

Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements

1.0 INTRODUCTION

The Executive Branch has adopted privacy and information security policies to protect confidential and personally identifiable information (hereinafter all referred to as Confidential Information). This Notice sets forth the vendor's responsibilities for safeguarding this information.

2.0 DEFINITIONS

- 2.1 Breach** shall mean the acquisition, access, use or disclosure of Confidential Information which compromises the security or privacy of such information.
- 2.2 Confidential Information**, shall include, but is not limited to, trade secrets, personally identifiable information, protected health information, financial information, financial account number, credit card numbers, debit card numbers, driver's license numbers, State ID numbers, social security numbers, employee home addresses, employee marital status, employee maiden name, etc.
- 2.3 Security Incident** means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information.

3.0 BACKGROUND

Agencies maintain Confidential Information, including, but not limited to, trade secrets, personally identifiable information, protected health information, financial information, financial account numbers, credit card numbers, debit card numbers, driver's license numbers, State ID numbers, social security numbers, employee home addresses, etc. Federal laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Privacy Act of 1974, Fair Credit Reporting Act and State laws require that certain information be safeguarded. In some situations, Agencies delegate, through contract provisions, functions to vendors that involve the vendor's collection, use and/or disclosure of Confidential Information. WV State government must take appropriate steps to ensure its compliance with those laws and desires to protect its citizens' and employees' privacy, and therefore, must require that its vendors also obey those laws.

Utilization of safeguards can greatly minimize potential exposure to sensitive information, and vendors are expected to adhere to industry standard best practices in the management of data collected by, or on behalf of, the State, and in the vendor's possession for a business purpose. Even when sound practices and safeguards are in use, exposures can occur as the result of a

Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements

theft, loss, or compromise of data, or systems containing data. At these times, vendors must be accountable for the loss of data in their possession by ***immediately reporting*** the incident surrounding the loss, and by absorbing any cost associated with the appropriate response actions deemed by the State to be reasonable and necessary. Additional vendor funding may be needed for required activities, such as: rapid notification to affected persons, and provision of a call center to handle inquiries. Notification and call handling will use a State-specified method, format, language, and personnel staffing level.

4.0 POLICY

- 4.1** All vendors for the Executive Branch of West Virginia State government shall sign both the RFP or RFQ, as applicable, and the Purchase Order which contain the confidentiality statement, incident response accountability acknowledgement, and adopt this policy by reference.
- 4.2** Vendors must contact the Privacy Officer of the Agency with which they are contracting to obtain Agency-specific privacy policies, procedures and rules, when applicable.
- 4.3** For vendors' information, Agencies generally require at least the following minimum standards of care in the handling of their Confidential Information:
 - 4.3.1** Confidential Information shall only be used or disclosed for the purposes designated in the underlying contract and at no time shall it be disclosed or used for a personal, non-work or non-contract related reason, unless specifically authorized in writing by the Agency.
 - 4.3.2** In all circumstances, vendors shall have no ownership rights or interests in any data or information, including Confidential Information. All data collected by the vendor on behalf of the Agency, or received by the vendor from the Agency, is owned by the Agency. There are no exceptions to this provision.
 - 4.3.3** In no circumstance shall a vendor use Confidential Information, or data, in any way detrimental to the Agency or to any individual whose records reside in the vendor's control. This prohibition shall not be construed to curtail a vendor's whistleblower rights under Federal and State law. If, in the process of making a good faith report under the provisions of W. Va. Code § 6C-1-1 et seq. or the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), (Pub. L. No. 104-191) as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the Federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA") or any other relevant whistleblower law, a vendor finds it necessary to

Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements

disclose Confidential Information to an appropriate authority in accordance with those statutes, the disclosure will not be treated as a Breach of the Agency's security, privacy or confidentiality policies, as long as the confidential nature of the information is explicitly conveyed to the authorized recipient.

