Exhibit A – Statement of Work

1. OVERVIEW

Renewal for support/service of Graphic Arts hardware to provide preventative maintenance and break/fix for high output/yield print hardware.

2. CONTRACTED PARTIES:

This agreement is between the Department of State Hospitals (DSH), and TBD, (Contractor).

3. SCOPE:

Contractor shall provide DSH Monthly Base Charge-Option 1 Maintenance and Support for the following equipment:

IMAGEPRESS C910 – Clicks per month 48,000 color and 24,000 B&W	
Monthly Base Charge – includes OEM toner, parts, and labor (no staples)	
Overage Rate for COLOR	
Overage Rate for B&W	
% Increase in rate for inclusion of staples for COLOR	
% Increase in rate for inclusion of staples for B&W	
% Increase in rate for Rural Service Zone	
% Increase in rate for Remote Service Zone	
VARIOPRINT DP LINE 115 – Clicks per month 100,000 B&W	
Monthly Base Charge – includes OEM toner, parts, and labor (no staples)	
Overage Rate for B&W	
% Increase in rate for inclusion of staples for B&W	
% Increase in rate for Rural Service Zone	
% Increase in rate for Remote Service Zone	

4. CONTACTS:

Department of State Hospitals: Aaron Steinbock 10333 El Camino Real Atascadero, CA 93422 (805)468.3292 Email: Aaron.Steinbock@dsh.ca.gov	**Contractor:**

5. GEN AI TECHNOLOGY USE & REPORTING:

The State of California seeks to realize the potential benefits of GenAI, through the development and deployment of GenAI, while balancing the risks of these technologies.
Bidder/Offeror must notify the State in writing if it: (1) intends to provide GenAI as a deliverable to the State; or (2), intends to utilize GenAI, including GenAI from third parties, to complete all

or a portion of any deliverable that materially impacts: (i) functionality of a State system, (ii) risk to the State, or (iii) Contract performance. For avoidance of doubt, the term "materially impacts" shall have the meaning set forth in State Administrative Manual (SAM) 4986.2.

Failure to report GenAI to the State may result in disqualification. The State reserves its right to seek any and all relief it may be entitled to as a result of such non-disclosure.
Upon notification by a Bidder/Offeror of GenAI as required, the state reserves the right to incorporate GenAI Special Provisions into the final contract or reject bids/offers that present an unacceptable level of risk to the state.

Government Code 11549.64 defines “Generative Artificial Intelligence (GenAI)” as an artificial intelligence system that can generate derived synthetic content, including text, images, video, and audio that emulates the structure and characteristics of the system’s training data

6. AGREEMENT TERMS:

The term of this agreement is from **November 1, 2024**, through **October 31, 2025**

7. COST:

The total cost of this agreement is **$**.

8. Terms and Conditions

(a) IT General Provisions for Non-Cloud Goods and Services (Effective 02/20/2025)

9. LOCATIONS:

The services shall be performed for the Department of State Hospitals at the following location(s):

☒ **DSH-Atascadero** 10333 El Camino Real P.O. Box 7001 Atascadero, CA 93423-7001	☐ **DSH-Coalinga** 24511 West Jayne Avenue P.O. 5000 Coalinga, CA 93210
☐ **DSH-Metropolitan** 11401 South Bloomfield Avenue Norwalk, CA 90650	☐ **DSH-Patton** 3102 East Highland Avenue Patton, CA 92369
☐ **DSH-Napa** 2100 Napa-Vallejo Highway Napa, CA 94558-6293	☐ **DSH-Sacramento** 1215 O Street Sacramento, CA 95814

10. AMENDMENT: .

This agreement may be amended at the DSH's sole discretion to extend the term for up to one (1) additional year and to add funding sufficient for that period at the same rates if it does not exceed the DSH's Purchasing Authority at the time of amendment. Any amendment shall be in writing and approved by both parties and, if applicable, be approved by the Department of General Services/or California Department of Technology.

