HIPAA Compliance

Preamble: This section of the Contract is the Business Associate Agreement as required by HIPAA.

1. **Definitions**.

   a. "Business Associate," as used in this Contract, means the "Contractor" and generally has the same meaning as the term "business associate" at 45 CFR 160.103. Any reference to Business Associate in this Contract includes Business Associate's employees, agents, officers, Subcontractors, third party contractors, volunteers, or directors.

   b. "Business Associate Agreement" means this HIPAA Compliance section of the Contract and includes the Business Associate provisions required by the U.S. Department of Health and Human Services, Office for Civil Rights.

   c. "Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, with the exclusions and exceptions listed in 45 CFR 164.402.

   d. "Covered Entity" means DOC, a Covered Entity as defined at 45 CFR 160.103, in its conduct of covered functions by its health care components.

   e. "Designated Record Set" means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or Used in whole or part by or for the Covered Entity to make decisions about Individuals.

   f. "Electronic Protected Health Information (EPHI)" means Protected Health Information that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 CFR 160.103.

   g. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as modified by the American Recovery and Reinvestment Act of 2009 ("ARRA"), Sec. 13400 – 13424, H.R. 1 (2009) (HITECH Act).

   h. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and Part 164.

   i. "Individual(s)" means the person(s) who is the subject of PHI and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

   j. "Minimum Necessary" means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.

k. “Protected Health Information (PHI)” means individually identifiable health information created, received, maintained or transmitted by Business Associate on behalf of a health care component of the Covered Entity that relates to the provision of health care to an Individual; the past, present, or future physical or mental health or condition of an Individual; or the past, present, or future payment for provision of health care to an Individual. 45 CFR 160.103. PHI includes demographic information that identifies the Individual or about which there is reasonable basis to believe can be used to identify the Individual. 45 CFR 160.103. PHI is information transmitted or held in any form or medium and includes EPHI. 45 CFR 160.103. PHI does not include education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USCA 1232g(a)(4)(B)(iv) or employment records held by a Covered Entity in its role as employer.

l. “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

m. “Subcontractor” as used in this HIPAA Compliance section of the Contract (in addition to its definition in the General Terms and Conditions) means a Business Associate that creates, receives, maintains, or transmits Protected Health Information on behalf of another Business Associate.

n. “Use” includes the sharing, employment, application, utilization, examination, or analysis, of PHI within an entity that maintains such information.

2. **Compliance**. Business Associate shall perform all Contract duties, activities and tasks in compliance with HIPAA, the HIPAA Rules, and all attendant regulations as promulgated by the U.S. Department of Health and Human Services, Office of Civil Rights.

3. **Use and Disclosure of PHI**. Business Associate is limited to the following permitted and required uses or disclosures of PHI:

a. Duty to Protect PHI. Business Associate shall protect PHI from, and shall use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to EPHI, to prevent the unauthorized Use or disclosure of PHI other than as provided for in this Contract or as required by law, for as long as the PHI is within its possession and control, even after the termination or expiration of this Contract.

b. Minimum Necessary Standard. Business Associate shall apply the HIPAA Minimum Necessary standard to any Use or disclosure of PHI necessary to achieve the purposes of this Contract. See 45 CFR 164.514 (d)(2) through (d)(5).

c. Disclosure as Part of the Provision of Services. Business Associate shall only Use or disclose PHI as necessary to perform the services specified in this Contract or as required by law, and shall not Use or disclose such PHI in any manner that would violate Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health

Information) if done by Covered Entity, except for the specific uses and disclosures set forth below.

d. Use for Proper Management and Administration. Business Associate may Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

e. Disclosure for Proper Management and Administration. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.

f. Impermissible Use or Disclosure of PHI. Business Associate shall report to DOC in writing all Uses or disclosures of PHI not provided for by this Contract within one (1) business day of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required at 45 CFR 164.410 (Notification by a Business Associate), as well as any Security Incident of which it becomes aware. Upon request by DOC, Business Associate shall mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure.

g. Failure to Cure. If DOC learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate's obligations under the terms of this Contract and reasonable steps by DOC do not end the violation, DOC shall terminate this Contract, if feasible. In addition, If Business Associate learns of a pattern or practice of its Subcontractors that constitutes a violation of the Business Associate's obligations under the terms of their contract and reasonable steps by the Business Associate do not end the violation, Business Associate shall terminate the Subcontract, if feasible.

