DPS INFORMATION TECHNOLOGY (IT) STANDARDS AND REQUIREMENTS

Table of Contents

1.1 DEFINITIONS 4
1.2 INFORMATION TECHNOLOGY (IT) STANDARDS AND REQUIREMENTS 6
1.2.1 Vendor-Hosted System or DPS-Provided Cloud-Hosted System 6
1.2.2 DPS-Hosted System 8
1.2.3 Intersystem Communication Standards 10
1.2.4 Network Topography 10
1.2.5 Workstation Software Installation Packaging 10
1.3 MAINTENANCE AND SUPPORT 10
1.3.1 Software Updates 11
1.3.2 Hardware Maintenance 11
1.3.3 Change Control Participation 12
1.3.4 Service Outage Escalation and Communication Plan 12
1.3.5 Application Outages, Release Rollbacks and Degradation in Performance Reporting 12
1.4 BASIC SERVICE LEVEL STANDARDS 13
1.4.1 System Production Control 14
1.4.2 Vendor Customer and System Support 14
1.5 SYSTEM PERFORMANCE 15
1.5.1 Basic Requirements 15
1.5.2 Calculation of System Performance Rate 16
1.5.3 Response Time 16
1.5.4 Data Backups 16
1.5.5 Recovery Points 17
1.5.6 Hardware and Software Refresh Plans 18
1.5.7 Vendor Business Continuity and Disaster Recovery Plan 18
1.6 SYSTEM TRAINING PLAN FOR TECHNICAL STAFF 20
1.7 TESTING REQUIREMENTS, IMPLEMENTATION AND ACCEPTANCE 21
1.7.1 Implementation and Acceptance 21
1.7.2 Cloud-Hosted Infrastructure Environment 21
1.7.3 Unit Testing 22
1.7.4 System Testing 23
1.7.5 Performance/Load Testing 23

1.7.6 System Integration Testing 24
1.7.7 User Acceptance Testing (UAT) 25
1.7.8 Final Acceptance 25
1.7.9 Failure Resolution 26
1.7.10 Retest 26
1.8 QA ENTRY AND EXIT CRITERIA 26
1.8.1 Purpose 26
1.8.2 Scope 27
1.9 GENERAL ENVIRONMENT ENTRY/EXIT CRITERIA AND PROCESS 27
1.9.1 General Environment Requirements 27
1.9.2 Development Environment Entrance/Exit Process/Criteria 27
1.9.3 QA Environment Entrance/Exit Process/Criteria 28
1.9.4 UAT Environment Entrance/Exit Process/Criteria 28
1.9.5 PRD Environment Entrance Process/Criteria 28

1.1 DEFINITIONS

A. **API** means Application Programming Interface.

B. **Change Control Board (CCB)** means the DPS work group responsible for coordinating any requested change to existing DPS systems.

C. **Change Order** means a document used to capture customer and job information summarizing any labor or materials used to complete the task.

D. **Change Request** means the formal process to initiate and manage the Change Order process.

E. **Cloud-Hosted or Cloud Services** means a service available to users on demand through the Internet from a cloud provider's servers or services as opposed to an agency's on-premises servers.

F. **COTS** means Commercial off the Shelf Software.

G. **ETL** means Extract, Transform, Load and is a process that extracts, transforms, and loads data from multiple sources to a data warehouse or other unified data repository.

H. **DPS-Hosted** means a combination of traditional IT functions to be provided to the Department such as infrastructure, applications Software (including COTS Software), security, monitoring, storage, provider of Hardware and Hardware Maintenance, and email, over the internet or other Wide Area Networks (WAN).

I. **Hardware** means the physical elements of a computing system including the physical components thereof.

K. **Hardware Maintenance** means the Hardware is maintained to run efficiently, increase component lifespan, decrease the likelihood of Hardware failure and replace hardware, should it fail.

L. **Hardware Refresh Plan** means the implementation of hardware which has reached end of life and no longer supported that will be replaced.

M. **Maintenance** means the act of keeping the System in good condition by making repairs, applying updates or upgrades, addressing problems, etc. to ensure that the System continues to meet user requirements in their present operating context.

N. **Preventive Maintenance** means the care and services by personnel for the purpose of maintaining equipment, and facilities in satisfactory operating condition by providing for systematic inspection, detection, and correction of incipient failures either before they occur or before they develop into major defects.

O. **Recovery Point Objective (RPO)** means the point in time to which data must be recovered after an outage.

P. **Response Time** means the total amount of time it takes to respond to a request for service.

Q. **Services** means the furnishing of labor, time, or effort by the Vendor, which may or may not involve the delivery of a specific end product other than reports.

R. **Service Level Standards** means the Performance Standards that govern work under the contract which are agreed upon by both parties during implementation that defines timeliness or quality of products or service.

