Task 2 Quality Requirements(USU Operating System)

Introduction

The functional prerequisite USU Officers may plan regional and national events by creating, editing, promoting, cancelling, and coordinating event information within the federated student union network with the use of FR-USU-2 (Management of USU Events).

The following quality standards specify how effectively the event management subsystem must function in order to guarantee that this capability is operationally resilient. In a real-world federation context, these standards guarantee dependability, performance, usability, security, and accountability.

Reliability and Availability

- The event module should maintain a minimum uptime of 99.95% annually, to avoid service interruptions during critical event periods.
- Data associated with events shall be automatically replicated and backed up in real time across at least two geographically separated data centres, preserving consistency and continuity in case of infrastructure failure.
- In the event of a system outage or critical failure affecting the event subsystem, recovery to fully operational status must occur within six hours, ensuring minimal disruption to the union network.

Performance and Responsiveness

- The subsystem shall support up to 1,000 concurrent event-related operations (e.g., event creation, updates, registrations) without degradation in responsiveness.
- The average interface response time (e.g., loading the event dashboard, rendering event details) should be ≤ 3 seconds, in line with usability expectations for interactive systems (Nielsen Norman Group, 2023).
- When an event is updated (e.g., location change, date change), the system is required to propagate the update to all relevant student and union interfaces within 10 seconds, ensuring near real-time synchronization.

Usability and Accessibility

- The USU-OS event management interface must conform to WCAG 2.1 Level AA accessibility standards, ensuring that users with disabilities can effectively manage events (W3C, 2018).
- The design of the event dashboard should feature clear visual status indicators (e.g., pending, active, archived) and intuitive controls, reducing cognitive load for USU

Officers.

- Training for a new officer to competently use the event management feature should not exceed two hours, reflecting a high degree of system learnability.

Security and Data Protection

- Access to event management operations (creation, editing, cancellation) shall be limited to authorised USU Officers via role-based access control (RBAC) mechanisms.
- All event data, including updates and participant lists, must be encrypted both in transit and at rest using strong cryptographic protocols (e.g., AES-256).
- The event module shall undergo quarterly vulnerability scans and annual penetration testing to detect and remediate security weaknesses, aligning with recommended cybersecurity best practices (ENISA, 2024).

Compliance and Auditability

- The system is required to comply fully with UK GDPR and the Data Protection Act 2018 in all processing of personal data related to events, registrations, and communications.
- All officer actions within the event management module (e.g., create, modify, cancel) should be logged, retaining records for a minimum of five years to support audit and oversight.
- Audit logs must be tamper-resistant and exportable in standard formats (e.g., JSON, CSV) to facilitate internal or external review.

References (Harvard Style – Web Sources)

- Microsoft (2023) *Best practices for building reliable, scalable, and secure cloud applications*. Available at: https://learn.microsoft.com/en-us/azure/architecture/best-practices/index-best-practices
- Nielsen Norman Group (2023) *Response time limits: Usability guidelines*. Available at: https://www.nngroup.com/articles/response-times-3-important-limits/
- W3C (2018) *Web Content Accessibility Guidelines (WCAG) 2.1*. Available at: https://www.w3.org/TR/WCAG21/
- ENISA (2024) *Best Practices for Cyber Crisis Management*. Available at: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management