Contents

ANNEX B: NON-FUNCTIONAL REQUIREMENTS

1. GENERAL

1.1. Cloud Service

1.1.1. The cloud service is Multi-Tier Cloud Security ("**MTCS**") Certified and adheres to Cloud Security Alliance ("**CSA**") Open Certification Framework.

1.1.2. The Supplier shall provide any other information requested by The University for the assessment of the System proposed, e.g. primary and secondary data locations of the cloud service.

1.2. Environment

1.2.1. The Supplier shall propose and provide details for the system architecture and the type of environments (e.g. Development, User Acceptance Test, Production) and the respective integration points with other University applications (both cloud and on-premise).

1.2.2. The Supplier shall provide a technical specifications document which describes all of the system software and tools necessary for each of the environments proposed.

1.3. Integration

1.3.1. The System shall support interfaces to University's existing systems as listed in the ITQ **Section 1 Requirement Specifications, Paragraph 2. SCOPE OF WORKS.**

1.3.2. The Supplier shall provide the scope, method or tools used for batch or real-time interfaces used within the System.

1.3.3. The Supplier shall provide network and architecture diagram that covers the integration points from cloud to on-premise and any 3rd party solutions to achieve a secure and scalable integration.

1.3.4. The Supplier shall provide end-to-end automated integration which does not require end users to manually upload and download files or vice versa.

1.3.5. The Supplier shall provide a comprehensive list of APIs and web-services with details that are available as standard out-of-the-box for University's consideration.

1.4. Change Control Management

1.4.1. External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the Supplier (e.g. ITIL service management processes).

1.4.2. The Supplier shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.

1.4.3. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer, and/or authorisation by, the customer as per agreement (SLA) prior to deployment.

1.4.4. The Supplier shall provide the SLA for patch management and release management

1.5. Applications

1.5.1. The Supplier shall use open and published Application Programming Interface (API)s to ensure support for interoperability between components and to facilitate migrating applications.

1.5.2. All structured and unstructured data shall be available to University and provided to University upon request in an industry-standard format (e.g. .docx, .xlsx, .pdf, and flat files).

1.5.3. The Supplier shall provide advance notice in writing to University for any maintenance activities to be performed on the System, i.e. minimally two (2) weeks' notice.

2. SECURITY

2.1. General Security

2.1.1. The Supplier shall ensure and show proof that the solution is designed and coded using industry's security best practices and implemented in a secure manner with proper input and output validation, such that the solution is secure and robust, and not affected by known vulnerabilities.

2.1.2. The Supplier shall ensure and show proof that all applications / software (including client-side scripts, applets, etc.) developed by the awarded vendor follow secure software development lifecycle practices and are free of malicious codes or unauthorised codes, adequately tested, reviewed, and approved before deploying. Failing which, the awarded vendor shall be responsible and shall make good all data loss, cost of downtime and rectification.

2.1.3. NTU shall reserve the right to audit full section of non-functional security requirements.

2.1.4. The Supplier shall engage a qualified information security consultant in architecting, reviewing and presenting the solution proposal to NTU.

2.1.5. The Supplier shall ensure Solution is protected against Advance Persistent Threat.

2.2. Information Handling

2.2.1. The Supplier shall protect and safeguard all information that is entrusted to it and ensure that such information is not used for other purposes unless authorised in writing by

University. The Supplier shall also ensure that any personnel of the Supplier shall protect and safeguard all information that is entrusted to him/her.

2.2.2. In the event the Supplier requires any information to be sent to a 3rd party, e.g. product principal, the Supplier shall seek the prior written approval of University before releasing the information.

2.2.3. Termination or expiry of this Contract for whatever cause shall not put an end to the obligation of confidentiality imposed on the Supplier, its employees, agents and/or Sub-contractors under this Clause.

2.2.4. The Supplier shall sanitise the information to remove any classified information and shall obtain University's written approval before releasing the sanitised information. For the avoidance of doubt, the Supplier shall note that the declassification of information does not amount to University's approval for its disclosure. The Supplier shall request written approval for the disclosure of declassified information of University to any third party.

2.2.5. The Supplier shall implement and document all necessary measures and processes to protect information against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use, or modification. The documentation shall include administrative, technical, physical and personnel control measures, and shall be submitted to University for written approval. The documentation shall be made immediately available when required by University.