S. **Severity Level** means defining the level of impact to the organization
T. **Software (SW)** means any application programs for the exclusive use with the System.
U. **Software Development Defect Severity** is defined in five classifications. Each classification and its corresponding definition is as follows:
    a. BLOCKER – When running of test cases is stopped because of the defect or when the application is not working at all.
    b. CRITICAL – When a large number of test cases are affected by the defect, or a major application failure has occurred. Example: A new feature is not working at all.
    c. MAJOR – Denotes a defect the affects the overall functioning of a feature. Example: A new feature is not working as specified; or an ungraceful functionality failure.
    d. MINOR – Indicates when the impact of a defect is less important to the overall health of the feature or application but is required to meet the specifications. Example: a usability issue; user interface inconsistency; or an uninformative or missing error message.
    e. TRIVIAL – Indicates a defect of little importance.
V. **Software Refresh Plan** means the implementation of software that has either been deprecated, updated or replaced.
W. **Solicitation** means Pricing Requests (PR), Request for Proposals (RFP), Request for Offers (RFO), Invitation for Bids, or Requests for Qualifications (RFQ).
X. **Solution** means a collection of information management techniques involving computer automation (Software/Hardware/database/network) to support and improve the quality and efficiency of business operations.
Y. **System** means a collection of information management techniques involving computer automation (Software/Hardware/database/network) to support and improve the quality and efficiency of business operations.
Z. **Test Cases** means a specific executable test that examines all aspects including inputs and outputs of a system and then provides a detailed description of the steps that will be taken, the results that will be achieved, and other elements that will be identified.
AA. **UAT** means User Acceptance Testing.
BB. **Unit Testing** means a Software testing method by which individual units of source code, sets of one or more computer program modules together with associated control data, usage procedures, and operating procedures are tested to determine whether they meet specifications.
CC. **Vendor-Hosted** means a combination of traditional IT functions to be provided by the Vendor such as infrastructure, applications, Software as a Service, (including COTS Software), Infrastructure as a Service, Platform as a Service, security, monitoring, storage, and provider of Hardware and Hardware Maintenance.

1.2 INFORMATION TECHNOLOGY (IT) STANDARDS AND REQUIREMENTS

The Vendor must comply with the following IT standards and requirements, as applicable to this Contract, including this IT Standards and Requirements Exhibit. The Vendor must also comply with any DPS, or state amended, standards and requirements throughout the term of this Contract, including any renewal or optional Contract periods.

The Vendor's systems must comply with DPS standards and requirements when there is a need to migrate from a Vendor-hosted infrastructure to a DPS-hosted infrastructure.

All requests for documentation, narratives, diagrams, exceptions, etc., identified in this IT Standards and Requirements Exhibit, must be submitted with the Vendor's Response.

If the DPS Cyber Security Contract Requirements Exhibit is also incorporated by reference or included as an exhibit in the Solicitation and the resulting Contract, the Vendor must also comply with those cyber security requirements.

1.2.1 Vendor-Hosted System

A. System and Architectural Documentation

The Vendor must provide, within its Response, documentation for a Vendor-hosted system consisting of the following:

- An overall narrative for any System which is hosted within the Vendor's computing infrastructure or within the DPS provided cloud infrastructure;
- Narratives and detailed diagrams for the following:
    - Product architectural diagram;
    - Security diagram(s) (including security diagrams for database, network, application, etc.);
    - Network diagram;
    - Communications port diagram; and
    - For cloud-hosted systems, provide an inventory of cloud-based products and services required to support the bulleted items above; and
- An itemized list of any assumed capabilities of DPS IT systems required to access or support the Vendor's proposed product(s) or solution(s).

B. Server, Workstation, Peripheral Documentation

The Vendor must provide, within its Response, an inventory for a Vendor-hosted System for the components listed below.

- Any applicable server Hardware will identify:
    - The processor requirements;
    - The memory requirements;

  - Operating system details and dependencies; and
  - Data storage requirements.
- All workstation requirements will identify:
  - The processor requirements;
  - Display requirements;
  - The memory requirements;
  - Operating system details and dependencies;
  - Data storage requirements; and
  - Any support applications required such as Internet Explorer, Adobe PDF Reader, etc.
- Peripherals required must be identified.

C. Desktop, Laptop, or Mobile Device Documentation

The Vendor must provide, within its Response, how it will support each of the following items. The Vendor must also document any exceptions.

- DPS-issued desktop or laptop PCs
  - Win10 Enterprise OS: 19042 (20h2)
  - Next version Win10 - 19044 (21h2)
  - 14393 (LTSB 2016) - THP incar systems
  - 17763 (LTSC 2019) - THP incar systems imaged after 5/2022
  - Win11 Enterprise OS: Future deployment
  - 22000 (21h2)
  - Browsers:
    - EDGE – 102.0.1245.41
    - Firefox – 91.10.0 esr
    - Chrome- 102.0.5005.63
- Current Enterprise Operating Version of Google Chrome
- Current Enterprise Operating Version of Microsoft Edge
- Current Enterprise Operating version of Firefox
- Splunk
- CrowdStrike
- Sophos
- Bitlocker
- DPS-issued Mobile Devices
- IOS Smart tablet (latest available for purchase)
- IOS Smart phone (latest available for purchase)

- Current Microsoft Enterprise Operating Version
- Current Enterprise Operating version of Mac OS X
- Current Enterprise operating version of Safari
- Current Enterprise Operating version of Firefox
- Current Enterprise Operating version of Google Chrome
- PCs (desktop or laptop), mobile devices, phones, and tablets [used by DPS customers or the general public for DPS information or services]
- Using Current IOS supported version
- Using Current Android supported version

1.2.2 DPS-Hosted System

A. System and Architectural Documentation

The Vendor must provide, within its Response, documentation for a DPS-hosted System consisting of the following.

- An overall narrative for any System which is hosted within the DPS-provided infrastructure.
- Narratives and detailed diagrams for the following:
    - Product architectural diagram;
    - Security diagram(s) (including security diagrams for database, network, application, etc.);
    - Network diagram;
    - Communications port diagram; and
    - For cloud-hosted, provide an inventory of products and services required to support the bulleted items above.
- An itemized list of any assumed capabilities of DPS IT systems required to access or support the Vendor's product or System.

B. DPS Standards and Requirements for Software/Hardware

The Vendor must follow the DPS standards and requirements for any Software or Hardware that are to be hosted within the DPS infrastructure. The existing DPS infrastructure framework supports several industry standard products and platforms. All Works for Hire created for DPS as part of this contract must be stored on DPS's local source code management repository, BitBucket. In addition, any application artifacts must be stored in DPS's Artifactory repository. The Vendor will use the agency's CI/CD pipeline and tool chain for build and deployment automation.

