MODEL DATA SHARING AGREEMENT

DATA SHARING AGREEMENT
BETWEEN
STATE OF WASHINGTON AGENCY A
AND
AGENCY B

This Agreement is entered into by and between AGENCY A, hereinafter referred to as "AA" and AGENCY B or "BB".

Agency Contacts: AGENCY A

Agreement Administrator: Technical Administrator:

Name: ____________________________
Title: ____________________________
Division: _________________________
Address: _________________________
Phone: __________________________
Email: __________________________

Agency Contacts: AGENCY B

Agreement Administrator: Technical Administrator:

Name: ____________________________
Title: ____________________________
Division: _________________________
Address: _________________________
Phone: __________________________
Email: __________________________

IN CONSIDERATION of the mutual promises made to each other, as hereinafter set forth, AA and BB agree as follows:

1. PURPOSE: The purpose of this Data Sharing Agreement is to establish the terms and conditions under which AA agrees to transfer to BB (take from data request form) and to grant BB use of such data.

2. DEFINITIONS: As used throughout this Agreement, the following terms shall have the meanings set forth below:

   2.1 "AA" shall mean the AGENCY A, any division, section, office, unit, or other entity of AA, or any of the officers, other officials, employees, volunteers, or others acting as representatives lawfully representing AA.

   2.2 "Agreement" means this Data Sharing Agreement, including all documents attached or incorporated by reference.

   2.3 "Data" shall include any computer readable data provided by AA, whether that data originated in AA or in another entity.

   2.4 Data Classification Categories used in this Agreement are defined as follows:

   2.4.1 Category 1 Data – Public Information – information that can be or currently is released to the public and cannot be defined as confidential or restricted. Category 1 data does not require authorization to be released but does need integrity and availability protection controls.
2.4.2 Category 2 Data – Sensitive Information – information that may not be specifically protected from disclosure by law and is for official use only. Category 2 data is generally not released to the public unless specifically request but does not require authorization to be released for official agency business.

2.4.3 Category 3 Data – Confidential Information – information that is specifically protected from disclosure by law. Category 3 data requires an approved data sharing agreement for release. It may include but is not limited to:

- Personal information about individuals, regardless of how that information is obtained.
- Information concerning employee personnel records.
- Information regarding IT infrastructure and security of computer and telecommunications systems.

2.4.4 Category 4 Data – Confidential Information Requiring Special Handling – information that is specifically protected from disclosure by law and for which:

- Especially strict handling requirements are dictated, such as by statutes, regulations or agreements.
- Serious consequence could arise from unauthorized disclosure, such as threats to health and safety or legal sanctions.

2.5 “Data Encryption” refers to ciphers, algorithms or other encoding mechanisms that will encode data to protect its confidentiality. Data encryption can be required during the data transmission or data storage depending on the level of protection required for this data.

2.6 “Data Storage” refers to the state data is in when at rest. Data shall be stored on secured environments.

2.7 “Data Transmission” refers to the methods and technologies to be used to move a copy of the data between systems, networks, and/or workstations.

2.8 “Disclosure” means to permit access to or release, transfer, or other communication of personally identifiable information contained in criminal justice records by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record.

2.9 “Information” shall mean material provided by AA in any format, including reports.

2.10 “Personally Identifiable Information” means information that can be used to distinguish or trace an individual’s identity, such as their name, Social Security Number, state identification number, biometric records, etc. along or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. Personally Identifiable Information also includes other information that, alone or in combination, would allow a reasonable person in the community, who does not have personal knowledge of the relevant circumstance, to identify the person with reasonable certainty.

3. BASIC TRANSACTION: The Agreement sets forth the responsibilities of the parties and the terms and conditions under which the data will be provided.

3.1 Responsibilities of Agency A: AA shall:

3.1.1 Provide BB with: (take from Data Request Form).

3.1.2 Provide BB with access to a FTP server containing the data files.

3.2 Responsibilities of Agency B: BB shall:

3.2.1 Comply with the provisions of this Agreement and all of the terms and conditions contained herein or attached hereto.
3.2.2 Establish written procedures which shall describe the process BB uses to meet the terms and conditions of this section of the Agreement.

3.2.3 Recognize and hereby acknowledge that the user identifiers and passwords, if any, supplied by AA to BB are the confidential property of AA, subject to the proprietary rights of AA, and BB agrees to hold such user identifiers and passwords, if any, in the strictest confidence. BB further agrees to exercise at all times the same care with respect to the user identifiers and passwords, if any, or any other materials or information provided hereunder by AA as BB would exercise in the protection of BB's own confidential information or property and to not release or disclose it to any other party except with the written consent of AA.