2.2.6. If the Supplier suspects or detects any loss of information and unauthorised access, the Supplier shall notify University immediately in writing. The Supplier shall take preventive measures to prevent further loss of information and perform investigations to ascertain the root cause of the loss of information. The Supplier shall take instructions from University for any further actions that may be required.

2.2.7. The Supplier shall ensure that all applications/software (including client-side scripts, applets etc.) proposed/used by the System do not cache any credentials.

2.2.8. If the System stores, processes or transmits cardholder data and/or sensitive authentication data, the System shall ensure compliance to the Payment Card Industry Data Security Standard ("**PCI DSS**"). The Supplier shall provide a copy of the Attestation of Compliance ("**AOC**") issued by a Qualified Security Assessor ("**QSA**") to University on an annual basis.

2.2.9. The Supplier shall provide a Statement on Standards for Attestation Engagements ("**SSAE**") 18 – Service Organization Control ("**SOC**") 1 and 2 report to University on an annual basis.

2.3. Data Protection

2.3.1. The Supplier shall document and maintain data flows for data that is resident within the geographically distributed applications, infrastructure network and systems components.

2.3.2. Data that traverses public networks shall be appropriately protected from fraudulent activity, unauthorised disclosure, or modification in such a manner as to prevent contract dispute and compromise of data.

2.3.3. Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from University.

2.3.4. The Supplier shall have necessary process and tool in place to ensure that deleted data or sensitive software is properly deleted and cannot be recovered by unauthorised personnel. Secure erasure of data and disposal of media shall meet industry media sanitization standards such as National Institute of Standards and Technology (NIST) Special Publication 800-88 'Guidelines for Media Sanitization'.

2.4. Cryptography and Standards

2.4.1. The Supplier shall ensure that all data transmissions on the System and end users are encrypted; the Supplier shall also ensure that all sensitive information is encrypted in storage, in use and in transmission.

2.4.2. The Supplier shall ensure that cryptographic mechanisms implemented in the System are capable of handling the expected peak loads without degrading the system performance.

2.4.3. The Supplier shall ensure that the cryptographic algorithms used are well established open standards and which have been subjected to rigorous scrutiny by an international community of cryptographers, or approved by authoritative professional bodies, reputable security contractors or government agencies which minimally meet the following cryptography standard unless otherwise approved in writing by University:

(a) Symmetric Encryption and Key Wrappings
    (i) Advanced Encryption Standard (AES) with key sizes of 256 bits (NIST FIPS 197).

(b) Asymmetric Encryption
    (i) RSA Public-key Cryptography with key lengths of at least 2048 bits; or
    (ii) Elliptic Curve Cryptography Standard with key lengths of at least 256 bits (using curves over prime fields such as P-256, P-384, P-521 or equivalent).

(c) Digital Signature Generation and Verification (NIST FIPS 186-4)
    (i) RSA Signature with key sizes of at least 2048 bits;
    (ii) Digital Signature Algorithm (DSA) Signature with key lengths of at least 2048 bits (parameter p of at least 2048 bits and parameter q of at least 224 bits); or

(iii) Elliptic Curve Digital Signature Algorithm (ECDSA) with key lengths of at least 256 bits (using curves over prime fields such as P-256, P-384, P521 or equivalent).

(d) Hash Algorithm for non-digital signature generation applications (NIST FIPS 180-4 and FIPS 202)
  (i) SHA-2 (SHA-256, SHA-384, SHA-512); or
  (ii) SHA-3.

(e) Key Exchange in accordance to NIST SP800-56A Rev 2, SP800-56B, and SP800-135
  (i) Elliptic Curve Diffie-Hellman (ECDH) supporting curves over prime fields such as P-256, P-384, P-521 or equivalent;
  (ii) Finite Field Diffie-Hellman (FFDH) with parameter p of at least 2048 bits and parameter q of at least 224 bits; or
  (iii) RSA Key Agreement using RSA key pair with key lengths of at least 2048 bits.

(f) Random Number Generation
  (i) Random Number Generators (RNGs) as specified in NIST FIPS 186-4; or
  (ii) Random Bit Generators (RBGs) as specified in NIST SP800-90A (excluding Dual_EC_DRBG).