The Vendor must identify, within its Response, the products required to properly support the System in the DPS infrastructure.

The Vendor must provide, within its Response, an inventory for the DPS-hosted System consisting of the following:

- Required Hardware platforms and operating system to support the proposed System
  - The processor requirements
  - The memory requirements
  - Operating system details and dependencies
  - Data storage requirements
  - AWS or Azure Cloud services product (or equivalent, if applicable)
- Required application server platforms
  - The processor requirements
  - The memory requirements
  - Operating system details and dependencies
  - Data storage requirements
  - AWS or Azure Cloud services product (or equivalent, if applicable)
- Required web server platforms
  - The processor requirements
  - The memory requirements
  - Operating system details and dependencies
  - Data storage requirements
  - AWS or Azure Cloud services product equivalent, if applicable
- Required support services such as email servers, etc.
  - The processor requirements
  - The memory requirements
  - Operating system details and dependencies
  - Data storage requirements
  - AWS or Azure Cloud services product equivalent, if applicable

The Vendor must provide, within its Response, its ability to support each of the following DPS standards. The Vendor must also document any exceptions to our standards.

- DPS-provided infrastructure only allows the following database platforms.
  - AIX DB2 11 on premise
  - N-1 (N = current Microsoft SQL release)
  - AWS RDS services and Azure SQL cloud database services
- DPS-provided infrastructure report services use
  - Microsoft SQL Server Reporting Services
  - AWS and Azure Cloud Services reporting tools
- DPS-provided infrastructure platform services use
  - Current VMWare (ESXi) supported version
  - AWS or Azure Cloud services infrastructure products

1.2.3 Intersystem Communication Standards

The System will support integration with other applicable DPS systems using standard web services, provide Application Programming Interface (API) tools that can be incorporated into DPS applications, or secure file transfer protocol with data encryption.

1.2.4 Network Topography

DPS uses a combination of public and private TCP/IP network resources. All internal communications between client resources, other systems, and system services will be through this network. The Vendor's System will use standard TCP/IP network access ports. The System will be accessible on Port 80 for standard web browser access and Port 443 for secure web browser support.

The Vendor must provide, within its Response, documentation on each of the following, as applicable.

- An estimate on the amount of bandwidth or formulas to calculate usage required to support the number of expected internal DPS Users and volume of work.
- For a Vendor-hosted System, the Vendor must provide, within its Response, narrative on how adequate network capacity for DPS Users and External, non-DPS Users will be delivered.

1.2.5 Workstation Software Installation Packaging

The Vendor must provide, within its Response, its level of compliance with the Workstation Software Installation Packaging requirements listed below. The Vendor must also document any exceptions.

If a Software system is client-based and needs to be installed on each computer, the Vendor must provide the client Software in an .msi format, compatible with the current version of Windows Installer (and n-2), which allows for full control over the installer user interface, as defined by Microsoft for Windows-based systems. Any Vendor supplied .msi will fully support distributed deployment through the System Center Configuration Manager (and n-1) Application Model. OS X applications will support Apple Application installation package standards. Any Software required for mobile devices will be available from the appropriate App store based on the device operating system. Mobile device Software will also be compatible with Mobile Device
Management (MDM) Software distribution tools currently used by the Agency.

1.3 MAINTENANCE AND SUPPORT

The Vendor must, within its Response, indicate its level of compliance with each of the following Maintenance and Support standards. The Vendor must also document any exceptions.

The Vendor must provide a Software Maintenance system that includes the following.

A. Support for the System to include Software changes that the Vendor develops for DPS or makes available to DPS as managed in accordance with this Contract, including any Service Level Agreement (SLA) or Service Level Standards.
B. Preventive scheduled and unscheduled System diagnosis and correction of faults as well as modification of the Software to maintain the SLA or Service Level Standards.
C. A web-based support portal for DPS to report minor problems which will be available 24 hours per day, seven days per week, and 365 days a year with a searchable knowledge base for known issues. Response to reported problems will be managed as defined in the SLA or Service Level Standards.
D. Maintenance services to resolve usability problems to include bugs, security issues, installation of Software updates, and major Software releases.
E. New Software versions or releases occurring in the normal Maintenance yearly support as referenced in this Solicitation. These Software versions or releases will be provided to DPS at no additional cost.

1.3.1 Software Updates

The Vendor must provide periodic Software updates to incorporate corrections of any defects or implement enhancements to the System's Software.

A. Scheduled and unscheduled Software updates released by the Vendor will be installed during periods of the Maintenance window as mutually agreed upon by DPS and the Vendor.
B. Updates to documentation or manuals resulting from Software updates will be provided or made available upon DPS request.

1.3.2 Hardware Maintenance

The Vendor must provide Maintenance services for Hardware equipment owned by the Vendor that is installed to support a Vendor's Hosted System.

A. Scheduled Hardware Maintenance Notification

The Vendor must provide notice to DPS a minimum of ten business days prior to scheduled Maintenance including length of anticipated downtime plus the description or purpose of scheduled Hardware Maintenance. DPS reserves the right to delay or reschedule maintenance at its discretion to prevent maintenance from occurring during peak hours.

B. Unscheduled Hardware Maintenance Notification

The Vendor must provide notice to DPS as soon as the Vendor is aware of an issue, prior to unscheduled Hardware Maintenance including length of anticipated downtime plus the description or purpose of unscheduled Maintenance.

