
SINGAPORE POLYTECHNIC
DEPARTMENT OF INFORMATION AND DIGITAL TECHNOLOGY
SERVICES

**Implementation of Enterprise Content Management
System (ECM) Using SharePoint 2013
and Migration of Existing Content**

PART 2

REQUIREMENT SPECIFICATIONS

All rights reserved. This document may not be reproduced in any form or by any means without the prior permission of Singapore Polytechnic.

The information given in this document is not to be communicated, either directly or indirectly, to the press or to any person not authorised to receive it.

Your attention is drawn to the official secrets act (chapter 213), which relates to the safeguarding of official information.

CONTENTS

1. BACKGROUND	6
2. OBJECTIVE	6
3. EXISTING ENVIRONMENT.....	6
4. COMMENCEMENT AND DURATION OF CONTRACT.....	6
5. TERMINATION OF CONTRACT	7
6. SERVICE CREDITS	7
7. PAYMENT SCHEDULE AND INVOICES.....	7
8. CLARIFICATIONS	7
9. DESCRIPTION OF TENDER.....	10
10. SCOPE OF TENDER	10
11. SCOPE OF WORK.....	13
12. PLANNED IMPLEMENTATION SCHEDULE	14
13. OTHERS	15
14. GENERAL REQUIREMENTS.....	17
15. FUNCTIONAL REQUIREMENTS.....	19
16. APPLICATION PLATFORM AND CODE STANDARDS REQUIREMENTS	25
17. INTERFACE REQUIREMENTS	28
18. WEBSPHERE PORTAL INTEGRATION	28
19. ACTIVE DIRECTORY FOREST.....	28
20. OVERVIEW OF TECHNICAL REQUIREMENTS.....	31
21. SP TECHNICAL ARCHITECTURE.....	31
22. MULTI-VENDOR SERVICE ENVIRONMENT	31
23. SP INFRASTRUCTURE REQUIREMENTS	32
24. SYSTEM SECURITY AND CONTROL REQUIREMENTS	36
25. APPLICATION SYSTEM LOGS.....	36

26. TECHNOLOGY PROTECTION	36
27. IPV6 REQUIREMENT.....	37
28. CONTENT MIGRATION	40
29. SYSTEM PERFORMANCE REQUIREMENTS.....	44
30. AVAILABILITY	45
31. RELIABILITY.....	45
32. ICT SECURITY REQUIREMENTS	46
33. APPLICATION SECURITY	53
34. SYSTEM SECURITY.....	54
35. TESTING AND ACCEPTANCE.....	66
36. TRAINING	69
37. INTRODUCTION	72
38. CHANGE CONTROL MANAGEMENT REQUIREMENTS	72
39. CLASSIFICATION AND SERVICE REQUEST SERVICE LEVELS.....	72
40. SERVICE REQUEST MANAGEMENT	73
41. SERVICE REQUEST EVALUATION REPORT	74
42. PAYMENT SCHEDULE FOR SERVICE REQUESTS	74
43. INSTALLATION AND IMPLEMENTATION	76
44. DOCUMENTATION	78
45. QUALITY MANAGEMENT SYSTEM (QMS)	79
46. MOBILISATION OF PERSONNEL REQUIREMENTS	81
47. PROJECT ORGANISATION	81
48. PROJECT MANAGEMENT PLAN	82
49. ROLE OF SP REPRESENTATIVE	82
50. PROJECT MANAGER (CONTRACTOR)	83
51. ROLE OF PROJECT MANAGER	83
52. PROGRESS REPORTING	84

53.	REPLACEMENT OF PERSONNEL REQUIREMENT	84
54.	DATA PROTECTION	85
55.	PROJECT TECHNICAL REVIEWS	85
56.	RIGHTS TO THE SOFTWARE & DOCUMENTATION	88
57.	PERFORMANCE GUARANTEE PERIOD/SYSTEM WARRANTY	90
58.	INTRODUCTION	92
59.	INCIDENT MANAGEMENT REQUIREMENTS	92
60.	SERVICE LEVEL FOR INCIDENT RESOLUTION TIME.....	92
61.	SCOPE OF WORK.....	97
62.	SUPPORT HOURS (SYSTEM).....	98
63.	MAINTENANCE	98
64.	APPLICATION & SYSTEM SOFTWARE MAINTENANCE SUPPORT	98
65.	SOFTWARE SUPPORT	102
66.	TRANSITION AND EXIT MANAGEMENT	104
67.	EXPIRATION OF CONTRACT	105
68.	COMPLIANCE WITH REGULATORY REQUIREMENTS.....	107
69.	INFRASTRUCTURE INFORMATION	109

SECTION A

INTRODUCTION

1. BACKGROUND

- 1.1. SP invites vendors to submit proposals for Implementation of Enterprise Content Management System (ECM) using Microsoft SharePoint 2013 and content migration from existing Documentum repository (known as DARE).
- 1.2. There is approximately 1,700 staff using the existing system.

2. OBJECTIVE

- 2.1. The implementation of the ECM System aims to achieve the following objectives:
 - Deploy a content and document management system that is easy to use, accessible anywhere and from all devices
 - Provide a seamless integration with user's commonly used applications such as MS Office, Email client, Windows Explorer
 - Configure the Enterprise Search features to search content from common data sources
 - Migrate the content from existing repository DARE to SharePoint
 - Implement a user-friendly landing page that shall be a launch-pad to all existing and future SharePoint sites and applications
 - Procure maintenance and support for the entire SharePoint farm including existing servers

3. EXISTING ENVIRONMENT

- 3.1. Singapore Polytechnic (SP) is currently using EMC Documentum v6.5 SP2. The system runs on a combination of Solaris and Windows servers. For details, please refer to section 69-1. Details of Existing Documentum System (DARE).
- 3.2. Staff accesses DARE through a customized EMC Documentum DAM client. The supported desktop environment in SP is Microsoft Windows 8.x, Windows 7, Mac OS Mountain Lion and Maverick. Supported browsers are Internet Explorer 7 or higher, and Firefox 3.X or higher. Standard software suite includes Microsoft Office 2007, 2010 and 2013 with Outlook 2007, 2010 and 2013 for Windows OS, and Mac Office 2011 for Mac OS.
- 3.3. SP enterprise backup is based on Symantec NetBackup.
- 3.4. SP will provide Microsoft software licences through existing Microsoft Campus Agreement, Wintel server hardware (or Virtual Machines) and Symantec NetBackup licences through existing term contracts.
- 3.5. SP has an existing SharePoint 2013 farm being used for other applications. This farm shall be expanded with additional server resources to support the new ECM system as per contractor's recommendations.

4. COMMENCEMENT AND DURATION OF CONTRACT

- 4.1. This Contract shall commence on the date stated in the Letter of Acceptance and shall remain in force for a period of 4 years after the System Acceptance.
- 4.2. The Contract shall be reviewed and renewed by SP on a yearly basis.

5. TERMINATION OF CONTRACT

- 5.1. SP reserves the right to terminate the contract with 30-day written notice to the Contractor in the event of SLA breach or any material breach as stated in the requirement specification.
- 5.2. In addition, SP reserves the right to terminate the contract during the yearly review.

6. SERVICE CREDITS

- 6.1. In the event, if Contractor is unable to meet the Service Level Agreements (SLAs) specified in **Section G – System Performance, Availability & Security**. SP will be eligible to claim for Service Credits. The Tenderer shall detail the computation of service credits for breach in agreements (SLA) during the project, warranty and maintenance periods. The service shall be benchmarked against the SLA stated in this tender specification document.

7. PAYMENT SCHEDULE AND INVOICES

- 7.1. The payment schedule will be based on the key milestones and completing the necessary acceptance as shown below:

S/N	Stage	% of Price Quoted	Cumulative Total	Deliverables
1	Acceptance of Requirements and Detailed Design Specifications	30%	30%	Sign off Requirements Specification and Detailed Design Specifications
2	Acceptance of User Acceptance Tests	30%	60%	Sign off on Successful User Acceptance Tests
3	Acceptance of Performance Test and on Commissioning	15%	75%	Sign off System Performance Test and Commission Letter
4	System Acceptance – Completion of Performance Guarantee Period	25%	100%	Acceptance Letter
5	Payment for Annual Maintenance and Support will be released at the beginning of every six-month period.			

- 7.2. E-invoices should be submitted electronically via the Vendors@Gov portal (www.vendors.gov.sg). On enquires related to the invoice submission, contractor may contact the AGD Helpdesk by calling 1800-VENDORS (1800-8363677) or send enquiries by clicking on the "Contact Us" link at <http://www.vendors.gov.sg>.

8. CLARIFICATIONS

- 8.1. All enquiries regarding this tender should be made in writing and emailed to:

<p>K V Ramana Rao (Ram) Manager Department of Information & Digital Technology Services Singapore Polytechnic Tel: 68707852 Email: ramanarao@sp.edu.sg</p>
--

- 8.2. SP reserves the right to make clarifications submitted by Tenderer available to all other Tenderers. This clause is applicable where there is a site briefing conducted and attendees' details are obtained.
- 8.3. All clarifications shall be deemed not to be confidential.
- 8.4. All telephone and facsimile enquiries shall not be entertained.

SECTION B
SCOPE OF TENDER & WORK

9. DESCRIPTION OF TENDER

- 9.1. Tenderers are invited to submit a complete proposal for the design, development, supply, delivery, installation, testing, training, commissioning and maintenance of the Enterprise Content Management (ECM) System using Microsoft SharePoint 2013 including migration of content from existing DARE Documentum system, with Option to procure additional 100 man-days for professional services as term contract.

10. SCOPE OF TENDER

- 10.1. The scope of the project is to implement the ECM System. The requirements specified are mandatory, while the Options are for SP to exercise when awarding the tender.
- 10.2. “Option”, “Optional” are options to SP and NOT options for Tenderers. Tenderers must quote for ALL components specified in this Requirement Specification. Tenderers who do not quote for Options will be disqualified from the evaluation.
- 10.3. MANDATORY REQUIREMENTS:
- To design the ECM system architecture, propose additional server resources required and provide professional services to setup and configure SharePoint software, services and components (such as web-applications, sites, libraries, content types, meta-data, permissions and other necessary artefacts) for expanding SP’s existing SharePoint farm to support the functionalities specified in this tender specification. Setup development environment and staging environment (also referred to as Test environment meant to be used for integration testing and UAT) for application development and testing purposes.
 - To provide all tools (e.g. tools for migration, system monitoring, etc.) and professional services needed to migrate all the content, meta-data, information and functionalities of existing DARE system to SharePoint platform.
 - Design and implement a user-customizable visually attractive landing page to function as a launch-pad to access sites within the ECM system and other existing and future SharePoint Applications.
 - Provide ONE Year warranty period for the ECM system starting from the System Acceptance Date and sign-off for all deliverables.
 - Provide 3 years of maintenance and support for the ECM System including all servers and system components.
 - Provide maintenance and support for the entire SharePoint farm including existing servers from the date of the project award and during system implementation, warranty and maintenance periods.
- 10.4. Provision of 100 (One Hundred) man-days as an OPTION (indicate a man-day rate charged) for professional services for application enhancements e.g. for new features, enhancements, server setup, etc (These man-days are not to be consumed for bug-fixes which shall be covered by warranty and system maintenance). Separate purchase orders shall be raised by SP for consuming these man-days. The validity period will be from the date of award till the last day the system is under 1 Year warranty or 3 Years maintenance with the contractor.

- 10.5. SP has the rights to award this tender in part.
- 10.6. The successful Tenderer, shall be required to conduct a detailed requirement study after the award of the Tender to study the existing systems, clarify the details and confirm the user requirements.
- 10.7. The Tenderer shall propose a solution that best meets SP functional requirements to a level of quality acceptable by SP with optimal customisation and incorporating best practices available in the product solutions. The proposed solution shall utilize the latest features and API to maintain upward compatibility with future product releases.
- 10.8. The Tenderer's submission shall include a detailed system architecture diagram with the specifications of the servers (Number of servers, CPU, RAM, Storage, etc) and software needed to enhance the existing SharePoint farm to meet all requirements specified in this tender document. It shall be noted that virtualized (VMWare) servers shall be provided by SP according to the specifications provided by the tenderer. The tenderer shall be responsible for complete system installation, software setup & configuration and for meeting the performance requirements.
- 10.9. Proposals shall include professional services for installation and configuration of system software, database software, development tools, or any peripherals/systems/services deemed necessary for the implementation and maintenance of the System for SP. Tenderers shall specify clearly the purpose for each peripheral, system software components, third-party software components and services proposed for SP.
- 10.10. The Tenderer shall provide interface components for the System to interface with SP's existing application systems as well as those Systems belonging to third party vendors if applicable. Please refer to **Section D- Interface Requirements** for more details on the interface requirements.
- 10.11. The Tenderer shall review the existing SP hardware and system software solutions, and recommend architecture to meet the requirements. An architecture diagram with description of proposed changes must be included in the tender submission. Please refer to **Section E– Technical Requirements** for details of the technical requirements.
- 10.12. The Contractor shall provide for offsite development of the System (Office space provided by the Contractor and Development Hardware/Software to be owned and provided by the Contractor). All initial development and testing work for the System shall also be provided and carried out at the Contractor's premises.
- 10.13. Subsequently, the System shall be progressively migrated to the test and production environments to be setup at SP for System Performance Testing and User Acceptance Testing (UAT). The Contractor shall ensure the system performance criteria are met. After the successful completion of UAT, the System shall be hosted in the production environment at SP.
- 10.14. The Contractor shall be responsible for assessing the impact and applying the

updated OS patching/upgrade, database patching/upgrade and software patching/upgrade without or with minimum disruption to the service.

- 10.15. The support and maintenance for the System, if such option is elected by SP, shall be for up to 3 years, to be reviewed and renewed by SP on a yearly basis. The Contractor shall also grant SP an option to extend the support and maintenance of the System for a further period of up to 5 years after the expiry of the initial 3 years, to be reviewed on a yearly basis. Such support and maintenance services shall commence only after the expiry of the System Warranty Period.
- 10.16. The existing DARE system based on Documentum will have its maintenance contract expiring by 20th May 2015. Hence the contractor must ensure all content is migrated and users shall be able to fully use new ECM system by 15th May 2015. If the ECM system is not rolled out to users by the above cut-off date for any reason, the contractor shall provide support for DARE system at their own cost until it is completely migrated.
- 10.17. The major milestones for the implementation of the System are listed as follows:
- Implementation of ECM System and migration for THREE departments by 30th September 2014
 - Implementation of complete ECM system and migration for all remaining departments by 15th May 2015

10.18. The other planned major milestones are listed as follows:

Phase	Planned Milestone
Commissioning Date	As soon as the System has successfully passed all the Acceptance Tests, SP will forthwith issue a certificate or letter of commissioning the System and the date of the certificate or letter shall be the Commissioning Date of the System.
Performance Guarantee Period (PGP)	Commence on commissioning Date for a period of 90 working days. The System shall have successfully completed the PGP if the System meets the standard of performance or service availability level as stipulated in the contract.
System Acceptance Date	Successful completion of PGP and acceptance by SP. Once the System has successfully completed the PGP, SP shall forthwith issue a written notice accepting the System. The date of the notice shall be the System Acceptance Date.
System Warranty Period	Commence on System Acceptance Date for a period of 12 calendar months.



11. SCOPE OF WORK

11.1. The Tenderer's proposal shall include at least the following scope of work:

11.2. Methodology and Strategy

- To state the methodology, implementation strategy and tools used during the implementation.
- To state the approach, tools and detailed execution and verification strategy for migration of data from DARE to the new ECM system.
- To state the configuration and customization approach to implement the functionality of DARE in the new ECM system

11.3. Project Management and Execution

- To put in place a project management framework to ensure well-organised and successful execution of the project with timely completion of key deliverables, within budget and proper mitigation of risks.
- To formulate a concrete plan of action covering comprehensive stage-by-stage upgrade activities, project schedule and resources required. Roles and responsibilities of both Contractor's and SP's teams shall be clearly defined.

11.4. System Infrastructure to Enhance SP's existing SharePoint Farm

- To propose the system architecture to meet SP's requirement in terms of functionality, integration, performance, availability, disaster recovery and security.
- The Contractor will provide a comprehensive additional server recommendation, including server, storage, server sizing, storage sizing, etc for the implementation of the proposed solution on SP's existing SharePoint farm. SP's SharePoint farm is based on VMWare and additional servers proposed should be similarly virtualized.
- Please note that the hardware is not included as part of this procurement. SP will provide the required servers of similar configuration, not necessarily of the same make and model, as proposed by the Contractor to meet the performance requirement set out in this document. The Contractor, however, is still responsible for the integration and performance requirements of the whole system as stated in this tender specification and to ensure the successful commissioning of the System.

11.5. System Setup

- To install, test, configure all components of the System to meet SP requirements. The setup shall include the Test and Production environments.
 - To configure and ensure all existing integration and interfaces with other related or supporting systems are functioning properly.
 - To propose the additional software licenses required for the system. SP's existing farm is based on SharePoint 2013 and MS SQL server 2012. SP shall procure the additional licenses as proposed by the contractor.
- 11.6. Testing Strategy
- To propose an overall testing strategy and put in place the overall test plan to ensure that the proposed system satisfies all requirements defined in this specification. To put in place a rigorous testing process and QA team to test and verify all the deliverables before submitting them with corresponding evidence to SP.
 - To provide the tools and propose verification strategy to validate that migration of documents has been completed. Reports shall be provided to tally each of the individual documents have been successfully migrated.
- 11.7. Training
- To provide suitable and customized training for identified staff to ensure proficient management and operation of the System. Please refer to Section I – Training and Awareness Programme for details of training requirements
- 11.8. System Rollout /Performance Guarantee Period/System Warranty
- To provide a comprehensive transition and rollout plan to ensure a smooth and straightforward cut-over. To provide Performance Guarantee Period and System Warranty as specified.
- 11.9. Documentation
- To provide a comprehensive set of documentation to ensure smooth operation and administration of the System, and effective use of the System by the users. Please refer to Section L – Documentation for details of documentation requirements
- 11.10. Post Warranty Application Software Maintenance Support
- To submit a proposal for the provision of maintenance and application software support after warranty period, as specified in Section Q – Support & System Maintenance.

12. PLANNED IMPLEMENTATION SCHEDULE

- 12.1. The Tenderer shall provide a detailed project schedule that can meet the milestones of this project. The project schedule shall show details up to the task level, how each milestone could be achieved within the timeframe specified above. The project schedule shall reflect possible overlaps between key activities and their interdependencies.
- 12.2. The Tenderer may propose a schedule where the milestones can be achieved earlier.
- 12.3. The Tenderer shall draw up the Schedule using Microsoft Project format.

13. OTHERS

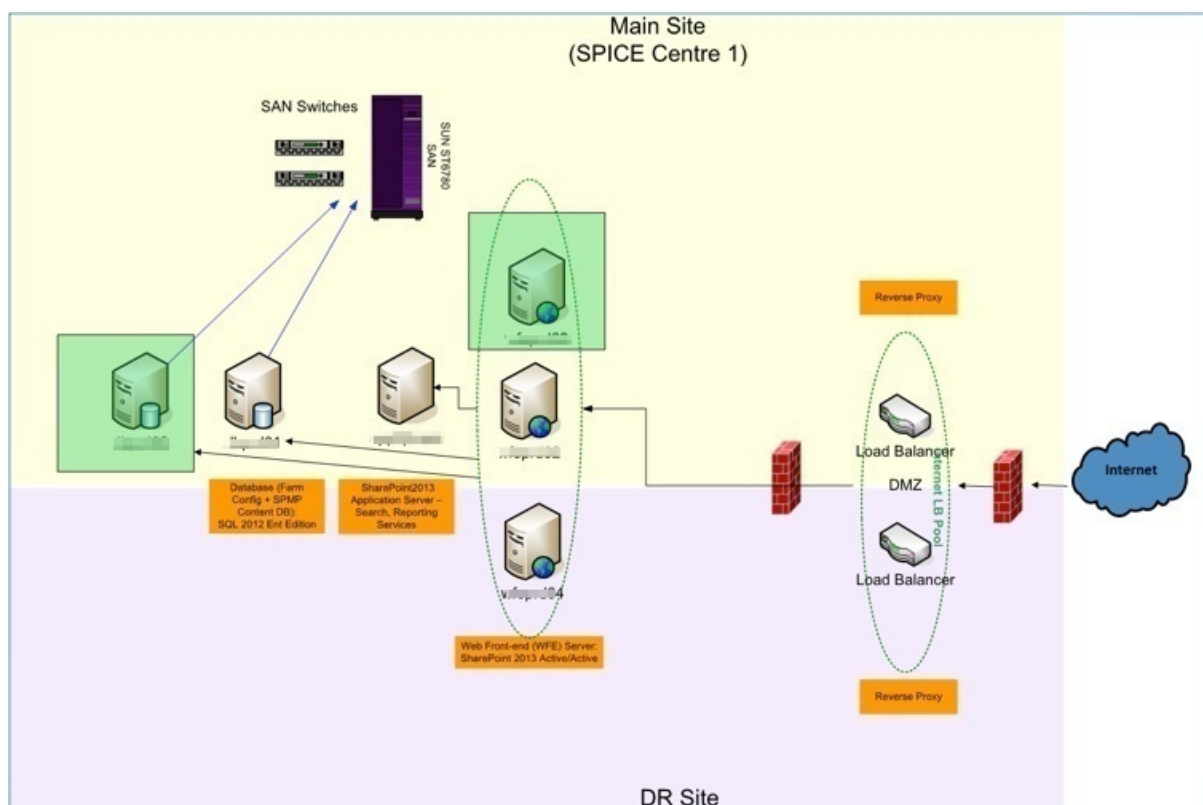
- 13.1. The shortlisted Tenderers shall be invited by SP to conduct a formal presentation to SP on the proposed solutions. Shortlisted Tenderers shall be required to cover the following areas in their presentations:
- Project scope and outcomes
 - Key areas of concern (including change management issues and critical success factors) which SP should take note of
 - Tenderer's proposed solution aided with screenshots, diagram, graphics, work flow, mock-up etc, that can best demonstrate the Tenderer's proposed solutions
 - Tenderer's proposed team's structure, credentials and experience
 - Tenderer's track record in undertaking projects of the similar nature and scale
 - Future product development plans
 - Migration and Change Management strategy that has the least impact to users
- 13.2. The shortlisted Tenderers may be required to demonstrate how their proposed solutions work under specific business case scenarios to be prepared by SP. The timeframe for making the presentation and completing the demonstration will be decided by SP after a preliminary review of all Proposals after the closing date of this invitation to tender.
- 13.3. Tenderer should present the proposed team's experiences and commitment that the team will not be changed throughout the execution of the project. SP reserves the right to request the vendor to change any member of the project team if they are found not to be competent.
- 13.4. Tenderer shall bear all costs incurred in conjunction with the submission of the Proposal, including the aforesaid presentation and prototype development where necessary. SP shall not be required to reimburse the Contractor for all such costs.
- 13.5. SP prefers to award the entire Contract to one Contractor where possible. However SP reserves the right to award parts of the Contract to one or more Contractors in its sole and absolute discretion.