3.2.4 Explain the provisions that will be taken to securely protect any information and data that is confidential (e.g. physical locks, computer passwords and/or encryption).

4. TERM AND EFFECTIVE DATE OF AGREEMENT:

4.1 This Agreement becomes effective on the date of the last party’s signature.

4.2 The initial term of this Agreement is from the date of its execution by AA through December 31 of the current year, unless sooner terminated as provided herein.

4.3 This Agreement automatically extends for successive one year periods unless either of the parties notifies the other in writing, electronic mail being sufficient, at least 30 days prior to the automatic renewal date that they wish to terminate the Agreement.

4.4 The Agreement may be terminated in accordance with the provisions of Subsection 23.14.

5. COSTS: There are no costs associated with this Agreement and data transfer.

6. DATA TRANSMISSION: To ensure data is encrypted during data transmission, all data transfer to/from BB shall be transmitted using the Consolidated Technology Services FTP Service with login and hardened password security. AA shall create an account for BB if an account does not already exist.

7. DATA SECURITY: All data provided by AA shall be stored on a secure environment with access limited to the least number of staff needed to complete the purpose of this Agreement.

7.1 Protection of Data

7.1.1 Workstation Hard disk drives. Data stored on local workstation hard disks. Access to the data will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. If the workstation is located in an unsecured physical location the hard drive must be encrypted to protect AA data in the event the device is stolen.

7.1.2 Network server disks. 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 complex 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. Backup copies for DR purposes must be encrypted if recorded to removable media.

7.1.3 Optical discs (e.g. CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Data provided by AA 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 Agreement purpose, such discs must be locked in a drawer, cabinet or other container to which only
authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access AA data on optical discs must be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

7.1.4 Optical discs (e.g. CDs, DVDs, Blu-Rays) in drives or jukeboxes attached to servers. Data provided by AA 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 complex 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 individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

7.1.5 Paper documents. Any paper records must be protected by storing the records in a secure area which is only accessible to authorized individuals. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

7.1.6 Access via remote terminal/workstation over the State Governmental Network (SGN). Data accessed and used interactively over the SGN. Access to the data will be controlled by AA staff who will issue authentication credentials (e.g. a unique user ID and complex password) to authorized individuals. BB will notify the AA Agreement Administrator immediately whenever an authorized person in possession of such credentials is terminated or otherwise leaves, and whenever a user’s duties change such that the user no longer requires access to perform work for this Agreement.

7.1.7 Access via remote terminal/workstation over the Public Internet only through Secure Access Washington. Data accessed and used interactively over the SGN. Access to the data will be controlled by AA staff who will issue authentication credentials (e.g. a unique user ID and complex password) to authorized individuals. BB will notify the AA Agreement Administrator immediately whenever an authorized person in possession of such credentials is terminated or otherwise leaves, and whenever a user’s duties change such that the user no longer requires access to perform work for this Agreement.

7.1.8 Data storage on portable devices or media.
   a) Category 3 and 4 data from AA shall not be stored by BB on portable devices or media unless specifically authorized within this Agreement. If so authorized, the data shall be given the following protections:
      i. Encrypt the data with a key length of at least 128 bits
      ii. Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.
      iii. 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.
      iv. Physically protect the portable device(s) and/or media by:
         • Keeping them in locked storage when not in use;
         • Using check-in/check-out procedures when they are shared; and
         • Taking frequent inventories.
   b) When being transported outside of a secure area, portable devices and media with confidential AA data must be under the physical control of BB staff with authorization to access the data.
   c) Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and
laptop/notebook computers.

d) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs, Blu-Rays),
magnetic media (e.g. floppy disks, tape, Zip or Jaz disks), or flash media (e.g. CompactFlash, SD, MMC).

7.2 Safeguards Against Unauthorized Access and Re-disclosure: BB shall exercise due care to
protect all Personally Identifiable data from unauthorized physical and electronic access. Both
parties shall establish and implement the following minimum physical, electronic and managerial
safeguards for maintaining the confidentiality of information provided by either party pursuant to this
Agreement:

7.2.1 Access to the information provided by AA will be restricted to only those authorized staff,
officials, and agents of the parties who need it to perform their official duties in the
performance of the work requiring access to the information as detailed in the Purpose of this
Agreement.

7.2.2 BB will store the information in an area that is safe from access by unauthorized persons
during duty hours as well as non-duty hours or when not in use.

