



Virginia Community College System Third-Party Non-Disclosure Agreement

(To be used when a contractor will be given access to sensitive IT systems and/or data for which there is a risk associated with data disclosure.)

CONFIDENTIALITY OF AGENCY INFORMATION:

1. Contractor shall take all precautions and measures necessary to ensure the integrity, nondisclosure, confidentiality and protection of all data and information obtained from the Virginia Community College System ("VCCS"), including but not limited to all original reporting forms and data in any other form. Sensitive data used for research purposes may be disclosed only if aggregated in a manner that prevents the release of any personally identifiable information.
2. The contractor hereby declares in writing prior to the commencement of any work for the VCCS that he, she or it understands that all sensitive data and information obtained from the VCCS or derived therefrom and will be held in the strictest confidence by Contractor, its officers, directors, agents, and employees, with the exception that information and data derived from sensitive data may be released where allowed by law and/or where aggregated to prevent the personal identification of data subjects by third parties. Contractor, its officers, directors, agents, and employees shall be governed by, and comply with, Federal and Virginia laws prohibiting the disclosure of information obtained or compiled during the course of their work for the VCCS.
3. The attached list (see Attachment 1) shall describe the sensitive data to which the contractor will be given access and which will be covered by this agreement. All information obtained and work performed under this agreement and the Contractor's VCCS contract/order is considered sensitive, requires use of sensitive and personal data and information and/or falls under one or more categories of information that is subject to protection from disclosure and misuse, including but not limited to: personal information and highly restricted personal information in connection with motor vehicle records under the Federal Drivers Privacy Protection Act, 18 USC 2721 *et seq.*, law enforcement sensitive data and information, the Privacy Act of 1974, 5 U.S.C. § 552a *et seq.*, the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g *et seq.* (FERPA), personal, vehicle and driver information as defined under and governed by Va. Code § 46.2-208 *et seq.* and personal information as defined under and governed by the Government Data Collection and Dissemination Practices Act, Va. Code § 2.2-3800 *et seq.*
4. All source materials/data/information and resultant work products compiled or created and any information or portion of information derived therefrom are the property of the VCCS and must not be used by the contractor for any purpose other than the purpose outlined by the contract/order and/or this agreement.
5. Except as may otherwise be allowed herein, neither Contractor, nor its officers, directors, agents, or employees shall divulge, sell, or distribute any information obtained from the VCCS or derived therefrom at any point in time, even after termination or expiration of a contract/order, except as may otherwise be required by law.
6. If the VCCS has released education records to the Contractor pursuant to FERPA, then Contractor and its authorized representatives specifically agree to protect the records

in a manner that does not permit the disclosure of personally identifiable information of individuals to third parties; and Contractor shall destroy such records when they are no longer needed for the purpose for which they were released.

7. Except as specifically authorized by the contract/order, Contractor, its officers, directors, agents, and employees are prohibited from reproducing the VCCS source media, written products, or any portion thereof.

8. The Contractor shall notify each of its officers, directors, agents, and employees having access to the VCCS data and/or information that such data and/or information may be used only for the purpose and to the extent authorized in this agreement.

9. The Contractor shall create or have on file and available for review a security plan outlining the steps and methods taken to secure and protect the information provided by the VCCS to address the following points:

- Security of Files and/or Copies of Records (for Hardcopy).
- Security of on-line Computer Terminals (On-Line Users Only).
- Designation of Authorized Users/Assignment of Access Codes.
- For automated interfaces/electronic extraction and storage of data, if applicable:
 - Security of Records, Files, and Systems, use of encryption for storage.
 - Names and addresses of data extraction method and software creators/vendors,
 - Network Diagrams and descriptions of Data Extraction methods and software,
 - Descriptions of system support processes including backup methods and frequencies.
- Proposed Audit/Management Controls Over Access and Dissemination of Requested Information.

10. Contractor agrees to comply with all applicable federal and state statutes, rules and regulations and understands that disclosure of any information, by any means, for a purpose or to an extent unauthorized herein, shall be grounds for immediate termination of the contract/order and this agreement, and may subject the offender to criminal and civil sanctions.

11. Contractor shall indemnify, defend, and hold harmless the Commonwealth, the VCCS, its officers, directors, employees and agents from and against all losses, liabilities, damages and all related costs and expenses (including reasonable attorneys' fees and disbursements and costs of investigation, litigation, settlement, judgments, interest and penalties), incurred in connection with any action or proceeding arising directly or indirectly from unauthorized use or disclosure by Contractor, its agents, directors, officers or employees, of any data or information obtained from the VCCS pursuant to this agreement, or derived therefrom.

12. Contractor shall disclose any breach of the security of the data system following discovery or notification of the breach in the security of the data to any Virginia resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

13. Contractor shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification required may be delayed if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation. Contractor shall allow the agency both to participate in the investigation of incidents and to exercise control over decisions regarding external reporting.

- Notice may be provided by one of the following methods:
 - 1) written notice to the most recent available address the person or business has in its records;
 - 2) telephone notice;
 - 3) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or
 - 4) substitute notice, if the individual or entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:
 - (i) e-mail notice if the individual or the entity has email addresses for the members of the affected class of residents;
 - (ii) conspicuous posting of the notice on the Web site page of the individual or the entity, if the individual or entity maintains one; and
 - (iii) notification by major statewide media, including newspaper, radio and television.
- In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to *Code of Virginia*, §18.2-186.6(E), the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. §1681(a)(p), of the timing, distribution, and content of the notice.
- Notification must include:
 - 1) a general description of what occurred and when;
 - 2) the type of personal information that was involved;
 - 3) what actions have been taken to protect the individuals' personal information from further unauthorized access;
 - 4) what if anything, the contractor will do to assist affected individuals, including providing the contact information of those individuals who can offer more information and assistance; and
 - 5) what actions the contractor recommends that the individual take. The actions recommended should include monitoring their credit report and

reviewing their account statements.

VCCS System or Data Owner:

Name: _____ Title: _____

Signature Date

Contractor or Vendor:

Name: _____ Title: _____

Signature Date

Business Address and Contact Information:

Attachment 1:

VCCS Data Classification Covered Under This Agreement:

The table below delineates the data elements that are classified as sensitive or confidential and which the contractor will be given access and therefore is covered under this agreement:

Data Element	Description	File or Table Name