SECTION C

FUNCTIONAL REQUIREMENTS

14. GENERAL REQUIREMENTS

- 14.1. The Contractor shall conceptualise, design, build and integrate the System with existing infrastructure. SP may choose to have the architecture validated by a 3rd Party.
- 14.2. The System will be used by staff and collectively known as users.
- 14.3. The system is rated as confidential for the data stored in the repository. Upon award the contractor shall comply with requirements specified in the Government procedures for handling and accessing of data.
- 14.4. The Contractor shall be responsible for the creation and setup configuration on SharePoint that are essential for the operation of the System.
- 14.5. SP is using SharePoint 2013 with MS SQL 2012 to host the existing farm. There are several applications already deployed to the farm. The servers (VMWare, Windows 2012) currently support access from the Internet and Intranet as shown below: The servers highlighted in GREEN are in the process of being setup. The contractor is expected to enhance the farm with additional server resources to meet the requirements of this tender without affecting the existing applications.



- 14.6. The database shall be configured to make use of VMware's HA/DR functionalities such as vMotion and SRM.
- 14.7. The servers used for the SharePoint farm are virtualized using VMWare. SP prefers to keep the configuration of any newly proposed virtual server to be of

similar configuration to the existing ones shown below:

Server Function: Web-FrontEnd Server and App Server
CPU: 8 Memory: 16 GB Disk Controllers: VMware SCSI Controller System Disks: 100 GB Data Disks: 200 GB NICs: 1 x Intel PRO/1000MT Network
Software Configuration:
OS: Windows 2012 Datacenter server Symantec Endpoint Protection 12.x

Server Function: MS SQL Database Server
CPU: 4 Memory: 32 GB Disk Controllers: VMware SCSI Controller System Disks: 100 GB Data Disks: 200 GB Log Disks: 50 GB NAS and SAN: 5 TB for other projects NICs: 2 x Intel PRO/1000MT Network
Software Configuration:
OS: Windows 2012 Datacenter server MS SQL Server 2012 Veritas Netbackup Client 7.5 Symantec Endpoint Protection 12.x

- 14.8. The expected Recovery Time Objective (RTO) period for the system shall be 7 working days.
- 14.9. The system shall be designed to scale for future growth of data. The Tenderer shall submit their proposal with a suitable SharePoint design with web-applications, Site-collections, libraries, etc.
- 14.10. The design shall ensure optimal paths for data transfer via Internet and Intranet.
- 14.11. Friendly URLs must be setup for all sites and displayed from the landing page.
- 14.12. The design shall make use of SAN, NAS and RBS (Blob store) for storage. The tenderer shall propose the details of estimated disk storage required and the distribution of data for optimal cost and performance.
- 14.13. Documents maybe of sensitive nature, data must be encrypted on the SAN and NAS.
- 14.14. Backup must be configured for the system and integrated with SP's existing backup infrastructure.

- 14.15. The Contractor shall review the existing contents; information and knowledge base in SP's DARE system, and recommend the best approach and strategy for increased content usage and collaboration among SP staff. This shall minimally include best practices, processes, workflow, information architecture, page layout, designs, themes and appropriate System tools.
- 14.16. The Contractor shall minimally comply with the following system design requirements to support data sharing:
- The system design must be flexible and facilitate extraction of data in open, machine-readable formats:
 - (a) Minimally either CSV, TXT or XML
 - (b) Other recommended formats : API, Atom, JSON, RDF, RSS
- 14.17. The Contractor shall adopt a prototyping development approach for the development of the System such that the design and usability of the web pages and contents have to be approved by SP before actual development is carried out.
- 14.18. The Contractor shall be responsible for the migration and development of all existing content, functionalities and processes from the existing system into the new system.
- 14.19. The Contractor shall be responsible for the smooth implementation of the System. The Contractor shall submit a proposal to SP with details on the implementation plan and strategy of the system that will provide minimal disruption to work operations.
- 14.20. The Contractor shall conduct review sessions to demonstrate the proposed System to the key stakeholders as and when required. SP shall not be required to reimburse the Contractor for all such costs.

15. FUNCTIONAL REQUIREMENTS

The contractor shall implement the system to meet the following functional requirements in addition to enabling and configuring all the SharePoint components and services provided with the product.

Landing Page

- 15.1. Design and implement a user-customizable landing page as a launch-pad for the ECM system and other existing and future SharePoint Applications.
- 15.2. Custom site design shall be implemented to cater for SP's branding and compliance requirements.
- 15.3. In order to simplify the user interface, selected power-user features (e.g. Ribbon, Site-settings, etc) shall be hidden from view. The contractor shall propose the pros and cons for each feature for SP's decision.
- 15.4. The design of this landing page shall be visually attractive and similar to that of

AppStore with icons, ratings, titles and descriptions of application. The user shall be able to search/filter the links on the page via keywords.

- 15.5. The links and App-icons on the landing page shall be filtered by access rights of the logged in user.
- 15.6. During requirements gathering session, other web-parts e.g. NewsFeed, Calendar, Staff Directory, Recent Documents, Favourite Documents, Favourite folders, Updates, Organization Chart, etc shall be implemented as identified by SP to make this landing page useful to the staff.
- 15.7. The landing page shall have a corresponding Admin view for system administrators to add additional links along with icons and meta-data.

AD Authentication

- 15.8. The ECM system shall integrate to Microsoft Active Directory (AD) for authentication, groups and memberships. AD userid and password shall be used for such authentication.
- 15.9. There shall be no prompt for login if the user is logged into the AD via his/her computer (e.g. Windows Claims). All necessary claims-based authentications shall be implemented to achieve this Single Sign On. This is applicable for both web-based and desktop integration components.
- 15.10. The tenderer shall ensure that if the user logs in from the Internet without logging into AD (e.g VPN) there shall be a HTML form login to authenticate the user. AD userid and password shall be used for such authentication. The Login form shall be customized to align with SP's standards and branding.
- 15.11. The system shall provide the feature of authenticating and sharing documents with pre-registered users who are not present in AD (e.g business partners)
- 15.12. The users/owners shall be able to define the permissions for their respective sites, folders and documents.
- 15.13. Creation of sub-sites, document-libraries and other artefacts shall be restricted to a specific group of users from each department/school.
- 15.14. The system shall allow users to share documents via links. However only those users with permissions shall be able to view the documents.

Desktop Application Integration

- 15.15. The system shall provide desktop application integration client from the user computers, which allows easy depositing of documents into the ECM repository.
- 15.16. Users shall be able to retrieve and save documents directly from common desktop applications such as MS Office, etc.
- 15.17. The system shall enforce meta-tags on the documents when they are saved from the Desktop. See below section Meta-Tags (Document Properties).

15.18. In addition to desktop access, access from mobile devices shall be provided.

Explorer Integration

15.19. The Windows Explorer integration shall display the ECM repository as a shared-drive. The users shall be able to open the files directly from the shared drive. The system shall support drag-and-drop of files between local drives and the repository.

15.20. For platforms such as Apple Mac and mobile devices, the contractor shall propose a suitable mechanism to achieve the integration (e.g. using WebDAV or alternatives)

15.21. The system shall enforce meta-tags on the documents.

Email Client Integration

15.22. System shall provide the ability to save and retrieve documents from the repository directly MS Outlook Client (Office 2010 or later). This includes saving an email message and attachments directly to ECM repository from the email application via drag-and-drop. SharePoint team folders should be configured to be accessible from SharePoint, Outlook, and Outlook Web Access.

15.23. The system shall enforce meta-tags on the documents deposited via email. See below section Meta-Tags (Document Properties).

Meta-Tags (Document Properties)

15.24. The tenderer shall create content types in SharePoint and configure the system with the meta-tags currently existing in DARE and additional ones specified by SP. The system shall prompt for entry of meta-tags when a document that is being created or updated is saved to the repository. Custom content types and meta-data shall be centralized for standardization and reusability. The system shall make use of type inheritance, Managed Meta Data services, Terms, etc, for maximizing reusability and standardization.

15.25. To minimize manual entry from the user, the system shall auto-fill tags such as Author, Date, Title, etc., to the maximum extent possible. The user will be given a choice of accepting the proposed values or to change the values as required. The tenderer shall implement this feature.

15.26. SP technical team should be able to define new meta-tags/properties and remove old ones. The system shall provide features to define mandatory meta-tags/properties and force the user to fill-in these tags. The system shall support promoting user entered tags to common system-level tags (term sets).

15.27. The ECM shall provide a comprehensive and flexible system that allows for a maximum customisation in terms of the presentation of the fields and their format for the properties of the document.

15.28. To minimize user typing, the system shall pre-populate the File-name with the available fields such as Department, date and document type.

- 15.29. The system shall allow users to select multiple documents and update meta-data for the batch.
- 15.30. The system shall be designed to minimize impact of business changes such as department name changes, user names changes, etc, on meta-data or fields of documents. Where the impact cannot be eliminated, the contractor shall provide a patching tool to batch update the affected fields.
- 15.31. The properties should be capable of being populated with additional fields according to the following types:
- Free format text fields
 - Validated formatted fields (drop down lists, rules for valid field entry, linkage to external databases) it should be possible to link fields for validation purposes

Off-Line Capabilities

- 15.32. The system shall be configured to provide offline capabilities, where users can select folders and documents from repository to sync to local PC for offline usage. When the user connects to the system again, the documents shall be automatically synchronized both ways.

Folder Structure

- 15.33. System shall support a hierarchical structure for documents to be organized and stored into folders and sub-folders.
- 15.34. There shall be no restriction on the format of the documents to be saved to repository. Documents saved to repository shall retain the original format i.e. no conversion shall be performed unless specified.
- 15.35. The system shall be able to whitelist and blacklist the file formats that can be uploaded.
- 15.36. The system shall allow for restricting file-sizes that can be uploaded.
- 15.37. If files or folders are moved between folders, such objects shall inherit the permissions of the destination folder.

Document Templates

- 15.38. System shall support the storing of document templates in the repository. When users choose to create a new document in the repository, they will be given a list of document templates available for choosing depending on format of new document.

Check-In and Check-Out

- 15.39. The Tenderer shall ensure that the system shall support document check-in and check-out for editing of content. Documents shall be locked when it is checked out to prevent more than one person from editing the same document.
- 15.40. Users shall be able to continue viewing the document when a document is

checked out.

- 15.41. User shall be able to cancel the checkout for document that was checked out by him.
- 15.42. The versioning facility shall support major and minor versions, comment entry and version label entry. Depending on access rights users can choose to overwrite the current version or select a major or minor version increase. When a new version is created, a new version of the content and metadata is created.
- 15.43. Recycle bin feature shall be configured as per requirements from stakeholders.
- 15.44. Two Document approval workflows for seeking approvals will be provided for the following sequences 1) Draft-Approval and 2) Draft-Vetting-Approval
- 15.45. All the necessary house-keeping, system self-monitoring and tuning jobs shall be configured.

Rendition Support

- 15.46. The tenderer shall ensure that the system shall support content renditions. Renditions are different forms of the same content. For example, a Microsoft Word document could have an HTML rendition and a PDF rendition. When source document is versioned, system should re-generate the rendition automatically.
- 15.47. The system shall provide preview using Office Web Apps server that shall be implemented as part of the system.
- 15.48. Co-authoring and web-viewing of all SharePoint supported document formats including but not limited to MS Word, MS Excel, MS PowerPoint will be implemented. The document owner shall be able to specify who can co-edit the document. Audit trail of changes made to document shall be implemented.

Search

- 15.49. The tenderer shall propose a design for achieving Enterprise Search fully leveraging the features of SharePoint search such as tuning search queries and result types and item templates.
- 15.50. The Search engine shall provide features to search across all the sites and applications in the ECM System. Crawling of selected network shared drives and web-sites will be configured. Discovered files from file-servers should be viewable from SharePoint web-interface. Preview of search results shall be implemented using the necessary SharePoint components.
- 15.51. All the built-in features of SharePoint search shall be enabled and made available to users including clustering and refining of results. Users shall be able to make use of advanced search and specific meta-data to match, etc.
- 15.52. Search feature shall support confining the query to the following scopes - across the entire ECM system, within Site Collection, within a Site, within a site and its

Sub-sites, Folder and its sub-folders, Current folder, etc. The default action will be search across the Site-collection with option for user to pick a check-box/dropdown to refine the scope of search.

- 15.53. At all times, only those users with authorization to access to documents will be allowed to discover and view those documents.
- 15.54. System shall support all forms of search including Simple Search, Advanced Search, Wild-card, Phrase search, meta-data search.
- 15.55. Search Results shall display contextual information in a visual manner such as display of icons for file formats, previews of images, pdf, presentations, selected meta-data, Hyper-link to view all the detailed meta-data of a document.
- 15.56. Search results matches shall include folders. Suitable weight shall be added to folders to allow them to rise to top of search results.
- 15.57. The Search results shall be tuned such that if the keywords match a document's file-name, title, section-titles or headings, such documents shall be ranked higher in the results.
- 15.58. Search shall display a clickable breadcrumb of the file-path that allows user to navigate to folders directly.

Audit Tracking and Reports

- 15.59. The tenderer shall ensure that the activities that are performed on the repository are logged for the purpose of generating audit trails.
- 15.60. The tracking shall be driven by system events, so that events such as check in, check out, access to documents, deletion of documents, and workflow and all other activities can be logged into an audit trail. The tenderer shall provide the list of fields captured in the audit logs for the common events that occur on the ECM.
- 15.61. Each audit trail record shall contain all the important meta-data including but not limited to the event name, user name, time stamp, and the repository objects involved. Information shall be stored in database tables for easy reporting.
- 15.62. The tenderer shall develop custom reports with graphs as needed by SP. Reports shall be in Excel format. As an alternative, the tenderer can provide 3rd party tools to achieve the same functionality (Cost of tools to be included in tender cost). The detailed requirements shall be confirmed during the requirements gathering phase. Some of the reports include but not limited to:
 - Reports on the folder-structure to allow the administrator to know what are the files, folders, etc., that are created and what are the types of files filed in the repository.
 - Reports on the folder-structure and files to identify which groups and users are able to read the list of files and folders. This report shall be used for user-access rights reviews.
 - Reports on the frequency of document retrieval

- Reports about usage of Folders such as number of accesses, which users access which file/folder, etc.
- 15.63. It shall be possible to generate these reports upon request and as a monthly scheduled job.
- 15.64. The reports shall be filed in the system in a separate collection segregated by department and further categorized by month and report types. This is to facilitate audit reviews and declaration. Access shall be provided to specified reps from each department using a configuration file. The reps shall be able to submit a declaration form stating that they have conducted the review. ECM system administrator shall be able to trigger the reviews and monitor the status of declarations via a dashboard or a list.
- 15.65. The feature for reports, reviews and declarations shall be implemented as a reusable module that can be used for other sites and applications in the SharePoint farm.
- 15.66. The tenderer shall indicate a fixed cost per report for additional reports in the proposal.

16. APPLICATION PLATFORM AND CODE STANDARDS REQUIREMENTS

- 16.1. The proposed solution shall align with the following platform and technologies (or latest versions) that are currently used in SP. The contractor shall propose additional technologies if required for the proposed solution:
- Microsoft .NET Framework 4.5
 - Programming Language C# 5.0
 - Visual Studio 2012/2013
 - ASP.NET, MVC, Web API and related technologies
 - JavaScript Libraries – JQuery and Bootstrap
 - MS SQL 2012
 - SharePoint 2013
- 16.2. The contractor shall ensure that all source code provided follows industry best-practices and coding standards. Contractor shall utilize static code analysis tools to automate code-quality checks. Code shall be provided to SP from the early phases of development to ascertain code quality and for design verification.
- 16.3. Standard design patterns shall be used for design of architecture where applicable. During application design, the contractor shall work with SP team to identify functional modules or components that can be reused and implement them as web-services and stand-alone classes that can be called from other applications within and outside the system. Architecture and design recommendations shall be supported with suitable evidence and reference materials. Where applicable, working prototypes shall be provided to demonstrate and ascertain feasibility of requirements and design.
- 16.4. If the application architecture requires the use of third-party libraries or frameworks, SP shall prefer libraries that are open-source. If closed-source

libraries are necessary, the contractor shall present alternatives to SP for final decision. If the contractor uses an in-house framework or utility library, complete code, knowledge-transfer and documentation shall be provided.

- 16.5. The contractor shall provide SP with the full source-code with documentation and comments for all the deliverables of this project. The contractor shall check-in the files into a source-code version control system specified by SP (Subversion or Mercurial)
- 16.6. The contractor shall setup a full-workspace that compiles without errors on the build server specified by SP. Build-steps documentation (and build-scripts) necessary to compile the source-code shall be provided. Automated unit tests suites (e.g. Test Explorer with NUnit, xUnit.net or equivalent) shall be created during project development and deployed on the build-machine to be used as part of pre-release verification and deployment process.
- 16.7. Graphics artefacts if any shall be provided in an editable hi-res format such as Photoshop or Illustrator files.
- 16.8. The contractor shall deploy the applications to servers provided in accordance to standard deployment procedures after suitable testing. When deploying to shared servers, the contractor shall ensure that existing applications on the server are not impacted (for example due to a different version of .NET)
- 16.9. The contractor shall conduct a code walk-through and handover session to SP team. The contractor shall provide all documentation for the application including but not limited to Technical Design documents following UML standards, Unit Test cases and UAT test cases.
- 16.10. All source-code used for this project shall be provided to SP and shall be owned by SP unless otherwise stated in writing. SP shall have full-rights to use the source-code in other projects. The contractor shall not disclose, reuse or resell either in whole or in part to other parties, source-code or artefacts of this application without written permission of SP.

SECTION D

INTERFACE REQUIREMENTS

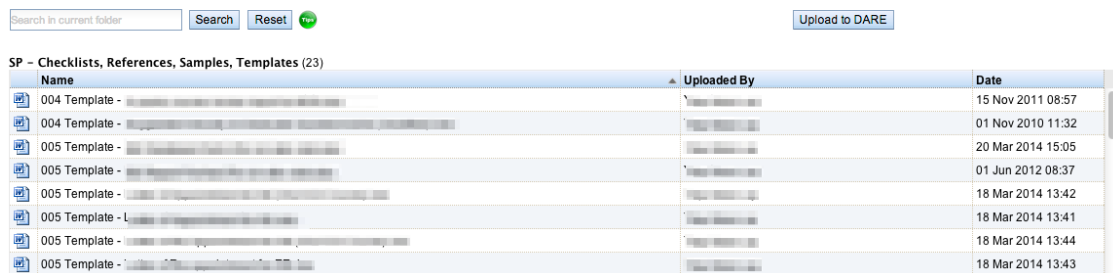
17. INTERFACE REQUIREMENTS

- 17.1. The proposed System shall interface with applications and infrastructure currently in SP.
- 17.2. Contractor is required to make the necessary modification and changes to the applications to integrate with the proposed System.
- 17.3. However any modification to backend systems has to be proposed and endorsed by SP. Contractor shall engage either SP's current vendor maintaining such backend system or the principal of the backend system to carry out such modification.

18. WEBSPHERE PORTAL INTEGRATION

- 18.1. Contractor is required to quote for this optional item.
- 18.2. SP staff portal is developed on IBM Websphere Portal v8.0. The current portlets use SP web single sign-on system (SSO) based on IBM Tivoli Access Management (TAM) system to achieve SSO. Contractor shall implement an alternative SSO approach or integrate with TAM. The contractor shall work closely with the web SSO vendor to ensure that other applications are not affected.
- 18.3. The Contractor shall enhance the two existing portlets developed for DARE and integrate them to ECM. Source code will be provided upon award. (Screen-capture of the portlets UI is shown below).
- 18.4. Portlets shall use a Single-Sign-On to retrieve information from SharePoint.

CHECKLISTS AND TEMPLATES



Name	Uploaded By	Date
004 Template - [redacted]	[redacted]	15 Nov 2011 08:57
004 Template - [redacted]	[redacted]	01 Nov 2010 11:32
005 Template - [redacted]	[redacted]	20 Mar 2014 15:05
005 Template - [redacted]	[redacted]	01 Jun 2012 08:37
005 Template - [redacted]	[redacted]	18 Mar 2014 13:42
005 Template - L [redacted]	[redacted]	18 Mar 2014 13:41
005 Template - [redacted]	[redacted]	18 Mar 2014 13:44
005 Template - [redacted]	[redacted]	18 Mar 2014 13:43

19. ACTIVE DIRECTORY FOREST

- 19.1. SP staff account resides in a SP staff AD forest while SP student account is created in a separate student AD forest. SP is in the progress of migrating the student AD from the student AD forest to SP AD forest. Contractor is required to work with the existing staff and student forests to and integrate the system for authentication and groups.
- 19.2. Groups are provisioned to AD from SP's Identity Management System (IDMS). The Contractor shall be required to perform a periodic verification and refresh any gaps between groups found in Group management system, AD and SharePoint.

