BUSINESS REQUIREMENTS

State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
Initial Filing of Request for Commission Action					
B1.1	User enters information and uploads filing: Credentialed user will login in and indicated that they wish to make an adjudicative filing. User will provide required information identifying and categorizing the filing.	M			
B1.2	Accept and hold filing: Filing is held to determine whether it is complete and whether it should be docketed. Document is held until complete, referred to Staff, and/or used to open a new docket.	M			
B1.3	Review initial docket information: Clerk ensures information entered is correct and further categorized the filing and type of docket. Based on certain selections, auto-populate additional data fields and trigger workflows.	M			
B1.4	New docket number: Allow creation of docket numbers that are a combination of user identification of docket type and sequential numbering across all Commission dockets, as well as a separate numbering system for SEC dockets.	M			
B1.5	Create initial service list: Create a service list based on user information from initial filing and include automatic entries, such as executive director and OCA.	M			
B1.6	Create acknowledgement or rejection letters from template: When the clerk selects accept or reject, create acknowledgement from template and distribute to service list. Current distribution requirements are US Mail; system must be able to create printable letters and envelopes for mailing.	M			
B1.7	Withdraw a document: Users may edit or withdraw a document filed in the same login session only until the clerk has accepted the filing. Once accepted, users can only withdraw a document by filing a request to do so.	M			
Subsequent filing to a docket					
B2.1	User enters information and uploads filing: Credentialed users will login in and indicated that they wish to make an filing to a docket. User will provide required information identifying and categorizing the filing. System will enforce business rules with respect to attachments and cover letters.	M			
B2.2	Non-credentialed user wishes to make a filing: A non-credentialed user should be able to submit a filing to a docket and receive a templated email receipt for their filing.	M			
B2.3	Identify the document type and follow business rules for filing: Clerk reviews the filing, and, for filings from uncredentialed users, determines whether to accept the filing. All documents are saved with structured names and/or keyword tags.	M			
B2.4	Generate other workflows triggered by an initial petition or separate finding: These include determining if a statutory deadline exists, setting statutory deadlines, notifying staff of deadlines and assigning tasks to staff.	M			
B2.5	Generate a daily mail log: At the end of each business day, auto-generate a daily mail log for posting to the Commission website (puc.nh.gov). Business rules will determine what is included in the log.	M			
B2.6	Prevent changes and deletions to external documents: Once filed, documents cannot be altered or removed without Clerk approval.	M			
B2.7	Withdraw a document: Users may edit or withdraw a document filed in the same login session only until the clerk has accepted the filing. Once accepted, users can only withdraw a document by filing a new request to do so. Filings withdrawn by request remain in the record but are marked “withdrawn.”	M			
B2.8	Allow user access to filings: All credentialed users should have a dashboard detailing all of their filings into the system, and access to all non-confidential documents in dockets to which they are a party. (Access to documents and dockets to which an external user is not a party is available through the Commission web site.)	M			
Confidential filings					
B3.1	User requests confidential treatment for a filing in a docket: User must file a separate petition requesting confidential treatment, which will require Commission action.	M			