11. PAYMENT PROVISIONS

(a) Invoicing and Payment

i) Contractor shall submit one original and three copies of each invoice, unless emailed.

ii) Invoices shall clearly reference the agreement and PO number.

iii) To expedite the processing of invoices submitted to the DSH for payment, all invoice(s) shall be submitted to the DSH for review and approval at either:

Department of State Hospitals – Atascadero
Attention: Accounting Office
10333 El Camino Real
Atascadero, CA 93423-70001
Email: ashaccounting@dsh.ca.gov

iv) Licenses shall be paid annually upon each term start date(s).

v) Hardware Maintenance shall be paid monthly, in arrears.

vi) Hardware Warranty shall be paid in full

(b) Budget Contingency Clause:

i) It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall no longer be in full force and effect. In this event, the State shall have no liability to pay any funds whatsoever to Contractor or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.

ii) If funding for any Fiscal Year (FY) is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Agreement with no liability occurring to the State or offer an Agreement amendment to Contractor to reflect the reduced amount.

iii) If this Agreement overlaps Federal and State FY's, should funds not be appropriated by Congress or approved by the Legislature for the FY in which the Agreement was entered into, and/or any subsequent years covered under this Agreement, the State may exercise its option to cancel this Agreement.

iv) In addition, this Agreement is subject to any additional restrictions, limitations, or conditions enacted by Congress or the Legislature which may affect the provisions or terms of funding of this Agreement in any manner.

(c) Prompt Payment Clauses:

i) Payment will be made in accordance with, and within the time specified in, Government Code section 927, et seq.

(d) Travel and per Diem

i) DSH will not pay for Travel or Per Diem.

EXHIBIT F (Non-HIPAA/HITECH Act Contracts)
INFORMATION PRIVACY AND SECURITY REQUIREMENTS

This Information Privacy and Security Requirements Exhibit (For Non-Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health (Non-HIPAA/HITECH Act Contracts) (hereinafter referred to as "this Exhibit") sets forth the information privacy and security requirements Contractor is obligated to follow with respect to all personal and confidential information (as defined herein) disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on behalf of the California Department of State Hospitals (hereinafter "DSH"), pursuant to Contractor's agreement with DSH. (Such personal and confidential information is referred to herein collectively as "DSH PCI".) DSH and Contractor desire to protect the privacy and provide for the security of DSH PCI pursuant to this Exhibit and in compliance with state and federal laws applicable to the DSH PCI.

I. Order of Precedence: With respect to information privacy and security requirements for all DSH PCI, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the agreement between Contractor and DSH, including Exhibit A (Scope of Work), all other exhibits and any other attachments, and shall prevail over any such conflicting terms or conditions.

II. Effect on lower tier transactions: The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, and the information privacy and security requirements Contractor is obligated to follow with respect to DSH PCI disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on behalf of DSH, pursuant to Contractor's agreement with DSH. When applicable the Contractor shall incorporate the relevant provisions of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. Definitions: For purposes of the agreement between Contractor and DSH, including this Exhibit, the following definitions shall apply:

A. Breach: "Breach" means:

1. the unauthorized acquisition, access, use, or disclosure of DSH PCI in a manner which compromises the security, confidentiality or integrity of the information; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29, subdivision (f).

B. Confidential Information: "Confidential information" means information that:

1. does not meet the definition of "public records" set forth in California Government Code section 7920.530, or is exempt from disclosure under any of the provisions of Section 7920.000, et seq. of the California Government Code or any other applicable state or federal laws; or

2. is contained in documents, files, folders, books or records that are clearly labeled, marked or designated with the word "confidential" by DSH.

C. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

D. PCI: "PCI" means "personal information" and "confidential information" collectively (as these terms are defined herein).

E. Personal Information: "Personal information" means information, in any medium (paper, electronic, oral) that:

1. directly or indirectly collectively identifies or uniquely describes an individual; or

2. could be used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the other information; or

3. meets the definition of "personal information" set forth in California Civil Code section 1798.3, subdivision (a); or

4. is one of the data elements set forth in California Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

5. meets the definition of "medical information" set forth in either California Civil Code section 1798.29, subdivision (h)(2), or California Civil Code, section 56.05, subdivision (j); or

6. meets the definition of "health insurance information" set forth in California Civil Code section 1798.29, subdivision (h)(3); or

7. is protected from disclosure under applicable state or federal law.