- 19.3. As SP is in the progress of migrating accounts from “SD” to “STUDENT” domain, tenderer shall test out the authentication at both domain in test environment and provide the steps for the migration when SP is ready to use “STUDENT” domain in production in future.
- 19.4. The AD integration shall include the logging if there is any requirement to rely on AD logs. For examples, tenderer shall ensure the necessary log entries are captured in AD logs and they are captured correctly with enough info for log review. Tenderer shall ensure the relevant logs are extracted at the centralised location, such as sending it to a mailbox or saved to a shared folder.
- 19.5. The contractor shall setup the feature for incoming and outgoing emails in SharePoint, and make selected (pattern-based) generated email-ids of Lists and Document Libraries available in the Global Address List of Microsoft Exchange.
- 19.6. For populating of meta-data or workflow routing, the contractor shall make use of information from SharePoint User-Profiles which shall be integrated with AD to retrieve data. If additional attribute information is necessary, the contractor shall fetch data from specified data-sources e.g. RDBMS, CSV, etc.

SECTION E

TECHNICAL REQUIREMENTS

20. OVERVIEW OF TECHNICAL REQUIREMENTS

- 20.1. The information presented in this section serves to provide the Contractors, an understanding of the SP environment in which they are expected to deploy the System.
- 20.2. The System shall be deployed on Windows 2012 or higher. However, SP may choose to upgrade to the next higher version or model. Hence, where possible, the System shall be set up in a manner that will minimise effort when upgrading to the next version or model.
- 20.3. Contractor shall ensure that the software and configuration proposed can co-exist with existing clients and browser environment in SP and to make the necessary remediation, if required:
 - Windows 7 and above
 - Mac Snow Leopard and above
 - Mobile devices available in the market including Phones and Tablet running IOS 6.x and above & Android 4.x and above
 - Microsoft Office 2007 and above
 - Microsoft Mac Office 2011 and above
 - Safari 3.0 and above
 - Internet Explorer 8 and above
 - Firefox 2.0 and above
 - Google Chrome 17 and above

21. SP TECHNICAL ARCHITECTURE

- 21.1. The proposed design shall be in accordance to SP Agency Wide Technical Infrastructure standards and Whole of Government Enterprise Architecture (WOG EA) which will be provided upon award of the contract and after the signing of the Non-Disclosure Agreement (NDA).
- 21.2. The proposed infrastructure shall be hosted in SP Data Centre 1 and 3 (also known as SPICE Centre 1 and 3). The Contractor shall utilise the available network infrastructure and optimise the infrastructure to meet the requirements in this tender.
- 21.3. Contractor shall propose a System that can be supported on virtualised environments. SP uses VMware extensively in SP Data Centres.
- 21.4. Contractor shall recommend the Wintel hardware specification to meet the requirements in this tender. SP shall provision for Microsoft licences through existing Microsoft Campus Agreement, Wintel server hardware and Symantec Netbackup licences through IDA term contract.
- 21.5. The development/customisation of the System shall be carried out at the Contractor's site but from the conduct of Acceptance Tests onwards, it shall be carried out at SP.

22. MULTI-VENDOR SERVICE ENVIRONMENT

- 22.1. The Contractor is required to work with third party vendors or contractors to ensure that the service levels for both applications and IT infrastructure are met. If necessary, the project operations management procedures will have to be aligned to accommodate and/or complement SP's other existing systems.
- 22.2. The Contractor, together with SP Representative and SP's third party vendors or contractors, shall meet as often as required by SP to discuss the operational issues and other problems that may be encountered in the provision of the Services. The relevant project and technical managers or officers involved in the provision of the Services shall attend the meetings.
- 22.3. The contractor shall ensure that project specific changes to shared infrastructure shall not disrupt any other existing systems, applications or data.

23. SP INFRASTRUCTURE REQUIREMENTS

- 23.1. Hardware and Software Requirement
 - Contractor shall propose all server resources (virtualized) and system software required for the proposed environments such as test and production environments.
 - The proposal shall specify clearly the configuration of each of the proposed server such as CPU and memory configuration.
- 23.2. High Availability
 - Contractor shall ensure that the production environment design will achieve High Availability (HA) with active-active load balancing and Disaster Recovery (DR) capability across 2 different data centres within SP. The HA capability shall ensure that in the event of server unavailability within the cluster of server performing the same function, the service shall not be disrupted (but running at proportionally lower capacity) as long as one server in the cluster is still alive. The HA capability shall also ensure that SP can perform backup, OS patching/upgrade, database patching/upgrade and software patching/upgrade without or with minimum disruption to the service. If the proposed solution is based on active-passive failover, the failover shall be automated and the time taken to complete the failover shall not be more than 15 minutes.
 - The HA design shall use SP's load-balancer to load balance the servers whenever possible.
 - The HA design shall ensure that online backup (backup without the need to shutdown the service) shall be implemented for operating system, software tools, data, contents and databases.
- 23.3. Capacity Sizing
 - The Contractor shall carry out capacity sizing for the applications based on current and projected growth (20%).
 - The Contractor shall explain clearly with detailed calculations how the configuration will meet the requirements specified for system availability, reliability, response time, data storage and performance
 - The Contractor shall also state and justify all assumptions made in the calculation and substantiate the explanations with performance statistics from existing installations.

- The Contractor shall specify sizing requirement and justification. The Contractor shall propose the capacity sizing to support the application requirement.
- (a) Total number of users = 1700
- (b) Concurrent users = 150
- The Contractor shall be responsible for the performance of the application using the common services and any proposed new services.

23.4. Application Architecture

- The Contractor shall provide description and diagrams of the application architecture proposed. The application architecture describes logical components used, the relationship between the components and how components are deployed in the application. The logical components shall include SP services, new services (if any), hardware, software, interconnections and interfaces with existing environment and any other resources used.
- The Contractor shall include advantages and disadvantages of the proposed architecture.
- The Contractor shall also indicate if the application requires additional system resources, Operation support or any other specific resources. The Contractor shall propose the amount or duration for these additional resources to meet the application operational requirements.
- The Contractor shall brief SP on the proposed application architecture. The application architecture shall be subjected to SP's approval.
- The Contractor shall provide necessary scripts to facilitate deployment of applications in the test and production environments.
- The Contractor shall ensure that all applications related access shall be SSL enabled.

23.5. System backup and restoration

- SP is using Symantec Netbackup for backup of servers. Contractor shall propose the number and types of Symantec Netbackup licenses for the proposed servers and SP will procure them separately.
- Contractor must also indicate in the proposal the type of Symantec Netbackup licenses that will be able to back up the System within 5 hours.
- Contractor is required to install and configure the Symantec Netbackup software on the proposed servers.
- Contractor is responsible to install, configure and integrate the backup of the System into SP backup infrastructure to ensure that the entire system can be fully recovered using the backup.
- The backup mechanism proposed shall allow granular control to restore individual sites, lists, documents and folders.
- Online backup (backup without the need to shutdown the service) shall be implemented for operating system, software tools, data, and databases.
- In certain cases where the operating system, software and databases used is not supported by Symantec Netbackup, vendor should propose other system backup and restoration products or mechanisms.

23.6. Deployment

- All software components shall be hardened based on the software principal published best practices before performing user acceptance tests.

- Contractor shall tune the systems (including operating systems, application engine and database) based on best practices so as to achieve optimum performance of the entire system from desktop to the backend system before performing user acceptance tests.
- Contractor is responsible to install, configure and integrate the backup of the system into SP backup infrastructure to ensure that the entire system can be fully recovered using the backup

23.7. Business Continuity & IT Disaster Recovery Plan

- According to the Business Continuity Plan, the maximum tolerable outage for the system is 7 days.
- Contractor is required to develop an IT Disaster Recovery Plan (IT DRP) for the entire SharePoint System based on the template to be supplied upon award of the tender.
- The IT Disaster Recovery Plan that include recovery strategies for disasters arising from potential or likely threats which as a minimum can be classified and categorized into the scenarios described below:
 - (a) Loss of access and destruction to premises.
 - Threats that could lead to this scenario include fire, terrorism/bomb threat, building collapse and explosion.
 - The Polytechnic has an alternate data centre situated within campus. The Contractor can propose the use of this facility.
 - (b) Loss of access to the systems without physical damage to the systems.
 - Threats that could lead to this scenario include machine failure, computer virus and hacking.
 - Alternate site may not have to be activated and recovery may be performed at the primary site, e.g. recovery from backup media.
 - (c) Loss of utilities.
 - Threats that could lead to this scenario include power failure and loss of telecommunications.
 - Contractor to note that SP's disaster recovery site has an alternate power feed from Singapore Power and telecommunication link with SingTel.
- The Contractor shall ensure that all the components required to ensure the proper and timely recovery of the system in the event of a disaster for the above scenarios are supplied in this tender, unless explicitly specified and agreed upon by both parties. These components may include but are not limited to the following:
 - (a) Backup or stand-by servers, either in a cold standby, hot standby, rush order or other methods as appropriate. (Cold standby servers are not preferred)
 - (b) Redundant configuration to provide resiliency and expedite recovery, e.g. the use of clustering or backup using a spare hard-disk.
 - (c) Recovery Procedures for the various scenarios. The documentation shall include at least the following:
 - All scenarios covered and the specific procedures needed for the recovery and verification that the services are restored.
 - Configuration of the IT DRP infrastructure, the various components and their relationship or dependencies.
 - (d) Backup or stand-by Network Interface should be available when required.

- Conduct an IT DRP test exercise for the ECM System based on an agreed test scenario.
- The plan shall cover the following scenario:
 - (a) System not able to boot due to disk failure or OS corruption
 - (b) Data corruption
 - (c) Hardware and software failure or corruption
 - (d) Destruction of one data centre
- The plan shall include details such as:
 - (a) How to diagnose and troubleshoot the problem
 - (b) How to failover service from 1 data centre to another and the return home procedure
 - (c) How to perform a full operating system disk restore from backup tape media
 - (d) How to perform a full data disk restore from backup tape media
- The testing of the plan shall be included in the User Acceptance Test Plan.

23.8. Handover

- The Contractor shall work closely with SP administrators, Facility Management team or 3rd Party Contractors (collectively known as SP Operation) to ensure a smooth handover.
- The Contractor shall brief SP Operation on all relevant system setup/configuration, operational information and documents required to achieve a smooth hand-over process and allow the latter to shadow its team to learn the routine operational activities.
- The Contractor shall provide the following handover documentation:
 - (a) Application Architecture
 - (b) System setup, configuration etc
 - (c) Operational Architecture
 - (d) Operation manuals, documented processes & procedures required to put the application into production and maintenance.
- The handover documentation is subjected to SP's review and approval.
- The Contractor shall work closely with SP Operation to deploy applications.
- The Contractor shall document down all resolved incidents/problems and close all open cases and/or unresolved incidents/problems. SP reserves the right to approve which incidents or problems can be carried forward to SP Operation.
- The Contractor shall completely hand over all application, scripts or data in original source code as well as executable format.
- The Contractor shall plan resources to conduct daily briefing sessions (minimum 1 hour per session) to hand over the day-to-day running to SP Operation.
- The Contractor shall present weekly progress updates to SP for proper tracking and monitoring the progress of transition during the handover phase.
- If the Contractor demonstrates unwillingness in cooperating fully with SP Operation to achieve a smooth transition process or incomplete documentation, SP reserves the right to further extend the transition period until the whole transition

process is completed to satisfaction of SP. The Contractor shall bear the full costs incurred as result of extension.

24. SYSTEM SECURITY AND CONTROL REQUIREMENTS

- 24.1. The Contractor shall study the overall system security requirements and propose security policies and procedures for the System. The Contractor shall also implement the security design, in accordance to SP IT Security Policies, Standards & Best Practices and Policy on ICT Security. The details can be found in **Section G – System Performance, Availability & Security**.
- 24.2. The Contractor shall ensure provision of necessary security features to guard against unauthorised access, intrusion, loss of information, software errors and vulnerability to virus attacks.

25. APPLICATION SYSTEM LOGS

- 25.1. The Contractor shall submit descriptions of arrangements for elimination of detrimental efforts on the System caused by improper operation and, in connection herewith, indicating remaining risks for such efforts describing the nature of these effects.
- 25.2. The System shall have the capability of logging all transactions and updates to configurable parameters, staff's activities, attempted access and security violations. Access control logs and audit reports shall be provided.
- 25.3. The System shall automatically log all critical transaction activities to ease troubleshooting.
- 25.4. The System shall log all unauthorised attempts to access the production databases.
- 25.5. The Contractor shall recommend an audit trail analysis to perform trend and pattern analysis and report significant conditions or events that would indicate possible fraudulent use of the System.
- 25.6. The System shall provide effective control reports for reconciling the System's files and transactions. There shall be adequate control mechanisms built in to validate acceptable interfaces and flag interface problems, e.g. control reports, control totals and exception reporting.
- 25.7. The Contractor shall provide capability of retaining as well as automatically archiving the relevant logs on disk as well as backup media.

26. TECHNOLOGY PROTECTION

- 26.1. The Contractor shall keep SP informed of any new announcements of product replacement pertaining to this project and provide information on the capabilities of any new products.
- 26.2. The Contractor shall provide, at the time of delivery, products that incorporate the most current technology or standards or latest version or model. The Contractor

must provide the latest upgraded products at the time of delivery and must ensure that the latest upgraded products meet all the tender requirements.

- 26.3. Where an update or new release for the system implemented is available during the duration of the project, the Contractor shall notify SP immediately in writing, provide details on the specifications of the update/new release and advise SP on the actions to be taken accordingly. SP shall not be obliged to accept any updates or new releases.
- 26.4. At any time during the project duration, SP may require that new updates/releases be supplied at no additional charge by the Contractor and the Contractor's obligations in relation to the system shall continue to apply in all respects to the update or new releases. The Contractor shall install the updates/new releases at no additional charge.

27. IPV6 REQUIREMENT

27.1. General

- The Contractor shall design the application and software to support the co-existence of IPv4 and IPv6. If it is not compliant, the Contractor shall advise the roadmap and propose how the system can be upgraded.

27.2. Connectivity

- The Contractor shall propose and demonstrate how the system is operated in the following scenarios, but not limited to:
 - (a) Connect to legacy network and application, which support IPv4 protocol only;
 - (b) Connect to local ISP with IPv6 service and the end-user using IPv6 protocol only; and
 - (c) Connect to local ISP with IPv4 service and the remote ISP with IPv6 service, and the remote end-user using IPv6 protocol only.

27.3. Standards

- The Contractor shall
 - (a) Demonstrate how the design, software and/or enhancement* is aligned with the prevailing Singapore IPv6 Profile found in www.ida.gov.sg/, recognised international standards such as IETF, ITU and good software development practices (e.g. no hard coding of IP addresses). Exceptions to these guidelines shall be clearly highlighted.
 - (b) Provide documentation and presentation on the tests that have already undergone to meet the required functionalities to ensure a smooth transition roadmap to co-existence of IPv4 and IPv6.

27.4. Maintenance and Support

- The Contractor shall provide information on whether any patches, upgrades or additional hardware and/or software and/or services are needed to be purchased or installed in order for the proposed software and/or enhancement to support the co-existence of IPv4 and IPv6 environment.

27.5. Capability

- The Contractor should preferably have documented qualifications in IPv4 and IPv6.
- The Contractor should preferably have experience in designing and/or implementing IPv4 and IPv6 projects.

SECTION F

CONTENT MIGRATION

28. CONTENT MIGRATION

28.1. General

- The Contractor shall be fully responsible for the configuration, migration of the existing content and meta-information from DARE to ECM system. All necessary automation and verification tools for complete, automated migration shall be provided by the contractor. Migration shall not involve users expect for random sample verification. Content migration shall achieve a full-migration of the DARE system to ECM system including but not limited to:
 - (a) Cabinets and Folder structure with documents and meta-data shall be migrated
 - (b) Permission-sets (ACLs) in DARE, along with groups and users shall be migrated over to the new repository
 - (c) Folder and Document Ownership and rights must be migrated
 - (d) Linked and Virtual Documents in DARE must be migrated with suitable alternative approaches
 - (e) Existing functions in DARE to prefill meta-data, roles, etc, shall be implemented in the ECM system. ECM UI shall be simplified by hiding unneeded power-user features.
 - (f) DARE has built-in features to sync and handle group and user-rename scenarios from AD. Similar automated feature shall be implemented in ECM system to ensure that at any point of time the group and user-names shall be in sync with those in AD.
- DARE contains several cabinets owned by individual schools and departments. The contractor shall execute migration one cabinet at a time and rollout the system to respective department(s). The cabinets in DARE shall be made Read-only by the Contractor upon successful migration of each cabinet, briefing and training will be conducted by the Contractor for respective departments and schools. The Contractor shall provide learning materials such as online user-guides, videos and FAQs.
- Contractor shall ensure the data integrity of the migrated/converted contents. To prevent loss of critical data, multiple methods of automated checking must be employed and reports shall be generated to validate correct migration.

28.2. Content Migration Plan

- An overall content migration strategy, tools and detailed plan shall be proposed in the tender submission. The Contractor shall propose an overall content mapping and migration/conversion strategy. It shall incorporate the content mapping requirements and the details of contents to be converted to ensure that the System, when implemented, shall contain correct and consistent information.
- Photos and Videos, which are SP's digital assets, have to be to be migrated to a different SharePoint repository from Documents. Streaming should be supported for videos.
- The Contractor shall plan the migration/conversion of the existing contents into the System according to the implementation plan. The Contractor shall provide the content migration/conversion plan together with the preliminary design specification.
- The data migration/conversion plan shall include the following:

- (a) Tasks required to be carried out for the data migration/conversion
- (b) Cutover periods, which shall take into consideration the implementation timeline of the System. The data freeze periods have to be minimized to weekends to prevent interruption to business users.
- (c) Interim measures, if any, during the cutover period, both operational as well as system-related, to ensure a smooth transition from the current system to the new System
- (d) Content mapping between the current system and the new System

28.3. Content Cleansing and Migration/Conversion

- Where there is need to perform content cleansing before migration, the Contractor shall define the cleansing requirements and plan the required activities at least 1 month before cutover of each cabinet in DARE. The Contractor shall be responsible for directing, coordinating and reporting the progress of Content Cleansing.
- The Contractor shall be responsible and shall bear the cost to make good the contents if any inaccurate contents arise from any negligence or error on their part.
- The Contractor shall ensure the correctness of contents prior to the actual migration/conversion. If any error or inconsistency is detected, such content shall be highlighted for SP's decision and the content shall be corrected prior to the Commission date. Where necessary, the contractor shall be responsible for manual patching of data to correct any inconsistencies.
- The Contractor shall liaise directly with the current vendor(s) who are maintaining the current systems and the facility management, to extract the contents for the purpose of the content migration/conversion exercise.
- The Contractor is required to ensure that the content mapping requirements are clearly documented prior to the content migration/conversion.
- The Contractor shall ensure that there is minimal impact to the users during migration/conversion process. All the required contents shall be migrated/converted from the existing application systems across all platforms. The migration/conversion shall not cause any system unavailability to the users.
- The System shall provide full details of files migrated/converted and checks to verify the accuracy of the migration/conversion and to ensure database integrity. Error and Audit logs shall be captured during entire migration to trace the history of actions performed. Summarized and detailed reports shall be provided for verification after thorough checking by tenderer's testing team. The users shall be asked to perform verification (sampling) only after the contractor has shown evidence that migration and verification is 100% successful.
- The contractor shall use automated tools to assist in the data mapping. The tools shall be able to provide reports to compare the data before and after the data mapping exercise.
- The System shall provide means to verify the accuracy of data migration/conversion and data loading. If there is data to be corrected as a result of migration/conversion, the Contractor shall correct these data.
- If any content required by the new System is not available in the existing systems, the Contractor shall be responsible for the following:
 - (a) Coordinate the collection of these contents

- (b) Ensure the contents required and captured are verified for consistency prior to loading into the System.
- (c) Successfully load the contents into the new System.

SECTION G

SYSTEM PERFORMANCE, AVAILABILITY & SECURITY

29. SYSTEM PERFORMANCE REQUIREMENTS

- 29.1. SP has an estimated population of 1700 staff. The proposed system is expected to serve up to 150 concurrent active users during peak hours assessing the system
- 29.2. Contractor shall conduct performance load testing of the proposed solution using but not limited to the following tools provided by SP in SP live network environment.
 - IBM Rational Performance Tester
 - IBM Tivoli Composite Application Manager (ITCAM RTT)
- 29.3. Microsoft Visual Studio by vendor for initial testing if requirements can be met and further insights into performance are available from the tool. In the event other load testing and performance monitoring tools are proposed for this project, the Contractor shall provide all hardware and software required to setup these tools in SP to carry out the performance load tests, at no additional cost to SP.
- 29.4. Performance load testing shall be carried out by Contractor to demonstrate that the proposed system can meet the performance requirements
- 29.5. The load testing shall simulate 150 users accessing the System for at least 30 minutes with a think time of not more than 3 seconds between each activity per virtual user. The initial ramp-up rate will be 150 users over 5 minutes and will remain at 150 active users for the remaining period. The test scenario will need to be repeated to ensure that all 150 users are actively performing the transactions for duration of at least 150 minutes.
- 29.6. The expected response time shall be less than 3 seconds for all the transactions (measured at 95th percentile). Contractor shall tune the system and conduct the performance testing iteratively till the above performance target is achieved. The response time shall include loading all the components of the page including stylesheets, scripts, ajax calls, images, etc.
- 29.7. Contractor shall provide a breakdown of the performance timing within the end-to-end connection between the client PC and the servers so as to be able to clearly identify the component(s) that is (are) the cause of any performance bottleneck. Such breakdown shall include both hardware and software performance timing. The Contractor shall also need to help SP eliminate such performance problems. Contractor shall propose any tools required in order to meet this requirement at no additional cost to SP.
- 29.8. If the Contractor claims that the performance bottleneck is caused by SP's existing infrastructure (e.g. network), quantitative measurements must be provided by the Contractor to prove the claim.
- 29.9. If the bottleneck is due to the hardware proposed, the Contractor shall provide the additional infrastructure (hardware and/or software) required to eliminate such bottlenecks at no additional cost to SP. Supplier shall be required to implement the recommended solution and conduct the above performance testing till the performance target is achieved

- 29.10. At the end of the performance testing phase, all test plans and test results shall be compiled and submitted to SP for acceptance.
- 29.11. Contractor shall provide the test plan and test scripts for SP to conduct future load testing using the same scripts and test plan.