(g) Message Authentication Codes (MACs)
  (i) HMAC in accordance to NIST FIPS 198-1 and SP800-107 using a Hash Algorithm as specified in Clause 2.6.3 (c)(d)with at least 128-bit security (provided by SHA-256 and above);
  (ii) CMAC in accordance to NIST SP800-38B using a Symmetric Encryption Algorithm as specified in Clause 2.6.3 (c)(i);
  (iii) CCM and GCM/GMAC in accordance to NIST SP800-38C and SP80038D using AES.

2.4.4. The Supplier shall ensure that the digital certificate implemented shall minimally meet the following standard unless otherwise approved by The University.

(a) Hash Function for Digital Certificate and CRL (NIST FIPS 180-4 and FIPS 202); and
  (i) SHA-2 (SHA-256, SHA-384, or SHA-512); or
  (ii) SHA-3.

(b) Key Length.
  (i) RSA Public Key Encryption with key sizes of at least 2048 bits.
  (ii) Elliptic Curve Cryptography Standard with key sizes of at least 256 bits (supporting P-256, P-384, P-521 curves or better).

(c) The Supplier shall comply with the X.509 v3 standards for the implementation of digital certificate and certificate revocation lists.

2.4.5. The Supplier shall ensure that the authentication implemented shall minimally meet the following standard unless otherwise approved in writing by University:

(a) Kerberos, RADIUS, TACACS+, SAML 2.0 or above, LDAP or LDAPS Authentication for Windows-based systems, or for systems supporting Windows applications;
(b) Transport Layer Security (TLS) version 1.2 or above for certificate-based mutual authentication;
(c) Software-based token using Time-based One-time Password Algorithm (TOTP) as specified in RFC 6238 or HMAC-based One-time Password Algorithm HOPT) as specified in RFC 4226;
(d) EAP-TLS (RFC 5216) or EAP-IKEv2 (RFC 5106) for Challenge-Handshake based authentication;
(e) TLSv1.2 or above for HTTPS form-based authentication; or
(f) SAML 2.0 or above for websites or web application authentication and authorization.

2.4.6. The Supplier shall ensure that the access implemented shall minimally meet the following standard unless otherwise approved in writing by University:
(a) Use TLSv1.2 or above for web browser access;
(b) OAuth 2.0 or above for websites or web application access delegation;
(c) Use secure custom client application with cryptographic algorithms.

2.4.7. If virtual private network (VPN) is implemented, the Supplier shall ensure that the VPN shall minimally meet the following standard unless otherwise approved in writing by University:
(a) Supports Perfect Forward Secrecy;
(b) Use TLSv1.2 or above for SSL VPN;
(c) IPsec-v3 [IKEv2 (RFC 7296), IP Encapsulating Security Payload (RFC 4303)]

2.5. Encryption Key Management

2.5.1. Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.

2.5.2. The Supplier shall implement procedures for the lifecycle management of cryptographic keys from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for the use of encryption protocols for protection of sensitive data in storage, data in use, and data in transmission.

2.5.3. Keys shall be maintained by University or trusted key management provider. Key management and key usage shall be separated duties.

2.6. Hardening

2.6.1. The Supplier shall propose security-hardening baselines in accordance with industry standards with the following order of precedence, subject to University's written approval:

(a) Center for Internet Security (CIS) Benchmark;

(b) Hardening Benchmark endorsed by Product Principal Vendor;

(c) If there is no reference hardening benchmark available, each operating system, application and/or database shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.

2.6.2. The Supplier shall perform the following:

(a) Process to seek deviation from specific checklist items if the checklist items cannot be implemented due to operational or compatibility concerns;

(b) Roles and responsibilities of various parties that are involved in the system/service hardening process;

(c) Process to update system/service hardening checklists during Operations Phase;

(d) Any other information and processes related to the hardening process that are deemed necessary by University.

2.7. Access Control

2.7.1. The Supplier shall identify types of System users and services, design the access matrix, detailing the roles and rights for all the resources (application, servers, network appliances and system infrastructure).

2.7.2. The Supplier shall ensure access to the System shall be granted on a need-to-access basis.

2.7.3. The Supplier shall ensure that account shall be granted with privilege based on the principle of least privilege.

2.7.4. The Supplier shall ensure that individual unique account shall be granted to each individual user. No sharing of account shall be allowed unless otherwise approved by University.