h. Termination for Cause. Business Associate authorizes immediate termination of this Contract by DOC, if DOC determines that Business Associate has violated a material term of this Business Associate Agreement. DOC may, at its sole option, offer Business Associate an opportunity to cure a violation of this Business Associate Agreement before exercising a termination for cause.

i. Consent to Audit. Business Associate shall give reasonable access to PHI, its internal practices, records, books, documents, electronic data and/or all other business information received from, or created or received by Business Associate on behalf of DOC, to the Secretary of DHHS and/or to DOC for use in determining compliance with HIPAA privacy requirements.

j. Obligations of Business Associate Upon Expiration or Termination. Upon expiration or termination of this Contract for any reason, with respect to PHI received from DOC, or created, maintained, or received by Business Associate, or any Subcontractors, on behalf of DOC, Business Associate shall:

k. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

l. Return to DOC or destroy the remaining PHI that the Business Associate or any Subcontractors still maintain in any form;

m. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to Electronic Protected Health Information to prevent Use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate or any Subcontractors retain the PHI;

n. Not Use or disclose the PHI retained by Business Associate or any Subcontractors other than for the purposes for which such PHI was retained and subject to the same conditions set out in the "Use and Disclosure of PHI" section of this Contract which applied prior to termination; and

o. Return to DOC or destroy the PHI retained by Business Associate, or any Subcontractors, when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

p. Survival. The obligations of the Business Associate under this section shall survive the termination or expiration of this Contract.

4. **Individual Rights**. Accounting of Disclosures.

a. Business Associate shall document all disclosures, except those disclosures that are exempt under 45 CFR 164.528, of PHI and information related to such disclosures.

b. Within ten (10) business days of a request from DOC, Business Associate shall make available to DOC the information in Business Associate's possession that is necessary for DOC to respond in a timely manner to a request for an accounting of disclosures of PHI by the Business Associate. See 45 CFR 164.504(e)(2)(ii)(G) and 164.528(b)(1).

c. At the request of DOC or in response to a request made directly to the Business Associate by an Individual, Business Associate shall respond, in a timely manner and in accordance with HIPAA and the HIPAA Rules, to requests by Individuals for an accounting of disclosures of PHI.

d. Business Associate record keeping procedures shall be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested.

5. **Access.**

a. Business Associate shall make available PHI that it holds that is part of a Designated Record Set when requested by DOC or the Individual as necessary to satisfy DOC's obligations under 45 CFR 164.524 (Access of Individuals to Protected Health Information).

b. When the request is made by the Individual to the Business Associate or if DOC asks the Business Associate to respond to a request, the Business Associate shall comply with requirements in 45 CFR 164.524 (Access of Individuals to Protected Health Information) on form, time and manner of access. When the request is made by DOC, the Business Associate shall provide the records to DOC within ten (10) business days.

6. **Amendment**.

a. If DOC amends, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and DOC has previously provided the PHI or record that is the subject of the amendment to Business Associate, then DOC will inform Business Associate of the amendment pursuant to 45 CFR 164.526(c)(3) (Amendment of Protected Health Information).

b. Business Associate shall make any amendments to PHI in a Designated Record Set as directed by DOC or as necessary to satisfy DOC's obligations under 45 CFR 164.526 (Amendment of Protected Health Information).

7. **Subcontracts and other Third Party Agreements**. In accordance with 45 CFR 164.502(e)(1)(ii), 164.504(e)(1)(i), and 164.308(b)(2), Business Associate shall ensure that any agents, Subcontractors, independent contractors or other third parties that create, receive, maintain, or transmit PHI on Business Associate's behalf, enter into a written contract that contains the same terms, restrictions, requirements, and conditions as the HIPAA compliance provisions in this Contract with respect to such PHI. The same provisions must also be included in any contracts by a Business Associate's Subcontractor with its own business associates as required by 45 CFR 164.314(a)(2)(b) and 164.504(e)(5).

8. **Obligations**. To the extent the Business Associate is to carry out one or more of DOC's obligation(s) under Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information), Business Associate shall comply with all requirements that would apply to DOC in the performance of such obligation(s).