C. Preventive Maintenance

1. The Vendor must provide Preventive Maintenance services in order to maintain the System in good condition and working order on a mutually agreed upon, scheduled basis.
2. The Preventive Maintenance schedule is to be based on the Vendor's and DPS's mutual agreement of the particular service required for each System Component, it being understood that this schedule will be oriented to avoid periods when the System is expected to have the heaviest use.
3. During the term of this Contract, DPS may, by providing five calendar days' prior written notice, select any alternative period of Maintenance coverage whether or not such alternative represents an increase or decrease in service.

D. Remedial Maintenance

The Vendor must provide remedial Maintenance to the System on a 24-hours-per day, seven-days-per-week basis, with a Response Time in correspondence with the SLA specified for the system.

1.3.3 Change Control Participation

The vendor must inform the contract monitor or the delegated designee of all planned production updates prior to their implementation to ensure that the potential impact is assessed, and will be subject to the DPS Change Management process. This includes the initial deployment and all subsequent updates to the production system.

1.3.4 Service Outage Escalation and Communication Plan

The Vendor must provide, within its Response, a draft Service Outage and Escalation Communication Plan. The draft Communication Plan will specify the service outage notification and escalation process including how DPS is expected to notify the Vendor and how the Vendor will notify DPS. Upon contract award, DPS and the Vendor will finalize a Service Outage and Escalation Communication Plan.

1.3.5 System Performance Reporting

A. Vendor must follow the requirements of this section when a solution has a (1) significant degradation in performance; (2) application outage; (3) a software release must be rolled back due to defects or issues in the software release.

B. A significant degradation in performance is defined as a user being unable to use the solution because the performance of the system is degraded to a point to where the application does not perform as defined in the Response Time section of this document.

C. Application outages are defined as an unplanned disruption of the software solution that prevent the application user from accessing or using the application. This excludes application outages that are due to a network service outage that made it impossible for a user to access the application.

D. Software release rollbacks are defined as the rollback or removal of a software release or software update that had been previously approved through the Agency Change Control process and deployed into a production environment.

E. A Vendor must complete the following assessment and send to the DPS Contract Monitor for review and approval.

Event Name: [Type event name here]
Event Date: [Type event start date and end date here – format MM/DD/YYYY HH:MM – MM/DD/YYYY HH:MM] (Military time please)
Related Change Request: [Type CR number here – format CR ####
Purpose of Change Request: [Type the purpose of the CR here from the actual CR ticket] **Event Description:** [Type the event description here – include high-level details to adequately inform the audience of the change and expected resolution]
Event details: [Type a highly-detailed description of what happened during the event]
Event Impact: [Describe the timeline of the event and the user impact]
Future Prevention Steps: [Detail the steps for preventing this event in the future – numbered bullets are preferred if specifically ordered steps are required]

1.4 BASIC SERVICE LEVEL STANDARDS

These Basic Service Level Standards define the requirements, responsibilities, and obligations of DPS and the Vendor to ensure the Vendor provides DPS with the optimal level of System performance.

Additional standards are located throughout this Exhibit and Solicitation – if any, and include Maintenance and Support; System Performance; System Training Plan for Technical Staff; and Testing Requirements, Implementation and Acceptance.

Please see the following chart for DPS's Severity Level Definitions for the contract:

Severity Level	Description
1. Outage	Mission Critical System Down
2. Critical	Mission Critical System Degraded with Moderate customer impact
3. Urgent	End User Impact initiated
4. Important	Potential for performance impact if not addressed
5. Monitor	Issue addressed but could be impactful in the future
6. Informational	Inquiry for information

1.4.1 System Production Control

The Vendor must schedule production management such as batch processing, job scheduling, automated import/exports, etc. at intervals agreed upon between the Vendor and DPS.

The schedule will likely be oriented around periods when the System is expected to have the lightest use.

1.4.2 Vendor Customer and System Support

The Vendor must support all Software licensed to DPS and provide vendor system support for use during the term of this Contract.

The Vendor must provide a toll-free telephone number or email accessibility to DPS for the System, 24 hours per day/7 days per week. The Vendor must provide the DPS Contract Monitor a means to report trouble outside of normal business hours.

A. Vendor System support for DPS includes responsibilities such as the following.

- DPS employee training for the system
- System configuration
- System navigation
- Data query or export procedures
- Search criteria, best practices, parameters, etc.
- Troubleshooting for System Hardware, System Software, network, etc.
- Acting as primary support provider of the identified services and ensuring any subcontractors perform any assigned duties
- Informing DPS regarding scheduled and unscheduled service outages due to maintenance, troubleshooting, disruptions or as otherwise necessary that aligns with DPS current change management policy
- Transition responsibilities

B. Vendor System support for DPS excludes responsibilities such as the following.

- Record content
- Record quality
- Assisting in correcting data through an agreed-upon process (such as ETL, providing data updates via code)
- Assisting in modifying the system to reduce the number of data-entry errors (such as using a drop-down selection instead of using a free-form box)
- Record interpretation
- Employee administration (including new accounts, password creation or resets)
- Non-system Software owned, purchased, installed, developed or used by DPS or DPS's Hardware
- DPS's/User's Internet Service Provider (ISP) or other internal method of access

1.5 SYSTEM PERFORMANCE

1.5.1 Basic Requirements

The Vendor must maintain optimal System performance 24 hours per day, seven days per week, 365 days per year at a rate of 99% (the Rate) as calculated by Calculation of System Performance Rate below.

The Vendor is cautioned to quickly resolve the source or sources of failure. Inability to meet or exceed the Rate in any 12-month period may, at DPS's sole discretion, result in the following actions.

A. First Remedy: Written warning.
B. Continuing Remedy: DPS may begin exercising Contract breach remedies.

1.5.2 Calculation of System Performance Rate

The Vendor must measure the System performance rate by the amount of time the System is unavailable (downtime) during a calendar month. Vendor must report that information to DPS no later than the third Business Day of the following month. IT leadership will determine if any changes are necessary. This metric gauges the System performance as a percentage of available hours tracked to the quarter of an hour (rounded). The rate of System performance will be measured and monitored as follows in this Section.