30. AVAILABILITY

- 30.1. The System is required to run continuously for 24 hours per day and 7 days per week. Availability is computed as (Total number of hours of scheduled uptime per year - Total hours of disruption a year)/Total number of hours of scheduled uptime per year
- 30.2. The System shall meet the Standard of Performance with a System Availability Level of not less than 98%, for each calendar month or part thereof.
- 30.3. The Contractor shall specify the shutdown time duration required for system maintenance.
- 30.4. The System shall be able to run unattended operations after normal working hours to backup databases and to run end-of-day processes such as batch job, report generation etc.
- 30.5. In the event the System is deemed to be unreliable by SP, the Contractor shall investigate the cause of the problem. After investigation, if it was found to be due to components supplied by the Contractor, or proposed server hardware is undersized, the Contractor shall carry out all remedial actions and services at no extra cost to SP. In the event the Contractor diagnoses and shows concrete evidence that the problem is due components inherent within SP services, the Contractor shall be required to propose the necessary recommendations to SP to resolve the problem.

31. RELIABILITY

- 31.1. The System shall provide recovery and restart facilities to ensure minimum downtime. Contractors shall provide clear instructions on such facilities in their respective Proposals.
- 31.2. Failure of any transaction shall not affect integrity of the data captured/stored in the System.
- 31.3. The System shall be able to recover all data stored up to the last successfully completed transaction before a system failure occurs. Contractor shall use tools which SP is currently using if possible, unless unavailable or otherwise, contractor may propose.
- 31.4. Contractors shall propose automated performance monitoring and analysis to enable proper capacity planning, tuning and maintenance.
- 31.5. The proposed automated monitoring should alert system administrator on breaching of capacity thresholds, and any service unavailability.

- 31.6. The Contractors shall work out the monitoring report mechanism and format in consultation with SP during implementation. The report should include but not limited to:
- System Capacity Utilisation, and Trend
 - System Performance (include Response Time)
 - Service and System Availability, and Trend
 - Service Usage, and Trend
- 31.7. The System shall be designed such that it provides an effective and automatic unattended backup facility.
- 31.8. All proposed system hardware, accessories and peripheral devices shall have fault tolerance and reliability features quoted for SP's consideration. These features should be commensurate with the requirements of the proposed System, and be subjected to the satisfaction of SP.
- 31.9. All software shall be fully tested and quality assured before implementation so as to ensure maximum reliability.

32. ICT SECURITY REQUIREMENTS

- 32.1. The objective of this section is to define the security requirements for the System and aims to protect the integrity, confidentiality and availability of data, Systems and operations.
- 32.2. General
- The Tenderer and/or Contractor shall note that all security requirements under this section are mandatory unless otherwise explicitly stated, and each security requirement, regardless of the sub-section it is located, shall be applicable to the entire scope of this Contract unless otherwise explicitly stated.
 - The Tenderer and/or Contractor shall note that unless otherwise stated explicitly, all additional resources and manpower provided by the Contractor to resolve IT security related issues under the responsibilities of the Contractor, such as rectifying vulnerabilities and mitigating risks, shall not incur additional cost to the Polytechnic.
 - The Contractor shall be responsible for the overall security of the System. The Contractor shall also exercise due care and due diligence to ensure security of the System, such that confidentiality, integrity, availability and accountability are assured.
 - The Contractor 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.
 - The Contractor shall communicate the appropriate security policies, standards and procedures to all its personnel.
 - The Tenderer and Contractor shall produce evidence (i.e. in written form) that they have the full support of all their products principals.
 - Tenderers, who had attained the relevant security certifications (e.g. ISO 27001) for previous projects, and have included documentary proof of these accomplishments within their tender proposal, is preferred.

- Unless the context otherwise requires, the terms used herein shall have the following meanings assigned to them that are in addition to what had been defined in the Conditions of Contract

“Personnel of the Contractor” or its equivalent shall refer to Contractor's duly appointed representatives, successors, permitted assignees, Contractor's employees, agents, partners and sub-contractors engaged to work on the System in any capacity related to design, development, implementation, operations, maintenance and troubleshooting.

“System” shall refer to all Hardware and Software that reside within or outside their operating environments, so long as they are necessarily related to the functioning of the System and the meeting of the services and other requirements as stated in the Security Requirements.

“Privileged account”, “privileged role”, “privileged user” or its equivalent shall refer to an administrator or operator account that is used to administer or perform an operational or management function to an operating system, application, network appliance, security appliance or any other device or component within the System. Examples include the system, backup, firewall/switch, database and security administrators, etc.

32.3. Security Management

- The Contractor shall follow the existing security management and governance framework in use by SP. In events where other security aspects are required, the framework shall minimally include at least the following:
 - (a) Security policies, standards and procedures for the System;
 - (b) Security architecture and design; and
 - (c) Security management and operation processes.
- The Contractor shall propose a Security Management Plan specific to the System. The Security Management Plan is a formal document that shall fully translate the IT Security Risk Register into the required security controls, processes and operations (i.e. tasks and activities) needed to achieve the security requirements for the System. The Security Management Plan shall minimally include the following:
 - (a) Security design, controls and processes (i.e. technical and procedural), such as:
 - Security Architecture;
 - Authentication and Access Control;
 - Risk Management;
 - Incident Management;
 - Patch Management
 - Backup and Recovery; and
 - Log Management;
 - (b) Roles and Responsibilities (e.g. IT Security Operations, IT Security Deliverables, etc.);
 - (c) Schedule pertaining to IT Security Milestones and expected Deliverables, which is aligned to overall Project Plan and Schedule; and

- (d) IT Security Risk Register (please refer to Risk Management section for more information)
- The Contractor shall develop, implement and maintain the Security Management Plan as well as the Security Management and Governance framework specific to the System. The Security Management Plan, the Security Management and Governance framework, as well as their subsequent updates and changes, shall be reviewed and approved by the Polytechnic.
 - The Contractor shall submit the Security Management Plan as well as the Security Management and Governance framework as part of the user requirements specifications.
 - The Contractor shall be required to develop and maintain both the existing and new (if any) security policies, standards and procedures specific to the System. The security policies, standards and procedures and their subsequent updates or changes shall be reviewed and approved by the Polytechnic.
 - The Contractor shall ensure that any deviation from the approved policies, standards, guidelines, configurations, procedures must be supported by strong justification and documented. All deviations must be reviewed and approved by the Polytechnic.
 - The System shall fully comply with the Polytechnic ICT security policies, standards and instructions as well as standards and policies issued by the Polytechnic subsequently.
 - The Contractor shall comply with the security requirements of the Polytechnic's hosting and network environments, and to liaise with the relevant personnel to ensure that the implementation adheres to such requirements.
 - The Contractor shall appoint a point of contact for all security related matters. The point of contact shall fulfil the following requirements:
 - (a) Shall be a group or person;
 - (b) Shall NOT be the same person who will be engaged in the security operations of the System; and
 - (c) Shall minimally possess the relevant experience (5 years) and qualifications (academic and professional certifications) of an IT Security Consultant.
 - (d) The point of contact shall have the following key responsibilities:
 - Shall be overall responsible and accountable for the security of the System throughout its entire lifecycle from pre-commission onwards; and
 - Shall be the interface between the Polytechnic and the Contractor, subcontractors and any other 3rd-parties on all IT security matters.
 - The point of contact shall fully participate in all security-related forums (meetings, discussions, etc) and tests albeit a secondary point of contact who is equally competent can participate on-behalf during exigencies.
 - The Contractor shall conduct regular security assessments to review the security status of the System components to ensure that all controls and measures (for example, review of policies and procedures, vulnerability assessments, system configuration reviews, log and audit trail reviews) are intact and working effectively. The Contractor shall submit reports for such activities to the Polytechnic on a regular basis (e.g. monthly).
 - The Contractor shall establish and maintain up-to-date documentation on all information and assets of the System, which minimally includes hardware,

software, network, personnel, system/user accounts, as well as all the policies, standards, guidelines, operations and security processes, procedures, system configurations and asset ownership.

32.4. Risk Management

- The Tenderer shall adopt the IDA ICT Risk Management Methodology for the Risk Management to assess security risks that impact the System and implement effective control measures for mitigating the risks.
- The Contractor shall implement the security risk management process for the System and demonstrate conformity to the IDA ICT Risk Management Methodology via deliverables such as the IT Security Risk Register and Assessment report. The security risk management framework shall cover the following:
 - (a) Risk Identification;
 - (b) Risk Assessment;
 - (c) Risk Response;
 - (d) Risk Control Activities; and
 - (e) Risk Monitoring and Review.
- The Contractor shall implement appropriate control strategies that are consistent with the Polytechnic security policies and standards, and mitigates the identified threats and vulnerabilities.
- The Contractor shall conduct regular security risk assessment to identify internal and external threats that may undermine the System security, interfere with the System or result in the destruction of information. The Contractor shall submit the security risk assessment report to the Polytechnic on a monthly basis.
- The Contractor shall ensure that all security risks associated with the System are addressed before the commissioning of the System. Business/System Owner approval is required for any residual risk.
- The Contractor shall have clearly defined roles for all information security responsibilities in accordance to the System security policy. The information security roles shall take into account the need for segregation of duties required of each role and the level of authorization accorded to the roles.

32.5. Personnel Security

- The Contractor shall observe the secure usage and handling of all the Polytechnic information. All the Contractor's personnel shall sign a confidentiality agreement to protect the Polytechnic information against unauthorised disclosures by the Contractor's personnel in the course of their work. The Contractor shall ensure that all its personnel and subcontractors are informed that failure to comply with this agreement would be a criminal offence and may also lead the Contractor to take disciplinary action against the Contractor's personnel and subcontractors.
- The Contractor shall subject all their personnel, who will be involved in the development, operations and maintenance of the System, to security clearance by the Polytechnic before commencing their work.
- The Contractor shall ensure that all the Contractor's personnel security clearance is commensurate with the highest security classification of information that he/she has been given access to. In addition, the Contractor's personnel shall only be

granted access to information that is relevant to the performance of his/her responsibility.

- The Polytechnic reserves the right at any time to reject any of the Contractor's personnel and the Contractor is responsible to find replacements immediately and at the Contractor's own cost and expense.
- The Contractor shall define and communicate the roles and responsibilities to all personnel involved in the System. The Contractor shall provide detailed description of the roles and responsibilities against the list of personnel who will be involved in the System.
- All the Contractor's personnel shall fully comply with any written instructions on security matters that may be issued by the Polytechnic.

32.6. Information Handling

- The Contractor shall be accountable to protect all information relating to the System to ensure that it is not used for other purposes unless the use has been authorised by the Polytechnic.
- The Contractor shall not disclose any security-classified information received or generated under the Contract or Tender to anyone unless specifically authorised in writing by the Polytechnic. This includes the source of the information.
- Information that has been declassified is not automatically authorised for disclosure. The Contractor shall request approval for disclosure of declassified information from the Polytechnic.
- The Contractor shall be responsible for the safeguarding of security-classified information under its care. All the Contractor's personnel are responsible for safeguarding security-classified information entrusted to them.
- The Contractor shall put in place processes to ensure that security-classified information obtained in the course of the project, are protected against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use, or modification. The process shall include administrative, technical, physical and personnel control measures. The Contractor shall protect the information regardless of the format they are held and in particular, all given information in softcopy shall be encrypted in storage.
- The Tenderer shall provide detailed description of the system the organisation use to manage and protect security-classified information and data, which shall at least include the security features, the technologies and solutions, the administration and usage processes and procedures.
- Termination or expiry of this Contract for whatever cause shall not put an end to the obligation of confidentiality imposed on the Contractor, its employees, agents and/or subcontractors under this Clause. The Contractor shall ensure that no person shall remove any security-classified information upon resignation from his/her appointment or retain such information when he no longer requires them, as all such information must remain in the possession of the Polytechnic.

32.7. Access Control

- The purpose of the authentication service is to check and validate the identity of a user. Other security services, such as access control or audit, are dependent on the authentication service to ensure that the identification of a user is correctly established.
- The Contractor shall propose and explain how the user roles, their rights management and the application access control matrix are implemented.

- The Contractor shall propose options for strict access controls to be exercised on important resources, and at the same time, provides the flexibility of assigning the access rights of other resources on a discretionary or need-to-know basis.
- Segregation of roles shall be clearly defined and documented for Privileged Users. Privileged Users refer to users such as administrator of operating system and database, security administrator as well as users with critical ERP authorisations.
- The Contractor shall ensure that individual user accounts for access to the System are granted on a job needs basis to provide clear user accountability. The user accounts shall be reviewed on a regular basis to be defined by the Polytechnic, and to ensure that redundant accounts are removed.
- The System shall provide online reports to support user account management by each school/department, e.g. active account and their respective roles assigned, inactive accounts not used for the past 'X' months, list of changes to user account and access rights for the past 'X' months, etc.
- The Tenderer shall propose security measures to prevent system and database administrators or other privileged users from having direct access to the stored data.
- The Contractor shall provide detailed description and implementation of the security measures to prevent the privileged users from having direct access to the stored data that shall at least include the security features, the technologies and solutions, the administration and usage processes and procedures.
- Strong access controls shall be used to prevent unauthorised Privileged Users from accessing important system resources, including the use of tamper evidence in the audit trails.
- The Tenderer shall propose an approval process and tracking mechanism(s) for all access to the System and information to ensure proper usage and accountability. The Tenderer shall provide samples of the relevant reports.
- The Contractor shall provide detailed description of the access approval and tracking processes and mechanism.
- The Contractor shall not allow remote access to the System unless the access is properly justified and approved by the Polytechnic.
- If data in databases are replicated, the access controls enforced on the replicated data shall be the same as the access controls enforced on the source data.

32.8. Authorisation and Controls

- The Tenderer shall propose a change control process to ensure that all changes are made in development environment and transported through the test system to production environment in a controlled manner. All application modifications shall be planned, tested and implemented as per change control process.
- All changes to configurations affecting critical information such as master data shall be controlled by the Contractor to ensure data integrity. Access to change or develop the data dictionary and / or queries shall be restricted to authorised personnel and all changes made shall be reviewed regularly.
- All components (including the following where applicable) shall be secured by the Contractor appropriately to prevent unauthorised use and modification:
 - (a) All customised programs;
 - (b) Modules and tools used to monitor, control, and configure the System;
 - (c) Remote Function Calls and Common Programming Interfaces;

- (d) Batch processing user accounts, default user accounts as well as super-user accounts;
- (e) Super user or equivalent system profiles; and
- (f) All log and trace files.
- The Contractor shall review all default settings and reconfigure them to suit operational requirements and to enhance security. All communications into and out of the system shall be secured according to industry best practices for the proposed environments.
- The Tenderer shall propose and document a process and access matrix to ensure that duties within the security administration environment are adequately segregated and adequate security authorisation documentation is maintained and reviewed regularly. As well, the Contractor shall provide a dedicated security administration function and propose a user access change management process which is to be reviewed by the Polytechnic and subsequently implemented by the Contractor upon approval. Access to all system administration functions shall also be restricted.
- The Contractor shall ensure that all authorisation groups that contain powerful users are restricted and changes to all user administration functions as well as to critical tables are authorised, logged by the system and reviewed regularly.

32.9. Authentication

- The Contractor shall leverage existing SP authentication infrastructure for user authentication.
- The Contractor shall ensure that the System supports the other authentication mechanisms such as Microsoft Active Directory and other site-specific authentication mechanism.
- The Contractor shall implement control measures that are needed to protect the integrity of the user credentials, which include the users' passwords, and other security-classified information. The Tenderer shall provide detailed description of the control measures.
- The Contractor shall implement end-to-end encryption of the users' passwords and other sensitive information. This means that the encryption is kept intact from the point of entry to the final system destination where decryption or authentication takes place.
- The Contractor shall provide detailed description of the security measures or mechanisms, which include the solutions and associated processes, for achieving end-to-end encryption of users' passwords and other sensitive information.
- The Contractor shall at least adhere to the existing SP password policy, management and distribution mechanisms in order to protect the confidentiality and integrity of the passwords.
- The System shall support enforcement rules on the password which shall at least include minimum password length, password history, password complexity, password age and account lockout (both temporary and permanent) after predefined number of invalid logon attempts.
- If passwords are stored in the System for simulated logon to any other systems, they shall always be stored in cryptographically hashed form.
- The password administration process shall be secured such that any information related to the password is not exposed to the personnel managing, administering

(including generation), safekeeping, transporting or involved in any other ways with the password.

- The Contractor shall provide detailed description and documentation of the password administration process.
- Should the Polytechnic choose an alternate 2FA solution (e.g. for user authentication, remote administrative access, etc), the Contractor shall integrate this 2FA solution into the System when it is available.

32.10. Encryption and Key Management

- The Contractor shall note that certain data are to be encrypted in the System where applicable. The Contractor shall select encryption algorithm which is currently used by SP or as recommended per Singapore Government Technology Reference Model (SG-TRM) or SP Technical Architecture. The Contractor shall implement measures and processes to ensure that there is no direct access to security-classified information to prevent unauthorised disclosure, modification or deletion of the Polytechnic's security-classified information.
- The Contractor shall provide detailed description of the security measures and processes to prevent direct access to security-classified information.
- The Contractor shall ensure that no single individual have access to the protected information and data, e.g. not a single person will know the entire encrypting key or have access to all the constituents making up these keys. The Contractor shall ensure that all cryptographic keys, which include master keys, key encrypting keys or data encrypting keys, shall be created, stored, distributed or changed without compromising the security of the cryptographic keys.
- The Contractor shall provide detailed description and documentation of how the cryptographic keys are created, stored, managed and protected.
- The Contractor shall note that certain data in the current system may be encrypted and shall make provision for the migration and re-encryption of existing encrypted data in the System. The Contractor shall provide details on how the migration and re-encryption are to be carried out.
- The System shall also encrypt selected data in transmission. The Tenderer shall propose the encryption mechanism for this purpose. The encryption mechanism shall be consistent with any other encryption algorithm used in the System and subject to approval by the Polytechnic.

33. APPLICATION SECURITY

- 33.1. The Contractor shall ensure that the application implemented is based on a multi-tier architecture which differentiates session control, presentation logic, server side input validation, business logic, database access, and system management.
- 33.2. The Tenderer shall implement the security controls for the following:
 - OWASP Top 10 risks
 - Input/Output Validations;
 - Workflow Controls;
 - Message Integrity; and
 - Out of range Validations.
- 33.3. The Contractor shall ensure that checks are conducted on its application's functional capabilities and implementation to ascertain that adequate security

measures are taken throughout the entire lifecycle of the System. The Tenderer shall provide details on how this would be done.

- 33.4. The Contractor shall ensure that all input validation failures are logged to a central location separate from system logs.
- 33.5. The Contractor shall ensure that the System 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 System is secure and robust, and not affected by known vulnerabilities. Some common examples of known vulnerabilities, which are by no means exhaustive, are listed as follows:
- Non-validated input;
 - Insecure or broken access control;
 - Insecure or broken authentication and session management (i.e. use of account credentials and session cookies);
 - Cross-site scripting (XSS);
 - Cross-site request forgery (CSRF);
 - Buffer overflows;
 - Injection vulnerabilities flaws (for example, SQL injection, XPath queries, command injection, etc);
 - Race conditions;
 - Improper error / exception handling;
 - Insecure storage of encrypted or non-encrypted data;
 - Insecure direct object references;
 - Phishing-related;
 - Denial of service (DOS) or Distributed Denial of service (DDOS); and
 - Insecure configuration management.
- 33.6. The Contractor shall ensure all administration modules of the System are not accessible via untrusted networks such as the Internet.
- 33.7. The Contractor shall ensure all confidential and restricted access sections of the System are protected by sufficiently strong authentication and proper access control.
- 33.8. The Contractor shall ensure that changes to user details deemed critical to the security of that account or profile be adequately verified before implementing the change within the System. An example of such a detail could include a user's email or postal address to which a reset password could be dispatched to.
- 33.9. Business/System Owners or their designates shall sign off the security test plans and test results for the Application System upon the completion of the security testing.

34. SYSTEM SECURITY

- 34.1. General
- The Contractor shall provide detailed description of the security mechanisms that are used in the System.

- The System shall have a timeout and automatic logout feature for non-active sessions. The Polytechnic shall be allowed to specify the duration.
- The Contractor shall develop built-in redundancies to prevent single point of failure which can bring down the entire System.
- The Contractor shall provide detailed description of the measures for preventing single point of failure that could bring down the entire System.
- The Contractor shall propose secure means, using standards such as IPSEC, SSH2 or SSLv3, to allow for direct real-time data transfer between the System and its other interfaces.
- Security configuration of critical IT resources, such as operating systems, firewalls, database and web services, shall be hardened and reviewed before the System becomes operational.
- The Contractor shall provide detailed descriptions of the system hardening and secure configuration checklists for the System, from applications down to the operating system level.
- The Contractor shall develop and maintain detailed security configurations of the System, from applications down to the operating system level.
- The Contractor shall perform periodic scanning for unauthorised codes and applications, viruses and system vulnerabilities, on the System. The report shall be provided to the Polytechnic after the completion of the scanning. If any of the security weaknesses mentioned above has been found, the Contractor shall be required to inform the Polytechnic immediately and perform follow-up actions to rid the System of these weaknesses in a timely manner.
- The Contractor shall provide detailed description of the frequency, process, products and tools, used for vulnerability scanning.
- The Contractor shall ensure that any changes to the original design, implementation and setup of the System are approved by the Polytechnic before making the change.
- The Contractor shall provide detailed description of the proposed change and security risk assessment for approval by the Polytechnic before deployment. The Contractor shall include the detailed description of this process as part of the change control process.
- The Contractor shall define and implement procedures to ensure that all data and information stored in the System are securely erased such that the stored data and information cannot be recovered when these data are not required.
- The Contractor shall provide detailed description and documentation of the procedures, tools and solutions, used to ensure secure erasure of security-classified data.