9. **Liability**. Within ten (10) business days, Business Associate must notify DOC of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based

on an allegation of violation of the HIPAA Rules and must inform DOC of the outcome of that action. Business Associate bears all responsibility for any penalties, fines or sanctions imposed against the Business Associate for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.

10. **Breach Notification**.

a. In the event of a Breach of unsecured PHI or disclosure that compromises the privacy or security of PHI obtained from DOC or involving DOC clients, Business Associate will take all measures required by state or federal law.

b. Business Associate will notify DOC within one (1) business day by telephone and in writing of any acquisition, access, Use or disclosure of PHI not allowed by the provisions of this Contract or not authorized by HIPAA Rules or required by law of which it becomes aware which potentially compromises the security or privacy of the Protected Health Information as defined in 45 CFR 164.402 (Definitions).

c. Business Associate will notify the DOC Contact shown on the cover page of this Contract within one (1) business day by telephone or e-mail of any potential Breach of security or privacy of PHI by the Business Associate or its Subcontractors or agents. Business Associate will follow telephone or e-mail notification with a faxed or other written explanation of the Breach, to include the following: date and time of the Breach, date Breach was discovered, location and nature of the PHI, type of Breach, origination and destination of PHI, Business Associate unit and personnel associated with the Breach, detailed description of the Breach, anticipated mitigation steps, and the name, address, telephone number, fax number, and e-mail of the individual who is responsible as the primary point of contact. Business Associate will address communications to the DOC Contact. Business Associate will coordinate and cooperate with DOC to provide a copy of its investigation and other information requested by DOC, including advance copies of any notifications required for DOC review before disseminating and verification of the dates notifications were sent.

d. If DOC determines that Business Associate or its Subcontractor(s) or agent(s) is responsible for a Breach of unsecured PHI:

(1) requiring notification of Individuals under 45 CFR § 164.404 (Notification to Individuals), Business Associate bears the responsibility and costs for notifying the affected Individuals and receiving and responding to those Individuals' questions or requests for additional information;

(2) requiring notification of the media under 45 CFR § 164.406 (Notification to the media), Business Associate bears the responsibility and costs for notifying the media and receiving and responding to media questions or requests for additional information;

(3) requiring notification of the U.S. Department of Health and Human Services Secretary under 45 CFR § 164.408 (Notification to the Secretary), Business

Associate bears the responsibility and costs for notifying the Secretary and receiving and responding to the Secretary's questions or requests for additional information; and;

(4) DOC will take appropriate remedial measures up to termination of this Contract.

11. **Miscellaneous Provisions**.

a. Regulatory References. A reference in this Contract to a section in the HIPAA Rules means the section as in effect or amended.

b. Interpretation. Any ambiguity in this Contract shall be interpreted to permit compliance with the HIPAA Rules.

Exhibit A – Data Security Requirements

1. **Definitions**. The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:

a. “AES” means the Advanced Encryption Standard, a specification of Federal Information Processing Standards Publications for the encryption of electronic data issued by the National Institute of Standards and Technology (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf).

b. “Authorized Users(s)” means an individual or individuals with a business need to access DOC Confidential Information, and who has or have been authorized to do so.

c. “Business Associate Agreement” means an agreement between DOC and a contractor who is receiving Data covered under the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996. The agreement establishes permitted and required uses and disclosures of protected health information (PHI) in accordance with HIPAA requirements and provides obligations for business associates to safeguard the information.

d. “Category 3 Data” is Confidential information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:

1. Personal information as defined in RCW 42.56.590 and RCW 19.255.10.

2. Information about public employees as defined in RCW 42.56.250.

3. Lists of individuals for commercial purposes as defined in RCW 42.56.070

4. Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

e. “Category 4 Data” is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. Data classified as Category 4 includes but is not limited to data protected by: the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 45 CFR Parts 160 and 164; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g; 34 CFR Part 99; Internal Revenue Service Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf); Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2; and/or Criminal Justice Information Services, 28 CFR Part 20.

f. “Cloud” means data storage on servers hosted by an entity other than the Contractor and on a network outside the control of the Contractor. Physical storage of data in the cloud typically spans multiple servers and often multiple locations. Cloud storage can be divided between consumer grade storage for personal files and enterprise grade for companies and governmental entities. Examples of consumer grade storage would include iTunes, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, and Rackspace.

