Incident Response Action Plan ("IRAP")

1. Purpose. The purpose of this cyber incident response action plan ("IRAP") is to provide a structured and systematic incident response process for all information security incidents (as defined in Section 4, Definitions) that affect any of the UCR Plan's[1] information technology ("IT") systems, network, or data, including the UCR Plan's data held or IT services provided by third-party vendors or other service providers. Specifically, the UCR Plan intends for this IRAP to:

(a) Define the UCR Plan's cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.

(b) Assist the UCR Plan and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents.

(c) Mitigate or minimize the effects of any information security incident on the UCR Plan, its registrants, employees, and others.

(d) Help the UCR Plan consistently document the actions it takes in response to information security incidents.

(e) Reduce overall risk exposure for the UCR Plan.

(f) Engage stakeholders and drive appropriate participation in resolving information security incidents while fostering continuous improvement in the UCR Plan's information security program and incident response process.

2. Scope. This IRAP applies to the Board of Directors of the UCR Plan and any other individuals with access to CONFIDENTIAL INFORMATION pursuant to the developing, implementing, and administering of the UCR Agreement[2] and the IT systems, network, data, and any computer systems or networks used in connection therewith.

3. Accountability. The UCR Plan has designated its Executive Director to implement and maintain this IRAP (the "Information Security Coordinator").

3.1 Information Security Coordinator Duties. Among other information security duties, as defined in the UCR Plan's written information security program ("WISP") available at *https://plan.ucr.gov/policy-resource-center/*, the Information Security Coordinator shall be responsible for:

[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

(a) Implementing this IRAP.

(b) Identifying the incident response team ("IRT") and any appropriate sub-teams to address specific information security incidents, or categories of information security incidents (see Section 5, Incident Response Team).

(c) Coordinating IRT activities, including developing, maintaining, and following appropriate procedures to respond to and document identified information security incidents (see Section 6, Incident Response Procedures).

(d) Conducting post-incident reviews to gather feedback on information security incident response procedures and address any identified gaps in security measures (see Section 6.7, Post-Incident Review).

(e) Providing training and conducting periodic exercises to promote employee and stakeholder preparedness and awareness of this IRAP (see Section 7, Plan Training and Testing).

(f) Reviewing this IRAP at least annually, or whenever there is a material change in the UCR Plan's business practices that may reasonably affect its cyber incident response procedures (see Section 8, Plan Review).

3.2 Enforcement. Violations of or actions contrary to this IRAP may result in disciplinary action, in accordance with the UCR Plan's information security policies and procedures.

4. Definitions. The terms defined below apply throughout this IRAP:

4.1 "Personal Information" - Personal information means individually identifiable information as defined in the UCR Plan's WISP, available at Section 2 of the UCR Plan Written Information Security Policy, that the UCR Plan owns, licenses, or maintains and that is from or about an individual including, but not limited to (a) first and last name; (b) home or other physical address, including street name and name of city or town; (c) email address or other online information, such as a user name and password; (d) telephone number; (e) government-issued identification or other number; (f) financial or payment card account number; (g) date of birth; and (h) health information, including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by the UCR Plan.

4.2 "Information Security Incident" - Information security incident means an actual or reasonably suspected (a) loss or theft of personal information; (b) unauthorized use, disclosure, acquisition of or access to, or other unauthorized processing of personal information that reasonably may compromise the privacy or confidentiality, integrity, or availability of personal information; or (c) unauthorized access to or use of, inability to access, loss or theft of, or malicious infection of the UCR Plan's IT systems or third party systems that reasonably may

compromise the privacy or confidentiality, integrity, or availability of personal information or the UCR Plan's operating environment or services.

5. Incident Response Team. The incident response team ("IRT") is a predetermined group of UCR Plan personnel and resources responsible for responding to information security incidents.

5.1 Role. The IRT provides timely, organized, informed, and effective response to information security incidents to (a) avoid loss of or damage to the UCR Plan's IT systems, network, and data; (b) minimize economic, reputational, or other harms to the UCR Plan, individuals, and partners; and (c) manage litigation, enforcement, and other risks.