7.2.3 Unless specifically authorized in this Agreement, BB will not store any confidential or sensitive
AA data on portable electronic devices or media, including, but not limited to laptops,
handhelds/PDAs, Ultramobile PCs, flash memory devices, floppy discs, optical discs
(CDs/DVDs), and portable hard disks.

7.2.4 BB will protect the information in a manner that prevents unauthorized persons from retrieving
the information by means of computer, remote terminal or other means.

7.2.5 BB shall take precautions to ensure that only authorized personnel and agents are given
access to on-line files.

7.2.6 BB shall instruct all individuals with access to the Personally Identifiable Information regarding
the confidential nature of the information, the requirements of Use of Data and Safeguards
Against Unauthorized Access and Re-Disclosure clauses of this Agreement, and the sanctions
specified in federal and state laws against unauthorized disclosure of information covered by
this Agreement.

7.2.7 BB shall take due care and take reasonable precautions to protect AA’s data from
unauthorized physical and electronic access. Both parties will strive to meet or exceed the
requirements of the State of Washington’s policies and standards for data security and access
controls to ensure the confidentiality, availability, and integrity of all data accessed.

8. DATA CONFIDENTIALITY: BB acknowledges the personal or confidential nature of the information and
agrees that their staff and contractors with access shall comply with all laws, regulations, and policies that
apply to protection of the confidentiality of the data. If data provided under this Agreement is to be shared
with a subcontractor, the contract with the subcontractor must include all of the data security provisions
within this Agreement and within any amendments, attachments, or exhibits within this Agreement. If the
Contractor cannot protect the data as articulated within this Agreement, then the Contract with the
subcontractor must be submitted to the AA Agreement Administrator specified for this Agreement for review
and approval.

8.1 Non-Disclosure of Data

8.1.1 Individuals will access data gained by reason of this Agreement only for the purpose of this
Agreement. Each individual (staff and their contractors) with data access shall read and sign
Exhibit A, Statement of Confidentiality and Non-Disclosure, prior to access to the data.
Copies of the signed forms shall be sent to the AA Agreement Administrator identified on
Page 1 of this Agreement, who will distribute them to the other educational agencies as
appropriate.

8.1.2 AA may at its discretion disqualify at any time any person authorized access to confidential
information by or pursuant to this Agreement. Notice of disqualification shall be in writing
and shall terminate a disqualified person’s access to any information provided by AA pursuant to this Agreement immediately upon delivery of notice to BB. Disqualification of one or more persons by AA does not affect other persons authorized by or pursuant to this Agreement.

8.2 Penalties for Unauthorized Disclosure of Information. In the event BB fails to comply with any terms of this Agreement, AA shall have the right to take such action as it deems appropriate. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

9. USE OF DATA

9.1 Data provided by AA will remain the property of AA and will be returned to AA or destroyed when the work for which the information was required has been completed.

9.2 This Agreement does not constitute a release of the data for BB’s discretionary use, but may be accessed only to carry out the responsibilities specified herein. Any ad hoc analyses or other use of the data, not specified in this Agreement, is not permitted without the prior written agreement of AA. BB shall not disclose, transfer, or sell any such information to any party, except as provided by law. BB shall maintain the confidentiality of all Personally Identifiable Information and other information gained by reason of this Agreement.

9.3 BB is not authorized to update or change any AA data and then cite as AA data. Any updates or changes without appropriate citation shall be cause for immediate termination of this Agreement.

9.4 BB is allowed to combine AA data with other agency data in order to complete the responsibilities and research specified in this Agreement. BB shall cite that this ‘hybrid’ dataset is a combination of data from multiple sources and cite those sources.

9.5 Neither Washington State nor AA guarantees the accuracy of the data provided. All risk and liabilities of use and misuse of information provided pursuant to this Agreement are understood and assumed by BB.

9.6 Data provided by AA cannot be re-disclosed or duplicated unless specifically authorized in this Agreement.

9.7 Publicly-reported aggregated results will not contain any group of fewer than # individuals, and percent ranges should be used, where the greater the uncertainty (smaller number of observations) the greater width of the reporting range.

9.8 BB shall include the following excerpts with any public release using AA data:

“The research presented here utilizes confidential data from AA. The views expressed here are those of the author(s) and do not necessarily represent those of the AA or other data contributors. Any errors are attributable to the author(s).”

9.9 Provide draft report to AA and data contributors at least ten (10) working days prior to any public release of reports and communicate with AA or data contributors when questions arise regarding data provided.