g. “Encrypt” means to encode Confidential Information into a format that can only be read by those possessing a “key”; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.

h. “FedRAMP” means the Federal Risk and Authorization Management Program (see www.fedramp.gov), which is an assessment and authorization process that federal government agencies have been directed to use to ensure security is in place when accessing Cloud computing products and services.

i. “Hardened Password” means a string of at least eight characters containing at least three of the following four character classes: Uppercase alphabetic, lowercase alphabetic, numeral, and special characters such as an asterisk, ampersand, or exclamation point.

j. “Mobile Device” means a computing device, typically smaller than a notebook, which runs a mobile operating system, such as iOS, Android, or Windows Phone. Mobile Devices include smart phones, most tablets, and other form factors.

k. “Multi-factor Authentication” means controlling access to computers and other IT resources by requiring two or more pieces of evidence that the user is who they claim to be. These pieces of evidence consist of something the user knows, such as a password or PIN; something the user has such as a key card, smart card, or physical token; and something the user is, a biometric identifier such as a fingerprint, facial scan, or retinal scan. “PIN” means a personal identification number, a series of numbers which act as a password for a device. Since PINs are typically only four to six characters, PINs are usually used in conjunction with another factor of authentication, such as a fingerprint.

l. “Portable Device” means any computing device with a small form factor, designed to be transported from place to place. Portable devices are primarily battery powered devices with base computing resources in the form of a processor, memory, storage, and network access. Examples include, but are not limited to, mobile phones, tablets, and laptops. Mobile Device is a subset of Portable Device.

m. “Portable Media” means any machine readable media that may routinely be stored or moved independently of computing devices. Examples include magnetic tapes, optical discs (CDs or DVDs), flash memory (thumb drive) devices, external hard drives, and internal hard drives that have been removed from a computing device.

n. “Secure Area” means an area to which only authorized representatives of the entity possessing the Confidential Information have access, and access is controlled through use of a key, card key, combination lock, or comparable mechanism. Secure Areas may include buildings, rooms or locked storage containers (such as a filing cabinet or desk drawer) within a room, as long as access to the Confidential Information is not available to unauthorized personnel. In otherwise Secure Areas, such as an office with restricted access, the Data must be secured in such a way as to prevent access by non-authorized staff such as janitorial or facility security staff, when authorized Contractor staff are not present to ensure that non-authorized staff cannot access it.

o. “Trusted Network” means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DOC Data on that network. Controls would include a firewall between any other networks, access control lists on networking devices such as routers and switches, and other such mechanisms which protect the confidentiality, integrity, and availability of the Data.

p. “Unique User ID” means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.

q. "Biometric identifier" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's retina or iris scan, fingerprint, voiceprint, DNA, or scan of hand or face geometry, except when such information is derived from:

(i) Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color;

(ii) Donated organ tissues or parts, or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency;

(iii) Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996; or

(iv) X-ray, roentgen process, computed tomography, magnetic resonance imaging (MRI), positron emission tomography (PET) scan, mammography, or other image or film of the human anatomy used to diagnose, develop a prognosis for, or treat an illness or other medical condition or to further validate scientific testing or screening.

2. **Authority**. The security requirements described in this document reflect the applicable requirements of Standard SEC-08 (formerly 141.10) (https://ocio.wa.gov/policies) of the Office of the Chief Information Officer for the state of Washington, WA DOC Policy 280.310 – Information Technology Security; WA DOC Policy 280.515 – Data Classification and Sharing; the terms and conditions set forth in this Agreement; and all applicable state and federal laws in its treatment of WA DOC Data

3. **Administrative Controls.** The Contractor must have the following controls in place:

a. A documented security policy governing the secure use of its computer network and systems, and which defines sanctions that may be applied to Contractor staff for violating that policy.

b. Any data center security controls must meet or exceed those expected by the Federal Information Security Management Act (FISMA) for low to moderate impact systems as described in FIPS 199 and 200, and in the most current release of National Institute of Standards and Technology (NIST) Special Publications SP800-53, including all other referenced NIST publications.

c. Contractor warrants that all data collected, processed, routed, and/or stored by or through the service, or third-party service providers, remains at all times within the United States.

d. If the Data shared under this agreement is classified as Category 4, the Contractor must be aware of and compliant with the applicable legal or regulatory requirements for that Category 4 Data.

e. If Confidential Information shared under this agreement is classified as Category 4, the Contractor must have a documented risk assessment for the system(s) housing the Category 4 Data.