B3.2	User uploads confidential document and redacted document: The user must identify the confidential and redacted versions of the document. The system must support maintaining confidentiality of any document marked confidential	M			
B3.3	Confidential treatment denied: The Commissioners will determine if the requested confidentiality is granted in full or in part, or denied. The original documents shall remain redacted or confidential; if the Commission denies part or all of the confidential treatment, the user must file the new public version into the system.	M			
B3.4	User requests confidential treatment for a report or other document already deemed confidential: The system will allow the Clerk to identify reports and documents for which the user may designate a report or document as confidential without filing a separate petition.	M			
Commission Orders					
B4.1	Types Commission Orders: • Orders of Notice • Final Orders • Amendments to the Above	M			
B4.2	Appeals and Effective Dates: Automate business rule-driven workflows for the types of orders to establish windows for reconsideration and effective dates.	M			
B4.3	Orders as Docket Filings: Orders and amendments are entries in a docket as part of the official record of the Commission	M			
B4.4	Secretarial Letters: Secretarial letters are actions of the Commission and are entered into dockets as part of the official record of the Commission.	M			
B4.5	Docket closure: When a Final Order is entered and the appeal period has expired without activity, send a reminder to the Clerk to close the docket. Provide a data entry screen allowing the Staff analyst to enter details of a Closed Docket including data closed, method of closing (Secretarial Letter or Memo, Order Nisi, Order) and comments.	M			
Exhibits					
B5.1	Exhibits: Support the addition by the Clerk of Exhibits to the docket	M			
B5.2	Transcripts:Support the uploading of transcripts to dockets by the court reporter.	M			
Discovery					
B6.1	Discovery Records, Generally: Discovery requests and responses are not a part of the docket record unless introduced as an exhibit.	M			
B6.2	Discovery Requests: Provide functionality to accept a single document representing the discovery requests, requiring the user to identify the number of discovery questions, e.g., the number of responses expected.	M			
B6.3	Discovery Response Management: Provide functionality to accept discovery responses of multiple parts in response to each discovery request, and maintain discovery questions and responses as a unit.	M			
B6.4	Discovery Exhibits: Allow the identification of discovery responses as exhibits in the docket with requiring duplication of the documents.	M			
Email					
B7.1	System-generated emails: Emails generated in the system should not be part of the docket record. Internal email reminders do not need to be saved or logged. External emails must be logged in some fashion.	M			
B7.2	User emails: The Commission would be interested to hear solutions that allow the storing and retrieval of emails that document procedures or outline policies.	M			
Forms and Reports Filings					
B8.1	Fillable forms: The system will support self-validating forms for submission through the portal.	M			
B9.2	Reports from utilities: The system will support and manage the filing and tracking of required and ad hoc reports.	M			
Schedules					
B10.1	Procedural Schedule: Provide the ability to establish key dates for a docket, including, but not limited to, multiple technical sessions, multiple hearings (both hearings that take place at different times and single hearings that last multiple days), due dates for issuing discovery, discovery responses, motions, replies to motions, briefs and reply briefs.	M			

B10.2	Identifying deadlines: Deadlines can be ordered by the Commission, required by statute, established by business rules, or casual. The system should support the identification of events, types of documents and dockets, and other criteria that determine deadlines. Business rules will direct how Staff can add, change or remove any due dates, whether system-calculated or directly entered.	M			
B10.3	Calculation of deadlines: The system will support the calculation of due dates that incorporate for the following factors: • Exclude the day of filing • If the deadline falls on a Saturday, Sunday, or State holiday, move the deadline to the next business day • If the allowed time period is less than 7 days, exclude Saturdays, Sundays, and State holidays • Add an additional 3 days if the method of service is US Mail (indicated on the Certificate of Service) Items received after 5:00 pm are considered to have arrived on the next business day (allow this clock to be varied, in the event of electronic filing). Staff must be able to manage/change the calendar of State holidays	M			
B10.4	Changes to deadlines: For the procedural schedule items and statutory or commission-ordered deadlines, only the Clerk shall have the ability to change a date. All other deadlines may be edited by Staff.	M			
B10.5	Notices: The system will generate reminders to internal Commission staff on the service list of a docket and to external parties only when the deadline is a) relevant to that party and b) the party requests such notices.	M			
B10.6	Synchronize calendars: The system must be able to push scheduled events from the docket calendar to the personal calendars of assigned staff on request.	M			
Service Lists					
B11.1	Service List entries: People placed on a service list fall into six categories: Petitioner, Staff, Intervenor, Participant and Courtesy, and will receive notices and copies of documents specific to their role.	M			
B11.2	Petitioner: (see B1.5) A service list shall include the petitioner on whose behalf the docket was opened.	M			
B11.3	Staff (Executive Director): The executive director is on all service lists.	M			
B11.4	Staff (Analyst): Require Staff analyst assignment with three days of docket initiation. Allow default assignments to be established based on docket criteria. Remind Staff Utility Director to assign Staff analyst to docket. Once identified, add Staff analyst to service list. There may be multiple Staff assigned to a docket.	M			
B11.5	Staff (Attorney): Require Attorney assignment with three days of docket initiation. Allow default assignments to be established based on docket criteria. Remind Staff Legal Director to assign Staff Attorney to docket. Once identified, add staff attorney to service list. There may be multiple Staff assigned to a docket.	M			
B11.6	Intervenors (OCA): Following business rules, the OCA is added to most dockets as an Intervenor without the need for petition or approval.	M			
B11.7	Intervenors: Intervenors will file a petition for intervention, which is in the docket and held for Commission action. The Clerk will designate the petition approved or denied. If approved, add the intervenor to the service list. There may be multiple Intervenors.	M			
B11.8	Full Parties: Petitioners, intervenors and Staff are all full parties to a docket, and should all be credentialed system users with access to all non-confidential documents filed in the docket.	M			
B11.9	Participant: The Clerk may add multiple Participants to the docket. Particpants are not full parties and only receive selected materials based on business rules.	M			
B11.10	Courtesy: The Clerk may add multiple Courtesy entries to the docket. Courtesy designates are not full parties and only receive Commission orders in the docket.	M			
B11.11	Service list notification: Use business rules to automatically trigger service list notification and document distribution for full parties to the docket.	M			