9.10 The requirements in this section shall survive the termination or expiration of this agreement or any subsequent agreement intended to supersede this DSA.

9.11 BB shall not:

9.11.1 Disclose any of the information or data in a form which is identifiable to an individual in any project report or in any other manner whatsoever;

9.11.2 Make copies of any of the information or data provided other than what is necessary for research, evaluative, or statistical purposes.

9.12 To the extent that the information and data being accessed are covered by other laws, statutes, court rules, and administrative rules and regulations which restrict access to and use of such
information and data, the restrictions contained in such laws, statutes, court rules, and administrative rules and regulations shall apply to the information and data accessed under this Agreement.

9.13 Any exceptions, revisions, or waivers to these limitations requested by BB must be approved in writing by AA and received by BB prior to the requested use or dissemination of the information and data received under this Agreement.

10. DISPOSITION OF DATA

10.1 Upon termination of the agreement, BB shall dispose of the Category 2, 3 or 4 data received and provide written notification of disposal (See Exhibit B). Failure to do so may prevent data sharing agreements with the organization in the future.

10.2 Upon the destruction of AA data, BB shall complete Exhibit B Certification of Data Disposition, and submit it to the AA Agreement Administrator within fifteen (15) days of the date of disposal.

10.3 Acceptable destruction methods for various types of media include:

10.3.1 For paper documents containing confidential or sensitive information, a contract with a recycling firm to recycle confidential documents is acceptable, provided the contract ensures that the confidentiality of the data will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.

10.3.2 For paper documents containing Confidential Information requiring special handling, recycling is not an option. These documents must be destroyed by on-site shredding, pulping, or incineration.

10.3.3 If confidential or sensitive information has been contained on optical discs (e.g. CDs, DVDs, Blu-ray), the data recipient shall either destroy by incineration the disc(s), shredding the discs, or completely deface the readable surface with a coarse abrasive.

10.3.4 If confidential or sensitive information has been stored on magnetic tape(s), the data recipient shall destroy the data by degaussing, incinerating or crosscut shredding.

10.3.5 If data has been stored on server or workstation data hard drives or similar media, the data recipient shall destroy the data by using a “wipe” utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).

10.3.6 If data has been stored on removable media (e.g. floppies, USB flash drives, portable hard disks, or similar disks), the data recipient shall destroy the data by using a “wipe” utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).

Use 10.3.1 through 10.3.6 -- OR -- 10.3.7

10.3.7 Unless otherwise specified in the contract, BB agrees that upon termination of this Agreement it shall erase, destroy and render unrecoverable all AA data and certify in writing that these actions have been completed within 30 days of the termination of this Agreement or within 7 days of the request of an agent of AA, whichever shall come first. At a minimum, media sanitization is to be performed according to the standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization SP 800-88, Appendix A – http://csrc.nist.gov/publications/PubsSPs.html#SP-800-88 (see attached).

11. ON-SITE OVERSIGHT AND RECORDS MAINTENANCE: BB agrees that AA shall have the right, at any time, to monitor, audit and review activities and methods in implementing the Agreement in order to assure compliance therewith, within the limits of BB’s technical capabilities.

Both parties hereto shall retain all records, books, or documents related to this Agreement for six years, except data destroyed in Section 10. The Office of the State Auditor, federal auditors, and any persons duly
authorized by the parties shall have full access to and the right to examine any of these materials during this period.

12. AMENDMENTS AND ALTERATIONS TO THIS AGREEMENT: With mutual consent, AA and BB may amend this Agreement at any time, provided that the amendment is in writing and signed by authorized staff.

13. ORDER OF PRECEDENCE: In the event of an inconsistency in this Contract, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

13.1 Applicable Federal and State laws;
13.2 Any other provisions of the Contract whether by reference or otherwise.

14. COOPERATION WITH AA AND PROSECUTORIAL AUTHORITIES:

14.1 BB agrees to cooperate with the AA and other authorities authorized by law in any audit that is conducted of BB.

14.2 BB agrees to cooperate fully with prosecutorial authorities in any action brought against BB relating to the reproduction, distribution, dissemination, or other use of the information and data provided by the AA under this Agreement. PROVIDED, that nothing in this provision limits or abridges BB's constitutional rights against self-incrimination.

14.3 Failure to cooperate with prosecutorial authorities may result in the immediate termination, without notice, of this Agreement.