4. **Authorization, Authentication, and Access.** In order to ensure that access to the Data is limited to authorized staff, the Contractor must:

a. Have documented policies and procedures governing access to systems with the shared Data.

b. Restrict access through administrative, physical, and technical controls to authorized staff.

c. Ensure that user accounts are unique and that any given user account logon ID and password combination is known only to the one employee to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which employee performed a given action on a system housing the Data based solely on the logon ID used to perform the action.

d. Ensure that only authorized users are capable of accessing the Data.

e. Ensure that an employee's access to the Data is removed immediately:

(1) Upon suspected compromise of the user credentials.

(2) When their employment, or the contract under which the Data is made available to them, is terminated.

(3) When they no longer need access to the Data to fulfill the requirements of the contract.

f. Have a process to periodically review and verify that only authorized users have access to systems containing DOC Confidential Information.

g. When accessing the Data from within the Contractor’s network (the Data stays within the Contractor’s network at all times), enforce password and logon requirements for users within the Contractor’s network, including:

(1) A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.

(2) That a password does not contain a user’s name, logon ID, or any form of their full name.

(3) That a password does not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.

(4) That passwords are significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.

h. When accessing Confidential Information from an external location (the Data will traverse the Internet or otherwise travel outside the Contractor’s network), mitigate risk and enforce password and logon requirements for users by employing measures including:

(1) Ensuring mitigations applied to the system don’t allow end-user modification.

(2) Not allowing the use of dial-up connections.

(3) Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.

(4) Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network networks (using key lengths of 128 bits or greater) Algorithm modules validated by the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) are required. The traffic must be encrypted at all times while traversing any network, including the Internet, which is not a Trusted Network.

(5) Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 20 minutes of inactivity.

(6) Ensuring use of Multi-factor Authentication to connect from the external end point to the internal end point. Authentication mechanisms must meet or exceed those described in the most recent version of NIST SP 800-63 for information requiring assurance level 3 or higher. One of the authentication factors should be provided by a device separate from the computer gaining access.

(7) Ensuring all system and service accounts use Enterprise Active Directory or a similar centralized authentication and authorization mechanism. If authentication methods such as SQL authentication are required by the system, Contractor uses credentials secured during transmission through encrypted sessions such

as TLS1.2 (or greater) or IPSec, and in storage using a secure hash method validated by the National Institute of Standards and Technology (NIST). Within 72 hours of a request from DOC, Contractor must provide documentation showing how the credentials are secured during all transmissions using encrypted sessions such as TLS or IPSec, and in storage using a secure hash method validated by the National Institute of Standards and Technology (NIST).

i. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition, iris scan) or token (software, hardware, smart card, etc.) in that case:

(1) The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor

(2) Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)

(3) Must not contain a “run” of three or more consecutive numbers (12398, 98743 would not be acceptable)

j. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:

(1) Be a minimum of six alphanumeric characters.

(2) Contain at least three unique character classes (upper case, lower case, letter, number).

(3) Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.

k. Render the device unusable after a maximum of 10 failed logon attempts.

l. Ensure the system/service supports single sign-on for state government employees, and external users by integrating the system's authentication mechanisms with the Washington State Enterprise Active Directory and Secure Authentication Gateways (post listeners are typically used for processing the gateway host headers).

m. Utilize application authentication controls that are consistent with those described in the most recent version of NIST SP 800-63 for information requiring assurance level 2 or higher.

5. **Protection of Data**. The Contractor agrees to store Data on one or more of the following media and protect the Data as described:

a. **Hard disk drives**. For Data stored on local workstation hard disks, access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

b. **Network server disks**. For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

   For DOC Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

c. **Optical discs (CDs or DVDs) in local workstation optical disc drives**. Data provided by DOC on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the contracted purpose, such discs must be Stored in a Secure Area. Workstations which access DOC Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers**. Data provided by DOC on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

e. **Paper documents**. Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a Secure Area.

f. **Remote Access**. Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DOC staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor's staff. Contractor will notify DOC staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.

g. **Data storage on portable devices or media**.