B11.12	Service List maintenance: Allow the Clerk to update service lists, to include additions and removals.	M			
Other People					
B12.1	Witnesses: Allow external parties to register one or more witnesses to a docket and upload certain document types such as pre-filed testimony and exhibits that are associated to a specific witness. Witnesses are not added to the service list	M			
B12.2	Court Reporter: Allow the Clerk to establish the need for a court reporter and send reminders of docket number, dates and times to the reporter. The reporter is not added to the service list	M			
B12.3	Clerk: Allow assignment of a clerk to a hearing and push the date, time and location to the clerk's Outlook calendar. The clerk is not added to the service list.	M			
Reports and Dashboards					
B13.1	Report - Open Dockets: Provide management reports tracking the statutory and commission deadlines for open dockets. Allow filtering by division, staff, utility, etc.	M			
B13.2	Report - Statistics: Provide statistical management reports on key milestones such as dockets opened by year, average time from petition to hearing, average time from petition to final order, etc.	M			
B13.3	Director dashboard: Produce a filterable report to Division directors and Executive Director of active cases, staff assignments, statutory deadlines, scheduled events and statuses for all open dockets. Filters shall include industry, docket type, date ranges for scheduled events.	M			
B13.4	Docket progress dashboard: For each staff member assigned to a docket, provide a window that displays the status of their dockets and related documents, upcoming event dates and deadlines, actions past due. For directors, provide the same view across all dockets assigned to their staff, filterable by all associated metadata	M			
B13.5	Resource management dashboard: Provide Utility and Legal directors the ability to see overall workloads of individual staff members – dockets assigned, deadlines, events	M			
Other Desired Functions					
B14.1	RSS Functionality: Describe functionality that would allowing docket parties and the general public to subscribe to automatic notification of filings using various meta data selections such as docket industry type, filing type, specific petitioner name	M			
B14.2	RSS Functionality: Describe possible calendar management functionality. The Commission uses specific rooms and staff or Pre-hearings, Technical Sessions and Public Hearings on and off site and seeks functionality to allow: • Room reservation • Automatic calendar management • Populate date and time from a smart form to publication platforms • Synchronize staff calendars with Commission calendars • Automate or send reminders for public and party noticing	M			
B14.3	Archiving documents: • Automation • Recall • Cloud or no cloud	M			
B14.4	Searching active and archived document repository: Enable a simple search by specifying values for one or more metadata types, such as filer name, company name, docket number, industry, docket/document type) Enable advanced search including Boolean include/exclude operators, specific phrased and fuzzy concept searching	M			
Non-functional requirements of software					
B15.1	Authentication: Single sign-on using active directory?	M			
B15.2	Audit trail	M			
B15.3	Historic document migration: Propose options for moving dockets and history into the system	M			
B15.4	Search: Search for documents by metadata such as date range, industry, company or person filing. Search content for key words or phrases.	M			
B15.5	End user and administrator capabilities: Ability of staff to update business rules, menu drop down contents. Ability of admin to add or delete data elements	M			
B15.6	Administrative load: Estimated ongoing software and server administrative requirements and workload.	M			

