information Security Management * Provide audit reports and compliance assessments. |
| **Incident Response Plan:** | * Provide an incident response plan stating the processes to be followed in case of a security issue. * Document records of security occurrences, including as logs, reports, and post-incident analyses. * Document proof of incident identification, reaction, containment, and resolution. |
| **Change Management:** | * Documentation of change requests, including change descriptions, justifications, and impact assessments. * Change implementation plans and records of change execution. * Reviews and approvals of changes by the appropriate stakeholders. |

| **Quality Management Approach** | | | | | |
| --- | --- | --- | --- | --- | --- |

The migration of OzCasual's e-commerce website and Active Directory to the Amazon AWS cloud environment is ensured to achieve the stated quality objectives due to the quality management strategy for the SecureNET AWS CyberShift Initiative project.  
  
The strategy entails planning, establishing quality goals, carrying out activities for quality assurance and control, documenting and reporting, managing risks, and pursuing continuous improvement. At appropriate checkpoints throughout the AWS CyberShift Initiative, project and product quality audits are planned to evaluate adherence to quality standards and criteria, track development, and pinpoint opportunities for improvement.

These audits help to guarantee that the migration process is in line with the established quality objectives and offer insightful information about the project's quality state.

| **Quality Control Approach** | | | | | |
| --- | --- | --- | --- | --- | --- |

The quality management approach includes testing and verification procedures to identify and resolve any quality issues in the cloud environment. This is achieved by conducting regular testing, to ensure the proper operation, performance, and security of the system.

SecureNET will implement continuous monitoring techniques to track system activity, security incidents, and compliance. Incident response procedures are regularly tested through drills and exercises to ensure their effectiveness in identifying, addressing, and mitigating security incidents.

Finally, a robust change management procedure will be implemented to carefully examine the impact of any changes made to the cloud environment, for both quality and security, ensuring thorough evaluation and risk assessment.

| **Applicable Quality Procedures** | | | | | |
| --- | --- | --- | --- | --- | --- |

The quality management strategy includes routine audits and inspections to make sure that security standards, design principles, and best practices are being followed. To ensure quality and accuracy, project documentation, design specifications, security configurations, and other deliverables are thoroughly reviewed.   
  
To find and fix any problems or vulnerabilities in the cloud infrastructure, security protocols, and data migration process, testing and validation activities will be carried out. To ensure adherence to pertinent compliance laws and best practices, routine reviews and audits will be carried out. These steps aid in upholding specified standards to a high degree of quality throughout the project.