Available hours equal the total number of hours in a month (24 hours multiplied by the number of days in the month). Downtime is the total number of hours (rounded to the quarter hour) during which the System is not in operation. Uptime is the actual amount of time the system is available minus downtime. System Performance Rate is equal to uptime.

For example, take the month of January:

Available hours in January: 744 hours (31 days X 24 hours);

Downtime: 1.86 hours per week, or 7.44 downtime hours for the month

Calculation:

744 available hours – 7.44 downtime hours = 736.56 uptime hours; and

736.56 uptime hours ÷ 744 available hours = 99% uptime.

1.5.3 Response Time

The Vendor must maintain response times that fall within benchmarks set by industry standards. Response times for government applications will be between 0.3 seconds and no longer than eight seconds. Response times will be reported as the average of the total response time for a quarterly period. Time period used in calculating the rate will be used to calculate the Response Time average. The Vendor must provide performance metrics based on the applications performance for the period specified.

For Vendor-hosted Systems, the Vendor must provide monitoring tools and reports that DPS can access to verify capacity and throughput.

1.5.4 Data Backups

The Vendor or the System must perform backups on all System records once every 24 hours, seven days per week, and 365 days per year to facilitate data and System restoration in the event of any failures. The data backup schedule will be mutually agreed upon by both the Vendor and DPS and will be performed when the System is expected to

have the lightest use. Data and System Backups should be based on the business's recovery point objective (RPO).

The Vendor or the System must be able to restore to development or test environments and must demonstrate the operability of a backup during the testing phase of the project.

1.5.5 (?) Service Levels, Recovery Points, and Target Response

Purpose

The purpose of the Service Level Standards is to specify the requirements of the Vendor's services as regarding the following.

- Requirements for product or service that will be provisioned to DPS
- Agreed service targets
- Criteria for target fulfilment evaluation
- Roles and responsibilities of Vendor
- Duration, Scope and Renewal of service level expectations
- Supporting processes, limitations, exclusions and deviations.

Recovery Points and Times

The Vendor must, within its Response, provide Business Continuity Plan (BCP) documentation for each of the following.

A. System Crashes

- System crashes will be resolved within the SLAs noted below.
- Any exceptions to the SLA resolution requirement will be documented and will require email notifications explaining the reason for any delays to the DPS IT Chief Information Officer (CIO) and the DPS Contract Monitor.

B. Physical Infrastructure

Vendor must provide DPS with a location-independent restoration plan, including an Information System Contingency Plan (ISCP) that describes the policies, procedures, and processes required to recover a system at the current or alternate location, regardless of its hosted location.

1.5.6 Hardware and Software Refresh Plans

Hardware Refresh Plans will not be applicable for cloud solutions; however, Software refresh plans will need to be addressed as documented below.

Vendor must provide, within its Response, documentation for the following.

A. Vendor-Hosted System

The Vendor must ensure that all operating systems, hardware, software versions, databases, and tools must be kept current, using an "N – 1" model, unless a specific version is specified in the current IT Technology Standards. Such as the current Microsoft Operating System Model, N - 1 refers to the Major Build Number.

The Vendor must provide Hardware and Software Refresh Plans to address end-of support or end-of-life products. The plan will address System and application patches and implementation methodology and schedule. Refresh of Hardware and Software will be at the sole discretion of DPS.

B. DPS-Hosted System or DPS-Provided Cloud-Hosted System

The Vendor must provide Software refresh plans to address end-of-support or end of-life products. The plan will address System and application patches and implementation methodology and schedule. Refresh of Software will be at the sole discretion of DPS.

1.5.7 Vendor's Business Continuity and Disaster Recovery Plan

The Business Continuity and Disaster Recovery Plan is a documented set of plans related to preparations and associated activities which are intended to ensure that an organization's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them or will be recovered to an operational state within a reasonably short period of time.

Vendor must provide a disaster recovery capability for their disaster recovery planning and recovery efforts in their response to the solicitation by the agency. Vendor must provide the following to DPS within 30 days of contract execution and upon update to an existing plan:

- Business continuity and disaster recovery plans (BC/DRP), a DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency, to include Information System Contingency Plans (ISCP), a location independent plan that focuses on the procedures needed to recover a system at the current or an alternate location, regardless of hosted location for restoration;

- Requirements for business continuity and disaster recovery plans include the following:
    (a) Defined purpose and scope, aligned with relevant dependencies;
    (b) Accessible to and understood by those who will use them;
    (c) Owned by a named person who is responsible for their review, update, and approval;
    (d) Defined lines of communication, roles, and responsibilities;
    (e) Detailed recovery procedures, manual work-around, and reference information;
    (f) Method for plan notification and coordination with DPS; and
    (g) Detailed process by which DPS may declare a disaster recovery necessary for the system and recovery documentation to include DPS user acceptance testing be completed during disaster recovery.
- Appropriate plans, governance, and service management to ensure applicable planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and customers based on industry acceptable standards (such as, ITIL v4, COBIT 5, CSA CCM, NIST);
- Protection measures must be put into place to react to natural and human caused threats;
- Evidence that BC/DR plans will be tested at planned intervals (at least once annually) or upon significant organizational or environmental changes; and
- Information system documentation (such as administrator and user guides, architecture diagrams) to include the following:
    (a) Configuring, installing, and operating the information system;
    (b) Effectively using the system's security features;
    (c) Business Continuity and Disaster Recovery Plans (BC/DR) to include a location-independent plan that focuses on the procedures needed to recover a system at current or an alternate location;
    (d) Specific actions Vendor will take to meet or exceed DPS's Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO); and
    (e) Related artifacts for the methodology, test, training, and exercises (TT&E) used to validate BC/DR plans.
    (f) Provision of disaster recovery, testing or exercise results to DPS, within 30 days of the incident, with an Improvement Plan to include timelines to resolve any issues identified.