APPLICATION REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
GENERAL SPECIFICATIONS					
A1.1	Ability to access data using open standards access protocol (please specify supported versions in the comments field).	M			
A1.2	Data is available in commonly used format over which no entity has exclusive control, with the exception of National or International standards. Data is not subject to any copyright, patent, trademark or other trade secret regulation.	M			
A1.3	Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1	M			
APPLICATION SECURITY					
A2.1	Verify the identity or authenticate all of the system client applications before allowing use of the system to prevent access to inappropriate or confidential data or services.	M			
A2.2	Verify the identity and authenticate all of the system's human users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services.	M			
A2.3	Enforce unique user names.	M			
A2.4	Enforce complex passwords for Administrator Accounts in accordance with DoIT's statewide User Account and Password Policy.	M			
A2.5	Enforce the use of complex passwords for general users using capital letters, numbers and special characters in accordance with DoIT's statewide User Account and Password Policy.	M			
A2.6	Encrypt passwords in transmission and at rest within the database.	M			
A2.7	Establish ability to expire passwords after a definite period of time in accordance with DoIT's statewide User Account and Password Policy.	M			
A2.8	Provide the ability to limit the number of people that can grant or change authorizations.	M			
A2.9	Establish ability to enforce session timeouts during periods of inactivity.	M			
A2.10	The application shall not store authentication credentials or sensitive data in its code.	M			
A2.11	Log all attempted accesses that fail identification, authentication and authorization requirements.	M			
A2.12	The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place.	M			
A2.13	All logs must be kept for 1 years.	M			
A2.14	The application must allow a human user to explicitly terminate a session. No remnants of the prior session should then remain.	M			
A2.15	Do not use Software and System Services for anything other than they are designed for.	M			
A2.16	The application Data shall be protected from unauthorized use when at rest.	M			
A2.17	The application shall keep any sensitive Data or communications private from unauthorized individuals and programs.	M			

A2.18	Subsequent application enhancements or upgrades shall not remove or degrade security requirements.	M			
A2.19	Utilize change management documentation and procedures.	M			
A2.20	Web Services : The service provider shall use Web services exclusively to interface with the State’s data in near real time when possible.	M			

TESTING REQUIREMENTS

State Requirements			**Vendor**		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
APPLICATION SECURITY TESTING					
T1.1	All components of the Software shall be reviewed and tested to ensure they protect the State’s web site and its related Data assets.	M			
T1.2	The Vendor shall be responsible for providing documentation of security testing, as appropriate. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability.	M			
T1.3	Provide evidence that supports the fact that Identification and Authentication testing has been recently accomplished; supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users.	M			
T1.4	Test for Access Control; supports the management of permissions for logging onto a computer or network.	M			
T1.5	Test for encryption; supports the encoding of data for security purposes, and for the ability to access the data in a decrypted format from required tools.	M			
T1.6	Test the Intrusion Detection; supports the detection of illegal entrance into a computer system.	M			
T1.7	Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network.	M			
T1.8	Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	M			
T1.9	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network.	M			
T1.10	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system.	M			
T1.11	Test Input Validation; ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	M			
T.1.12	For web applications, ensure the application has been tested and hardened to prevent critical application security flaws. (At a minimum, the application shall be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten (http://www.owasp.org/index.php/OWASP_Top_Ten_Project).	M			
T1.13	Provide the State with validation of 3rd party security reviews performed on the application and system environment. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review (please specify proposed methodology in the comments field).	M			

T1.14	Prior to the System being moved into production, the Vendor shall provide results of all security testing to the Department of Information Technology for review and acceptance.	M			
T1.15	Vendor shall provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.	M			
NDARD TESTING					
T2.1	The Vendor must test the software and the system using an industry standard and State approved testing methodology.	M			
T2.2	The Vendor must perform application stress testing and tuning.	M			
T2.3	The Vendor must provide documented procedure for how to sync Production with a specific testing environment.	M			
T2.4	The vendor must define and test disaster recovery procedures.	M			