34.2. Network & Communications Security

- The Contractor shall ensure that only the required and approved network connections are allowed in the System. All unnecessary network connections and traffic shall be filtered.
- The Contractor shall ensure compliance with SP's network design which requires that all network traffic shall be routed through a properly configured firewall before leaving or allowing access to the network or subnet.
- The Contractor shall provide detailed physical and logical network diagrams to illustrate how the System will be securely designed and implemented.

- The Contractor shall specify clearly the list of network ports and services needed for the implementation of the System. This list of ports and services shall be reviewed and approved by the Polytechnic.
- The Contractor shall implement the following security design practices into the network infrastructure where applicable:
 - (a) Isolate the internal network segments from the extranet (e.g. internet) through appropriate access controls such as firewalls, reverse-proxy servers and/or application security gateways. Where possible, all incoming and outgoing traffic shall be subject to filtering and scrutiny;
 - (b) System is designed such that staff and student data are segregated. The Tenderer shall provide the design of the system as part of the proposal.
 - (c) Provide separate Development, Staging and Production environments;
 - (d) Implement strict network access controls to restrict remote administrative access to selected network segments;
 - (e) Use secure protocols or methods to manage and monitor all devices on the network;
 - (f) Use non-default network ports; and
 - (g) All network connections shall be authorized.
- The Contractor shall ensure that all data interfaces and transfers between systems and participating agencies and the System shall be secure, and comply with the existing ICT security policies, standards and procedures of the Polytechnic and said participating systems or agencies. In addition, external interfaces or connectivity to other systems that are not specified in this Tender, for example connecting to a Contractor's site for remote testing or maintenance, shall not be allowed.
- The Contractor shall propose how data transmitted between the System, and any participating agencies, shall be validated for errors and completeness.
- The Contractor shall ensure that the system is designed such that staff and student data are segregated. The Tenderer shall provide the design of the system as part of the proposal.

34.3. Security Monitoring

- The Contractor shall provide support to link the System to Cyber-Watch Centre (CWC) Security Monitoring Services, including Security Event Monitoring (SEM) Service, Network Intrusion Detection System (NIDS) Utility Service and Host-based IDS (HIDS) Utility Service. The subscription cost for CWC services shall be borne by the Polytechnic and the Contractor shall not include the cost of CWC Services in its proposal.
- The Contractor may be required to work with the CWC Contractor to implement the Network Intrusion Detection System (NIDS) and/or Host-based IDS (HIDS) in any parts of the System deemed necessary by the Polytechnic.
- The Contractor shall work with the CWC Contractor to ensure that security event generating systems and networks are fine-tuned to send only the necessary logs required by the CWC.
- The System shall be able to push a copy of the logs to the CWC log collector. Some examples of devices, components and applications with security related logs are as follows:

- (a) Intrusion Detection System (i.e. Network and Host-based);
 - (b) Firewall;
 - (c) VPN gateway;
 - (d) Network router and switch;
 - (e) Anti-malware solution;
 - (f) Web server and proxy;
 - (g) Server Operating System and services (for example, directory, DHCP);
 - (h) Database system; and
 - (i) Application (i.e. COTS and non-COTS).
- The Contractor shall ensure that all security related logs can be transferred (pushed) reliably to the CWC log collector via syslog or other agreed log transfer mechanisms.
 - The Contractor shall work with the CWC Contractor to ensure that problems attributed to the Contractor's systems/devices affecting the CWC capability to monitor the systems and networks for cyber threats are investigated, resolved within the stipulated turnaround time and effective measures implemented to prevent future occurrence of the same problems. In the event that the above dispute cannot be resolved amicably between the Contractor and the CWC Contractor, the decision of the Polytechnic shall be final.
 - The Contractor shall work with the CWC Contractor to ensure that any change to the systems and networks does not affect the cyber threat monitoring service of the CWC.

34.4. Change Control Management

- The Contractor shall provide detailed description of the change control process, which shall at least include the people involved in reviewing, authorising and implementing the change, the system products or solutions used if any.
- The Contractor shall propose a change control management process to manage changes to the security policies, standards, procedures and controls pertaining to the System. The Contractor shall document and implement the change management process which shall be approved by the Polytechnic.
- The Contractor shall ensure that any changes to the original design, implementation and setup of the System are approved by the Polytechnic before making the change.
- The Contractor shall implement a change control process to ensure that all intended changes to the production systems are properly reviewed, tested and authorized before implementation.
- The Contractor shall provide detailed description of the proposed changes and security risk assessment for approval by the Polytechnic before the implementation of any change. The Contractor shall include the detailed description of this process as part of the change control process.

34.5. Central Logging Server and Audit Trails

- The Contractor shall provide a detailed description of a central logging system to store all the application, system and security logs of the devices within the System, which shall include the servers and its applications, as well as the network and

security appliances. The logs shall preferably be encrypted and/or normalized to a consistent format without loss of data. The Contractor shall be responsible to implement, operate and maintain this proposed solution.

- The Contractor shall configure the relevant devices to send logs to the central logging system.
- The Contractor shall ensure that logs are accessible to authorised personnel only.
- The central logging system shall have capabilities to search/query audit information and generate audit reports. The Contractor shall propose the types of audit reports to be generated, which shall be reviewed and approved by the Polytechnic. The System shall have the facility to store all of its logs (i.e. application, database, network, system, security, etc.) for the following minimal durations:

- (a) Online – at least three (3) months; and
- (b) Offline / Alternate Site (i.e. archive) – at least one (1) year.

The retention periods shall be subjected to the decision and approval of the Polytechnic.

- The Contractor shall propose tamper protection measures to safeguard the integrity of logs and audit trails (for example, intentional abuse or unintentional misuse through modification or deletion). The Contractor shall implement the proposed security measures.
- The Contractor shall propose a mechanism to do the archival of the logging system. The archive shall preferably be encrypted.
- The Contractor shall conduct weekly review of all necessary logs to scan for security violations and highlight any issues or problems of concern and security violations to the Polytechnic. The Contractor shall ensure that such reviews are documented, and made available to the Polytechnic when requested. The Tenderer shall propose the processes for such regular review of logs.
- The Contractor shall log and monitor transaction/actions performed by the users/administrators/Contractor. The Tenderer shall propose adequate levels of logging to ensure that all unauthorised changes can be investigated when the need arises.
- The Contractor shall describe the processes and procedures for the maintenance and management of the audit logs.
- The Contractor shall ensure that the logs minimally include account, name, activities (both normal and exceptional activities), time, data and source of occurrence.
- The Contractor shall ensure that the individual actions of all personnel working on the System are accounted for and auditable.
- The Contractor shall enable logging on all servers, firewalls, and network devices to monitor the following critical activities:
 - (a) Successful and unsuccessful logins;
 - (b) Logouts;
 - (c) Unauthorised attempts to access resources related to the Service;
 - (d) Use of privileged functions and utilities;
 - (e) Privileged escalation;

- (f) Creation of new accounts and deletion of existing accounts;
 - (g) Changes and password updates to privileged accounts;
 - (h) Denied network traffic;
 - (i) Access violations from local and remote requests;
 - (j) Service start-up and shutdown;
 - (k) Service backup and recovery; and
 - (l) Configuration changes.
- The Contractor shall ensure that the logs are kept for the duration specified by SP.
 - The Contractor shall enforce segregation of roles to ensure that reviewer roles have no rights to the System except to the central logging system. The person assigned with reviewer role must not be assigned to another privileged role.
 - The Contractor shall ensure that all data exchanges are logged so that the parties involved can be uniquely identified and a strong audit trail of all accesses (create, delete and update at all levels) shall be maintained and proactively monitored.
 - The system clocks of all servers and network devices shall be configured to be synchronised to a common, accurate and secured time source. The Tenderer shall state in its proposal the time source that will be used.
 - The Contractor shall ensure that the retrieval of logs from the System and central logging facility for the purpose of investigation or troubleshooting is timely.
 - The Contractor shall ensure that storage used for the central logging system is dedicated for this purpose only.

34.6. Security Training and Awareness Requirement

- The Contractor shall ensure that all its personnel assigned to this project are equipped with the relevant skills and experience to operate the System. The personnel shall be familiar with the requirements of the System and shall adhere to the security policy, standards and procedures as approved by the Polytechnic.
- The Contractor shall ensure that all their personnel are informed of their security responsibilities and accountability/liability before putting the person in his/her assigned areas of work.
- The Contractor shall demonstrate that they have a comprehensive security programme to train its personnel in security and in their assigned role.

34.7. System Security Acceptance Test (SSAT)

- The Contractor shall propose a SSAT test plan that serves to demonstrate in a holistic and detailed manner that all the IT security requirements specified within the tender document are satisfied. In that respect, it therefore validates all the relevant areas of an entire IT system at the domain, server, appliance, network, application and operations level, and any other areas specified within the IT security tender requirements.
- The Polytechnic shall review and approve the proposed SSAT test plan, and reserves the right to provide input to the SSAT test plan. The Contractor shall provide the SSAT test plan at least four (4) weeks prior to the commencement of SSAT.
- The Contractor shall conduct and provide the latest vulnerability assessment results for all infrastructure components together with submission of the SSAT test plan.

- The Contractor shall perform the SSAT of the proposed solution based on the production environment or equivalent to ensure compliance with all the security requirements before the System can be commissioned. The SSAT shall be included within the Security Management Plan and shall commence together with UAT. The SSAT shall cover all changes related to SIT, UAT et cetera.
- The Contractor shall carry out the SSAT in the presence of a Polytechnic representative, and document the SSAT results, as well as any findings, recommendations and follow-up plan in the form of a report. The report shall be submitted to the Polytechnic for approval within one (1) week after completion of the SSAT. The SSAT shall be completed no later than two (2) weeks after the completion of UAT.
- The Contractor shall rectify all critical findings before report submission and provide corroborating evidence in the report. The Contractor shall implement the remaining approved recommendations within two (2) weeks upon acceptance of the report at no additional cost to the Polytechnic.
- The Polytechnic will conduct security testing on the System infrastructure and application during the SSAT. The Contractor shall rectify all critical vulnerabilities the Polytechnic identified within two (2) weeks upon notification.

34.8. System Review & Audit

- Before Commissioning of System
- The contractor shall conduct the security reviews of the System and processes before the System is commissioned, as well as to document the security findings and recommendations in a report. The security reviews shall commence at least four (4) weeks before UAT/SSAT and should be completed no later than two (2) weeks after the completion of UAT. The Polytechnic reserves the right to extend the duration of the security reviews if deemed necessary.
- Since this is a critical system Polytechnic will engage an independent third-party to perform scans periodically during the warranty and maintenance periods. The contractor shall support the third-party to facilitate the audit. The contractor shall fix all vulnerabilities identified during audits.
- The security reviews will minimally cover the following areas based on the production environment or equivalent:
 - (a) Security risk assessment;
 - (b) IT General Controls (ITGC) such as logical access over infrastructure, applications, transactions and data as well as segregation of duties on the applications, systems and network infrastructure; and
 - (c) Technical security controls.
- The Contractor shall be responsible to work with the Polytechnic and/or its appointed independent third-party in meeting the objectives of the review at no additional cost to the Polytechnic.
- Any issues identified with risk rating of MEDIUM and above shall be rectified by the Contractor within two (2) weeks upon acceptance of the report at no additional cost to the Polytechnic. The priority for rectification shall be based on risk ratings and any exception must be agreed by the Polytechnic.
- The Contractor shall be responsible to address the security findings identified during the third-party security review to a level that is acceptable by the

Polytechnic. The Contractor shall also bear the cost of any retrofitting and rectification resulting from the security review.

- After Commissioning Of System
- The Polytechnic will engage an independent third-party to conduct and complete a security review / audit on the System and processes within six (6) months after commissioning of the System to complement the pre-commission security review / audit.
- The security review / audit will minimally cover the following ITGC areas:
 - (a) Program change management;
 - (b) Physical security;
 - (c) Backup and disaster recovery; and
 - (d) Computer operation controls.
- The Contractor shall be responsible to work with the Polytechnic and/or its appointed independent third-party in meeting the objectives of the review at no additional cost to the Polytechnic.
- Any issues identified with risk rating of MEDIUM and above shall be rectified by the Contractor within two (2) weeks upon acceptance of the report at no additional cost to the Polytechnic. The priority for rectification shall be based on risk ratings and any exception must be agreed by the Polytechnic.
- The Contractor shall be responsible to address the security findings identified during the third-party security review to a level that is acceptable by the Polytechnic. The Contractor shall also bear the cost of any retrofitting and rectification resulting from the security review.

34.9. Annual Security Review/Audit

- The Polytechnic will engage an independent third-party security auditor to conduct a security review / audit on the System and operational support services bi-annually from System commissions to evaluate the adequacy of the security policies, standards and controls that are implemented.
- The Polytechnic reserves the right to extend the audit to the Contractor's subcontractors that are also involved in the System's services. This shall be at no additional cost to the Polytechnic.
- The annual security review / audit will minimally cover the following areas:
 - (a) Security risk assessment;
 - (b) ITGC review / audit for the following areas:
 - Logical access over infrastructure, applications, transactions and data;
 - Segregation of duties on the applications, systems and network infrastructure;
 - Program change management;
 - Physical security;
 - Backup and disaster recovery; and
 - Computer operation controls.
 - (c) Technical security controls; and
 - (d) Security penetration testing.

- The Contractor shall be responsible to work with the Polytechnic and/or its appointed independent third-party in meeting the objectives of the review / audit at no additional cost to the Polytechnic.
- Any issues identified with risk rating of MEDIUM and above shall be rectified by the Contractor within two (2) weeks upon acceptance of the report at no additional cost to the Polytechnic. The priority for rectification shall be based on risk ratings and any exception must be agreed by the Polytechnic.
- The Contractor shall be responsible to address the security findings identified during the third-party security review to a level that is acceptable by the Polytechnic. The Contractor shall also bear the cost of any retrofitting and rectification resulting from the security review.
- In the event that the Contractor fails the annual security audit, the Contractor shall engage the third-party independent security auditor to conduct the follow-up audit at no additional cost to the Polytechnic.

34.10. Ad-hoc Security Review/Audit

- The Polytechnic shall maintain the right to conduct reviews/audits on the System, Infrastructure components and security operations, whenever the need arises. The right to audit shall also be extended to the Contractor's subcontractors that are also involved in the System's services, as well as any outsourced services, supporting systems and processes that are managed by the Contractor and sub-contractors.
- The Contractor shall work with the Polytechnic and/or the security auditor to provide the necessary services and resources to assist in the security review/audit at no additional cost to the Polytechnic.
- The Contractor shall implement the review/audit recommendations according to the timeline agreed with the Polytechnic at no additional cost to the Polytechnic.
- The Contractor shall provide evidence, for the corrective follow-up actions carried out, to SP no later than 1-month after SP's approval of the audit report.
- In the event the Contractor fails the security review/audit, the Contractor shall engage the 3rd party independent security auditor to conduct the follow-up audit at no additional cost to SP.

34.11. Malicious Code Management

- The Contractor shall provide detailed description of the security measures and procedures to prevent malicious or unauthorized codes from harming the System and networks. The Contractor shall ensure that the proposed security measures and procedures are implemented.
- The Contractor shall ensure that any items provided (e.g. all files, CD-ROM and other storage media supplied to the Polytechnic) or installed are from authorized sources that are approved by the Polytechnic, and be free of malicious codes. Failing which, the Contractor shall be responsible and shall make good all data loss, cost of downtime, cost of removing the malicious codes from all infected items and any other costs incurred due to the infection.
- The Contractor shall scan all media (e.g. CD-ROMs, thumb drives) and laptops to ensure that they are free from malicious or unauthorized codes and obtain the Polytechnic's approval before bringing them into the hosting / servers environment.
- The System shall not contain any hidden functionalities that the Polytechnic is not aware of.

- The Contractor shall conduct a codes walkthrough for programs that perform critical functions with the Polytechnic as part of the acceptance requirement. The Polytechnic reserves the right to select such programs for codes walkthrough.
- The Contractor shall also ensure that the anti-malware solutions are updated regularly or when required by the Polytechnic, with patches and signatures from approved sources.
- The Contractor shall ensure provision of the necessary security capability to automatically scan for malware on all files being copied / transferred / uploaded into the System. Any malicious files found shall be quarantined for further verification, and the appropriate alerts and logs shall also be generated.

34.12. Security Incident Management

- The Contractor shall develop and implement a security incident handling and response plan for the System. The plan shall comply with the Polytechnic's procedures for incident reporting, and comprises at least the following:
 - (a) Monitoring of IT security incidents;
 - (b) Responding to IT security incidents;
 - (c) Assessment (e.g. cause, impact, severity) of IT security incidents;
 - (d) Recommendations for mitigation (if needed);
 - (e) Escalating or reporting to the appropriate management;
 - (f) Documenting or recording the IT security incidents; and
 - (g) Carrying out of follow up actions, e.g. recovery (if needed).
- The Contractor shall ensure that the timing to respond and handle security incident is timely.
- The System shall raise a security violation alarm to register a security violation when abnormal activities are detected. Available actions upon detection of a violation shall minimally include the following:
 - (a) Terminal message;
 - (b) Email;
 - (c) Log file;
 - (d) Terminate application or session; and
 - (e) Suspend account.
- The Contractor shall ensure that all their personnel are briefed on the security incident reporting procedures.
- All security incidents such as malware/virus infections, security compromises, unauthorised access and security vulnerabilities, shall be reported to the Polytechnic immediately. The Contractor shall take the necessary actions to ensure that all security incidents are properly handled and managed.
- In the event of any computer security incidents, the Contractor's responsibilities shall include:
 - (a) Investigating, resolving and recovering from security incidents;
 - (b) Ensuring the preservation and admissibility of evidence by protecting and documenting all access to incident information; and

(c) Exercising the prescribed incident response guidelines and procedures of the Security Incident Handling and Response Plan.

- The Contractor shall generate detailed incident investigation report/s (inclusive of logs and other evidence to support findings / suspected causes) for each incident and submit it to the Polytechnic within three (3) days from the date of incident. The investigation report should also contain details of measures (corrective, detective and preventive) which need to be implemented.
- The Contractor shall also implement preventive measures to prevent the recurrence of security incidents.

34.13. Physical Access Controls

- The Contractor shall not disclose or provide the location and address of the Polytechnic Data Centre (PDC) to any party unless it is required by work.
- The Contractor shall abide fully with the PDC Security Policies and Standards, including the security screening and clearance required for the personnel prior to the access, in the governing of the access to the PDC and the use of the hosting facility.
- The Contractor shall ensure that the access to the Data Centre, including PDC and the Contractor's premises hosting the Development Environment, and the System is limited to only authorised personnel. Permission has to be sought from the Polytechnic for any access to the System, and for any movement, dismantling, disposal or installation of hardware and software that may impact the operation of the System.
- The Contractor shall ensure that adequate physical security measures are implemented at its Data Centre for the hosting of the development environment, and to separate the System and network from other Systems hosted in the same premise. The Polytechnic reserved the rights to engage security auditor for the audit of the security of the Development Environment in the Contractor's Data Centre.

SECTION H

SYSTEM ACCEPTANCE TEST

35. TESTING AND ACCEPTANCE

- 35.1. The Contractor shall propose an overall Testing Strategy and devise the overall Test Plan which includes Test Methodology. The objective of the testing is to ensure that the proposed System satisfied all the User and Technical specifications in respect of functionality, stability and resilience.
- 35.2. The Contractor shall provide and make use of automated test tools to aid with testing where possible and with a view to ensuring that the testing is consistent and accurate.
- 35.3. Test cases shall be prepared by the contractor based on requirements and design specifications and submitted to SP for verification. Contractor shall maintain a requirements traceability matrix to ensure complete coverage of requirements implementation and verification. SP shall ask the contractor to include additional test cases if the coverage is not found to be complete.
- 35.4. The Contractor shall ensure all problems logged during the testing phase are documented for future reference and resolved prior to the implementation of the System in production unless otherwise agreed by SP.
- 35.5. The detailed procedures and conditions for testing shall include:
 - Submission of Test Specifications to SP for approval, 3 weeks before the commencement of each type of test. The test plan shall include, but not limited to the following:
 - (a) Test description, objective and requirements
 - (b) Scope of test and tests covered
 - (c) Test method
 - (d) Test evaluation criteria
 - (e) Test programs and a complete time sequence schedule of testing events
 - (f) Test team
 - (g) Test environment
 - (h) Traceability
 - The Contractor shall ensure that the Test Procedures include, but are not limited to, the following details:
 - (a) Scope of Testing
 - (b) Test Cases
 - (c) Detailed steps to execute the test
 - (d) Test Data
 - (e) Expected and Actual outputs
 - (f) Test Result/Test Execution Logs/Report
 - (g) Test Configuration
 - (h) Traceability
 - SP reserves the right to amend the test specifications.

- Preparation of a plan to set up the test environment and the configuration of the environment including hardware and software required for the implementation of the proposed System.
 - The Test logs shall record all major test activities and events in chronological sequence. It shall contain brief information on the date and time of each activity or event overall test results, observations, deviations, problems, remedial actions, etc. Evidence in the form of screen-captures shall be included in the test report to record that the contractor's team has performed a thorough test before submitting the deliverables to SP.
 - The Test Analysis Report shall contain a summary of all the test results on each test unit. It shall provide a summary and diagnosis of errors and deficiencies discovered and the follow-up actions to be taken, including the urgency of each correction. A "sign-off" by the users is required for the test items that have successfully passed all the necessary test and ready for production.
- 35.6. The Contractor shall provide the System Test Plan for the following, but not limited to:
- System Installation test, that includes:
 - (a) Connectivity Test
 - (b) Backup and Recovery Test
 - (c) Security and Authorisation Test
 - System Integration Testing, including high availability and disaster recovery scenarios.
 - Performance and Load Testing
 - User Acceptance Testing
- 35.7. All above test results shall be properly documented by the Contractor and made available to SP for inspection or verification, if necessary.
- 35.8. Contractor shall supply all consumable items and Tools for the Acceptance Tests.