TT&E results and Improvement Plan identified in annual review of Backup and recovery measures will be incorporated as part of BC/DR and tested accordingly for effectiveness.

The Vendor agrees to meet the SLA or Service Level Standards for all Vendor-provided Services including:

- Vendor's help desk or customer support
- Maintenance services
- Support services (such as, Software or Hardware)
- Hosting services
- Network services, if applicable

1.6 SYSTEM TRAINING PLAN FOR TECHNICAL STAFF

The Vendor must provide, within its Response, a detailed training plan. The plan must explain how the Vendor will train DPS technical staff to support the System. All training will be made available through DPS facilities located in the State of Texas. Training will be interactive so that students have the ability ask the instructor questions during the sessions. The schedule of training sessions will be mutually coordinated and agreed upon by DPS and the Vendor. It is estimated that DPS will receive a negotiated number of training sessions to be conducted during the Initial Term and Optional Renewal periods. The requirements of the training plan will address the following.

A. System Administration Training (if applicable)

- Daily operation and Maintenance of the Software
- User administrative duties (such as add users, delete users, password administration)
- System configuration
- Monitoring System availability and System status
- System error diagnostics
- System performance monitoring
- Administrative System reports

B. Developer Training (if applicable)

- Skills needed to integrate new data into the Software and to program the Software to develop new capabilities
- How the Software architecture handles various data types
- How the platform scales with users and data
- How the Software features interact with the security model
- How to integrate with internal and external data sources
- Understanding System's APIs to perform common tasks (such as exchanging information between the System and other applications)

C. Training Programs

- The Vendor training programs will allow DPS and Vendor to jointly alter the proportion of System Administration and Developer training programs to maximize the overall effectiveness of the training for DPS
- The Vendor must scale, detail, and tie training programs to match the System

D. Training Materials

- The Vendor must provide copies for each type of training consisting of the curricula and associated User Guides for acceptance by DPS no less than 15 Business Days prior to the first training program. The copies will be submitted to the DPS Contract Administrator.
- The Vendor must make available to DPS, video recorded training for each type of training program as a review/refresher resource for DPS personnel who previously completed the live training
- Vendor will transfer ownership of training material to DPS to use internally and with business partners that access Vendor's provided solution.

1.7 TESTING REQUIREMENTS, IMPLEMENTATION AND ACCEPTANCE

All testing activities will include the following.

1.7.1 Implementation and Acceptance

DPS must work closely with the Vendor to ensure requirements are met and completed; however, completion of any one requirement does not constitute full completion and acceptance of the Contract's requirements.

1.7.2 Cloud-Hosted Infrastructure Environment

DPS requires that all Cloud-hosted implementations that are deployed solely for the support of this contract use Infrastructure as Code to allocate cloud resources. The use of Infrastructure as Code is not required for SaaS products that include cloud hosting resources as part of a standard deployment which is used for all customers of the Vendor's SaaS product.

- All cloud service application deployments that are targeted for the cloud service provider's government-specific cloud service must be built using the available CJIS templates as a basis.
- All cloud service application deployments that are targeted for the cloud service provider's Public Cloud must be built using the available NIST 800-53, rev. 5 templates as a basis.
- The Infrastructure as Code templates must be able to deploy Development, Test, UAT, and Production environments from the same template by submitting multiple iterations with input parameters to specify the unique properties of each environment.
- The Infrastructure as Code template must be kept in a DPS-owned source repository.
- All Infrastructure as Code templates must include all required components required for the proper operation and auditing of the application. This includes

- all VPC and network configurations for subnets, route tables and access control lists;
- all compute resources and load balancers;
- all applicable Security Groups;
- any cloud services database services such as RDS or DynamoDB;
- all storage resources and applicable security policies;
- all applicable alerts and notifications; and
- all applicable cloud service Config rules to monitor the account.

DPS requires verification and acceptance as identified in the items below for all Cloud deployments that are specifically built by the Vendor to support the contract. This verification is not required for SaaS products that include cloud services resources as part of a standard deployment that is used for all customers of the Vendor's SaaS product.

- DPS IT resources will be provided all final versions of any Infrastructure as code templates prior to deployment for Production cloud resources. All testing, verification and audit results documentation must be provided to DPS IT prior to the deployment of Production cloud resources.
- DPS resources will perform an audit of deployed production environment to ensure compliance with any applicable regulatory standards prior to loading DPS data.
- DPS resources will perform an audit of any associated cloud services accounts associated with all environments used for DEV, SQA, STG and Production to ensure compliance with any applicable regulatory standards prior to loading DPS data.
- Natural progression of the scripts: Dev, SQA, STG, PROD.

DPS personnel will provide written approval of acceptance of any required
Infrastructure as Code templates and cloud services accounts once the auditing and the review process has been completed.

1.7.3 Unit Testing

- The Vendor must provide a listing of Unit Test Cases based on the requirements of this Contract.
- The Vendor must develop automated unit tests in all of its code.
- The Vendor must ensure execution of all unit tests in every build.
- The Vendor must also provide DPS with the results of the Unit Test Cases that were executed to completion.
- DPS will be the owner of all automated test cases developed as part of the project.
- Based on the outcome of successful unit testing, the Vendor will advance to the next step of system testing. Successful unit testing will be defined as 100% pass rate of all defined Unit Test Cases with no outstanding issues/defects. The Vendor must perform all these tests in a development environment.

