

1 **SAMPLE LANGUAGE AND CLAUSES**
2 **FOR**
3 **ACCEPTABLE USE ACKNOWLEDGMENT**
4

5 ***NOTE: THIS DOCUMENT IS NOT INTENDED TO BE USED "AS IS." THIS DOCUMENT MAY CONTAIN***
6 ***CLAUSES THAT ARE NOT APPLICABLE TO YOUR AGENCY. PLEASE CONSULT WITH YOUR AGENCY'S***
7 ***LEGAL COUNSEL, AND OTHERS, AS APPROPRIATE, BEFORE FINALIZING ANY AGREEMENT.***
8

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

- 13 1) Read this Acknowledgment;
 - 14 2) Certify his/her completion of [insert Agency] privacy and security training, "[insert title of
 - 15 **training**]", available at [insert website link, or indicate training will be provided to employee by
 - 16 **supervisor**]; and
 - 17 3) Sign and return this Acknowledgment form to his/her supervisor.
-

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

24 User understands and acknowledges the following:

- 25 • User will complete Agency privacy and security training prior to accessing any non-public data
26 and/or Agency information systems, and User will complete privacy and security training on an
27 annual basis thereafter;
- 28
- 29 • Agency-issued devices and systems are the property of the Agency and will be used only for Agency-
30 authorized purposes, except that incidental use of Agency resources/property is permitted as long
31 as it does not result in additional public expense. Incidental use is infrequent and minimal.
32 Unauthorized use of, or access to, an Agency-issued device or systems is strictly prohibited and may
33 subject User to human resources, and/or legal, actions;
- 34
- 35 • Agency-issued devices and systems must not be used for private purposes, including blogging,
36 commenting or posting on social media, sharing photographs, or other non-work related purposes,
37 without written permission from Agency executive management;
- 38
- 39 • The Agency may inspect and/or seize any Agency-issued device and/or data stored on any Agency-
40 issued information system and/or device. User acknowledges that he/she has no expectation of
41 privacy as to any communication and/or information stored within any Agency-issued information
42 system or device, whether or not that information is stored locally, on a hard drive, or on other
43 media in use with the unit;

- 44
- 45 • For network maintenance and security purposes, all Agency information systems are subject to
- 46 monitoring and interception of information. User acknowledges that the Agency may monitor and
- 47 intercept User's communications on Agency information systems for purposes including, but not
- 48 limited to, system testing, security, investigations of alleged personnel misconduct, and/or law
- 49 enforcement investigations;
- 50
- 51 • The Agency strictly prohibits the unauthorized modifying, defacing, deleting, or otherwise tampering
- 52 with or abusing an Agency website, server, database, information system, or other Agency
- 53 technology or information asset. User acknowledges that the Agency may use any legal and
- 54 appropriate measures to prevent, investigate, and mitigate such attempts or actions;
- 55
- 56 • The Agency's data classification schema categorizes information held by the Agency. The data
- 57 classification policy may be obtained from Agency's Privacy Liaison. User acknowledges that all
- 58 information must be protected and safeguarded according to the Agency's data classification
- 59 schema;
- 60
- 61 • User will not install software or hardware, on any Agency-owned system, network, computing
- 62 service or device without prior written approval from User's executive management;
- 63
- 64 • User will neither share his/her Agency-issued User ID and/or password with any other person, nor
- 65 knowingly allow any other person to use his/her User ID and/or password. If User suspects his/her
- 66 password has been compromised, he/she will inform Agency's Information Security Officer
- 67 immediately;
- 68
- 69 • User will neither store nor back-up any Agency, non-public information, to any non-Agency
- 70 information system or device such as portable hard drives, USB drives or cloud service offerings in
- 71 any form or format;
- 72
- 73 • User will not share, with any unauthorized individual(s), any Agency-held, non-public information, in
- 74 any form or format;
- 75
- 76 • User will access data, or use operating systems or programs, **only** after receiving authorization to do
- 77 so. User acknowledges that any unauthorized attempt to access data, or use operating systems or
- 78 programs, may result in human resources, and/or legal, actions;
- 79
- 80 • User will not use any personally owned device for business purposes and communications without
- 81 prior explicit written authorization from User's Agency executive management. If Agency executive
- 82 management explicitly authorizes such use of a personally owned device, software, and/or service,
- 83 User acknowledges that the personally owned device, software and/or service will be treated, for
- 84 policy requirement purposes, as an IT asset issued by the Agency. In the event of an information
- 85 security incident involving an IT device, software, or service, which is owned by User and is used to
- 86 perform job duties, User acknowledges that the Agency may require the User to provide access to
- 87 the device, software, and/or service, prior to any further use, for the purpose of incident
- 88 investigation and incident mitigation. Additionally, when User terminates employment, the
- 89 personally owned device will be required to be cleaned of Agency data and may be required to be
- 90 factory reset if no other means of validating data removal is available;

- 91
- 92 • User will not use, or link to, his/her personal email account(s) in the conduct of job duties through
- 93 the use of an Agency-issued device, unless such use or linkage has been approved in writing by
- 94 Agency executive management;
- 95
- 96 • User will not store his/her personal information, such as completed health benefits forms, payroll
- 97 statements, or any other personal information, on an Agency-issued device or system if the personal
- 98 information is unrelated to the performance of User's job duties;
- 99
- 100 • User will immediately report to his/her supervisor the suspected loss or theft of any Agency-issued
- 101 equipment;
- 102
- 103 • User will immediately report to his/her supervisor the actual, or suspected, unauthorized access to
- 104 any Agency information;
- 105
- 106 • User may be required to comply with supplemental requirements imposed for specific information
- 107 systems;
- 108
- 109 • Regardless of the physical location of User's workplace, e.g., telecommuting, User is subject to the
- 110 requirements of this Acceptable Use Acknowledgment;
- 111
- 112 • At termination of employment, User will not remove from Agency any information, hardware,
- 113 software, device, or any other workplace resource, without explicit written permission from Agency
- 114 executive management; and
- 115
- 116 • At termination of employment, User will return any and all Agency information, hardware, software,
- 117 device, or any other workplace resource to User's supervisor.
- 118

119 I have read, and understand, the above terms regarding use of Agency devices and systems, and access
 120 to non-public information created, used, and/or held by the Agency. I acknowledge my responsibilities
 121 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.

122 Employee Name:

123 Print

124 Signature

125 Date

126

127

128

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

130 Employee Name:

Print

Signature

Date