15. CONTRACT COMPLIANCE MONITORING AND AUDITING: BB agrees that the AA may include "control" or "salted" data as a portion of the provided information as a means to ensure that any personally-identifiable information is not used for commercial solicitation purposes or in an indiscriminate and reckless manner. Furthermore BB agrees to allow the AA to perform audits, at its discretion, to detect the unauthorized removal of control data or the warehousing of stale-dated information subsequently expunged, restricted, or amended by the AA.

16. COMPLIANCE WITH AUTHORITIES:

16.1 During the term of this Agreement, BB shall comply with all current, or as subsequently amended state and federal laws, court rules, administrative regulations and policies governing, regulating, and/or relating to the dissemination of information and data, to privacy, and to the confidentiality of the information and data provided by the AA under this Agreement.

16.2 In the event of BB's noncompliance or refusal to comply with any such state and federal laws, court rules, administrative regulations and policies, this Agreement may be rescinded, canceled or terminated in whole or in part, and BB may be declared ineligible for further agreements with the AA.

17. RIGHTS AND INTEREST: BB shall not gain any proprietary right to or interest in any information and data provided by AA as a result of this Agreement. Any rights or interest, or any portion thereof, derived by BB under this Agreement are personal to it and may not be transferred, assigned, or sold for any purpose whatsoever to any person, corporation, partnership, association, or organization of any kind.

18. CHANGES RELATING TO DATA: AA specifically reserves the right, at its sole discretion, to make any changes it deems appropriate relating to the information and data provided under this Agreement at any time and without prior notice. Such changes include, but are not limited to: altering the character and format of the information and data, changing the production media, and/or modifying the production schedule. If such changes are made, AA will notify BB as soon as is practical.

19. SUPPORT/ASSISTANCE: BB acknowledges and accepts that all data provided under this Agreement is provided on an AS IS basis and that AA shall not be responsible for providing support or assistance of any nature to BB on behalf of BB.
20. DISCLAIMER OF WARRANTIES:

20.1 AA provides no warranties, express or implied, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose, with respect to information or data provided under this agreement.

20.2 AA provides no warranties, express or implied, that the information or data provided is accurate, current, correct, or complete. It is expressly understood by the parties that it is the responsibility of the BB to verify information or data obtained under this agreement.

21. LIMITATION OF LIABILITY: BB acknowledges and accepts that all information and data provided under this agreement is provided on an as-is basis and that the information and data may be subject to error or omission and therefore agrees that AA shall not be responsible nor liable in any way whatsoever for the validity of any data provided or for the use of the information and data provided. specifically:

21.1 AA shall not be liable for any demand or claim, regardless of form of action, for any damages resulting from the use by the BB of any information or data provided under this agreement.

21.2 AA shall not be liable for any demand or claim, regardless of form of action, for any damages arising from incorrect or incomplete information or data provided under this agreement.

21.3 AA shall not be liable to BB or any other party for any loss, including revenue, profits, time, goodwill, computer time, destruction, damage or loss of data, or any other indirect, special, or consequential damage which may arise from the use, operation, or modification of data provided under this agreement.

22. INDEMNIFICATION: BB hereby agrees to defend, indemnify, and hold harmless AA, its employees, and the State of Washington from all loss, risk of loss, and damages (including expenses, costs, and attorney fees) sustained or incurred because of or by reason of any claims, demands, suits, actions, judgments, or executions for damages of any and every kind and by whomever and whenever made or obtained, allegedly caused by, arising out of, or relating in any manner to any use made of the information or data obtained under this Agreement.

23. GENERAL TERMS AND CONDITIONS:

23.1 ALTERATIONS AND AMENDMENTS: This Agreement may be amended by the AA at any time by sending notice to BB.

23.2 ASSIGNMENT: BB may not transfer or assign: (i) this Agreement or any portion thereof; (ii) any right or benefit accruing to BB under this Agreement; nor (iii) any claim arising under this Agreement.

23.3 DISPUTES: Except as otherwise provided in this Agreement, when a bona fide dispute concerning a question of fact arises between the AA and BB, and it cannot be resolved, either party may take the dispute to a Dispute Board which shall determine it in the following manner: Each party to this Agreement shall appoint one member to the Dispute Board. The members so appointed shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall review the facts, agreement terms and applicable statutes and rules and make a determination of the dispute. Both parties agree to exercise good faith in dispute resolution and to avoid litigation whenever possible. The determination of the Dispute Board shall be final and binding on the parties hereto.
23.4 **ENTIRE AGREEMENT:** This Agreement sets forth the entire agreement between the parties with respect to the subject matter hereof and supersedes all previous discussions and agreements. Understandings, representations, or warranties not contained in this Agreement or a written amendment hereto shall not be binding on either party.

