TITLE: ***DATA SECURITY AND PROTECTION AGREEMENT***

MASON - NSF VIRGINIA CITY AND COUNTY CYBERSECURITY PARTNERING, LEADERSHIP AND GOVERNANCE

Document Reference Number: VA Series-06

Last Updated 2/28/2018

NSF PROJECT NO. 1623653

Document Title: **Data Security and Protection Agreement**[1] [2]

Document Type: *Vendor/Contractor Agreement*

Scope of Application: New Government employees, contractors, consultants, constitutional employees, temporaries, and volunteers.

Document Purpose: The purpose of this agreement is to provide guidelines to all personnel employed by the Government in the safeguarding of the confidentiality, privacy and security of Government information and Government networked resources, and to ensure compliance with all applicable local, state and federal law or regulatory requirement.

1. Data Security and Protection

The Contractor will hold Government Information, as defined below, in the strictest confidence and will comply with all applicable Government security and network resources policies, as well as all local, state and federal laws and regulatory requirements concerning data privacy and security. The Contractor must develop, implement, maintain, continually monitor and use appropriate administrative, technical and physical security measures to control access to and to preserve the confidentiality, privacy, integrity and availability of all electronically maintained or transmitted information received from or created or maintained on behalf of the Government. For purposes of this provision, and as more fully described in this Contract and in the Government's Nondisclosure and Data Security Agreement (NDA)[3], "Government Information" includes, but is not limited to, electronic information; documents; data; images; financial records; personally identifiable information; personal health information (PHI); personnel, educational, voting, registration, tax and assessment records; information related to public safety; Government networked resources; and Government databases, software and security measures that are created, maintained, transmitted or accessed to perform the Work under this Contract.

[1] This policy template is based on policies provided by Arlington County as a response to the call, by the GMU-NSF project (No. 1623653), for cybersecurity partnership and information sharing among cities and counties.

[2] As used in this document, (i) "Government" means XXX County/City Government, (ii) "CIO" means Chief Information Officer or his/her designee, (iii) "Department of Technology and Information Services" or "DTS" refers to the department that manages the Information Communication Technology, (iv) "CISO" means the Chief Information Security Officer or his/her designee, (v) "Communications Office" refers to the department or designee that manages communications and public relations, (vi) "Chief Records Management Officer" or CRO means the officer that manages Government records policies and enforcement.

[3] Refer to the Mason - NSF City and County Cybersecurity Partnering, Leadership and Governance / Document VA Series-05.

(1) **Government's Nondisclosure and Data Security Agreement**: The Contractor and its Designees (Contractor Designees shall include, but shall not be limited to, all Contractor-controlled agents or subcontractors working on-site at Government facilities or otherwise performing any work under this Contract) must sign the NDA before performing any work or obtaining or permitting access to Government networked resources, application systems or databases. The Contractor will make copies of the signed NDAs available to the Government Project Officer upon request.

(2) **Use of data**. The Contractor will ensure against any unauthorized use, distribution or disclosure of or access to Government Information and Government networked resources by itself or its Designees. Use of Government Information other than as specifically outlined in the Contract Documents is strictly prohibited. The Contractor will be solely responsible for any unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access to or disclosure of Government Information and for any non-compliance with this provision by itself or by its Designees.

(3) **Data protection**. The Contractor will protect the Government's Information according to standards established by the National Institute of Standards and Technology, including 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth[4] and the Payment Card Industry Data Security Standard (PCI DSS)[5], as applicable, and no less rigorously than it protects its own data and proprietary or confidential information. The Contractor must provide to the Government a copy of its data security policy and procedures for securing Government Information and a copy of its disaster recovery plan(s). If requested by the Government, the Contractor must also provide annually the results of an internal Information Security Risk Assessment provided by an outside firm.

(4) **Security requirements**. The Contractor must maintain the most up-to-date anti-virus programs, industry-accepted firewalls and other protections on its systems and networking equipment. The Contractor certifies that all systems and networking equipment that support, interact with or store Government Information meet the above standards and industry best practices for physical, network and system security requirements. Printers, copiers or fax machines that store Government Data into hard drives must provide data-at-rest encryption. The Government's Chief Information Security Officer or designee must approve any deviation from these standards. The downloading of Government information onto laptops, other

[4] http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

[5] https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

portable storage media or services such as personal e-mail, Dropbox etc. is prohibited without the written authorization of the Government's Chief Information Security Officer or designee.

(5) **Conclusion of contract**. Within 30 days after the termination, cancellation, expiration or other conclusion of the Contract, the Contractor must, at no cost to the Government, return all Government Information to the Government in a format defined by the Government Project Officer. The Government may request that the Information be destroyed. The Contractor is responsible for ensuring the return and/or destruction of all Information that is in the possession of its subcontractors or agents. The Contractor must certify completion of this task in writing to the Government Project Officer.

(6) **Notification of security incidents**. The Contractor must notify the Government Chief Information Officer and Government Project Officer within 24 hours of the discovery of any unintended access to or use or disclosure of Government Information.

(7) **Subcontractors**. If subcontractors are permitted under this Contract, the requirements of this entire section must be incorporated into any agreement between the Contractor and the subcontractor. If the subcontractor will have access to Government Information, each subcontractor must provide to the Contractor a copy of its data security policy and procedures for securing Government Information and a copy of its disaster recovery plan(s).

Your signature means that you have read, understand and ***agree to comply*** with the requirements of this policy.

____ ___________________

Contractor / Vendor Signature Date

____

Contractor / Vendor Name (Print)

____ ___________________

Authorizing Government Supervisor / Project Officer Date

Department Charge Code (if applicable): ___________________