- 4.3.4** The State may periodically monitor and/or audit use of the information systems and other record-keeping systems at a vendor location or a State location in an effort to ensure compliance with this policy. In addition, the State may audit, and require strengthening of, vendor policies and/or practices as they impact security of State data within the vendor's possession.
- 4.3.5** Any collection, use or disclosure of information that is determined by the Agency to be contrary to the confidentiality statement, law or Agency policy may result in termination of the underlying contract.
- 4.3.6** The confidentiality and incident response accountability statement contained within the RFP or RFQ, as applicable, and the Purchase Order shall survive termination of the underlying contract.
- 4.4** If there is an incident that involves theft, loss, or compromise of State Confidential Information, the following reporting and/or actions must be taken by the vendor, on its own behalf, or on behalf of its subcontractor:
 - 4.4.1** If the event involves a theft, or is incidental to another crime, appropriate law enforcement officials shall be notified and a police report generated to document the circumstances of the crime, with a goal to establish whether the crime involved a motive to obtain the sensitive data. A copy of the police report will be forwarded in accordance with 4.4.2.3.
 - 4.4.2** Notification of Breach.
 - 4.4.2.1** Upon the **discovery** of Breach of security of Confidential Information, if the Confidential Information was, or is reasonably believed to have been, acquired by an unauthorized person, the vendor shall notify the individuals identified in 4.4.2.3 immediately by telephone call plus e-mail, web form or fax; or,
 - 4.4.2.2** Within 24 hours by e-mail or fax of any **suspected** Security Incident, intrusion or unauthorized use or disclosure of Confidential Information, in violation of the underlying contract and this Notice, of **potential** loss of confidential data affecting the underlying contract.
 - 4.4.2.3** Notification required by the above two sections shall be provided to:

Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements

(1) the Agency contract manager whose contact information may be found at www.state.wv.us/admin/purchase/vrc/agencyli.htm and,
(2) unless otherwise directed by the Agency in writing, the Office of Technology at incident@wv.gov.

- 4.4.2.4** The vendor shall immediately investigate such actual or suspected Security Incident, Breach, or unauthorized use or disclosure of Confidential Information. Within 72 hours of the discovery, if an actual Breach has occurred, the vendor shall notify the individuals identified in 4.4.2.3 of the following: (a) What data elements were involved and the extent of the data involved in the Breach (e.g. number of records or affected individual's data); (b) The identity of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or Confidential Information; (c) A description of where the Confidential Information is believed to have been improperly transmitted, sent, or utilized; (d) A description of the probable causes of the improper use or disclosure; and (e) Whether any Federal or State laws requiring individual notifications of Breaches are triggered.
- 4.4.2.5** Agency will coordinate with the vendor to determine additional specific actions that will be required of the vendor for mitigation of the Breach, which may include notification to the individual or other authorities.
- 4.4.2.6** All associated costs shall be borne by the vendor. This may include, but not be limited to costs associated with notifying affected individuals.
- 4.5** The State may require that a vendor provide evidence of adequate background checks, including a nationwide record search, for individuals who are entrusted by the vendor to work with State information.
- 4.6** The State requires that any vendor taking possession of State data have comprehensive policies and practices to adequately safeguard that information, and further that the sensitivity of the information is clearly identified and documented in writing, with signed acknowledgement by the vendor that the sensitivity is understood, before it is conveyed to the vendor. Vendor policy should articulate all safeguards in place for the State information, including provisions for destruction of all data, including backup copies of the data, at the end of the vendor's legitimate need to possess the data. All State-owned media containing State information will be returned to the State when no longer legitimately needed by the vendor.
- 4.7** All vendor owned devices that contain or transport any State Confidential Information must be encrypted using the AES algorithm, and an industry

**Notice of State of West Virginia
Confidentiality Policies and Information Security Accountability Requirements**

standard methodology. This includes desktop and laptop computers (whole drive encryption – not file encryption), personal digital assistants (PDA), smart phones, thumb or flash-type drives, CDs, diskettes, backup tapes, etc.