23.5 **GOVERNING LAW:** This Agreement shall be governed in all respects by the laws and statutes of the State of Washington. The jurisdiction for any action hereunder shall be the Superior Court for the State of Washington. The venue of any action hereunder shall be in the Superior Court for Thurston County, Washington. BB, by execution of this Agreement, acknowledges and agrees to the jurisdiction of the courts of the State of Washington in all matters relating to this Agreement.

23.6 **HEADINGS:** The headings and table of contents used herein are for reference and convenience only and shall not enter into the interpretation hereof unless otherwise specified herein. In the interpretation of this Agreement, the terms and conditions shall be construed to be complementary.

23.7 **CONFLICTS OF AUTHORITY:** If any provision of this Agreement shall be deemed in conflict with any statute or rule of law, such provision shall be deemed modified to conform to said statute or rule of law.

23.8 **INDEPENDENT STATUS OF PARTIES:** The parties to this Agreement will be acting in their individual capacities and not as agents, employees, partners, joint venturers, or associates of one another. The employees or agents of one party shall not be considered or construed to be the employees or agents of the other party for any purpose whatsoever.

23.9 **NON-EXCLUSIVITY:** This Agreement is non-exclusive. During the term of this Agreement, the AA reserves the right to enter into agreements with other parties as it deems fit. Nothing contained in this Agreement shall be construed to limit in any way the AA’s right to enter a like or similar agreement or grant a like or similar license to any other entity or party on such terms as the AOC may in its sole discretion deem appropriate.

23.10 **NOTICES:** Any notice required or permitted to be given under this Agreement shall be effective if and only if it is in writing. Notice must be given by personal delivery or sent by United States mail; mail to BB must be sent to BB’s address as set forth in this Agreement and mail to the address as each party has provided at the beginning of the Agreement.

23.11 **SEVERABILITY:** If any term or condition of this Agreement or the application thereof to any person(s) or circumstances is held invalid, such invalidity shall not affect other terms, conditions, or applications which can be given effect without the invalid term, condition, or application; to this end the terms and conditions of this Agreement are declared severable.

23.12 **SUBCONTRACTING:** BB shall not enter into subcontracts relating to this Agreement without obtaining prior written approval from the AA.

23.13 **SURVIVAL:**

23.13.1 For as long as BB continues to use any portion of the data provided under this Agreement, BB must comply with the terms of this Agreement.

23.13.2 In addition, the provisions of Sections 21, 22 and 23 of this Agreement shall survive the termination of the Agreement.

23.14 **TERMINATION:**

23.14.1 **General:** Either party may terminate this Agreement with thirty (30) days’ written notice to the other party’s Agreement Administrator named on Page 1. In case of termination, any and all information provided by AA pursuant to this agreement shall either be immediately returned to AA or immediately destroyed. Written notification of destruction to AA is required.
23.14.2 **Termination for Cause:** BB accepts full responsibility and liability for any violations of this Agreement by BB or any officer, employee, or agent of BB and any such violation shall result in immediate termination by the AA of all data and information provided to BB or any officer, employee, or agent of BB in any form and immediate forfeiture to the AA of any AA-provided data and information in any form held by BB or any officer, employee, or agent of BB. In such event, BB shall be liable for damages as authorized by law.

23.15 **WAIVER:** No term or condition of this Agreement shall be held to be waived, modified, or deleted, and no breach excused, except by a written instrument signed by the parties hereto. Waiver of any breach of any term or condition of this Agreement shall not be deemed a waiver of any prior or subsequent breach.

24. **SIGNATURES:** The parties hereto, having read this Agreement in its entirety, do agree thereto in each and every particular.

AGENCY A

AGENCY B

Signature/Title

Signature/Title

DATE: ___________________________  DATE: ___________________________
Appendix A. Minimum Sanitization Recommendation for Media Containing Data

Once a decision is made (see section 4) and after applying relevant organizational environmental factors, then Table A-1 can be used to determine recommended sanitization of specific media. This recommendation should reflect the Federal Information Processing Standard (FIPS) 199 security categorization of the system confidentiality to reduce the impact of harm of unauthorized disclosure of information from the media.

Although use of Table A-1 is recommended here, other methods exist to satisfy the intent of clear, purge (still relevant in some cases), and destroy, and methods not specified in this table may be suitable as long as they are vetted and found satisfactory by the organization. Not all types of available media are specified in this table. If your media are not included in this guide, organizations are urged to identify and use processes that will fulfill the intent to clear, purge, or destroy their media.