F. Security Incident: "Security Incident" means:

1. an attempted breach; or

2. the attempted or successful unauthorized access or disclosure, modification or destruction of DSH PCI, in violation of any state or federal law or in a manner not permitted under the agreement between Contractor and DSH, including this Exhibit; or

3. the attempted or successful modification or destruction of, or interference with, Contractor's system operations in an information technology system, that negatively impacts the

confidentiality, availability or integrity of DSH PCI; or

4. any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission. Furthermore, an information security incident may also include an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies.

G. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of information.

IV. Disclosure Restrictions: The Contractor and its employees, agents, and subcontractors shall protect from unauthorized disclosure any DSH PCI. The Contractor shall not disclose, except as otherwise specifically permitted by the agreement between Contractor and DSH (including this Exhibit), any DSH PCI to anyone other than DSH personnel or programs without prior written authorization from the DSH Contract Manager, except if disclosure is required by state or federal law. Contractor shall inform DSH of any disclosure required by law that is not contemplated by this Agreement, prior to making the disclosure.

V. Use Restrictions: The Contractor and its employees, agents, and subcontractors shall not use any DSH PCI for any purpose other than performing the Contractor's obligations under its agreement with DSH.

VI. Safeguards: The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of DSH PCI, including electronic DSH PCI. At each location where DSH PCI exists under Contractor's control, the Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities in performing its agreement with DSH, and incorporates the requirements of Section VII, Security, below. Contractor shall provide DSH with Contractor's current and updated policies within five (5) business days of a request by DSH for the policies.

VII. Security: The Contractor shall take any and all steps reasonably necessary to ensure the continuous security of all electronic data systems containing DSH PCI. These steps shall include, at a minimum, complying with all of the data system security precautions listed in the Contractor Data Security Standards set forth in Attachment 1 to this Exhibit.

VIII. Security Officer: At each place where DSH PCI is located, the Contractor shall designate a Security Officer to oversee its compliance and to communicate with DSH on matters concerning this Agreement.

IX. Training: The Contractor shall provide training on its obligations under this Agreement, at its own expense, to all of its employees who assist in the performance of Contractor's obligations under Contractor's agreement with DSH, or otherwise use or disclose DSH PCI.

A. The Contractor shall require each employee who receives training to certify, either in hard copy or electronic form, the date on which the training was completed.

B. The Contractor shall retain each employee's certifications for DSH inspection for a period of three years following contract termination or completion.

C. Contractor shall provide DSH with its employee's certifications within five (5) business days of a request by DSH.

X. Employee Discipline: Contractor shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other Contractor workforce members under Contractor's direct control who intentionally or negligently violate any provisions of this Agreement.

XI. Contractor California Consumer Privacy Protection Act (CCPA) Responsibilities: Contractor, its employees, agents, and sub-contractors, shall comply with all Contractor's applicable legal obligations pursuant to the CCPA, including but not limited to the handling and disclosure of personal information received resulting from this agreement, abiding by CCPA notice requirements on Contractor's website(s), safeguarding personal information received in connection with this agreement, refraining from using personal information received in connection with this agreement outside of the enumerated business purpose contained therein. Contractor's failure to comply with such laws and regulations shall constitute a material breach of this Agreement, and shall be grounds for immediate termination of the Agreement by DSH, pursuant to **ADMIN CONTRACT:** section 7 of Exhibit C OR If this is a **TSD IT CONTRACT:** IT Provisions for GSPD-ITGP. By executing this Agreement, Contractor certifies that it is aware of its legal obligations as set forth under the CCPA, that it is in compliance with the CCPA, and shall remain in compliance with all such laws and regulations for the term of this Agreement.

To the fullest extent permitted by State law, pursuant to section 5 of Exhibit C OR If this is a **TSD IT CONTRACT** TSD Contract IT Provisions for GSPD-ITGP of this Agreement, Contractor agrees to indemnify and hold the DSH harmless from and against any and all liability, loss, suit, damage or claim, including third party claims brought against the DSH, **ADMIN CONTRACT:** section 5 of Exhibit C OR If this is a **TSD IT CONTRACT:** IT Provisions for GSPD-ITGP], as well as damages and reasonable costs assessed against the DSH by a court of competent jurisdiction (or, at Contractor's option, that are included in a settlement of such claim or action in accordance herewith), to the extent such claim arises from Contractor's violation of the CCPA in relation to Contractor's performance under this agreement; provided, that (i) Contractor is notified promptly in writing of the claim; (ii) Contractor controls the defense and settlement of the claim; (iii) Contractor provides a defense with counsel approved by the DSH; and (iv) the DSH cooperates with all reasonable requests of Contractor (at Contractor's expense) in defending or settling the claim.