(1) Except where otherwise specified herein, DOC Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:

(a) Encrypt the Data.

(b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.

(c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

(d) Apply administrative and physical security controls to Portable Devices and Portable Media by:

i. Keeping them in a Secure Area when not in use,

ii. Using check-in/check-out procedures when they are shared, and

iii. Taking frequent inventories.

(2) When being transported outside of a Secure Area, Portable Devices and Portable Media with DOC Confidential Information must be under the physical control of Contractor staff with authorization to access the Data, even if the Data is encrypted.

h. **Data stored for backup purposes**.

(1) DOC Confidential Information may be stored on Portable Media as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DOC Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.

(2) Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DOC Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.

i. **Cloud storage**. DOC Confidential Information requires protections equal to or greater than those specified elsewhere within this exhibit. Cloud storage of Data is problematic as neither DOC nor the Contractor has control of the environment in which the Data is stored. For this reason:

(1) DOC Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:

(a) Contractor has written procedures in place governing use of the Cloud storage and Contractor attests in writing that all such procedures will be uniformly followed.

(b) The Data will be Encrypted while within the Contractor network.

(c) The Data will remain Encrypted during transmission to the Cloud.

(d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.

(e) The Contractor will possess a decryption key for the Data, and the decryption key will be possessed only by the Contractor and/or DOC.

(f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DOC or Contractor networks.

(g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DOC or Contractor's network.

(2) Data will not be stored on an Enterprise Cloud storage solution unless either:

(a) The Cloud storage provider is treated as any other Sub-Contractor, and agrees in writing to all of the requirements within this exhibit; or,

(b) The Cloud storage solution used is FedRAMP certified.

(3) If the Data includes protected health information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Cloud provider must sign a Business Associate Agreement prior to Data being stored in their Cloud solution.

6. **System Protection**. To prevent compromise of systems which contain DOC Data or through which that Data passes:

a. Systems containing DOC Data must have all security patches or hotfixes applied within 3 months of being made available.

b. The Contractor will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.

c. Systems containing DOC Data shall have an Anti-Malware application, if available, installed.

d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current. These anti-malware practices must meet or exceed those described in NIST SP800-40.

e. The architecture must provide continuous monitoring of both internal and external activity for anomalies and identify, report, and defend against security intrusions before data is compromised.

f. Contractor shall conduct penetration tests at least once every 24 months, system vulnerability assessments at least monthly, and application vulnerability assessments prior to the production release of any changes to source code.

g. Contractor has implemented application/system development practices consistent with the current version of NIST SP800-64 for low to moderate impact systems, and warrants the software does not contain any of the Open Web Application Security project (OWASP) top 10 vulnerabilities - https://www.owasp.org/index.php/Main_Page

h. Contractor has a practice of systematic collection, monitoring, alerting, maintenance, retention, and disposal of security event logs and application audit trails. Logs and audit trails are written to an area inaccessible to system users and are protected from editing. At a minimum the logs and audit trails will provide historical details on all transactions within the system that are necessary to reconstruct activities. Including recording; type of event, date, time, account identification and machine identifiers for each logged transaction. Audit and log files can be analyzed by type in order to find emerging issues or trends. Contractor has settings triggering an immediate notification to appropriate system administrators for severe incidents. Logs are secured against unauthorized changes. At a minimum, logs must be retained for a period of 6 months.

7. Data Segregation.

a. DOC Data must be segregated or otherwise distinguishable from non-DOC data. This is to ensure that when no longer needed by the Contractor, all DOC Data can be identified for return or destruction. It also aids in determining whether DOC Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.

(1) DOC Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DOC Data. And/or,

(2) DOC Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DOC Data. And/or,

(3) DOC Data will be stored in a database which will contain no non-DOC data. And/or,

(4) DOC Data will be stored within a database and will be distinguishable from non-DOC data by the value of a specific field or fields within database records.

(5) When stored as physical paper documents, DOC Data will be physically segregated from non-DOC data in a drawer, folder, or other container.

b. When it is not feasible or practical to segregate DOC Data from non-DOC data, then both the DOC Data and the non-DOC data with which it is commingled must be protected as described in this exhibit.

