Written Information Security Policy ("WISP")

1. Purpose. The purpose of this WISP is to:

(a) Ensure the security, confidentiality, integrity, and availability of personal and other sensitive information the UCR Plan[1] collects, creates, uses, and maintains.

(b) Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

(c) Protect against unauthorized access to or use of UCR Plan-maintained Personal Information that could result in substantial harm or inconvenience to any individual.

(d) Define an information security program that is appropriate to the UCR Plan's size, scope, and business, its available resources, and the amount of Personal Information that the UCR Plan owns or maintains on behalf of others, while recognizing the need to protect information.

2. Scope. This WISP applies to all members of the Board of Directors of the UCR Plan and any other individuals with access to Personal Information acquired by the UCR Plan in the course of developing, implementing, and administering the UCR Agreement.[2] It applies to any records that contain Personal Information in any format and on any media, whether in electronic or paper form.

(a) For purposes of this WISP, "Personal Information" means either a US resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

(i) Social Security number;

(ii) Driver's license number, other government-issued identification number, including passport number, or tribal identification number;

(iii) Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial account; or

(iv) Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

[1] "Unified Carrier Registration Plan" or "UCR Plan" means the organization of State, Federal, and Industry representatives responsible for developing, implementing, and administering the UCR Agreement.
[2] "Unified Carrier Registration Agreement" or "UCR Agreement" or "UCRA" means the interstate agreement developed under the UCR Plan governing the collection and distribution of registration information and UCR fees paid by motor carriers, motor private carriers, brokers, freight forwarders, and leasing companies pursuant to 49 U.S.C. Section 14504a

(b) Personal Information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state, or local government records.

3. Information Security Coordinator. The UCR Plan has designated its Executive Director to implement, coordinate, and maintain this WISP (the "Information Security Coordinator"). The Information Security Coordinator shall work with the UCR Plan's Managed Security Services Provider, and shall be responsible for:

(a) Initial implementation of this WISP, including:

(i) Assessing internal and external risks to Personal Information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);

(ii) Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5);

(iii) Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect Personal Information (see Section 6);

(iv) Ensuring that the safeguards are implemented and maintained to protect Personal Information throughout the UCR Plan, where applicable (see Section 6);

(v) Overseeing service providers that access or maintain Personal Information on behalf of the UCR Plan (see Section 7);

(vi) Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8);

(vii) Defining and managing incident response procedures (see Section 9); and

(viii) Establishing and managing enforcement policies and procedures for this WISP, in collaboration with the UCR Plan human resources and management (see Section 10).

(b) Director, contractor, and (as applicable) employee and stakeholder training, including:

(i) Providing periodic training regarding this WISP, the UCR Plan's safeguards, and relevant information security policies and procedures for all directors, contractors, and (as applicable) employees and stakeholders who have or may have access to Personal Information;

(ii) Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation; and

(iii) Retaining training and acknowledgment records.

(c) Reviewing this WISP and the security measures defined here at least annually, or whenever there is a material change in the UCR Plan's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing Personal Information (see Section 11).

(d) Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or the UCR Plan's information security policies and procedures.

(e) Periodically reporting to the UCR Plan management regarding the status of the information security program and the UCR Plan's safeguards to protect Personal Information.

4. Risk Assessment. As a part of developing and implementing this WISP, the UCR Plan will conduct a periodic, documented risk assessment.

(a) The risk assessment shall:

(i) Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing Personal Information;

(ii) Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the Personal Information; and

(iii) Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

(A) Director, contractor, and (as applicable) employee and stakeholder training and management;

(B) Director, contractor, and (as applicable) employee and stakeholder compliance with this WISP and related policies and procedures;

(C) Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

(D) the UCR Plan's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

(b) Following each risk assessment, the UCR Plan will:

(i) Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;

(ii) Reasonably and appropriately address any identified gaps; and

(iii) Regularly monitor the effectiveness of the UCR Plan's safeguards, as specified in this WISP (see Section 8).

5. Information Security Policies and Procedures. As part of this WISP, the UCR Plan will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders to:

(a) Establish policies regarding:

(i) Information classification;

(ii) Information handling practices for Personal Information, including the storage, access, disposal, and external transfer or transportation of Personal Information;

(iii) User access management, including identification and authentication (using passwords or other appropriate means);

(iv) Encryption;

(v) Computer and network security;

(vi) Physical security;

(vii) Incident reporting and response;

(viii) Director and contractor use of technology; and

(ix) Information systems acquisition, development, operations, and maintenance.

(b) Detail the implementation and maintenance of the UCR Plan's administrative, technical, and physical safeguards (see Section 6).

6. Safeguards. The UCR Plan will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of Personal Information that the UCR Plan owns or maintains on behalf of others.

(a) Safeguards shall be appropriate to the UCR Plan's size, scope, and business, its available resources, and the amount of Personal Information that the UCR Plan owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

(b) The UCR Plan shall document its administrative, technical, and physical safeguards in the UCR Plan's information security policies and procedures (see Section 5).

(c) The UCR Plan's administrative safeguards shall include, at a minimum:

(i) Designating one or more directors to oversee the information security program (see Section 3);

(ii) Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 4);

(iii) Training directors in security program practices and procedures, with management oversight (see Section 3);

(iv) Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7); and

(v) Adjusting the information security program in light of business changes or new circumstances (see Section 11).

(d) The UCR Plan's technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

(i) Secure user authentication protocols, including:

(A) Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;

(B) Restricting access to active users and active user accounts only and preventing former directors or terminated contractors from accessing systems or records; and

(C) Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

(ii) Secure access control measures, including:

(A) Restricting access to records and files containing Personal Information to those with a need to know to perform their duties; and

(B) Assigning to each individual with computer or network access unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.

(iii) Encryption of all Personal Information traveling wirelessly or across public networks;

(iv) Encryption of all Personal Information stored on laptops or other portable or mobile devices;

(v) Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to Personal Information or other attacks or system failures;

(vi) Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) Personal Information; and

(vii) Reasonably current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

(e) The UCR Plan's physical safeguards shall, at a minimum, provide for:

(i) Defining and implementing reasonable physical security measures to protect areas where Personal Information may be accessed, including reasonably restricting physical access and storing records containing Personal Information in locked facilities, areas, or containers;

(ii) Preventing, detecting, and responding to intrusions or unauthorized access to Personal Information, including during or after data collection, transportation, or disposal; and

(iii) Secure disposal or destruction of Personal Information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

7. Service Provider Oversight. The UCR Plan will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain Personal Information on its behalf by:

(a) Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and the UCR Plan's obligations;

(b) Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and the UCR Plan's obligations; and

(c) Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and the UCR Plan's obligations.

8. Monitoring. The UCR Plan will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated

to prevent unauthorized access to or use of Personal Information. The UCR Plan shall reasonably and appropriately address any identified gaps.

9. Incident Response. The UCR Plan will establish and maintain policies and procedures regarding information security incident response (see Section 5). Such procedures shall include:

(a) Documenting the response to any security incident or event that involves a breach of security;

(b) Performing a post-incident review of events and actions taken; and

(c) Reasonably and appropriately addressing any identified gaps.

10. Enforcement. Violations of this WISP will result in disciplinary action, in accordance with the UCR Plan's information security policies and procedures.

11. Program Review. The UCR Plan will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in the UCR Plan's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing Personal Information. The UCR Plan shall retain documentation regarding any such program review, including any identified gaps and action plans.

12. Effective Date. This WISP is effective as of December 5, 2019.

(a) Revision History.

(i) Original publication: December 6, 2019.

(ii) No Subsequent Revisions