SECTION I

TRAINING AND AWARENESS PROGRAMME

36. TRAINING

- 36.1. Contractor shall provide training to meet three main objectives:
- Pre-requirements gathering briefing on SharePoint to educate the stakeholders on Document Management with SharePoint, best practices and Out-of-the-box features available
 - To enable users and nominated personnel (end-users and power-users) to operate and use the System
 - To enable nominated technical personnel to operate and maintain the System
 - To enable a transfer of technology from the Contractor to the nominated technical personnel
- 36.2. The Contractor shall provide training onsite to enable SP Operation to operate and use all the features/functionalities delivered in the new System. The contractor shall also provide briefings and hands-on training to all users on the operation of the new System. The briefings and hands-on training to end-users shall be provided in 10 sessions for users' choice of attendance. The Contractor shall submit a training proposal indicating the schedule and type of training needed for them. Additional training sessions will be procured using the man-day rate if necessary.
- 36.3. The Contractor shall provide training for SP Representatives who are identified to conduct the Acceptance Tests, in order to guide the personnel on how to conduct the tests. The training shall be conducted at least two weeks before the commencement of the Acceptance Tests. The training shall cover, but not limited to the following:
- Guidance on the scope of tests and preparation of test scenarios for the System
 - User of the System
- 36.5. SP reserves all rights to accept part or all of the training courses and the Contractor shall be required to make the necessary amendments to the training course and materials wherever necessary.
- 36.6. SP will provide the premises and training facilities. Contractor shall set up the System or training facilities for the training purpose.
- 36.7. The medium of instruction and training documents shall be in English. Contractor shall supply each trainee with a complete set of training documents and materials, and trainees shall be allowed to keep the training materials. The set of training documents and materials provided by the Contractor shall be clear, concise and documented using user friendly terms and editable Microsoft word format. Contractor shall be required to make necessary amendments to the training materials whenever necessary upon request by SP.
- 36.8. For every course conducted by the Contractor, a complete set of the instruction guides, together with the presentation material in editable Powerpoint format, shall be made available to SP.
- 36.9. Contractor shall prepare an online version of the presentation slide with voice-over. This will allow SP to use the same material for future new staff training.

- 36.10. In the event where the feedback gathered on any training conducted by the Contractor is less than 85% with average rating. SP has the right to request for re-training.
- 36.11. Training shall be provided for all SP Operation staff that will be involved in the running of jobs for the System. The level of training shall be comprehensive and shall cover the usage of the System, system architecture, interface components and any other areas necessary for them to develop their local processes.
- 36.12. As part of the training materials for the Administrators, Contractor shall prepare a list of Frequently Asked Questions (FAQ), which cover the common error messages and rectification steps.
- 36.13. During the early phases of the project, the contractor shall maintain a web-site to create awareness among SP users. The web-site will include but not restricted to the following issues related to change management for the users:
- How the migration will affect them?
 - When and how their documents be migrated?
 - What tasks will be required of them to complete the migration?
 - Co-existence limitations and workarounds
 - Frequently Asked Questions

SECTION J

CHANGE CONTROL MANAGEMENT

37. INTRODUCTION

- 37.1. The aim of change control management is to ensure that all proposals for changes to the System are properly evaluated in terms of their costs, benefits and priorities.

38. CHANGE CONTROL MANAGEMENT REQUIREMENTS

- 38.1. The Contractor shall propose a Change Control Procedure describing how all proposed changes to the System or any of the subsystems are to be executed. The procedure will cover progress of a proposed change from its formal definition through to its implementation in a released version of software, or to its disposal for other reasons.
- 38.2. The Contractor shall provide services for the optional enhancement/changes to the System. SP shall raise Service Requests (SR) for such Services.
- 38.3. The Contractor shall ensure that all proposals for changes to the System are properly evaluated in term of costs, benefits and priorities.
- 38.4. The Change Control Procedure shall minimally include:
- Raising of SR through a service request form, detailing the proposed change and creating a log entry
 - Estimation of the resource cost, elapsed time for implementing changes and the impact on the System
 - Evaluation and approval of the proposed change
 - Definition of specific change to be applied to the modules of software, hardware and the documentation
 - Handling of changes to the existing System
 - Testing and acceptance of the modified System
- 38.5. The Contractor shall propose an SR format to facilitate a uniform submission of requests by the users. The SR form shall include details on the impact of changes to the System. The proposed SR format shall be approved by SP.
- 38.6. The Contractor shall ensure that programs/components/objects can be executed by client machines without the need to incur manual effort and installation into individual clients.
- 38.7. The Contractor shall ensure that there is proper version control for programs/components/objects and documentation.

39. CLASSIFICATION AND SERVICE REQUEST SERVICE LEVELS

- 39.1. The Contractor shall assess the man effort required for every SR and submit a SR evaluation document to SP. Effort is subjected to approval by SP.
- 39.2. All SRs shall be assessed, completed and implemented based on the following:

Estimated SR Man-day Effort	Response Time	Elapsed Completion Time Upon Approval of SR
Less than or equal to three man-day	Within three working days	Within five working days
Greater than three man-day but less than or equal to twenty man-day	Within five working days	Within two calendar weeks
Greater than twenty man-day	Within ten working days	Based on mutual agreement between the Contractor and SP
Urgent request	Within one working days	Based on mutual agreement between the Contractor and SP

Note: The ‘Response Time’ shall be the time taken by the Contractor to perform impact analysis and resource estimation for the SR

40. SERVICE REQUEST MANAGEMENT

- 40.1. SP shall prioritise the SR raised.
- 40.2. Contractor shall however note that in case of change of request priority by the users or under any unforeseen circumstances. SP reserves the right to re-prioritise SRs given earlier.
- 40.3. In the event that an SR cannot meet its handover deadline, it shall be the Contractor’s responsibility to prioritise the SRs with agreement from SP.
- 40.4. Contractor is responsible for ensuring that SR is successfully implemented according to agreed schedule based on agreed man-effort. If the Contractor cannot meet the pre-agreed schedule or man-efforts, any additional costs incurred shall be borne by the Contractor.
- 40.5. The Contractor shall note that the implementation of an SR may be on a one-time basis or in phases, to be specified by SP.
- 40.6. Software version control should be implemented based on the system used in SP.
- 40.7. The Contractor shall prepare relevant test scripts in a manner acceptable to users performing such tests and approved by SP. The Contractor shall make available necessary resources to facilitate such testing efforts and shall undertake to rectify errors surfaced during the tests to the users’ satisfaction.
- 40.8. The SR shall be subjected to UAT in the test environment, unless otherwise agreed by SP. The Contractor is allowed to use the test environment in SP for the purpose of rendering support services for this project. The test environment may be used for other projects by SP and other parties. The contractor shall ensure that existing services and applications are not disrupted.
- 40.9. The SR is considered as completed after the amended System has been implemented to Production environment and when all relevant documentations are prepared/updated and accepted by SP. For phase implementation, the System can be cutover to ‘live’ in phases.

- 40.10. Notwithstanding approval given by SP to any of the Contractor's proposal, designs and specifications, the Contractor shall remain solely responsible for the completeness and adequacy of the design, performance and specifications within the scope for any amendments made to the System.

41. SERVICE REQUEST EVALUATION REPORT

- 41.1. The Contractor shall submit a Service Request Evaluation Report that set out the requirements for the facilities and functions to be developed or enhanced and propose the manner in which work can be completed. It is anticipated that some matter of detail may have to be clarified during the early stages. In this context, SP reserves the right to issue written clarifications to the Service Request Evaluation Report to set out SP's requirements more precisely.
- 41.2. The Service Request Evaluation Report for any change request raised shall consist of requirement studies, impact analysis and evaluation. The Contractor shall provide these Service Request Evaluation reports.
- 41.3. After the receipt of the SR Evaluation Report, SP shall:
- Approve the SR based on the Contractor's assessment of effort
 - Confirm its requirement for the change, subject to the resolution of queries arising out of the SR. Both parties shall meet for the resolution thereof. At the conclusion of such meeting, SP shall at its sole discretion whether to approve the SR based on the Contractor's latest assessment or withdraw its requirement for the change concerned
 - Reject or amend the SR or request the Contractor to amend its Assessment of Effort or take follow up action until the SR document concerned has been approved by SP and the Contractor

42. PAYMENT SCHEDULE FOR SERVICE REQUESTS

- 42.1. Each SR shall be paid in full after completion, deployment into production of the change request and acceptance of the required documentation.

SECTION K

IMPLEMENTATION

43. INSTALLATION AND IMPLEMENTATION

- 43.1. Contractor shall supply a detailed implementation plan and shall assume responsibility for the overall implementation of the System. Contractor shall provide SP with the implementation strategy and approach. If existing hardware/system is being changed, the contractor shall ensure that existing applications and services are not disrupted in any fashion.
- 43.2. Contractor shall provide on-site qualified and competent personnel with relevant experience to co-ordinate all work involved and to liaise with other parties when necessary to ensure the successful implementation of the System.
- 43.3. All software supplied or proposed by the Contractor shall be new and of the latest version except otherwise stated in the Contractor's proposal and accepted by SP in writing.
- 43.4. Contractor shall provide advice on all matters pertaining to the installation and operation of the System, including but not limited to data communication and performance tuning.
- 43.5. Contractor shall provide site preparation services. The site preparation services shall include the following:
 - Study of site requirements such as network connectivity
 - Advice on acquisition of hardware and software
 - Oversee and ensuring that sites are ready to implement the System

SECTION L

DOCUMENTATION

44. DOCUMENTATION

- 44.1. Contractor shall ensure that proper documentation of new system configurations, changes made and reasons or rationale for change are recorded for traceability.
- 44.2. Contractor shall ensure that all documents are properly versioned and information in the documents is up-to-date.
- 44.3. All deliverables are considered in-complete until proper signed-off is obtained from the appropriate stakeholders for the documents.
- 44.4. All documentation shall be in good, simple and concise English using accepted technical terms and symbols. Where necessary, graphical representation shall be used (e.g. flow chart or diagram). All such documents shall have comprehensive indexes to facilitate quick references.
- 44.5. All final and signed-off documentation shall be made available in CD-ROM in editable Microsoft Word format for ready reference and subsequent maintenance.
- 44.6. All documents produced by the Contractor in fulfilling this contract, shall become the property of SP. SP reserves the right to reproduce, at no cost whatsoever, any documentation supplied with the System for its own use. Prior approval must be obtained from SP for any reproduction and distribution of documents produced by the Contractor in fulfilling this Contract.
- 44.7. Contractor shall be responsible for the provision of adequate and suitable documentation in respect of the System. All documentation shall be completed and delivered to SP as a pre-requisite to System commissioning.
- 44.8. Contractor shall adhere to the ISO9001:2000 compliant standards or other documentation standards for quality records. All documentation shall be completed and delivered to SP as a pre-requisite for payment.
- 44.9. Contractor shall provide satisfactory answers to any reasonable queries raised by SP concerning any information stated in the documentation.
- 44.10. The project documentation to be delivered by contractor shall include but is not limited to the following:
 - Project Plan
 - Project Schedule
 - Progress Report
 - Functional Requirements
 - Technical Requirements
 - Network and System Architecture and Design
 - Software System Architecture and Design (UML Standards)
 - Data Management Plan
 - Data Model, Data Schema and Data Dictionary
 - Database Design and Specification
 - Data Migration Plan
 - Installation Manual

- Configuration Manual
- System Test Plan
- User Acceptance Criteria, Test Plan, Report
- Performance Test Plan
- System Hardware and Software Inventory List
- User Guide
- Operation Guide
- System Administration Guide
- SharePoint Governance, Deployment and Standards
- IT Disaster Recovery Plan
- Change Management Plan (during project)
- Handover Plan
- Security Assessment Report
- Training Guide
- Metadata Profile and Glossary

44.11. The service documentation shall include but is not limited to the following:

- Training Plan, Training Guide, Awareness Programme and materials
- Change Management Plan
- System Operation Manual, including system operation, database archival, configuration, database backup and recovery etc
- System Administration and System Security Guide
- User Guide/User Operation Manual based on IND T Guidelines on User Guide.

45. QUALITY MANAGEMENT SYSTEM (QMS)

- 45.1. Contractor shall preferably be ISO9001:2008 certified.
- 45.2. Contractor should align its quality processes and procedures with SP QMS.
- 45.3. A copy of SP QMS shall be given to the Contractor upon contract is awarded.
- 45.4. Contractor shall explain in detail the quality controls that would be put in place to ensure that the System delivered is of high quality.
- 45.5. The QA plan shall cover at least the following areas:
 - Quality assurance activities and procedures for carrying them out
 - Standards, practices and conventions to be applied to the project
 - Duties and responsibilities of project personnel pertaining to QA
 - Fault reporting control and progress

SECTION M

PROJECT MANAGEMENT

46. MOBILISATION OF PERSONNEL REQUIREMENTS

- 46.1. Contractor shall mobilise his proposed manpower composition within 7 calendar days from the issue of Letter of Acceptance by SP.

47. PROJECT ORGANISATION

- 47.1. Contractor shall submit a detailed project structure clearly specifying the duties and responsibilities of all the personnel assigned to the project.
- 47.2. Contractor shall also provide a detailed resume for each of these personnel.
- 47.3. The project team shall comprise, but not limited to personnel with the following areas of expertise/skill:
- Project management
 - Application design and development (Especially Documentum and SharePoint)
 - Infrastructure architecture design
 - Database design and administration
 - IT security
 - Training
 - Quality assurance
- 47.4. As the System will be used by almost all SP staff, it is important that the personnel working on this project must have good communication and change management skill.
- 47.5. The key technical personnel working on this project shall possess Microsoft SharePoint certifications.
- 47.6. SP shall not be liable for loss or damage to the Contractor's property placed or left on SP's premises. All equipment and property belonging to the Contractor will be placed on SP's premises solely and entirely at the Contractor's own risk.
- 47.7. Contractor shall monitor and manage effectively any sub-Contractors that have been selected in the discharge of their duties to meet the requirements established. All matters that require interface between the sub-Contractor shall be co-ordinated by the Contractor to ensure harmony in the relationship among all parties concerned and to establish a common understanding of SP's requirements.
- 47.8. All sub-Contractors engaged by Contractor are subjected to SP's prior written approval.
- 47.9. SP representative shall be assigned throughout the duration of the project to manage the Contract. He will monitor the progress of the project, conduct checkpoint reviews and ensure the timely and quality delivery of the deliverables.
- 47.10. Contractor shall designate a Project Manager to manage the project. He shall be subjected to SP's approval. The contractor shall ensure that the key team members such as PM, Solution Architect, Business Analyst are stationed in Singapore and available throughout the project to be physically present at SP.

47.11. As project management is one of the key factors in ensuring the smooth deployment of the services, the appointed Project Manager shall possess the relevant experience, attitude and skill sets to ensure a successful project completion.

47.12. Relevant Experience

Contractor's proposed team should possess the experience and track record of migration of data into SharePoint preferably from a Documentum System within the last 5-years. The proposed tools must be used in the previous project.

Contractor shall submit at least 2 customers' references in the SharePoint platform projects that SP can contact.

48. PROJECT MANAGEMENT PLAN

48.1. The Contractor shall produce and maintain a detailed Project Management Plan showing the proposed strategy and approach of the complete development life cycle and the dates of all identifiable activities necessary for the commission of the System. The Contractor shall take into consideration the deadlines set by SP. The Project Management Plan shall be submitted to SP within 2 weeks of the issue of the Letter of Acceptance (LOA) by SP.

48.2. After issue of the LOA by SP, the Contractor shall update the Project Management Plan at least monthly to show the expected and actual completion dates. The updated Project Management Plan shall be made available to SP for review and approval.

48.3. The Project Management Plan shall include activities to be carried out by SP as well as all other people whose actions are required. The Project Management Plan shall include a diagram depicting the reporting structure and the key personnel who shall be involved in the project. It shall specify clearly the roles and responsibilities of all personnel assigned by the Contractor to the project.

49. ROLE OF SP REPRESENTATIVE

49.1. The Contractor shall involve the SP Representative at all project meetings and the SP Representative shall review all project deliverables. The SP Representative shall be involved in the whole development cycle of the System. However, the Contractor shall be fully accountable for the quality of the deliverables and for the delivery of the System on schedule.

49.2. SP Representative shall have the right to endorse all minutes of meetings to be produced by the Contractor. The Contractor shall keep SP Representative closely informed of the progress of the project at all times to enable him/her to determine whether all deliverables for a particular milestone are completed on schedule and whether the quality of the deliverables meets SP's requirements.

49.3. Upon attaining a milestone in the project schedule, the appropriate work and deliverables must be signed off by SP Representative after endorsement by the relevant approving committees. The sign-off shall signify that all requirements for that milestone have been met. SP reserves the right to withhold the sign-off

until all works and deliverables meet the requirements.

- 49.4. SP Representative shall be the single point of contact to the Contractor's Project Team.

50. PROJECT MANAGER (CONTRACTOR)

- 50.1. Contractor's PM is expected to have the following knowledge and experience:

- Possess related IT experience in messaging and at least five years in IT project management.
- Possess prior experience in managing project of such nature, scope and scale.
- Possess good communication skills in English
- Be conversant with the products and services that the Contractor is offering
- Be conversant with the methodology the Contractor is adopting for deployment
- Be Customer-oriented and possess experience in dealing with IT requirements from the business perspective.

51. ROLE OF PROJECT MANAGER

- 51.1. The Contractor's Project Manager must ensure that the deliverables are in accordance with the Requirement Specifications and completed on schedule. He will undertake full responsibility for the quality of work produced by his team and the sub-Contractors, if any. This includes ensuring that there is consistency and uniformity in the different work produced by his team and the sub-Contractors.
- 51.2. The Contractor's Project Manager will serve as the liaison between SP and his team members and shall report to SP periodically on the progress of the project. The frequency of the progress reporting shall be determined by SP.
- 51.3. Reviews of each milestone shall be incorporated at suitable junctures throughout the project. The Contractor is required to participate in all the reviews with SP. The Project Manager is expected to attend all reviews with SP. If the Project Manager is not available, a person of equal or higher seniority who shall have good knowledge of the project status and issues shall represent him. This person shall preferably be from the committee which the Project Manager reports to. Such changes in representation must be formally communicated to SP and shall be agreed upon by SP prior to the review meeting.
- 51.4. SP Representative shall call progress meetings at regular intervals. The Project Manager is expected to be present at each progress meeting and report the progress on the execution of contract at the meeting. If the Project Manager is not available, a person of equal or higher seniority who shall have good knowledge of the project status and issues shall represent him. This person shall preferably be from the committee which the Project Manager reports to. Such changes in representation must be formally communicated to SP and shall be agreed upon by SP prior to the progress meeting.
- 51.5. The Project Manager shall be responsible for establishing the time and agenda for each progress meeting in accordance with the milestones. The Project Manager must be prepared for each progress meeting with the necessary details for

discussion. The Project Manager shall notify to SP Representative which SP staff that may need to attend the meeting. He shall also ensure that all relevant personnel from the Contractor are prepared for the progress meeting.

- 51.6. All minutes of progress meetings shall be produced by the Project Manager and presented, within three days to SP Representative for endorsement.
- 51.7. The Project Manager shall co-ordinate the various activities within the development team, with the sub-Contractors, SP and the SP's third party Contractors and documents the progress of the project. The Project Manager shall maintain records of all activities performed during the contractual period.
- 51.8. The Project Manager shall inform SP of any impending slippage in the delivery dates and any matters likely to impede the progress of the project. The Project Manager shall recommend alternatives for SP's review and discussion.
- 51.9. SP shall have direct access to the Project Manager at all times during the performance of this contract and if the Project Manager is absent from Singapore for any duration, the Contractor shall inform SP minimally one month in advance, and designate another employee who must possess good knowledge of the project status and issues to perform its duties and functions. Such presentation must be formally communicated to SP and agreed upon by SP.
- 51.10. If the performance of the Project Manager is below expectation, SP shall escalate to the Contractor's management for necessary action to replace the Project Manager. The Contractor shall provide the replacement personnel within 2 weeks of notice from SP. All commitments from the Contractor, in terms of project schedule and deliverables, shall continue to apply.

52. PROGRESS REPORTING

- 52.1. The Project Manager shall provide progress and status reports at regular intervals to SP Representative. As a guide, Contractor shall submit monthly progress report by the 1st working day of each subsequent calendar month, commencing from the issue of the Letter of Acceptance by SP to the completion of the project. The format of the progress report will be given to Contractor by SP. However, the Contractor may be required to produce ad hoc progress reports as required by SP. Such ad hoc progress report shall cover all tasks which are in progress or which were scheduled to begin or end that month.

53. REPLACEMENT OF PERSONNEL REQUIREMENT

- 53.1. The Contractor shall not initiate changes in key personnel throughout the development of the System and during the System Warranty Period. Replacement of key Contractor personnel shall be permitted only after 3 months from the expiry of the system warranty period.
- 53.2. In the event of a need for replacement of key Contractor personnel, the Contractor shall seek prior approval from SP in writing at least 3 months prior to the date of replacement, indicating the personnel to be replaced, reasons for the replacement and particulars of the new personnel who will be assuming the responsibilities

concerned. SP reserves the right to accept or reject the proposed replacement personnel.

- 53.3. The Contractor shall be responsible for training the replacement personnel to be technically competent to carry out the works. The replacement personnel shall be available for at least a reasonable period (duration to be stipulated by SP) for the existing personnel to hand-over his responsibilities and duties. The cost incurred for the provision of the replacement personnel during the handing over period shall be borne by the Contractor.