HOSTING-CLOUD REQUIREMENTS

State Requirements			Vendor		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
OPERATIONS					
H1.1	Vendor shall provide an ANSI/TIA-942 Tier 3 Data Center or equivalent. A tier 3 data center requires 1) Multiple independent distribution paths serving the IT equipment, 2) All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture and 3)Concurrently maintainable site infrastructure with expected availability of 99.982%.	M			
H1.2	Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins.	M			
H1.3	The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center.	M			
H1.4	Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.	M			
H1.5	Vendor shall monitor System, security, and application logs.	M			
H1.6	Vendor shall manage the sharing of data resources.	M			
H1.7	Vendor shall manage daily backups, off-site data storage, and restore operations.	M			
H1.8	The Vendor shall monitor physical hardware.	M			
H1.9	Remote access shall be customized to the State’s business application. In instances where the State requires access to the application or server resources not in the DMZ, the Vendor shall provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).	M			
H1.10	The Vendor shall report any breach in security in conformance with State of NH RSA 359-C:20. Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office.	M			
DISASTER RECOVERY					
H2.1	Vendor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.	M			

H2.2	The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.	M			
H2.3	Vendor shall adhere to a defined and documented back-up schedule and procedure.	M			
H2.4	Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.	M			
H2.5	Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.	M			If Applicable
H2.6	Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.	M			If Applicable
H2.7	Data recovery – In the event that recovery back to the last backup is not sufficient to recover State Data, the Vendor shall employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.	M			
HOSTING SECURITY					
H3.1	The Vendor shall employ security measures ensure that the State's application and data is protected.	M			
H3.2	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	M			
H3.3	All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.	M			
H3.4	All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.	M			
H3.5	The Vendor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.	M			
H3.6	The Vendor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor' hosting infrastructure and/or the application upon request.	M			
H3.7	All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs.	M			
H3.8	Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA.	M			
H3.9	The Vendor shall notify the State's Project Manager of any security breaches within two (2) hours of the time that the Vendor learns of their occurrence.	M			

H3.10	The Vendor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.	M			
SERVICE LEVEL AGREEMENT					
H4.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M			
H4.2	The vendor shall maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M			
H4.3	The vendor shall repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M			
H4.4	All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.	M			
H4.5	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday through Friday EST.	M			
H4.6	The Vendor shall conform to the specific deficiency class as described: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	M			
H4.7	As part of the maintenance agreement, ongoing support issues shall be responded to according to the following: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract.	M			
H4.8	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M			
H4.9	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M			

H4.10	If The Vendor is unable to meet the uptime requirement, The Vendor shall credit State’s account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing.	M			
H4.11	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M			
H4.12	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M			
H4.13	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M			
H4.14	The Vendor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M			

SUPPORT & MAINTENANCE REQUIREMENTS

State Requirements			Vendor		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
SUPPORT & MAINTENANCE REQUIREMENTS					
S1.1	The Vendor’s System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M			
S1.2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M			
S1.3	Repair Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M			
S1.4	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday through Friday EST.	M			
S1.5	The Vendor response time for support shall conform to the specific deficiency class as described below or as agreed to by the parties: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	M			
S1.6	The Vendor shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.	M			

S1.7	For all maintenance Services calls, The Vendor shall ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) action plans, dates, and times; 4) expected and actual completion time; 5) Deficiency resolution information, 6) Resolved by, 7) Identifying number i.e. work order number, 8) Issue identified by;	P			
S1.8	The Vendor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.	P			
S1.9	As part of the Software maintenance agreement, ongoing software maintenance and support issues, shall be responded to according to the following or as agreed to by the parties: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract; or as agreed between the parties.	M			
S1.10	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M			
S1.11	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M			
S1.12	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: All change requests implemented; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M			
S1.13	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M			
S1.14	The Vendor shall give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M			
S1.15	The State shall provide the Vendor with a personal secure FTP site to be used by the State for uploading and downloading files if applicable.	M			

PROJECT MANAGEMENT

State Requirements			Vendor		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
PROJECT MANAGEMENT					
P1.1	Vendor shall participate in an initial kick-off meeting to initiate the Project.	M			
P1.2	Vendor shall provide Project Staff as specified in the RFP.	M			

P1.3	Contractor shall submit a finalized Work Plan within seven (7) days of contract effective date. The Work Plan shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, critical events, task dependencies, and payment Schedule. The plan shall be updated no less than every two weeks.	M			
P1.4	Contractor shall provide detailed bi-weekly status reports on the progress of the Project, which will include expenses incurred year to date.	M			
P1.5	All user, technical, and System Documentation as well as Project Schedules, plans, status reports, and correspondence must be maintained as project documentation. (Define how- WORD format- on-Line, in a common library or on paper).	M			