2.7.5. The Supplier shall provide detailed specifications of its Identity Access Management ("**IAM**") to clarify who is allowed to access the information and data in the hosting environment.

2.7.6. The Supplier shall ensure access to System shall comply with NTU Access Management Policy.

2.8. Identity Access Management

2.8.1. Access to, and use of, audit tools that interact with the information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.

2.8.2. User access policies and procedures shall be established and implemented for ensuring appropriate identity, entitlement, and access management for all access to data, application interfaces, infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:

a. Roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function
b. Access segmentation to sessions and data in multi-tenant architectures
c. Account credential lifecycle management from instantiation through revocation
d. Account credential and/or identity store minimization or re-use when feasible
e. Authentication, authorisation, and accounting rules for access to data and sessions

2.8.3. The Supplier shall implement procedures to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.

2.8.4. The System's design shall be designed with ~~support~~ two-step verification mechanism, i.e. 2-factor authentication ("2FA") for privileged account holder.

2.8.5. The Supplier shall ensure approval is sought from the University for any additional/removal of privileged account holder.

2.8.6. NTU shall reserve the right to view or audit all access logs of the Solution.

2.9. Vulnerability Management

2.13.1. The Supplier shall ensure all applications/software (including third party applications/software) proposed/used by the awarded vendor in the System are not affected by known vulnerabilities.

2.13.2. The Supplier shall ensure the provision of the necessary security mechanisms and processes to guard against unauthorised access, intrusion, leakage / corruption / destruction of information, errors and vulnerability to malicious attacks to the solution, hosting environment and its data.

2.13.3. The Supplier shall provide the service level agreement for patch management, vulnerability management and release management. The service level agreement must contain detailed specifications about vulnerability classification and actions taken according to the severity level.

2.13.4. The Supplier shall note that the service level agreement (SLA) for zero-day and critical vulnerabilities shall be one (1) week and one (1) month respectively. Deviation from this SLA shall be first approved in writing by University.

2.13.5. The Supplier shall implement procedures for timely detection of vulnerabilities within applications, infrastructure network and system components to ensure the efficiency of implemented security controls.

The Supplier shall provide the service level agreement for vulnerability management, defining detailed specifications on vulnerability classifications, action plan and response time according to the severity level.

2.10. Application and Interface

2.10.1. The System shall be designed, developed, deployed, and tested in accordance with leading industry standards, e.g. Open Web Application Security Project (OWASP) for web applications, OWASP_ASVS (Application Security Verification Standard) for non-mobile application, OWASP_MASVS (Mobile Application Security Verification Standard) for mobile application.

2.10.2. Data input and output integrity routines shall be implemented for application interfaces to prevent manual or systematic processing errors, corruption of data, or misuse.

2.10.3. The Supplier shall maintain data security (to include confidentiality, integrity, and availability) across multiple system interfaces, and business functions to prevent improper disclosure, alteration, or destruction.

2.10.4. The Supplier shall use secure network protocols for the import and export of data and to manage the service, and shall make available a document detailing the relevant interoperability and portability standards that are involved.

2.10.5. If there is a need for University to set up a web server or web portal accessible from the internet as part of the System,:

(a) a Web Application Firewall ("**WAF**") should be placed in-line and in-front of the web server/web portal to provide protection against web-based attacks which shall minimally include the top ten Open Web Application Security Project ("**OWASP**") attacks.

(b) Supplier shall propose how to configure WAF to maximise the effectiveness of WAF, and the proposal shall be subject to the written approval of University.

(c) After configuration of WAF, Supplier shall provide and explain the entire listing of WAF rules with clear explanation and justifications on the purpose of each rule and whether the rule is in blocking mode, learning mode or others.

2.10.6. Multi-tenant applications shall be designed, developed, deployed, and configured such that provider and customer access is appropriately segmented from other tenant users.