54. DATA PROTECTION

- 54.1. The Contractor shall take all reasonable measures to ensure that personal data held in connection with this agreement is protected against loss, and against unauthorised access, use, modification, disclosure or other misuse, and that only authorised personnel have access to the data.
- 54.2. The Contractor shall not disclose any personal data obtained in connection with this agreement only for the purposes of fulfilling its obligations under this agreement.
- 54.3. The Contractor shall not disclose any personal data obtained in connection with this agreement without the written authority of SP. The Contractor shall immediately notify SP where it becomes aware that a disclosure of personal data may be required by law.
- 54.4. The Contractor shall not transfer personal data held in connection with this agreement outside Singapore, or allow parties outside Singapore to have access to it, without the prior approval of SP.
- 54.5. The Contractor shall ensure that any employee of the Contractor or any sub-contractor, requiring access to any personal data held in connection with this agreement makes an undertaking in writing to not access, use, disclose or retain personal data except in performing their duties of employment and is informed that failure to comply with this undertaking may be a criminal offence and may also lead the Contractor to take disciplinary action against the employee.
- 54.6. The Contractor shall in respect of any personal data held in connection with this agreement immediately notify SP where the Contractor becomes aware of a breach by itself or any sub-contractor.
- 54.7. The Contractor shall in respect of any personal data held in connection with this agreement co-operate with any reasonable requests, directions or guidelines of SP arising in connection with the handling of personal data.
- 54.8. Data protection clauses shall continue to have effect after the termination or completion of this agreement.

55. PROJECT TECHNICAL REVIEWS

- 55.1. The Contractor shall provide SP with a schedule of the technical reviews to be performed on the system design. The technical reviews to be carried out are to

ensure the following:

- Completeness of interfaces between the System and other SP systems
- Robustness of the application infrastructure and system architecture
- Performance of the System taking into consideration the requirements for the various performance standards.

- 55.2. For all technical reviews, the Contractor shall document and keep all records of the review discussions, the rationale and final decision on the approaches and strategies approved and adopted by SP as part of the Quality Assurance records. Contractor shall grant SP access to all such technical review records.

SECTION N

RIGHTS TO THE SOFTWARE & DOCUMENTATION

56. RIGHTS TO THE SOFTWARE & DOCUMENTATION

- 56.1. Contractor shall not disclose, release or sell to any third party or otherwise deal with any work developed for the purpose of the delivery of the System or the documentation associated with such work without SP's prior consent in writing.
- 56.2. The Contractor's obligation under this Contract shall extend to enable SP to disclose information relating to the System to third parties for the purposes of such third parties undertaking the performance of services for SP.
- 56.3. SP reserves the right to customise and/or modify the Software and documentation delivered under this Contract solely for its own internal use.
- 56.4. SP reserves the right to use any of the Contractor's standards, methodologies, procedures and approaches delivered under this Contract solely for SP's own internal purpose.

SECTION O

PERFORMANCE GUARANTEE PERIOD/SYSTEM WARRANTY

57. PERFORMANCE GUARANTEE PERIOD/SYSTEM WARRANTY

- 57.1. After UAT and system commissioning, the system shall enter a Performance Guarantee Period (PGP) of 90 working days. A System Warranty Period of 12 months will start after successful completion of the PGP.
- 57.2. The system shall have successfully completed the PGP if it meets the standards of SLA and performance specified in this tender for a period of 90 working days. If the PGP cannot be met successfully due to a breach in SLA or a Priority 1 or Priority 2 defect, the PGP will extend day to day until the system is able to meet the specified standards of SLA and performance over a period of at least 30 consecutive working days. The total period of PGP will not being less than 90 working days after the commissioning date in any situation.
- 57.3. During the PGP and System Warranty Period, Contractor shall at all times and under all conditions be entirely responsible for the satisfaction operation of the System, and for the compliance of such additional requirements as may be mutually agreed upon between SP and the Contractor at no cost to SP. The terms of support will be same as those outlined in SECTION Q - SUPPORT & SYSTEM MAINTENANCE.
- 57.4. During the PGP and System Warranty Period, the Contractor shall render replacements/investigation/services and any other works required to make good all defects in the System at no cost to SP.
- 57.5. Contractor shall unconditionally guarantee that the amended System comply with SP's specifications.
- 57.6. Time shall be the essence in rectifying the defects reported to the Contractor during the PGP and System Warranty Period. In the event that any of the Software is found to be defective within the PGP or System Warranty Period, Contractor shall use its best effort to rectify the defects. Contractor shall not be relieved of his obligations stated herein until SP is satisfied that the repaired System performs satisfactory. Where the Contractor fails to remedy the defect, SP may have the System rectified by third party service providers and all costs and losses incurred by SP in this regard shall be borne by the Contractor. SP reserves the right to extend the the PGP and/or System Warranty Period if all defects are not satisfactory rectified by the end of the PGP and/or System Warranty Period.
- 57.7. Contractor shall provide production support and render investigations, services and any other works required to make good all defects at no cost to SP. SP will provide a written notice of such defects to the Contractor. The defects include production data errors arising from logic errors and performance related issues.
- 57.8. The assistance provided shall be on all services required to ensure the smooth running and availability of the System.
- 57.9. The Contractor shall note that the defects must be rectified in accordance with service levels spelt out in this document.

SECTION P
INCIDENT/PROBLEM MANAGEMENT

58. INTRODUCTION

- 58.1. The aim of incident management is to ensure that all incidents are attended to as soon as possible, so that the disruption caused by the incident to the operation of the System is minimised.
- 58.2. During the project phase, incidents will be classified as issues, whereas after the System is commissioned, it will be classified as incident.
- 58.3. A problem could arise from incident. A problem indicates an error in the IT infrastructure and remains at this state until a cause is found.

59. INCIDENT MANAGEMENT REQUIREMENTS

- 59.1. Contractor shall submit an incident management procedure illustrating the steps required to handle the incident from occurrence to resolution. The incident management procedure shall include the following steps:
 - Report all incidents through the incident report form, which shall be provided by the Contractor and create a corresponding log entry
 - Log all status information throughout the incident life cycle.
 - Identify the source of incident up to its component level
 - State any bypass/recovery procedures available for partial or complete circumvention of an incident prior to a final resolution. Take corrective action to fix the incident under the Change Control Procedure. Contractor shall take all necessary preventive action to deter the re-occurrence of the same or related incident.
- 59.2. Contractor shall have a mechanism to manage incident reporting of the System when it goes 'live', including during the System Warranty Period and maintenance period of the System.
- 59.3. Upon receiving an incident, Contractor shall assign the incident a ticket number. SP will review the form used by the Contractor to capture the incident, and may propose its own form to use.
- 59.4. Contractor shall maintain a master list all the issues, incidents and problems. SP may request for this list at any point in time for review.
- 59.5. The Contractor shall submit a detailed incident investigation report to SP within three (3) days from the date of incident. The investigation report should also contain details of measures (corrective, detective and preventive) which need to be implemented.
- 59.6. The Contractor shall implement preventive measures to prevent the recurrence of security incidents.

60. SERVICE LEVEL FOR INCIDENT RESOLUTION TIME

- 60.1. The response time shall start at the time when SP Service Desk or SP user makes a call to the Contractor's helpdesk or support hotline.



- 60.2. Incident resolution time shall commence from the start when SP Service Desk or SP Project Manager makes a call to the Contractor's helpdesk or support hotline till a solution is provided to resolve the incident.
- 60.3. Contractor shall ensure that all Helpdesk calls are attended to as per Service Levels defined below.
- 60.4. Incident resolution time shall depend on the priority level of the incident. The priority level is determined by a combination of its impact and urgency. The definitions below are used to establish the priority:

Priority Level	Definition
Priority 1	The incident impacts or threatens to impact: <ul style="list-style-type: none">· Smooth functioning of core business functions· Special business events· High/Medium Criticality system/service· Majority of the staff users of one department· More than 50 staff· Services used by public users, or· Image of the Institution.· VIP i.e. a member of SPM (P, DPs and Directors)
Priority 2	The incident impacts or threatens to impact: <ul style="list-style-type: none">· Smooth functioning of 5 to 49 staff users· 20 to 99 student users· Multiple public users, or· Affecting development/test system that is used to support the High Criticality production system/service
Priority 3	The incident is isolated and has minimal impact to SP's ability to perform its function.
Priority 4	The incident is isolated and is related to hardware failure of a supported end user devices such as notebook computers.
Priority 5	The incident has minimal impact and is related to software bugs of custom developed application.

60.5. The Priority Level for incident analysis and resolution shall be as follows:

Priority	Max Response Time	Response Target	Max Resolution Time	Resolution Target
P1	2 hours	95%	8 hours	95%
P2	2 hours		16 hours	
P3	4 hours		2 working days	
P4	4 hours		3 working days	
P5	4 hours		5 working days	

60.6. These Priority Levels shall apply to the System once the System goes 'live', including during the System Warranty Period and Maintenance Period.

60.7. If the Contractor is unable to resolve any outstanding incident/problem after the stipulated resolution time above, SP shall have the right to withhold payment to the Contractor. In addition, SP also have the right to engage a third party or in-house staff to resolve the incident/problem, and the cost incurred will be charged to the Contractor by deducting from the monthly payment. The Contractor shall facilitate the third party or in-house staff in performing the works, including but not limited to access to data centres and login to system accounts at no extra cost to SP.

60.8. An incident is considered resolved when the reporting party is informed and agreed with the resolution by the Contractor.

60.9. A problem which could arise from incident is considered closed when the root cause is determined and permanent solution is implemented and verified to be effective.

60.10. The Contractor is required to co-operate with third party vendors providing IT support services to SP. If necessary, the System's operation management procedure will have to be refined by the Contractor to accommodate the third party Contractor's systems.

60.11. It is the responsibility of the Contractor to provide FAQs and train the Contractor's Helpdesk to support the System.

60.12. For incident/problem that required third party Contractors for troubleshooting and rectification, Contractor shall follow up with the third party Contractor.

60.13. Contractor shall produce the consolidated report of all incidents/problems and show evidence that the overall response time and the other specified service levels are met. The report shall be submitted to SP on a monthly basis or when requested by SP.

60.14. For Priority Level 1 incidents, the Contractor shall provide an investigation report to SP within 3 working days. The report shall include the date & time of incident occurrences, all relevant events and actions in chronological order, root cause analysis, interim as well as permanent solutions and follow-up action plan to prevent incident from recurring.

- 60.15. In the event of changes resulting from defective products, Contractor will be responsible for incorporating the changes at no cost to SP. The Contractor shall be held solely liable for any time delay or damage, if such defects are not rectified.

SECTION Q
SUPPORT & SYSTEM MAINTENANCE

61. SCOPE OF WORK

- 61.1. SP intends to consolidate the maintenance and support of the entire SharePoint farm including various servers (virtualized), software components and database under a single contract.
- 61.2. The Contractor shall provide maintenance, support and governance for the entire SharePoint farm including existing servers, SharePoint components and services, Databases, etc, from the beginning of the project and during system implementation, warranty and maintenance periods. This shall include development and staging environments. Customized application codes implemented by other vendors are excluded and shall be supported by respective maintenance contracts.
- 61.3. The Contractor shall document and implement best practices, standards and policies to be followed by contractor's team, SP in-house team and other vendors for designing and deploying new SharePoint applications to the farm to avoid any negative impact to the farm.
- 61.4. The following two items are deemed a term-contract. The validity period of this term-contract shall be from the date of award till the last day the system is under warranty or maintenance whichever comes later with the contractor.
 - (a) The Tenderer shall indicate (in the tender submission) a fixed cost for man-days required for each instance of the following activities to enhance/upgrade the farm as required. SP will raise separate purchase order for this request.
 - To add new SharePoint server to the farm
 - To add a new databases to the farm
 - To add any other SharePoint Software components or services
 - (b) The Contractor shall allow extending maintenance and support to include new servers added to the farm. The Tenderer shall indicate (in the tender proposal) the additional cost to support each additional server. SP will raise a separate Purchase Order for this maintenance.
- 61.5. Contractor is wholly responsible for timely delivery of system and support maintenance service, software request services and software defect management services to SP according to the requirement specifications and contractual terms. (Refer to SECTION P)
- 61.6. Contractor is required to work closely with SP's appointed third party Contractors and in-house teams to provide impact assessment, governance future maintainability and deployment verification for new applications; ensuring service levels for the System are met.
- 61.7. Contractor shall abide by and follow all SP's Policies, Procedure and Processes in the duration of this contract.
- 61.8. The Contractor shall designate a Project Manager for the support and system maintenance service. The Project Manager shall be the single point of contact and to ensure all the service levels in the Contract are met.

- 61.9. The support and system maintenance service covers the entire SP SharePoint farm including various servers (virtualized), software components and databases.

62. SUPPORT HOURS (SYSTEM)

- 62.1. Contractor shall provide first-level support service from pre-commission to system warranty period and maintenance periods on all incidents/problems relating to application to the users.
- 62.2. The Support Hours and Service Level for such service are 24 hours by 7 days with a 4 hours response time.
- 62.3. The on-site support staff will be expected to carry out maintenance activities in the evening / weekend as part of the system/application (from application to database) regular maintenance.
- 62.4. All major repair works requiring system shutdown shall be carried out after office hours or at a convenience time as specified by SP at no additional cost.
- 62.5. In addition on-site engineer support will be required for any major Data Centre shutdown or IT DRP exercise to ensure the service is recovered properly. There will be 2 such on-site supports per year.
- 62.6. Contractor shall provide a single point of contact for incident reporting and also to provide user/support communication relating to the System.
- 62.7. The Contractor shall provide the contact details of the support personnel.

63. MAINTENANCE

- 63.1. The service level during the maintenance period will be the same as per the System Warranty period.
- 63.2. For systems and application maintenance services, Contractor shall:
- Provide advice on system enhancement, performance monitoring and tuning for planned changes to the farm.
 - Carry out periodic performance monitoring and tuning. This covers database, SharePoint and application health-check and tuning to be carried out at least once per year.
 - Inform SP on all future updates and new releases of the SharePoint and related patches from Microsoft within 1 month of its release and advise SP on the impact of the patches on SP's SharePoint applications. Upon approval by SP, the contractor shall install the patch and test for successful functioning of all applications. If the patch causes issues, the contractor shall rollback the patch and restores SharePoint to its pre-patched condition and apply the data changes made by users.

64. APPLICATION & SYSTEM SOFTWARE MAINTENANCE SUPPORT

- 64.1. Contractor will provide software maintenance activities of the following types:

- Corrective maintenance is performed to identify and correct software performance and implementation problems. Health check reports shall be run and provided to SP with analysis and recommendations.
 - Preventive maintenance focuses more on performance and it is intended to enhance performance, improve cost-effectiveness and improve process efficiency or maintainability.
 - Adaptive maintenance is carried out to adapt software to changes either in data requirements or the processing environments. Housekeeping and system self-tuning jobs shall be enabled to run as scheduled tasks and monitored regularly.
- 64.2. Contractor shall provide Application & System Software Maintenance and Support Services that include the following to include the ECM system, services, software components and databases being used by the entire SharePoint farm:
- Operational Support
 - (a) To ensure the smooth running of the System.
 - (b) To configure and fine-tune the system to meet the performance and security requirement and close any gaps in the security findings
 - (c) To keep track of all software installed on the system and regularly patch and upgrade the software to ensure that they are up-to-date.
 - (d) To document the design and setup of the system as specified in the Documentation section. Documents are to be kept up-to-date regularly.
 - (e) To ensure minimal unplanned downtime of the system.
 - (f) To provide corrective maintenance, troubleshoot and isolate software defects, including diagnosis and correction of all latent errors in the Application Software.
 - (g) Investigate and correct defects, security vulnerabilities in the application system as reported by SP within the service levels. The resolving effort includes but is not limited to resolving errors through developing, testing and implementing changes to existing application systems or to new application systems.
 - (h) Assess impact of new releases of system software (for example, operation system and security patches) to the application system.
 - (i) To use an incident/problem tracking system to log and track the progress of incident/problem resolution.
 - (j) To implement, at the request of SP, software change requests, for the purpose of operational enhancements. The Contractor shall prepare technical feasibility proposal including impact analysis for the service change request.
 - (k) To make modifications to the Application Software when requested and to perform system tests to ensure system integrity after modifications
 - (l) To ensure modifications to the Application Software are properly integrated with the necessary components (hardware and/or software) and that the system performance is not degraded.
 - (m) To prepare ad hoc reports when requested.

- (n) To develop and update Application & System Software documentations (user and/or technical).
- (o) To monitor the Application & System Software to ensure data integrity and efficient performance and provide expert advice on applications performance monitoring and tuning.
- (p) To train SP Operation on the software changes to enable them to be competent and self-reliant in the operation of the System.
- (q) Plan daily operations to ensure optimisation of resources and batch windows utilisation.
- (r) Schedule and ensure successful completion of ad-hoc, daily, weekly, monthly and other batch processing jobs in the System.
- (s) Provide application system support services, including technical advice and assistance to ensure continuity, availability and accessibility of the System.
- (t) To assist SP Operations team in the performance of software installation of the System and the new release. This includes and not limited to risk analysis, security patches, security hardening and follow-up to audit findings
- (u) To prepare monthly progress and status report, supplementary documentation in a format required by SP. Contractor shall update SP of all known software bugs and incident/problem resolution on a monthly basis.
- (v) Ensure that the system operation is well protected in data security and disaster recovery.
- (w) Ensure that all program source codes and executable codes are properly maintained (especially the versioning) and backed up. This is to allow the system to be rebuilt from scratch if required.
- (x) To attend to user queries and provide assistance to them in the operation of the System.
- (y) To handle escalated SP's Service Desk calls where incident/problem is related to the Application software and to work closely with the Service Desk towards resolution within the SLA.
- Preventive Maintenance Support
 - (a) The Contractor shall apply fix packs, security patches, bug fixes and fixes for all software components installed on the System on quarterly basis. Such fixes and patches shall be applied to the Devt/Test/Staging environments (where applicable) before applying to the Production environment.
 - (b) The Contractor shall provide bi-yearly preventive maintenance by checking the system and application related logs and implementation of fixes. This shall include health checks of software installed with fixing of faulty parts or tuning of software to achieve optimum configurations and system performance, application of fixes and/or security patch if necessary to resolve the problem.
 - (c) The Contractor shall execute performance load testing and tuning at least once a year to ensure the SharePoint farm meets the performance requirement.

- (d) The Contractor shall perform the above tasks on-site. Changes to Production shall be carried out after office hours or at a convenient time specified by SP at no additional cost.
- (e) The Contractor shall inform SP of any planned patch or upgrades. Any patch and upgrades shall be applied to the System with minimal disruption to the services.
- (f) The Contractor shall provide a report for each preventive maintenance activity.
- (g) For alert or vulnerability classified as “High Risk”, it shall be resolved by Contractor within 7 calendar days. For the alert or vulnerability classified as “Medium Risk”, it shall be resolved by Contractor within 14 calendar days.
- System Management Services
 - (a) Contractor shall provide on-site administration support
 - (b) Completion of Service Requests.
- Maintenance Log
 - (a) Contractor shall maintain a log of all maintenance activities, including preventive maintenance, corrective maintenance and other services. For each activity, the log will record at least the date, time, and the service personnel.
 - (b) The Contractor shall propose a format of the Maintenance Log and recommend procedure for its usage. The format and recommended procedures for the Maintenance Log shall be subjected to SP’s approval.
- Handover of Maintenance Support
 - (a) In the event that the maintenance contract is not renewed, Contractor shall furnish SP with a detailed handover plan and schedule at least 60 days prior to the effective date of termination. The handover plan and the detailed schedule shall be subjected to SP’s approval.
 - (b) Contractor shall be responsible to conduct a detailed handover of the complete System to the next Contractor during the last two months of the maintenance contract. The handover and taking over shall be conducted concurrently with the ongoing maintenance support required of the Contractor without affecting the maintenance service level.
- Service Escalation
 - (a) Contractor shall provide a service escalation list of personnel to contact in the event of unsatisfactory performance / service rendered.
- Support Personnel
 - (a) Contractor shall state the number of staff together with details of their qualifications and experience who will be giving support for the System.
 - (b) Contractor shall notify SP ONE months in advance of any changes in support staff. It shall be the Contractor’s responsibility to staff the System support services with qualified personnel having the necessary technical and communication skills. The System support personnel shall possess at least the following characteristics:
 - Possess the relevant technical IT expertise and skills
 - Be able to speak clear and good conversational English
 - Possess good telephone conversational skills

- Good at problem solving
- (c) The Contractor shall replace its personnel within 14 days from the date of written notice from the Authority that the said personnel are either:
 - Technically incompetent in carrying out the Services and all efforts by the Contractor have failed to resolve the issue within the said period; or
 - The conduct of the said personnel is found to be detrimental to the national security.

65. SOFTWARE SUPPORT

- 65.1. Successful Contractor shall provide the following service to SP during the warranty period:
- On-site engineer must respond on-site within 4 hours after receiving a service call.
 - All problems reported must be serviced (whether on-site or remotely, anytime of the day including Sunday and public holiday) and fixed by an engineer within 1 calendar day upon notification.
 - Faulty software shall be repaired as per SLA and all major repair works requiring the shutdown of the system shall be carried out after office hours or at a convenience time as specified/requested by Singapore Polytechnic at no additional cost.
 - Should the company, without a valid reason, failed to meet any of the service levels above, a charge of service credits shall be levied on the company. In addition, the customer shall also have the right to appoint a third party to execute such repairs and services and all costs and expenses incurred in the repairs and services, plus 20% administrative charge shall be recovered by the Customer from the Company, or made payable directly from the Company to the Customer, subject to a maximum of 10% of the tender value.

SECTION R

TRANSITION AND EXIT MANAGEMENT

66. TRANSITION AND EXIT MANAGEMENT

66.1. Transition Plan

- Contractor shall submit the Transition Methodology and plan 1 month prior to the expiration of the existing third party vendor contract.
- The Transition Plan to be prepared shall include, but is not limited to:
 - (a) Define an overall schedule of activities for the transition.
 - (b) Identify and document SP's resources in the scope of the Services.
 - (c) Identify and document the Contractor's resources and facilities that will be added to SP's environment as well as the Contractor's environment.
 - (d) Identify the training materials, documented common error messages and other necessary information for Helpdesk operations.
 - (e) Define the roles and responsibilities of all parties.
 - (f) Define the critical operational scenarios and the corresponding process workflow.
- Define the work-in-progress i.e. ongoing tasks, other pending tasks and problems that have not been resolved or followed up by the existing application vendors.
- Upon acceptance by SP, Contractor shall implement the Transition Plan to take over the responsibilities of providing Services from the existing vendor and forge an appropriate working relationship with the existing third-party vendors.
- Contractor is advised that the purpose of the Transition Plan is to ensure and achieve a smooth hand over of responsibilities. The Contractor shall ensure that the entire transition phase is as transparent as possible to SP users, that is, users shall not experience any disruption of Services and operations.
- The transition period shall be 2 weeks prior to the expiration of the existing Contract.