5.2 Authority. Through this IRAP, the UCR Plan authorizes the IRT to take reasonable and appropriate steps necessary to mitigate and resolve information security incidents, in accordance with the escalation and notification procedures defined in this IRAP.

5.3 Responsibilities. The IRT is responsible for:

(a) Addressing information security incidents in a timely manner, according to this IRAP.

(b) Managing internal and external communications regarding information security incidents.

(c) Reporting its findings to the Board of Directors and to applicable authorities, as appropriate.

(d) Reprioritizing other work responsibilities to permit a timely response to information security incidents on notification.

5.4 IRT Roster. The IRT consists of a core team, led by the Information Security Coordinator, with representatives from the UCR Plan Board of Directors, management personnel and contractors. The current IRT roster includes the following individuals:

Executive Director	NRS Project Manager
Depository Manager	Chief Legal Officer

On an as needed basis:

Chair, Board of Directors	Chair, Registration System Subcommittee

(a) Sub-Teams and Additional Resources. The Information Security Coordinator assigns and coordinates the IRT for any specific information security incident according to incident characteristics and UCR Plan needs. The Information Security Coordinator may:

(i) Identify and maintain IRT sub-teams to address specific information security incidents, or categories of information security incidents and

(ii) Call on external individuals, including vendor, service provider, or other resources, to participate on specific-event IRTs, as necessary.

6. Incident Response Procedures. The UCR Plan shall develop, maintain, and follow incident response procedures as defined in this Section 6 to respond to and document identified information security incidents.

The UCR Plan recognizes that following initial escalation, the information security incident response process is often iterative, and the steps defined in Sections 6.3, Investigation and Analysis; 6.4, Containment, Remediation, and Recovery; 6.5, Evidence Preservation; and 6.6, Communications and Notification may overlap or the IRT may revisit prior steps to respond appropriately to a specific information security incident.

6.1 Detection and Discovery. The UCR Plan shall develop, implement, and maintain procedures to detect, discover, and assess potential information security incidents through automated means and individual reports.

(a) Automated Detection. The UCR Plan shall develop, implement, and maintain automated detection means and other technical safeguards as described in the UCR Plan's WISP available at Section 6 of the UCR Plan's Written Information Security Policy.

(b) Reports from Personnel or other internal sources. Personnel, or others authorized to access the UCR Plan's IT systems, network, or data, shall immediately report any actual or suspected information security incident to the Executive Director. Individuals should report any information security incident they discover or suspect immediately and must not engage in their own investigation or other activities unless authorized.

(c) Reports from External Sources. External sources who claim to have information regarding an actual or alleged information security incident should be directed to the Executive Director. Personnel who receive emails or other communications from external sources regarding information security incidents that may affect the UCR Plan or others, security vulnerabilities, or related issues shall immediately report those communications to the Executive Director and shall not interact with the source unless authorized.

(d) Assessing Potential Incidents. The UCR Plan shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. The UCR Plan shall document each identified information security incident.

6.2 Escalation. Following identification of an information security incident, the Information Security Coordinator, or a designate, shall perform an initial risk-based assessment and determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to the UCR Plan and others.

Based on the initial assessment, the Information Security Coordinator, or a designate, shall:

(a) IRT Activation. Notify and activate the IRT, or a sub-team, including any necessary external resources (see Section 5.4, IRT Roster).

(b) IRT Expectations. Set expectations for IRT member engagement.

(c) Initial Notifications. Notify the Board of Directors, and (if necessary) organizational leadership and any applicable business partners or service providers (see Section 6.6, Communications and Notifications).

6.3 Investigation and Analysis. On activation, the IRT shall collaborate to investigate each identified information security incident, analyze its affects, and formulate an appropriate response plan to contain, remediate, and recover from the incident.

6.4 Containment, Remediation, and Recovery. Next, the IRT shall direct execution of the response plan it formulates according to its incident investigation and analysis to contain, remediate, and recover from each identified information security incident, using appropriate internal and external resources (see Section 6.3, Investigation and Analysis).

The IRT shall document its response plans and the activities completed for each identified information security incident.