When an organization or agency has a sanitization technology, method and/or tool that they trust and have validated, they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website. The FASP effort was initiated as a result of the success of the Federal Chief Information Officer (CIO) Council’s Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection (CIP) and security. FASP can be found at http://csrc.nist.gov/fasp/.

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
</table>
| Hard Copy Storages    |                        |                        | ▪ Destroy paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen (reference NSA Disintegrator EPL.).  
▪ Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash. |
| Paper and microforms  | See Physical Destruction. | See Physical Destruction. |                                                                                      |
### Media Sanitization Guidelines

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hand-Held Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Phones</td>
<td>Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td>Personal Digital Assistant (PDA) (Palm, PocketPC, other)</td>
<td>Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear.</td>
<td>▪ Incinerate PDAs by burning the PDAs in a licensed incinerator.</td>
</tr>
<tr>
<td><strong>Networking Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routers (home, home office, enterprise)</td>
<td>Perform a full manufacturer’s reset to reset the router back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td><strong>Equipment</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copy Machines</td>
<td>Perform a full manufacturer’s reset to reset the copy machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td>Fax Machines</td>
<td>Perform a full manufacturer’s reset to reset the fax machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedures.</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td><strong>Magnetic Disks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Floppies</td>
<td>Overwrite media by using agency-approved software and validate the overwritten data. Degauss in a NSA/CSS-approved degausser.</td>
<td></td>
<td>▪ Incinerate floppy disks and diskettes by burning the floppy disks and diskettes in a licensed incinerator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Shred.</td>
</tr>
</tbody>
</table>
### Guidelines for Media Sanitization

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
</table>
| ATA Hard Drives | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | 1. Purge using Secure Erase. The Secure Erase software can be downloaded from the University of California, San Diego (UCSD) CMRR site.  
2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.**  
3. Purge media by using agency-approved and validated purge technologies/tools.  
**Degaussing any current generation hard disk will render the drive permanently unusable. | - Disintegrate.  
- Shred.  
- Pulverize.  
- Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator. |
| USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | 1. Purge using Secure Erase. The Secure Erase software can be downloaded from the University of California, San Diego (UCSD) CMRR site.  
2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.**  
3. Purge media by using agency-approved and validated purge technologies/tools.  
**Degaussing any current generation hard disk will render the drive permanently unusable. | - Disintegrate.  
- Shred.  
- Pulverize.  
- Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator. |
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
</table>
| Zip Disks               | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | Degauss using a NSA/CSS-approved degausser. **Degaussing any current generation zip disks will render the disk permanently unusable.** | - Incinerate disks and diskettes by burning the zip disks in a licensed incinerator.  
- Shred. |
| SCSI Drives             | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand. **Degaussing any current generation hard disk will render the drive permanently unusable.** | - Disintegrate.  
- Shred.  
- Pulverize.  
- Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator. |
| Magnetic Tapes          | Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods. Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals. | Degauss using an NSA/CSS-approved degausser. Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape. | - Incinerate by burning the tapes in a licensed incinerator.  
- Shred.  
Preparatory steps, such as removing the tape from the reel or cassette prior to destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a destruction facility or for recycling measures. |
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optical Disks</strong></td>
<td></td>
<td></td>
<td><strong>Destroy in order of recommendations:</strong></td>
</tr>
<tr>
<td>CDs</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>▪ Removing the Information bearing layers of CD media using a commercial optical disk grinding device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Incinerate optical disk media (reduce to ash) using a licensed facility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). **</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>** This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm².</td>
</tr>
<tr>
<td>DVDs</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>▪ Removing the Information bearing layers of DVD media using a commercial optical disk grinding device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Incinerate optical disk media (reduce to ash) using a licensed facility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). **</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>** This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm².</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td></td>
<td></td>
<td><strong>Destroy media in order of recommendations.</strong></td>
</tr>
<tr>
<td>Compact Flash Drives, SD</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>See Physical Destruction.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Incinerate by burning in a licensed incinerator.</td>
</tr>
<tr>
<td>Dynamic Random Access Memory (DRAM)</td>
<td>Purge DRAM by powering off and removing the battery (if battery backed).</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Pulverize</td>
</tr>
<tr>
<td>Electronically Alterable PROM (EAPROM)</td>
<td>Perform a full chip purge as per manufacturer's data sheets.</td>
<td>Same as Clear.</td>
<td>▪ Shred</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Pulverize</td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Physical Destruction</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Electronically Erasable PROM</strong> (EEPROM)</td>
<td>Overwrite media by using agency approved and validated overwriting technologies/methods/tools. Remove all labels or markings that indicate previous use or confidentiality.</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Incinerate by burning in a licensed incinerator.</td>
</tr>
<tr>
<td><strong>Erasable Programmable ROM (EPROM)</strong></td>
<td>Clear media in order of recommendations.</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td></td>
<td>1. Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer's recommendations, but increase the time requirement by a factor of 3.</td>
<td></td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td>2. Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td></td>
<td>▪ Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Incinerate by burning in a licensed incinerator.</td>
</tr>
<tr>
<td><strong>Field Programmable Gate Array</strong> (FPGA Devices) (Non-Volatile)</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Pulverize.</td>
</tr>
<tr>
<td><strong>Field Programmable Gate Array</strong> (FPGA Devices) (Volatile)</td>
<td>Clear functioning FPGA by powering off and removing the battery (if battery backed).</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Pulverize.</td>
</tr>
<tr>
<td><strong>Flash Cards</strong></td>
<td>Overwrite media by using agency approved and validated overwriting technologies/methods/tools.</td>
<td>Same as Clear.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Pulverize.</td>
</tr>
<tr>
<td><strong>Flash EPROM</strong> (FEPROM)</td>
<td>Perform a full chip purge as per manufacturer's data sheets.</td>
<td>Purge media in order of recommendations.</td>
<td>▪ Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools</td>
<td>▪ Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Perform a full chip purge as per manufacturer's data sheets.</td>
<td>▪ Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Incinerate by burning in a licensed incinerator.</td>
</tr>
</tbody>
</table>
## Guidelines for Media Sanitization

