Document Title:	**Nondisclosure and Data Security Agreement**[1] [2]
Document Type:	*Employee Agreement*
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.
Scope of Application:	All Government employees, constitutional employees, temporaries, and volunteers.

I, the undersigned, agree that I will hold Government provided information, documents, data, images, records and the like (hereafter "information") confidential and secure and protect it against loss, misuse, alteration, destruction or disclosure. This includes but is not limited to the information of the Government, its employees, contractors, residents, clients, patients, taxpayers, and property and includes but is not limited to, data that the County shares with my employer for testing, support, conversion, or for support services.

I agree that I will maintain the privacy and security of Government information and I will not divulge or allow or facilitate access to Government information for any purpose or by anyone unless expressly authorized to do so by the Chief Information Officer. This includes but is not limited to information that in any manner describes, locates or indexes anything about an individual including, but not limited to, his/her (hereinafter "his") Personal Health Information, treatment, disability, services eligibility, services provided, investigations, real or personal property holdings, education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, social security number, tax status or payments, date of

[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, (vii) "Constitutional Employees" means staff that report under the Treasurer or Commissioner of Revenue both elected officials who report to the State even though the County provides work space, IT equipment, etc.

birth or that otherwise affords a basis of inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual, and the record of his presence, registration, or membership in an organization or activity, or admission to an institution (as also collectively referred to herein as "information" or "Government information").

I agree that I will not directly or indirectly use or facilitate the use or dissemination of information (whether intentionally or by inadvertence, negligence or omission verbally, electronically, through paper transmission or otherwise) for any purpose other than that directly authorized and associated with my designated duties. I understand and agree that any unauthorized use, dissemination or disclosure of information is prohibited and may also constitute a violation of Virginia or federal law/s, subject to civil and/or criminal penalties.

I also agree that I will not divulge or otherwise facilitate the disclosure, dissemination or access to or by any unauthorized person for any purpose of the information obtained directly, or indirectly, as a result of my work.

I agree to view, retrieve or access Government information only to the extent concomitant with my assigned duties and only in accordance with the Government's access and security policies or protocols (Electronic Communications and Internet Services Policy).

I agree that I will take strict security measures to ensure that information is kept secure, properly stored, that if stored that it is encrypted as appropriate, stored in accordance with industry best practices, and otherwise protected from retrieval or access by unauthorized persons or unauthorized purpose. I will also ensure that any device or media on which information is stored, even temporarily, will have strict security and access control and that I will not remove, facilitate the removal of or cause to be removed any information from the Government's physical facility without written authorization of the Chief Information Officer. If so authorized, I understand that I am responsible for the security of the electronic equipment or paper files on which the information is stored and agree to promptly return such information.

I will not use any devices, laptops, PDAs, netbooks, tablets, thumb drives or other media storage devices ("Device") during my work without pre-approval. I will ensure that any Device connected to the Government network shall be free of all computer viruses or running the latest version of an industry standard virus protection program. I will also ensure that my password is robust, protected and not shared.

I agree that I will notify the Chief Information Officer immediately upon discovery, becoming aware of or suspicious of any unauthorized disclosure of information, security breach, hacking or other breach of this Agreement or Government policy. I will fully cooperate with the Government

to help regain possession of any information and to prevent its further disclosure, use or dissemination.

It is the intent of this Nondisclosure and Data Security Agreement to ensure that the highest level of administrative safeguards and best practices are in place to ensure confidentiality, protection, 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. Therefore, to the extent that this Nondisclosure and Data Security Agreement conflicts with the underlying Government Agreement or any local, state or federal law, regulation or provision, the more stringent Government provision, law, regulation or provision shall control.

Upon completion or termination of my work, I agree to return all Government information to the Chief Information Officer. I understand that this Agreement remains in full force and effect throughout my employment.

Signed: _____

Printed Name: _____

Date: _____

Witnessed:

Manager:_____

Printed Name: _____

Date: _____