NOTE: THIS DOCUMENT IS NOT INTENDED TO BE USED “AS IS.” THIS DOCUMENT MAY CONTAIN CLAUSES THAT ARE NOT APPLICABLE TO YOUR AGENCY. PLEASE CONSULT WITH YOUR AGENCY’S LEGAL COUNSEL, AND OTHERS, AS APPROPRIATE, BEFORE FINALIZING ANY AGREEMENT.

Instructions: This Acceptable Use Acknowledgment (“Acknowledgment”) must be completed by any individual (“User”) who, in the course of his/her duties, will be given access to non-public data and/or [Insert Agency] (“Agency”) information systems. The User, prior to being issued a network user ID and password, and prior to being able to access any non-public data held by the Agency, must:

1) Read this Acknowledgment;
2) Certify his/her completion of [Insert Agency] privacy and security training, “[Insert title of training]”, available at [Insert website link, or indicate training will be provided to employee by supervisor]; and
3) Sign and return this Acknowledgment form to his/her supervisor.

The purpose of this Acknowledgment is to ensure that User understands and acknowledges his/her responsibility to protect and safeguard the Agency’s non-public information to which he/she will have access, and to prevent the unauthorized access to, and use and/or disclosure of, such information. This Acknowledgment also describes User’s responsibilities regarding the access to, and use of, Agency-issued information systems and/or devices (e.g., desktop computers, laptops, mobile phones, network drives, CDs, thumb drives, tapes, cloud services, and the data contained therein).

User understands and acknowledges the following:

• User will complete Agency privacy and security training prior to accessing any non-public data and/or Agency information systems, and User will complete privacy and security training on an annual basis thereafter;

• Agency-issued devices and systems are the property of the Agency and will be used only for Agency-authorized purposes, except that incidental use of Agency resources/property is permitted as long as it does not result in additional public expense. Incidental use is infrequent and minimal. Unauthorized use of, or access to, an Agency-issued device or systems is strictly prohibited and may subject User to human resources, and/or legal, actions;

• Agency-issued devices and systems must not be used for private purposes, including blogging, commenting or posting on social media, sharing photographs, or other non-work related purposes, without written permission from Agency executive management;

• The Agency may inspect and/or seize any Agency-issued device and/or data stored on any Agency-issued information system and/or device. User acknowledges that he/she has no expectation of privacy as to any communication and/or information stored within any Agency-issued information system or device, whether or not that information is stored locally, on a hard drive, or on other media in use with the unit;
• For network maintenance and security purposes, all Agency information systems are subject to monitoring and interception of information. User acknowledges that the Agency may monitor and intercept User’s communications on Agency information systems for purposes including, but not limited to, system testing, security, investigations of alleged personnel misconduct, and/or law enforcement investigations;

• The Agency strictly prohibits the unauthorized modifying, defacing, deleting, or otherwise tampering with or abusing an Agency website, server, database, information system, or other Agency technology or information asset. User acknowledges that the Agency may use any legal and appropriate measures to prevent, investigate, and mitigate such attempts or actions;

• The Agency’s data classification schema categorizes information held by the Agency. The data classification policy may be obtained from Agency’s Privacy Liaison. User acknowledges that all information must be protected and safeguarded according to the Agency’s data classification schema;

• User will not install software or hardware, on any Agency-owned system, network, computing service or device without prior written approval from User’s executive management;

• User will neither share his/her Agency-issued User ID and/or password with any other person, nor knowingly allow any other person to use his/her User ID and/or password. If User suspects his/her password has been compromised, he/she will inform Agency’s Information Security Officer immediately;

• User will neither store nor back-up any Agency, non-public information, to any non-Agency information system or device such as portable hard drives, USB drives or cloud service offerings in any form or format;

• User will not share, with any unauthorized individual(s), any Agency-held, non-public information, in any form or format;

• User will access data, or use operating systems or programs, only after receiving authorization to do so. User acknowledges that any unauthorized attempt to access data, or use operating systems or programs, may result in human resources, and/or legal, actions;

• User will not use any personally owned device for business purposes and communications without prior explicit written authorization from User’s Agency executive management. If Agency executive management explicitly authorizes such use of a personally owned device, software, and/or service, User acknowledges that the personally owned device, software and/or service will be treated, for policy requirement purposes, as an IT asset issued by the Agency. In the event of an information security incident involving an IT device, software, or service, which is owned by User and is used to perform job duties, User acknowledges that the Agency may require the User to provide access to the device, software, and/or service, prior to any further use, for the purpose of incident investigation and incident mitigation. Additionally, when User terminates employment, the personally owned device will be required to be cleaned of Agency data and may be required to be factory reset if no other means of validating data removal is available;
• User will not use, or link to, his/her personal email account(s) in the conduct of job duties through the use of an Agency-issued device, unless such use or linkage has been approved in writing by Agency executive management;

• User will not store his/her personal information, such as completed health benefits forms, payroll statements, or any other personal information, on an Agency-issued device or system if the personal information is unrelated to the performance of User’s job duties;

• User will immediately report to his/her supervisor the suspected loss or theft of any Agency-issued equipment;

• User will immediately report to his/her supervisor the actual, or suspected, unauthorized access to any Agency information;

• User may be required to comply with supplemental requirements imposed for specific information systems;

• Regardless of the physical location of User’s workplace, e.g., telecommuting, User is subject to the requirements of this Acceptable Use Acknowledgment;

• At termination of employment, User will not remove from Agency any information, hardware, software, device, or any other workplace resource, without explicit written permission from Agency executive management; and

• At termination of employment, User will return any and all Agency information, hardware, software, device, or any other workplace resource to User’s supervisor.

I have read, and understand, the above terms regarding use of Agency devices and systems, and access to non-public information created, used, and/or held by the Agency. I acknowledge my responsibilities regarding these devices, systems, and the information contained in them. I understand that willful violation of any provision of the above terms may result in disciplinary action, up to, and including, termination of employment.

Employee Name:  
Print        Signature        Date

I have completed the [insert Agency] privacy and security training, [insert Title of Training].

Employee Name:  
Print        Signature        Date