XII. Breach and Security Incident Responsibilities:

A. Notification to DSH of Breach or Security Incident: The Contractor shall notify DSH immediately upon the discovery of a breach (as defined in this Exhibit), and within twenty-four (24) hours by email of the discovery of any security incident (as defined in this Exhibit), unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made to DSH immediately after the law enforcement agency determines that such notification will not compromise the investigation. Notification shall be provided to the DSH Program Contract Manager, the DSH Chief Privacy Officer and the DSH Chief Information Security Officer, using the contact information listed in Section XII.F., below. If the breach or security incident is discovered after business hours or on a weekend or holiday and involves DSH PCI in electronic or computerized form, notification to DSH shall be provided by calling the DSH Chief Information Security Office at the telephone numbers listed in Section XII.F., below. For purposes of this Section, breaches and security incidents shall be treated as discovered by Contractor as of the first day on which such breach or security incident is known to the Contractor, or, by exercising reasonable diligence would have been known to the Contractor. Contractor shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee or agent of the Contractor.

Contractor shall take:

1. prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and

2. any action pertaining to a breach required by applicable federal and state laws, including, specifically, California Civil Code sections 1798.29 and 1798.82 (2021).

B. Investigation of Breach and Security Incidents: The Contractor shall immediately investigate security incidents/suspected breaches which potentially expose DSH data or impact DSH system. Within 8 hours of discovery (of the incident), and subject to the legitimate needs of law enforcement, Contractor shall inform the DSH Contract Manager, the DSH Chief Privacy Officer, and the DSH Chief Information Security Officer of:

1. what data elements were potentially involved, and the extent of the data disclosure or access involved in the breach, including, the approximate number of individuals whose personal information was suspected to be breached; and

2. a description of the unauthorized persons known or reasonably believed to have improperly used the DSH PCI and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the DSH PCI, or to whom it is known or reasonably believed to have had the DSH PCI improperly disclosed to them; and

3. a description of where the DSH PCI is believed to have been improperly used or disclosed; and

4. a description of impacted systems, including hardware or software elements which process, store, or transmit DSH data or provide services on behalf of DSH; and

5. a description of the probable and proximate causes of the breach or security incident; and

6. whether Civil Code sections 1798.29 and 1798.82 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: The Contractor shall provide a written report of the investigation to the DSH Contract Manager, the DSH Chief Privacy Officer, and the DSH Chief Information Security Officer as soon as practicable, but no later than ten (10) working days, after the discovery of the breach or security incident. The report shall include, but not be limited to, the information specified above, a complete list of impacted individuals, as well as a complete, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or security incident, and measures to be taken to prevent the recurrence or further disclosure of data regarding such breach or security incident.

D. Notification to Individuals: If notification to individuals whose information was breached is required under state or federal law, and regardless of whether Contractor is considered only a custodian and/or non-owner of the DSH PCI, Contractor shall, at its sole expense, and at the sole election of DSH, either:

1. make notification to the individuals affected by the breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal breach notice laws. Contractor shall inform the DSH Chief Privacy Officer, DSH Chief Information Officer, and DSH Contract Manager of the time, manner and content of any such notifications, prior to the transmission of such notifications to the individuals; or

2. cooperate with and assist DSH in its notification (including substitute notification) to the individuals affected by the breach.

E. Submission of Sample Notification to Attorney General: If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29 or 1798.82, and regardless of whether Contractor is considered only a custodian and/or non-owner of the DSH PCI, Contractor shall, at its sole expense, and at the sole election of DSH, either:

1. electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format. content and timeliness provisions of Section 1798.29, subdivision (e), or 1798.82, subdivision (f). Contractor shall inform the DSH Chief Privacy Officer of the time, manner and content of any such submissions, prior to the transmission of such submissions to the Attorney General; or

2. cooperate with and assist DSH in its submission of a sample copy of the notification to the Attorney General.