6.5 Evidence Preservation. The IRT shall direct appropriate internal or external resources to capture and preserve evidence related to each identified information security incident during investigation, analysis, and response activities (see Sections 6.3, Investigation and Analysis and 6.4, Containment, Remediation, and Recovery). The IRT shall seek counsel's advice, as needed, to establish appropriate evidence handling and preservation procedures and reasonably identify and protect evidence for specific information security incidents.

6.6 Communications and Notifications. For each identified information security incident, the IRT shall determine and direct appropriate internal and external communications and any required notifications. Only the IRT may authorize information security incident-related communications or notifications. The IRT shall seek counsel's advice to review communications and notifications targets, content, and protocols.

(a) Internal Communications. The IRT shall prepare and distribute any internal communications it deems appropriate to the characteristics and circumstances of each identified information security incident.

(i) Board of Directors. The IRT shall alert the Board of Directors to the incident and explain its potential impact on the UCR Plan and others as details become available.

(ii) General Awareness and Resources. As appropriate, the IRT shall explain the incident to the UCR Plan's personnel and other stakeholders and provide them with resources to appropriately direct questions from individuals, media, or others.

(b) External Communications. The IRT shall prepare and distribute any external communications it deems appropriate to the characteristics and circumstances of each identified information security incident.

(i) Public Statements. If the UCR Plan determines that external statements are necessary, the IRT shall provide consistent, reliable information to the media and public regarding the incident using the UCR Plan's website, press releases, or other means and ensure it coordinates with all other stakeholders that may be implicated in such statements.

(ii) Law Enforcement. The IRT shall report criminal activity or threats to applicable authorities, as the UCR Plan deems appropriate.

(c) Notifications. While the IRT may choose to authorize discretionary communications, certain laws, regulations, and contractual commitments may require the UCR Plan to notify various parties of some information security incidents. If applicable to a specific information security incident, after consultation with counsel, as required, the IRT shall:

(i) Authorities. Notify applicable regulators, law enforcement, or other authorities.

(ii) Affected Individuals. If an applicable breach of personal information occurs, prepare and distribute notifications to affected individuals.

(iii) Notify partners according to current agreements.

6.7 Post-Incident Review. Following each identified information security incident, the Information Security Coordinator, or a designate, shall reconvene the IRT, and others who participated in response to the incident, as appropriate, as a post-incident review team to assess the incident and the UCR Plan's response.

(a) Review Considerations. The post-incident review team shall consider the UCR Plan's effectiveness in detecting and responding to the incident and identify any gaps or opportunities for improvement. The post-incident review team shall also seek to identify one or more root causes for the incident and, according to risk, shall recommend appropriate actions to minimize the risks of recurrence.

(b) Report. The post-incident review team shall document its findings.

(c) Follow-Up Actions. The Information Security Coordinator shall monitor and coordinate completion of any follow-up actions identified by the post-incident review team, including

communicating its recommendations to and seeking necessary authorization or support from the UCR Plan Board of Directors.

7. Plan Training and Testing.

7.1 Training. The information security coordinator shall develop, maintain, and deliver training regarding this IRAP that periodically:

(a) Informs all employees, and others who have access to the UCR Plan's IT systems, network, or data, about the IRAP and how to recognize and report potential information security incidents.

(b) Educates IRT members on their duties and expectations for responding to information security incidents.

7.2 Testing. The information security coordinator shall coordinate exercises to test this IRAP periodically. The information security coordinator shall document test results, lessons learned, and feedback and address them in plan reviews (see Section 8, Plan Review).

8. Plan Review. The UCR Plan will review this IRAP at least annually, or whenever there is a material change in the UCR Plan's business practices that may reasonably affect its cyber incident response procedures. Plan reviews will also include feedback collected from post-incident reviews and training and testing exercises. The information security coordinator must approve any changes to this IRAP and is responsible for communicating changes to affected parties.

9. Effective Date. This IRAP is effective as of December 5, 2019.

9.1 Revision History.

(a) Original publication: December 6, 2019.

(b) No Subsequent Revisions