2.10.7. The Supplier shall provide application penetration and vulnerability assessment report on the application from an independent security vendor to University on an annual basis

2.11. Endpoint and Server Protection

2.11.1. The Supplier shall ensure that all servers and endpoints have the following protection and capabilities unless otherwise approved in writing by University:

(a) Anti-malware;
(b) Host-based IPS;
(c) Host-based firewall;
(d) File hash (e.g. MD5, SHA1, SHA2) search capability;
(e) File hash (e.g. MD5, SHA1, SHA2) blocking capability.

2.11.2. The Supplier shall ensure that the Anti-malware used is up-to-date and its signature is updated with latest signature.

2.11.3. The Supplier shall ensure that the Host-based firewall permits only necessary traffic that is required for the operation of the endpoint or server.

2.11.4. The Supplier shall ensure that file hash search can be performed for all endpoints and servers upon request by University.

2.11.5. The Supplier shall ensure there is a centralized management solution for the server and endpoint protection and capabilities listed in clause 2.9.1.

2.11.6. The Supplier shall ensure that specific file hash can be blocked promptly upon request by University.

2.11.7. The Supplier shall ensure audit trail and logging capability facilitating incident investigation and response of all the endpoints and servers are enabled.

2.11.8. The Supplier shall ensure that all the audit trail and logs shall be retained for a period of at least twelve (12) months.

2.11.9. The Supplier shall perform searching of keyword or other attributes of the audit trail and logs upon request by University. The Supplier shall revert with the full results of the search within three (3) calendar days after search is requested by University.

2.12. Network Protection

2.12.1. Production and non-production environments shall be separated to prevent unauthorised access or changes to information assets. Separation of the environments may include: different cloud accounts and/or VPC/VNet, application aware and/or stateful inspection firewalls, domain authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.

2.12.2. Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts.

2.12.3. The Supplier shall architect practical defense-in-depth network defenses (e.g. deep packet analysis, traffic throttling, and black-holing) for detection, protection and timely response to network-based attacks associated with anomalous traffic patterns (e.g. MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

2.12.4. The Supplier shall ensure that Firewall and Intrusion Prevention System (“IPS”) is in place to segregate and protect the system or application from the internet.

2.13. Security Incident Management

2.12.1. The Supplier shall provide details of its incident handling, response and management process that demonstrate alignment or in accordance to industry accepted standards such as

(a) National Institute of Standards and Technology Special Publication 800-61 (NIST SP800-61);

(b) International Organization for Standardization publication 27035 (ISO 27035);

2.12.2. The Supplier shall define and provide details of its Security Incident Response Service Level Agreement (SLA) to University

2.12.3. The Supplier shall enable and ensure availability of audit trail logs across all systems or applications or instances so that analysis and review of logs can be undertaken to triage and identify the root cause of the incident in a timely and thorough incident investigation.

2.12.4. The Supplier shall be capable of performing Logs review, Investigate and/or perform triage of the incident or breach to identify malicious activities, backdoor communications or potential data exfiltration etc.

2.12.5. The Supplier shall allow University access to the logs, all artifacts, findings as well as information that are surface during the security incident.

2.12.6. The Supplier shall have up to date documented "playbooks" or standard procedure for responding to security incidents

2.12.7. The Supplier shall put in place mechanisms or tools to ensure security events are closely monitored, so that any potential or suspected security incident are acted upon or contained in a timely manner.

2.12.8. The Supplier shall notify University of any Security Incident as well as their actions and measures that are undertaken to prevent a re-occurrence

2.12.9. The Supplier shall provide Incident statistic reports at pre-defined scope and agreed period to University.

2.12.10. Information security events shall be timely reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.

2.12.11. Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.

2.14. Audit and Compliance

2.14.1. Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations.

2.14.2. Independent reviews and assessments shall be performed at least annually to ensure addresses nonconformities of established policies, standards, procedures, and compliance obligations.

2.14.3. The system and application logs captured shall be agreed in writing by University. The retention period of the corresponding logs shall be defined in writing by University.

2.14.4. The Supplier shall ensure that all the audit trails and logs of the System can be piped to University's Log Management Server unless otherwise specified by University.

2.15. Pre-commission Security Assessment

2.15.1. The Supplier shall engage an independent security assessor to perform the Pre-Commission Security Assessment ("PCSA") for the System.