F. DSH Contact Information: To direct communications to the above referenced DSH staff, the Contractor shall initiate contact as indicated herein. DSH reserves the right to make changes to the contact information below by written notice to the Contractor. Said changes shall not require an amendment to this Exhibit or the agreement to which it is incorporated.

Contract Managers	**DSH Chief Privacy Officer**	**Chief Information Security Officer**
See Exhibit A - Scope of Work for contact information	Chief Privacy Officer Legal Division California Dept. State Hospitals 1215 O Street Sacramento, CA 95814 Email: privacy.officer@dsh.ca.gov Telephone: 916-654-2319	Chief Information Security Officer Information Security Office California Dept. State Hospitals 1215 O Street Sacramento, CA 95814 Email: iso@dsh.ca.gov and security@dsh.ca.gov Telephone: 916-654-4218

XIII. Documentation of Disclosures for Requests for Accounting: Contractor shall document and make available to DSH or (at the direction of DSH) to an Individual such disclosures of DSH PCI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of personal information as required by Civil Code section 1798.25, or any applicable state or federal law.

XIV. Requests for DSH PCI by Third Parties: The Contractor and its employees, agents, or subcontractors shall promptly transmit to the DSH Contract Manager all requests for disclosure of any DSH PCI requested by third parties to the agreement between Contractor and DSH.

XV. Audits, Inspection and Enforcement: DSH may inspect the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit. Contractor shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the DSH Contract Manager in writing.

XVI. Return or Destruction of DSH PCI on Expiration or Termination: Upon expiration or termination of the agreement between Contractor and DSH for any reason, Contractor shall securely return or destroy the DSH PCI. If return or destruction is not feasible, Contractor shall provide a written explanation to the

DSH Program Contract Manager, the DSH Chief Privacy Officer and the DSH Chief Information Security Officer, using the contact information listed in Section XII.F., above.

A. Retention Required by Law: If required by state or federal law, Contractor may retain, after expiration or termination, DSH PCI for the time specified as necessary to comply with the law.

B. Obligations Continue Until Return or Destruction: Contractor's obligations under this Exhibit shall continue until Contractor destroys the DSH PCI or returns the DSH PCI to DSH; provided however, that on expiration or termination of the agreement between Contractor and DSH, Contractor shall not further use or disclose the DSH PCI except as required by state or federal law.

C. Notification of Election to Destroy DSH PCI: If Contractor elects to destroy the DSH PCI, Contractor shall certify in writing within 30 days of the expiration or termination of the agreement to the DSH Contract Manager, the DSH Chief Privacy Officer and the DSH Chief Information Security Officer, using the contact information listed in Section XII.F, above, that the DSH PCI has been securely destroyed. The notice shall include the date and type of destruction method used.

XVII. Amendment: The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolves and that amendment of this Exhibit may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of DSH PCI. The parties agree to promptly enter into negotiations concerning an amendment to this Exhibit consistent with new standards and requirements imposed by applicable laws and regulations.

XVIII. Assistance in Litigation or Administrative Proceedings: Contractor shall make itself and any subcontractors, workforce employees or agents assisting Contractor in the performance of its obligations under the agreement between Contractor and DSH, available to DSH at no cost to DSH to testify as witnesses, in the event of litigation or administrative proceedings being commenced against DSH, its director, officers or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, workforce employee or agent is a named adverse party.

XIX. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Exhibit is intended to confer, nor shall anything herein confer, upon any person other than DSH or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

XX. Interpretation: The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with regulations and applicable Federal and State laws. The parties agree that any ambiguity in the terms and conditions of this Exhibit shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

XXI. Survival: If Contractor does not return or destroy the DSH PCI upon the expiration or termination of the Agreement, the respective rights and obligations of Contractor under Sections VI, VII and XI of this Exhibit shall survive the completion or termination of the agreement between Contractor and DSH.

Attachment 1
Contractor Data Security Standards

1. General Security Controls

A. ***Confidentiality Statement.*** All persons that will be working with DSH PCI must sign a confidentiality statement, within their organization. The statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DSH PCI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DSH inspection for a period of three (3) years following contract termination.

B. ***Background check.*** Before a member of the Contractor's workforce may access DSH PCI, Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

C. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store DSH PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128-bit key or higher. The encryption solution must be full disk unless approved by the DSH Information Security Office.

