Biometric Data Security Rules

As stated in the Company's Information Governance Policy, the following Rules apply to all employees and departments of Union Pacific (including Union Pacific Corporation and its subsidiaries, collectively the "Company"). These Rules are incorporated into the Company's Information Governance Policy. Failure to comply may result in disciplinary action.

These Biometric Data Security Rules set forth guidance for the collection, storage, use, and destruction of biometric data. All Union Pacific employees must protect biometric data from unauthorized use or disclosure. If there is a conflict between these Rules and any applicable law, the applicable law controls.

1. Definitions: Biometrics is the measurement and analysis of unique physical characteristics of an individual, typically for the purpose of confirming the individual's identity. As used in these Rules, "biometric data" includes, but is not limited to, identifiers such as retina or iris scans, fingerprints, voiceprints, and hand or face geometry, and analysis based on these identifiers. "Biometric data" does not include demographic data, signatures, photos, telephone voice recordings, human biological samples used for scientific testing or screening, or basic physical descriptions, such as height, weight, and eye color.

2. Approval: Any proposed new use of biometric data must be specifically approved, as set forth in the Compliance and Reporting section of the Information Governance Policy. Contact the Compliance Management Team to begin the approval process.

3. Requirements: Before using biometric data in any new application, Union Pacific employees must: (i) inform all affected individuals in writing of the collection of biometric data and its purpose; (ii) obtain written consent from all affected individuals; and (iii) confirm that the use of biometric data will comply with these Rules. The Company maintains a standard consent form that addresses the first two requirements.

4. Use of Biometric Data: Biometric data shall only be collected and used for the limited purposes of performing background checks as required for certain security clearances or authorizations, and/or verifying identity in connection with timekeeping and/or access to Company facilities and computing systems. Any other proposed use of biometric data must be specifically approved, as set forth in the Compliance and Reporting section of the Information Governance Policy. Neither the Company nor its employees may sell, lease, trade, or disclose biometric data to third parties, except as required for technical support and consistent with applicable law.

5. Protecting Biometric Data: The Company must treat biometric data with the same care as other sensitive personal information, such as social security numbers. Disclosure of, and

access to, biometric data must be limited to persons who need it to conduct authorized business. Biometric data should be transmitted and stored in a secure manner, including the use of encryption, consistent with the Information Governance Policy's Information Security section.

6. Retention and Destruction of Biometric Data: Biometric data should be treated as a transient record (i.e., a record of short-term value not required for ongoing business activities). Unless subject to a legal hold or other specific legal requirement, biometric data must be permanently destroyed when its business purpose is satisfied, and within no more than three years after the Company's last interaction with the subject individual.

7. Availability of Rules: These Rules shall be made available to employees, contractors, and others in connection with the Company's request to collect and use biometric data. Additionally, these Rules shall be made available to members of the public upon written request.

8. Compliance: Failure to comply with these Rules may result in disciplinary action, up to and including termination. Failure to comply with these Rules also may result in serious penalties for the Company and the individuals involved. See the Compliance and Reporting section of the Information Governance Policy for more information.

Effective February 2019