1.7.4 System Testing

- The Vendor must provide to DPS for review and approval by DPS Quality Assurance (QA) testing staff, documented Test Cases that will be performed during Vendor System testing to validate the successful migration and installation of the Software package before any System testing begins.
- The Vendor must perform System testing in the Vendor's QA environment and provide test results to DPS.
- The Vendor must log all defects found during the System testing in the agreed upon defect tracking application.
- The Vendor must investigate any defects found during System testing and participate in defect triage meetings with DPS to determine defect outcome and resolution.
- The Vendor must provide defect fixes in the timeframe as defined in the SLA or Service Level Standards.
- The Vendor must demonstrate all components of the application Software are performing as defined in the System Test Cases and business requirements, including interfaces with other systems (baseline interfaces), in the specified System hardware, operating Software and network environment (system environment).
- Based on the successful outcome of System testing, DPS will advance to Performance Testing. Successful System testing will be defined in the Quality Assurance Test Plan as well as in the Entry and Exit Criteria document, Section 1.8.
- System testing will not be considered successful if outstanding Blocker or Critical defects pending resolution remain, as defined in the agreed upon test plan.

1.7.5 Performance/Load Testing

Performance/Load Testing will be performed by DPS in coordination with the Vendor in instances where internal metrics (network load, etc.) cannot be captured by the Vendor. DPS will help coordinate internal resources to provide oversight and assistance when necessary.

- The Vendor must provide documented Test Cases to DPS that will be performed during Vendor performance and load testing to validate the successful performance of the Software package.
- The Vendor must capture the average data throughput for the System and the maximum number of concurrent users before service degradation to ensure user traffic does not have an adverse effect on the DPS network and will provide these results to DPS.
- The Vendor must be responsible for conducting performance and load testing that will demonstrate the Vendor's System is capable of meeting metrics as defined by DPS.

- The Vendor must provide performance and load test results to DPS for review and approval.
- Based on the outcome of successful performance and load testing, the Vendor will advance to the next step of System integration testing. Successful performance testing will be defined in the Performance/Load Test Plan documentation created by DPS. The Vendor must perform all these tests in a production-like environment.
- Performance/Load testing will not be considered successful if outstanding Blocker or Critical defects pending resolution remain as defined in the agreed upon test plan.

1.7.6 System Integration Testing

DPS will perform System integration testing independently or jointly with the Vendor following successful completion and documentation of Vendor and DPS System testing.

- The Vendor must provide assistance during the System integration testing process by providing technical and QA resources that will answer questions and will clarify or fix any issues encountered during the System integration testing cycle. This support can be performed remotely or in person at the DPS facility. Remote support will consist of remote server control mechanisms, videoconference review sessions, telephone conference calls and email exchanges. System integration testing will focus on the integration and interaction with other DPS systems, external systems, or third-party components and will be based on DPS requirements as well as the Vendor's System Design Specification.
- The Vendor must provide a User Acceptance Testing environment (STG) upon successful completion of System Integration Testing.
- DPS will log all defects found during the System integration testing in the agreed upon defect tracking application.
- The Vendor must investigate any defects and participate in defect triage meetings with DPS to determine defect outcome and resolution.
- The Vendor must provide a documented response to the documented defect in the agreed upon defect tracking application.
- The Vendor must provide defect fixes in the timeframe as defined in the SLA.
- The Vendor must provide release notes containing an open issues log for each test iteration.
- At DPS's sole discretion, Test Cases may be modified or added to ensure completeness, accuracy and quality of the delivered Software package as defined in business and technical documentation.
- Based on the successful outcome of System integration testing, DPS will advance to User Acceptance Testing (UAT). Successful System integration testing will be defined in the Quality Assurance Test Plan as well as in the Entry and Exit Criteria document, Section 1.8

- System Integration testing will not be considered successful if outstanding Blocker or Critical defects pending resolution remain as defined in the agreed upon test plan.

1.7.7 User Acceptance Testing (UAT)

- Following successful completion of the System integration testing, or System test for Vendor-Hosted Systems, DPS will coordinate and execute UAT in the Vendor's (STG) environment.
- UAT will be performed by DPS end users based on UAT Test Cases created by DPS.
- Based on level of configuration or customization, DPS may require Vendor to be onsite for UAT.
- DPS will notify the Vendor of any defects found during UAT of the Software System.
- The Vendor must investigate any defects and participate in defect triage meetings with DPS to determine defect outcome and resolution.
- The Vendor must provide defect fixes in the timeframe as defined in the SLA or Service Level Standards.
- If the number of defect failures prevents all systems from operating as described above, DPS may reject the entire final Software package.
- If all criteria is not met as defined in the User Acceptance test plan documentation created by DPS, or the Vendor's System does not meet the defined business requirements, DPS may reject the final Software System.

1.7.8 Final Acceptance

The software solution will undergo a stabilization and acceptance period. This stabilization period will not start until the solution is in production. Stabilization period will consist of 30 days of production operations after the final delivery of the Solution to the production environment.

Stabilization will be deemed completed if, at the conclusion of the 30-day period, there are:

1. Zero Blocker outstanding defects;
2. Zero Critical outstanding defects; and
3. No more than 10 Major outstanding defects.

Blocker, Critical, and Major severities are identified during the testing cycle of the Solution with inputs from DPS and Vendor teams.

Final acceptance will be documented in writing, on the Final Acceptance Form and will be executed by DPS and the Vendor.

1.7.9 Failure Resolution

Upon failure of any test within the control of the Vendor, the Vendor must submit report describing the nature of the failure and the actions to be taken to remedy the situation prior to any modification or replacement of the System, within ten business days. DPS will provide written approval or denial within five business days. If a System requires modification, the fault will be corrected, and the test repeated until successfully completed.