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
<th></th>
</tr>
</thead>
</table>
| Magnetic Bubble Memory | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | Purge by Collapsing the Magnetic Bubbles:  
1. Degaussing: Degauss in an NSA/CSS-approved degausser. However, care must be taken to insure that the full field (at least 1500 gauss) of the degausser is applied to the actual bubble array. All shielding materials must be removed from the circuit card and/or bubble memory device before degaussing.  
2. Raising the Magnetic Bias Field: Magnetic bubble memory with built-in magnetic bias field controls may be purged by raising the bias voltage to levels sufficient to collapse the magnetic bubbles. Recommend that specific technical guidance be obtained from the bubble memory manufacturer before attempting this procedure. | ▪ Shred.  
▪ Disintegrate.  
▪ Pulverize.  
When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device. |                      |
| Magnetic Core Memory | Clear media in order of recommendations.  
1. Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.  
2. Degauss in an NSA/CSS-approved degausser. | Purge core memory devices either by overwriting or degaussing.  
▪ Overwrite media by using agency approved and validated overwriting technologies/methods/tools  
▪ Degauss in an NSA/CSS-approved degausser. Remove all labels or markings that indicate previous use or confidentiality. NOTE - Attenuation of the magnetic field due to chassis shielding and separation distance are factors that affect erasure performance and should be considered. All steel shielding materials (e.g., chassis, case, or mounting brackets) should be removed before degaussing. | ▪ Shred.  
▪ Disintegrate.  
▪ Pulverize.  
When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance. |                      |
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
</table>
| Non Volatile RAM (NOVRAM) | See Physical Destruction. | Same as Clear. | - Shred.  
- Disintegrate.  
- Pulverize. |
| PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards | See Physical Destruction. | See Physical Destruction. | Destroy by incinerating in a licensed incinerator or use (an NSA evaluated) a disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size. |
| Programmable ROM (PROM) | See Physical Destruction. | See Physical Destruction. | Destroy by incinerating in a licensed incinerator |
| RAM | Purge functioning DRAM by powering off and removing the battery (if battery backed). | Same as Clear | - Shred.  
- Disintegrate.  
- Pulverize. |
| ROM | See Physical Destruction. | See Physical Destruction. | - Shred.  
- Disintegrate.  
- Pulverize. |
| USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) without Hard Drives | Overwrite media by using agency approved and validated overwriting technologies/methods/tools | Same as Clear. | - Shred.  
- Disintegrate.  
- Pulverize. |
| Smart Cards | See Physical Destruction. | See Physical Destruction. | - For smart card devices& data storage tokens that are in credit card form, cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded should instead be destroyed via incineration licensed incinerator or disintegration to 2 mm size particles. |
- Incinerate. Incineration of magnetic cards shall be accomplished by burning the magnetic cards in a licensed incinerator. |