8. **Data Disposition**. When the contracted work has been completed or when the Data is no longer needed, except as noted above in Section 5.b, Data shall be returned to DOC or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding
Cloud Storage (e.g. Azure, AWS, GCP)	Using a Crypto shredding utility

9. **Notification of Compromise or Potential Compromise**. Contractor shall implement incident response practices consistent with NIST SP 800-61. The actual compromise of DOC Data must be reported to the DOC Contact designated in the Contract within three (3) business days of discovery. If no DOC Contact is designated in the Contract, then the notification must be reported to the DOC Contracts and Legal Affairs office at docclacontracts@doc1.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DOC.

10. **Data shared with Subcontractors**. If DOC Data provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract. If the Contractor cannot protect the Data as articulated within this Contract, then the contract with the sub-Contractor must be submitted to the DOC Contact specified for this contract for review and approval.

11. **System Audit Requirements**. Contractor has completed a recent independent security audit by a SOC 2 Type 2 accredited firm of their development and operational practices, or that an independent security audit by an accredited firm will be completed within 6 months after contract execution. This audit must include vulnerability assessments, and penetration tests, and confirm compliance with the security requirements herein. The audit should include any specific data center facility where the service is deployed, and all failover facilities unless those facilities provide their own SOC 2 Type 2 audit.

12. **Disaster Recovery**. Contractor shall document, test and maintain a disaster recovery plan including an alternate facility to assure the system/service is recovered within 24 hours of a force majeure event. The recovery plan must protect against more than 24 hours of DOC data being lost.

13. **Records Maintenance**. The parties to this Agreement shall each maintain books, records, documents, and other evidence which sufficiently and properly reflect all direct and indirect costs expended by either party in the performance of the services described herein, if any. These records shall be subject to inspection, review, or audit by personnel of both parties, other personnel duly authorized by either party, the Office of the State Auditor, and federal officials so authorized by law. All books, records, documents, and other material relevant to this Agreement will be retained for six (6) years after expiration and the Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access and the right to examine any of these materials during this period.

14. **Rights in Data**. Unless otherwise provided in a Research Agreement, this Agreement will not be construed to effect any transfer of right or license to the embodiments of the Washington DOC's Data, except to the limited extent necessary to carry out the responsibilities specified herein. Commercialization of DOC Category 3 or Category 4 data, or sharing of DOC data with third parties without the written permission of DOC is strictly prohibited under these terms.

15. **Insurance Requirements.** If this agreement involves the Contractor collecting, storing, creating, altering, processing, transmitting, routing, or handling any DOC Category 3 or Category 4 data, then Contractor shall obtain and maintain for the duration of the Contract, at Contractor's expense, the following insurance coverages which the parties agree are unaffected by any limitation of liability language within this Agreement.

    a. **Technology Professional Liability (errors and omissions)**

    The Contractor shall maintain Technology Professional Liability (errors and omissions) insurance, to include coverage of claims involving infringement of intellectual property. This shall include but is not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion, network security, regulatory defense (including fines and penalties), and notification costs. The coverage limits must be at least $1,000,000 per covered claim without sublimit, and $2,000,000 annual aggregate.

    b. **Crime and Employee Dishonesty**

The Contractor shall maintain Employee Dishonesty and (when applicable) Inside/Outside Money and Securities coverages for property owned by the State of Washington in the care, custody, and control of Contractor, to include electronic theft and fraud protection. The coverage limits must be at least $1,000,000 per covered claim without sublimit, $2,000,000 annual aggregate.

c. **Cyber Risk Liability Insurance**

The Contractor shall maintain coverage for Cyber Risk Liability, including information theft, computer and data loss replacement or restoration, release of private information, alteration of electronic information, notification costs, credit monitoring, forensic investigation, cyber extortion, crises management, public relations expenses, regulatory defense (including fines and penalties), network security, and liability to third parties from failure(s) of contractor to handle, manage, store, and control personally identifiable information belonging to others. The policy must include full prior acts coverage. The coverage limits must be at least $1,000,000 per covered claim without sublimit, $2,000,000 annual aggregate.