D. ***Server Security.*** Servers containing unencrypted DSH PCI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

E. ***Minimum Necessary.*** Only the minimum necessary amount of DSH PCI required to perform necessary business functions may be copied, downloaded, or exported.

F. ***Removable/portable electronic devices.*** All electronic files that contain DSH PCI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, CD/DVD, smart devices tapes etc.). PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher

G. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store DSH PCI must install and actively use a comprehensive next generation anti-virus (NGAV) software solution with automatic updates scheduled at least daily. NGAV software must be able to provide real-time

detection and prevention of malware and non-malware attacks, including file based as well as memory-based and file-less attacks. NGAV software must be designed to detect and prevent abnormal behaviors including "zero day" (never before seen malware) attacks and use indicators of compromise to identify abnormalities. Vendor-managed devices operating within DSH networks will utilize DSH-provided endpoint protection software to permit monitoring and isolation of devices which exhibit abnormal behavior.

H. ***Patch Management.*** All workstations, laptops and other systems that process and/or store DSH PCI must have operating system and application security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. Patches rated critical or high, have a common vulnerability scoring system (CVSS) score of 7.0 or greater, or correct exploitable vulnerabilities, must be installed within a maximum 30 days from vendor release.

I. ***User IDs/User Accounts and Password Controls.*** All users must be issued a unique user account for accessing DSH PCI. User accounts must be promptly disabled or deleted upon the transfer or termination of an employee. Passwords are not to be shared. Passwords must be at least eight characters. Password policy requiring a length of fifteen characters or more does not require periodic password changes. Passwords of between eight and fourteen characters must require the password be changed at most every 90 days. Passwords must not be comprised of a single dictionary word. Passwords must not be stored in readable format on any computer or system. Passwords must be changed if compromised or revealed to any party other than the assigned user. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

J. ***Data Sanitization.*** All DSH PCI must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the DSH PCI is no longer needed.

2. System Security Controls

A. ***System Timeout.*** The system must provide an automatic timeout, requiring reauthentication of the user session after no more than 20 minutes of inactivity.

B. ***Warning Banners.*** All systems containing DSH PCI must display a warning banner each time a user attempts access, stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

C. ***System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DSH PCI, or which alters DSH PCI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users This logging must be included for all user privilege levels including, but not limited to, systems administrators. If DSH PCI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

D. ***Access Controls.*** The system must use role-based access controls for all user authentications, enforcing the principle of least privilege.

E. ***Transmission encryption.*** All data transmissions of DSH PCI outside the contractor's secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128-bit key or higher. This requirement pertains to any type of DSH PCI in motion such as website access, file transfer, and E-Mail.

F. ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting DSH PCI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

G. ***Multi-factor Authentication***. All systems involved in accessing, holding, transporting, and protecting DSH PCI that are accessible via the Internet, directly or through remote access solutions, must require multi-factor authentication (MFA)

3. Audit Controls

A. ***System Security Review.*** All systems processing and/or storing DSH PCI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.

B. ***Log Reviews.*** All systems processing and/or storing DSH PCI must have a routine procedure in place to review system logs for unauthorized access.

C. ***Change Control.*** All systems processing and/or storing DSH PCI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity / Disaster Recovery Controls

A. ***Disaster Recovery.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DSH PCI in the event of an

emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.

B. ***Data Backup Plan.*** Contractor must have established documented procedures to securely backup DSH PCI to maintain retrievable exact copies of DSH PCI. The backups shall be encrypted. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore DSH PCI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DSH data.

5. Paper Document Controls

A. ***Supervision of Data.*** DSH PCI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DSH PCI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. ***Escorting Visitors.*** Visitors to areas where DSH PCI is contained shall be escorted and DSH PHI shall be kept out of sight while visitors are in the area.

C. ***Confidential Destruction.*** DSH PCI must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the DSH PSCI is no longer needed.

D. ***Removal of Data.*** DSH PCI must not be removed from the premises of the Contractor except with express written permission of DSH.

E. ***Faxing.*** Faxes containing DSH PCI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.

F. ***Mailing.*** DSH PCI shall only be mailed using secure methods. Large volume mailings of DSH PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a DSH approved solution, such as a solution using a vendor product specified on the CALIFORNIA STRATEGIC SOURCING INITIATIVE.