66.2. Exit Plan

- Contractor shall propose and submit an Exit Plan 2 months after the award of the contract. The Exit Plan and the detailed schedule shall be subjected to SP's approval. The exit plan will be reviewed on an annual basis.
- The Exit Plan shall include but is not limited to:
 - (a) Processes and procedures
 - (b) Roles and Responsibilities
 - (c) Definition of major milestones
 - (d) Schedule for hand-over of outstanding tasks
 - (e) Contact list of vendors providing 2nd level escalation support
 - (f) Application/System documentation
 - (g) Operation Manual
 - (h) Security procedures
- The exit transition period shall be managed and supervised by SP.
- Contractor shall be responsible to conduct a detailed hand-over, inclusive of briefing and training sessions, of the complete System to SP and next Contractor. Any cost incurred during the period of hand-over will be borne by Contractor.

The hand-over shall be conducted concurrently with the ongoing support required of the Contractor without affecting the Service Levels.

- Contractor shall hand-over all necessary documentation of the database and application software and records of problem resolution required for the effective maintenance of the system.
- All user accounts and access rights assigned to the Contractor shall be revoked upon the expiration of the Contract. The revocation shall be carried out in a timely manner.

67. EXPIRATION OF CONTRACT

67.1. Should the contract expire or be terminated in accordance with the Conditions of Contract or for any reason whatsoever, the Contractor shall:

- Return to SP all materials, databases and records, components, images, information, data and records which had been provided by SP to the Contractor and/or created by Contractor to support the System.
- Delete all backups, materials and documents of any information on SP and its partners on the Contractor's servers and give SP and its agents the right to audit the Contractor's servers.

SECTION S

COMPLIANCE ON STANDARDS AND GUIDELINES

68. COMPLIANCE WITH REGULATORY REQUIREMENTS

- 68.1. Contractor shall ensure compliance with Government regulations which includes compliance to the Instruction Manual (IM8) on IT Management policies and standards and any other prevailing government and SP IT policies that are relevant to the project. The Contractor will be allowed to view the documents on-site upon signing the Confidentiality and Non-Disclosure Agreement.
- 68.2. As a minimum, the following IM8 policies and standards must be complied:
- IM8B – Plan
 - (a) Policy on ICT Security & Standards
 - IM8D – Deploy
 - (a) Policy on Security Monitoring
 - (b) Policy on Electronic Public Services
 - IM8F – Data Management
 - (a) Data Governance
 - (b) Data Architecture
 - (c) Data Protection
 - (d) Data Sharing
 - (e) Data Storage
 - (f) Preservation and Disposal of Electronic Records
- 68.3. Contractor is required to furnish a clause by clause compliance on each of the policy and standards prior to the design sign-off and system implementation. Justification must be given to for clauses which are not relevant. For clauses which are relevant evidence must be given to demonstrate compliance. Any non-compliance will not be accepted unless approval is given by the Project Steering Committee.

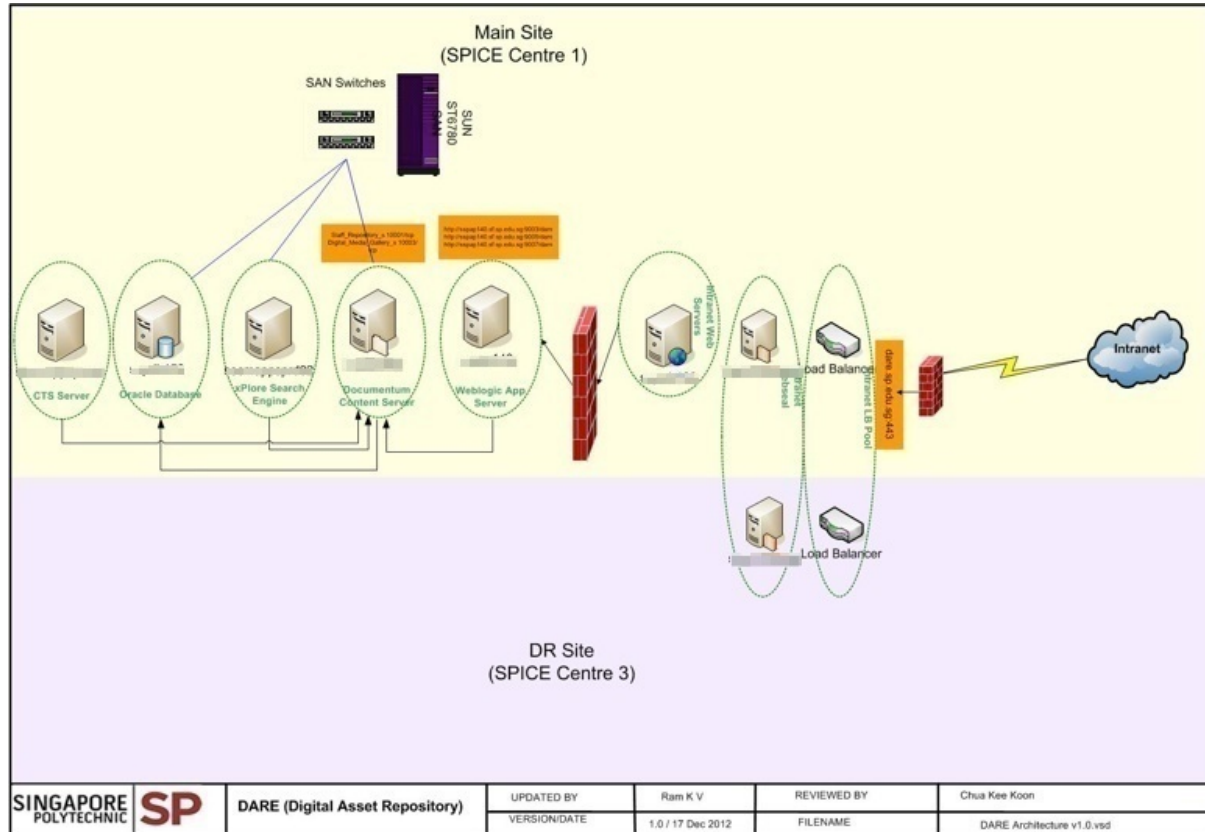
SECTION T

Infrastructure Information

69. INFRASTRUCTURE INFORMATION

69.1. Details of Existing Documentum System (DARE)

- SP's DARE system is implemented on EMC Documentum 6.5 SP2 and makes use of Oracle Weblogic and Database. The operating systems used are Solaris and Windows. Document, Image and Video rendering services are enabled. Trusted Content Services is enabled to encrypt data on the disk. The architecture and additional information about the system are as follows:

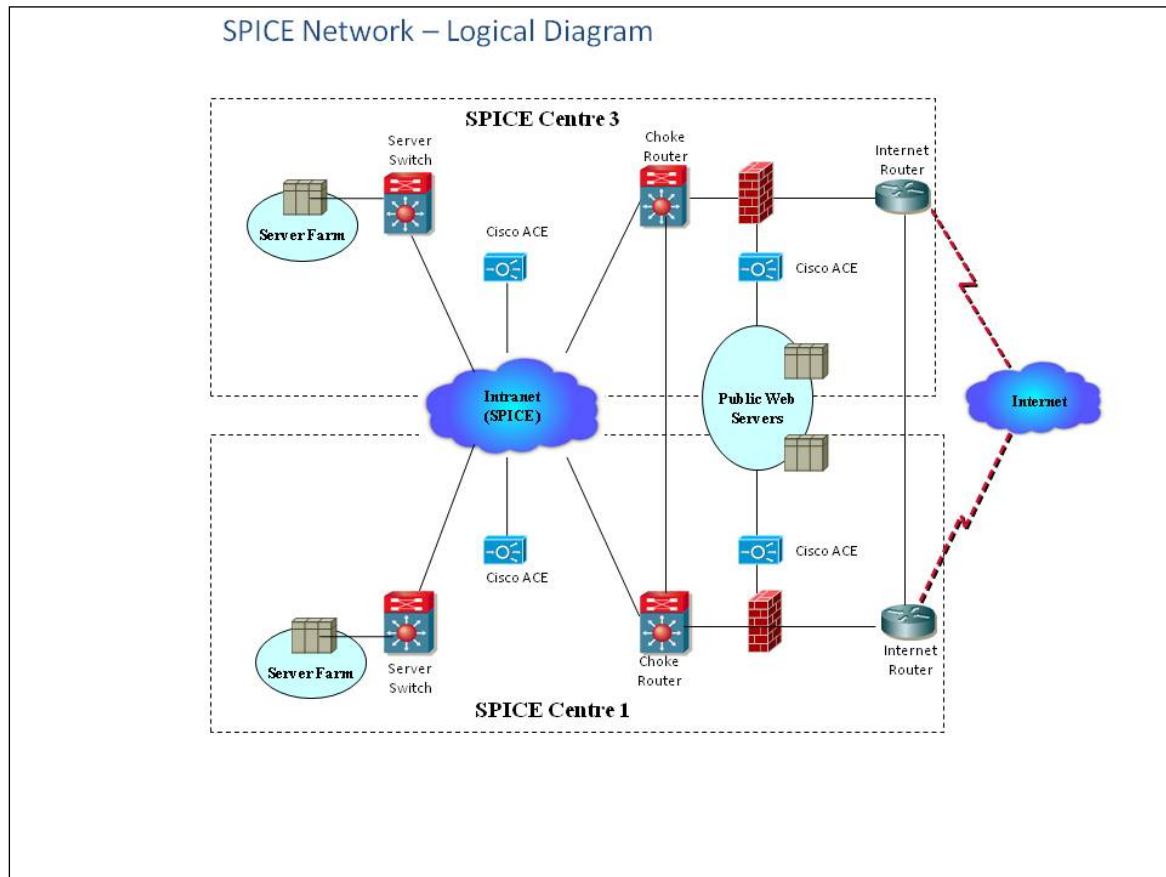


S/No.	Topics	Information based on DARE
1.	Current Documentum Version	Documentum D6.5 SP2
2.	Number of Documents	<p>350,000 with versions Total file-size is estimated to be around 1005GB (and Growing) for TWO production repositories</p> <ol style="list-style-type: none"> 1. Document Repository approximately 326GB with a complex Permission set & folder structure and would benefit from using a migration tool. Document Repository also contains ONE large cabinet for “Student Records” containing 442GB of TIFF files with a simple security. 2. Multi-media repository approximately 237GB in a relatively flat folder and simpler permission set structure <ul style="list-style-type: none"> • (Note: The tenderer to assess and propose a cost-efficient approach to migrate the less complex cabinets using custom-scripts rather than a full-fledged migration tool. The tenderer shall be responsible for complete migration regardless of the approach used.)
3.	Expected growth	20% yearly
4.	Number of users accessing the system.	1700 users on DARE /150 concurrent users
5.	Average Document upload size	5-10MB
6.	Maximum Upload Size	2GB
7.	Types of Documents (doc, docx, xls, xlsx, ppt, pptx, photos, videos, etc)	MS Office, Images, Videos
8.	Number of Documentum Repositories	2 Production Repositories and 1 Staging Repository Development server is separate
9.	Number of Cabinets	Around 60 Cabinets
10.	Number of custom types with inherited metadata	About 20 custom meta-data
11.	Are the documents searchable?	Yes. Query tuning shall be required

12.	Is advanced search required?	Yes
13.	What is the nature of each type of document? Who creates it? Who consumes it? Who can change and distribute it?	Documents in typical business use. Created and consumed by SP staff
14.	Do you want users to browse for documents?	Yes
15.	How will users access the documents?	Via Intranet and VPN
16.	Do the documents require versioning?	Yes
17.	Does the document migration take in consideration of versions?	Yes
18.	Do the documents require co-authoring?	Yes. To be implemented with all necessary components e.g. Office Web Apps, etc
19.	What is the existing version of Office Application?	Office 2010 & Office 2013
20.	Does the File Classification Plan (FCP) require inheritance?	Yes
21.	Number of permission levels?	7 levels supported by DARE. READ, WRITE and DELETE are extensively used. BROWSE is used to a smaller extend. To be assessed for mapping to SharePoint and indicated in the proposal
22.	Any existing Workflows in DARE	No
23.	Self-managed by departments and schools	Yes. Power-users are assigned roles and permissions
24.	Does the document requires conversion to PDF or PDF-A. Specify the type.	Yes (Depends on workflow)
25.	Does the document need to be stored as a Record? Specify the volume.	Yes (50,000)
26.	Do emails need to be archived? Any conversion requires.	Yes
27.	Any archival process?	Migrate selected files to low cost storage

69.2. Network Load Balancer

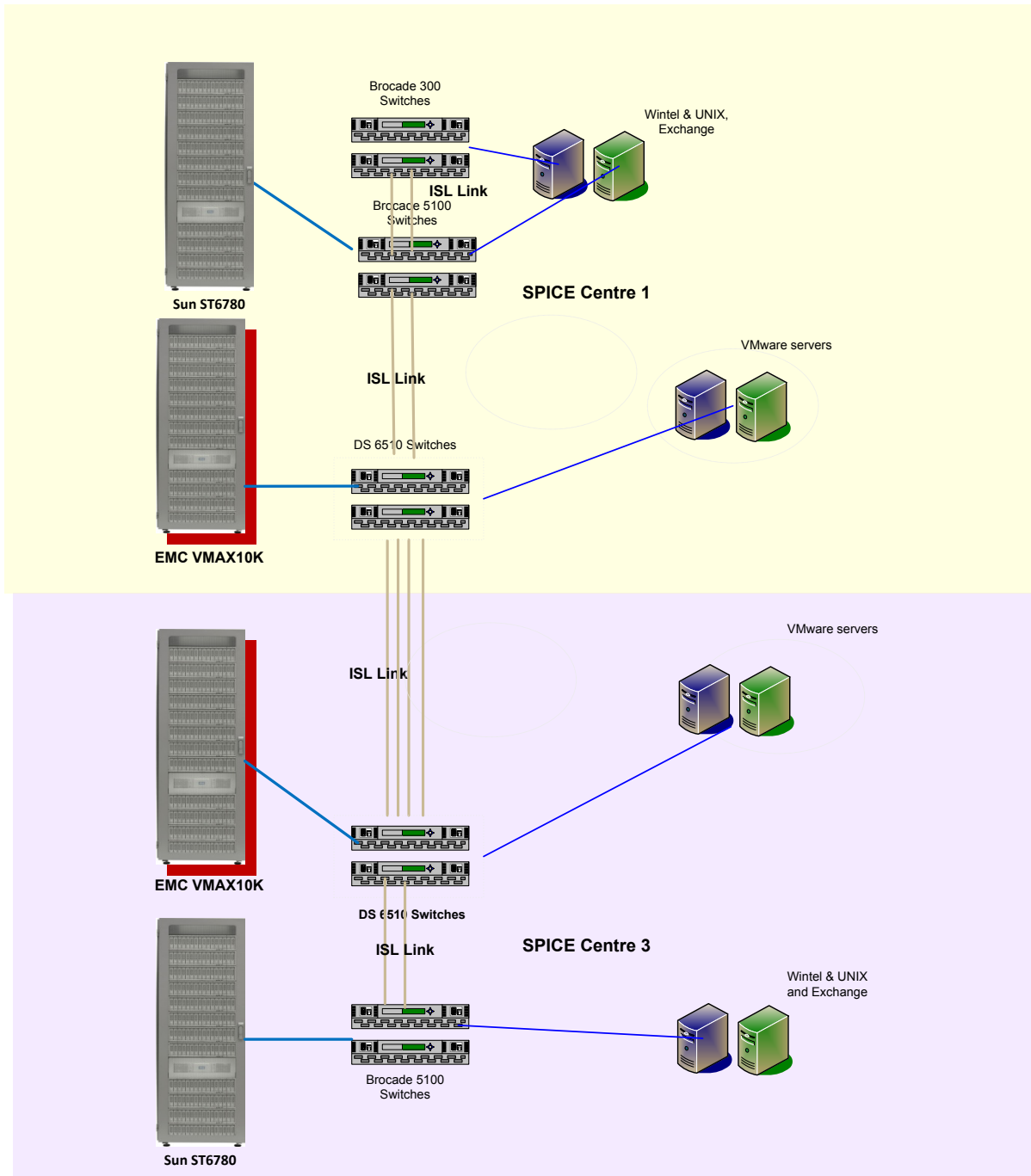
- SP is using Cisco ACE 4710 Application Control Engine to load balance web instances or application-specific instances. There are 2 pairs of Cisco ACE located in the DMZ to support the public web servers and Intranet to support the internal Server Farm as shown below:



- Physical servers are directly connected to the Server Switch and not to the Cisco ACE. This allows virtual IP hosted at the ACE to reference to servers that are located in different IP subnet and location.

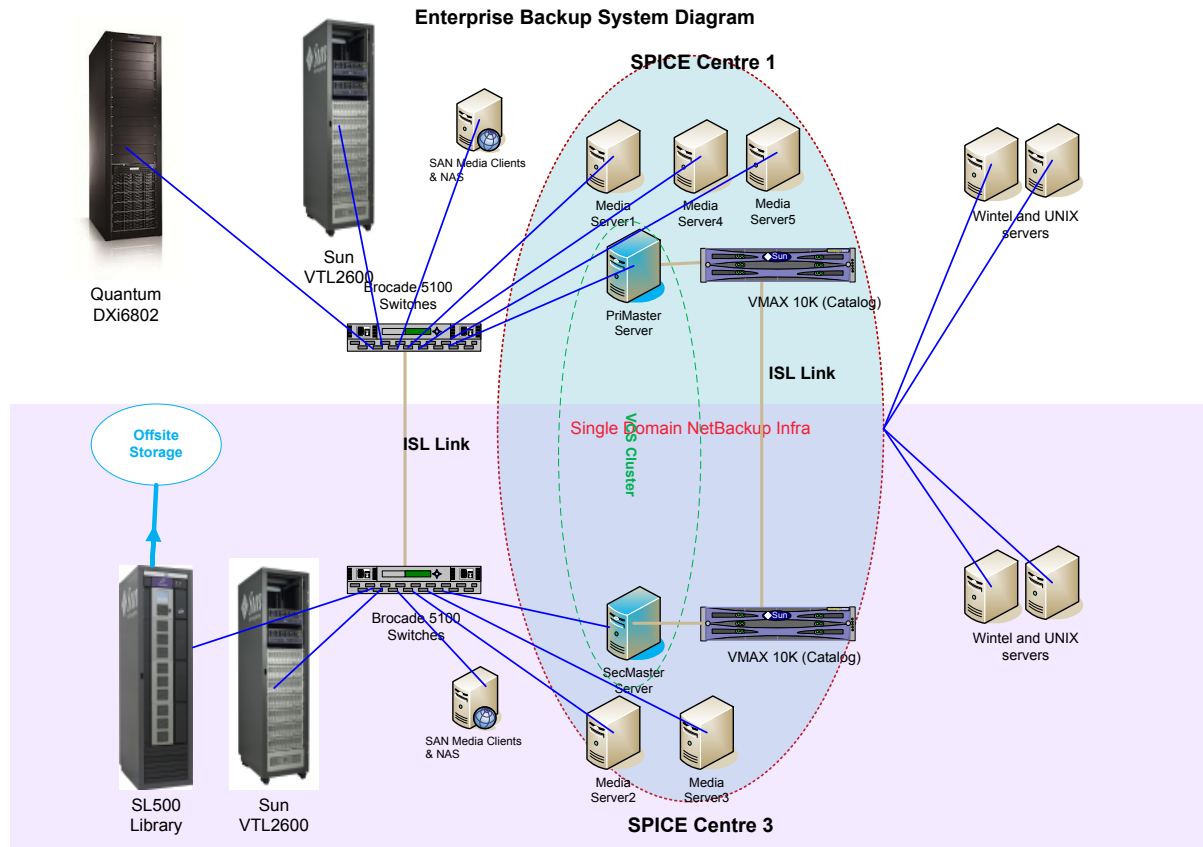
69.3. STORAGE AREA NETWORK

- SP is using Sun ST6780 and EMC VMAX 10K as our Enterprise Storage Area network (SAN). The SAN infrastructure is spanned across 2 data centers to support high availability and disaster recovery of storage. The architecture is shown in the figure below:



69.4. BACKUP SYSTEM

- SP is currently using Symantec Netbackup version 7.6.x, Sun VTL, Quantum DXi6802 VTL and Sun tape libraries across 2 data centers as the enterprise backup system. The architecture is shown in the figure below:



69.5. Active Directory

- There are 2 AD forests, i.e. Staff SP forest and Student Forest. The Staff domain (SF) is located within the Staff SP AD forest and the student domain (SD) is located in the Student AD forest. There is a one-way trust from the student (SD) to the staff (SF) domain. SP is in the progress of migrating the “SD” domain to a new student domain (STUDENT.SP.EDU.SF), the “STUDENT” domain is located at the SP forest. “SD” and “STUDENT” has a 2 way trust.

S/N	Forest	Domain Names	Remarks
1	SP Forest	sp or sp.edu.sg	Empty root domain
2	SP Forest	sf or sf.sp.edu.sg	Staff accounts
3	SP Forest	student or student.sp.edu.sg	New student domain
4	Student (SD) forest	sd or sd.sp.edu.sg	Existing student domain

- There are 2 environments, i.e. (i) development and test servers and instances, and (ii) staging and production servers and instances. The new student domain (TESTStudent) is available for testing.
- High Availability (HA) of the AD is achieved using the built-in HA feature of Windows AD. The LDAP port of the AD is load-balanced via hardware load balancer (LB) such that applications can query or update the AD via LDAP protocol.