2.15.2. The Supplier shall provide a concise write-up, during bidding stage, on how PCSA requirements are being met.

2.15.3. The PCSA shall include the following activities where applicable and agreed to in writing by The University:

(a) IT Security Review – to ensure that IT security configurations and controls of the System are implemented in compliance with the security requirements in this Tender.
(b) IT Vulnerability Assessment – to ensure that all known IT security vulnerabilities are addressed.
(c) IT Penetration Testing – to evaluate the security posture of the System by simulating attacks with malicious intent where possible.

2.15.4. Prior to the commencement of each security assessment, the Supplier shall seek The University's approval on the following:

(a) Scope of the security assessment;
(b) Schedule of the security assessment; and
(c) Methodologies to be used

2.15.5. A copy of the assessment report containing information of all the security risks and findings by the independent security assessor shall be provided to University.

2.15.6. The Supplier shall ensure that all HIGH and MEDIUM severity security risks and findings identified are remediated to a level that is acceptable to University; and verification on the remediation shall be performed by an independent security assessor.

2.15.7. For each security risk and finding that cannot be remediated immediately, the Supplier shall:

(a) Propose and implement mitigation measures or workaround to minimise the risk impact or risk likelihood for University's written approval;
(b) Record into the security risk register for tracking;
(c) Plan for and apply remediation when a fix or patch is made available;
(d) Present the remediation actions and verification results to University for written approval before official closure of the finding

2.15.8. The Supplier shall obtain University's written approval for PCSA closure before the Commissioning Date.

2.15.9. The Supplier shall ensure that the independent security assessor provides the corresponding final PCSA report to University before the Commissioning Date unless otherwise agreed in writing by University.

2.16. Annual Security Assessment

2.16.1. The Supplier shall provide application penetration and vulnerability assessment report on the application from an independent security vendor to The University on an annual basis

3. PERFORMANCE LEVEL

3.1. System Availability Level

(a) The System Availability is defined as

$$\text{System Availability} = \frac{(\text{SOH} - \text{SD})}{\text{SOH}} \times 100\%$$

Where:

SOH = **Scheduled Operating Hours** of the System, which is 24 hours a day for 7 days a week;

SD = **Service Downtime**, accumulated time due to unavailability of the System

(b) The System shall achieve 99.5% System Availability per calendar month, excluding the scheduled downtime.

3.2. System Performance Level

3.2.1. The System shall support an estimated of 1,200 users; and 200 concurrent users.

3.2.2. System Response Time is defined as the processing time of the System in the production environment to complete a particular transaction submitted from a web browser based on the number of users specified under Clause 3.2.1:

	Mode	**System Response Time**
(a)	Login	• Shall not exceed two (2) seconds for 90% of the time.
(b)	Navigate (Click on a link to access information or switch view)	• Shall not exceed two (2) seconds for 90% of the time.

(c)	Query/Search (Search for content related to a particular subject)	• Shall not exceed three (3) seconds for 90% of the time
(d)	Transact/Update (Submit a page with database or document transactions)	• During peak level operations – shall not exceed three (3) seconds for 90% of the time • Maximum response time shall not exceed five (5) seconds except for agreed to exclusions.
(e)	Report Generation	• Shall not exceed five (5) seconds for 90% of the reports. • Shall not exceed two (2) minutes for the remaining 10% For optimal testing of Reports, The University may request all users to run reports concurrently.

4. STANDARD OPERATING ENVIRONMENT

4.1. Standards

The System shall be compatible and able to support the following standard operating environment of The University:

	Type	The University Standard(s)	Remarks
(a)	Client Web Browser	• Google Chrome • Microsoft Edge • Safari • Internet Explorer 11	
(b)	Mobile Devices	• Android 7.0 and above • IOS 13 and above	
(c)	Directory Services	• Microsoft Active Directory 2016	Directory Service provides authentication services to the University network resources.
(d)	Single Sign On	• Active Directory Federation Services 4.0 • Elastic SSO Enterprise On-Premises	
(e)	Server Operating System	• Microsoft Windows Server 2016 or higher • Redhat Enterprise Linux 7	
(f)	Database	• Microsoft SQL Server 2017 or higher • Oracle Database 12c or higher	Standard edition is preferred. Only use Enterprise edition if the System requires specific features that are not supported in the Standard Edition.

4.2. Intentionally Left Blank

5. Intentionally Left Blank