- Major discrepancies that will substantially delay receipt and acceptance of the System will be sufficient cause for rejection of the System. Failure to satisfy the requirements of any test is considered a defect and the System will be subject to rejection by DPS. Any rejected Software package may be offered again for retest provided all noncompliance has been corrected.
- Resolution of System integration test failure. If the Software package fails the System integration test, Vendor will correct the fault and then DPS will repeat the Systems integration test until successfully completed.
- Resolution of final acceptance test failure. If a defect within the System is detected during the final acceptance test, DPS will document the failure. Vendor will be required to research, document and correct the source of failure. Once Improvement Plan is implemented, DPS will monitor the point of failure until a consecutive 30 calendar-day period free of defects is achieved.

1.7.10 Retest

Vendor and DPS will mutually agree to re-test per the Testing Requirements,

Implementation, and Acceptance section, as determined by the environment where the issue is to be addressed. If the system downtime exceeds 72 hours or the System does not meet the stability and acceptance criteria defined above, DPS may extend the test period by an amount of time equal to the greater of the downtime in excess of 72 hours or the number of days required to complete the performance requirement of an individual point of failure.

1.8 QA ENTRY AND EXIT CRITERIA

1.8.1 Purpose

Identify and clarify Entrance/Exit Criteria for all initiatives, projects or applications that use the controlled testing environment(s) and processes, commonly referred to as TST, SQA or PRD. The Quality Assurance Team maintains this document and should be referenced in all documents related to software changes that need to be released. This

document provides general guidance for requirements, wherein builds, code documents or artifacts are introduced into those environments and processes regarding entry/exit into/from the testing environment(s). This document does not attempt to cover those projects for which the QA Team is serving in an oversight and advisory role.

1.8.2 Scope

Maintain controlled environments and processes to enhance the organization's ability to implement code or applications into the DPS testing and performance environments, and, as result, reducing production defects, trouble tickets or downtime in production.

1.9 GENERAL ENVIRONMENT ENTRY/EXIT CRITERIA AND PROCESS

1.9.1 General Environment Requirements

- Project, Development and Test Leads will engage with Release Manager (RM) for Environment resource. RM should be engaged as early as possible to provide environment review and analysis for all environments.
- Project Lead/Manager, Development Lead and Test Lead must provide documentation sufficient for the RM to complete a testing environment analysis. This information is required to sufficiently gather and identify project resources and requirements for all applications (modified and new), to validate existence of required testing environments.
- RM will assess current environment(s) and identify environment deficiencies, providing feedback to Project Lead/Manager, Development Lead and Test Lead to identify presence or absence of environment(s) and hardware.
- Documentation must include Deployment steps with roll back strategy (as applicable), version number, be held in source control and be approved by the RM.

1.9.2 Development Environment Entrance/Exit Process/Criteria

- General Environment Requirements (above) have been met.
- Build artifacts must be provided, in advance, to the RM for review, prior to scheduled deployment to Development Environment.

Depending upon project size and intent (as defined and agreed upon by the Project Team), the items required for entrance, and acceptance, into the Development environment would include the following. Unit, Component and Integration test results

- Design Document
- Release Notes, including open issues

- Criteria to exit from Development Environment to QA will be governed by the QA Test Plan and should contain the following.
    - Unit, Component and Integration test results
    - Design Document
    - Release Notes, including open issues

1.9.3 QA Environment Entrance/Exit Process/Criteria

- General Environment Requirements (above) have been met.
- QA Test Plan(s) and test scenarios are reviewed and have approval by project team.
    - The intended functionality of all code changes per business requirements has been documented in test scenarios and these test scenarios have been reviewed and agreed upon within the Test Plan.
- All standard software components, including testing tools, must have been successfully installed and functioning properly.
- Criteria to exit from QA Environment to UAT Environment will be governed by the QA Test Plan, but the following must be included (at a minimum).
    - Test Summary Report (TSR)
    - Test Results
    - Defect Report(s)

1.9.4 UAT Environment Entrance/Exit Process/Criteria

- General Environment Requirements (above) have been met.
- UA Test Plan(s) and test scenarios are reviewed and signed off.
    - The intended functionality of all code changes per business requirements has been documented in test scenarios and these test scenarios have been reviewed and agreed upon within the Test Plan.
- All standard software components, including testing tools, must have been successfully installed and functioning properly.
- Criteria to exit from QA Environment to UAT will be governed by the QA and UA Test Plan but should contain the following (at a minimum).
    - Test Summary Report (TSR)
    - Test Results
    - Defect Report(s)

1.9.5 PRD Environment Entrance Process/Criteria

- General Environment Requirements (above) have been met.

- Project Lead/Manager, Development Lead and Test Lead must provide documentation sufficient within a Change Request (CR) for the Change Control Coordinator (CCC) to complete a CR analysis. This information is required to sufficiently gather and identify project resources and requirements for all applications (modified and new), to validate existence of required testing environment.
- Project Lead/Manager will schedule official Change Control Board (CCB) meeting when all build and release artifacts are ready for promotion into PRD.
- Build artifacts will be provided in advance for review by the CCC prior to the CCB meeting.
- QA and UA Test Plan(s) have received management approval and test execution complete. Documents have been submitted to the CR.
- Depending upon project size and intent (as defined and agreed upon by the Project Team), the items required for entrance and acceptance into the PRD environment would include the following.

  A – Approvals from all relevant parties at DPS
  C – Cyber scans (when required)
  T – Test results
    - Test Summary Report (TSR)
    - Test Plans
    - Test Results
    - Defect Reports
    - Release Notes

  I – Implementation, validation, rollback plans
  O – Operation support manual information (when required)
  N – Notification to users (when the change has downtime or user impact)