Legal Service Provider Information Security Requirements

Information security protects information from unauthorized access or destruction to ensure its integrity, availability, and confidentiality. Union Pacific relies on its outside lawyers, law firms, and other legal service providers to protect the information they access, store, transmit, and create on behalf of Union Pacific.

The Union Pacific Law Department has established the following requirements for its legal service providers. These requirements are intended to clarify Union Pacific's expectations and supplement, rather than replace, other ethical or legal requirements.

You are required by the terms of your engagement to comply with Union Pacific's Information Security Addendum. Those requirements include, but are not limited to, the following:

1. Protect Union Pacific computer systems. Do not share your Union Pacific password. Request Union Pacific computer security credentials for other members of your team when necessary.

2. Ensure that any computer system on which you store non-public Union Pacific information is protected by antivirus software, and that operating systems and applications are maintained with current security patches.

3. Ensure that laptops, mobile phones, tablets, or other mobile devices on which you store non-public Union Pacific information are protected by encryption and password technology.

4. Carefully consider the security of any third-party or "cloud" storage. Consumer-grade cloud storage platforms (e.g., free version of Dropbox) generally are not appropriate for non-public Union Pacific information. Nor are such sites typically accessible to Union Pacific employees without special permission. Email and eFiles should be your primary means of sharing documents.

5. Protect non-public Union Pacific information stored or transmitted on removable media such as CDs, DVDs, flash drives, and external hard drives. Consider encrypted media or other secure transfer methods for production of information, especially if subject to a protective order.

6. Protect non-public Union Pacific information in paper form. Consider security and confidentiality when printing and transporting paper documents.

7. **Notify your managing/supervising attorney immediately if non-public Union Pacific information is lost, stolen, or accessed without authorization.** This includes reporting lost or stolen devices (e.g., laptops), paper documents, or computer credentials, and system breaches.

Additionally, you are required to comply with Union Pacific's policy concerning Artificial Intelligence (AI) in the legal landscape. Your firm must:

1. Execute a consent agreement with Union Pacific before using AI for services and work products provided to Union Pacific.
2. Provide and document attorney oversight and accountability for any AI contributions to those services and work product.
3. Notify the managing/supervising attorney of any use of AI in producing and generating legal services and work products for Union Pacific.
4. Prohibit the use of Union Pacific information in training AI models.
5. Ensure billable hours or fees reflect the actual time expended by human professionals.
6. Protect and maintain the confidentiality of Union Pacific data according to the latest standards of cyber security.
7. Immediately cease using AI tools upon Union Pacific revoking consent to use AI tools**.**

For additional information and best practices, Union Pacific encourages its legal services providers to review ABA Model Rule of Professional Conduct 1.6: Confidentiality of Information and the Sedona Conference Commentary on Privacy and Information Security. All questions related to this document should be directed to Blake Loper – Union Pacific Chief Privacy Officer @brloper@up.com.

UNION PACIFIC INFORMATION SECURITY ADDENDUM

A. Information Security Program – Your law firm (hereinafter, "Consultant") agrees and represents that it currently maintains information protection policies, procedures and practices ("Security Program") that comply with industry best practice and applicable Privacy and Security Requirements (as defined below) to (i) preserve the confidentiality, availability, integrity, and security of Railroad Information (as defined below) and, (ii) protect Union Pacific (hereinafter, "Railroad") systems that Consultant accesses or contacts.

"Railroad Information" includes the following, regardless of form or the media in which it is maintained, that may be disclosed to or accessed by Consultant in connection with or incidental to the performance of services for or on behalf of Railroad or by any other means:

1. Any information relating to an identified or identifiable individual irrespective of whether such individual is a Railroad customer, employee or other status (including, but not limited to, name, postal address, email address, telephone number, date of birth, Social Security number, driver's license number, other government-issued identification number, financial account number, credit or debit card number, insurance ID or account number, health or medical information, consumer reports, background checks, biometric data, digital signatures, any code or password that could be used to gain access to financial resources, or any other unique identifier);

2. Non-public business information; and

3. Any information marked "Private" or "Confidential" or defined as "Confidential Information" in the Agreement.

B. Minimum Requirements – Consultant's Security Program must include at a minimum:

1. A comprehensive, written Security Program that includes appropriate administrative, technical and physical safeguards and other security measures designed to ensure the confidentiality, availability, integrity, and security of Railroad Information.

2. A security design intended to prevent any compromise of its own information systems, computer networks or data by unauthorized users, viruses or malicious computer programs, including those that could in turn be propagated to Railroad.

3. Appropriate practices including, but not limited to, access controls including a process to authorize, establish, modify and terminate access; encryption of data; using and maintaining appropriate firewall and antivirus software; maintaining operating systems and other applications with up-to-date virus definitions and security patches so as to avoid any adverse impact to Railroad's systems or Information; appropriate logging and alerts to monitor access and to assure data integrity and confidentiality; intrusion detection systems; appropriate password management, including use of strong passwords and periodically changing passwords; installing and operating security mechanisms in a manner sufficient to ensure Railroad business operations are not disrupted; permitting only authorized users access to systems and applications; and preventing unauthorized access to Railroad's systems via the Consultant's networks and access credentials.

4. Physical access – Consultant represents and warrants that it has established and during the term it will at all times enforce: (i) physical protection mechanisms for all information assets and information technology to ensure such assets and technology are stored and protected in appropriate data centers

and/or locations; (ii) appropriate facility entry controls to limit physical access to systems that store or process data; and (iii) processes to ensure access to facilities are monitored and restricted to a "need to know" basis.

5. All persons with authorized access to Railroad Information must have a demonstrable genuine business need-to-know prior to access, supported by appropriate policies, protocols and controls to facilitate access authorization, establishment, modification and termination.

C. Training and Supervision - Consultant agrees that it maintains adequate training programs to ensure that its employees and any others acting on its behalf are aware of and adhere to its Security Program. Consultant must exercise necessary and appropriate supervision over its relevant employees and others acting on its behalf to maintain appropriate confidentiality, integrity, availability, and security of Railroad Information.

D. Data Incidents - **Consultant agrees to immediately notify Railroad's Response Management Communications Center (RMCC) by phone at 1-888-877-7267 of any reasonably suspected or actual loss of data or breach or compromise of its Security Program which has or may result in the loss or unauthorized access, disclosure, use or acquisition of Railroad Information** (including hard copy records) or otherwise presents a potential threat to any Railroad systems (all collectively a "Data Incident"). While the initial phone notice may be in summary form, a comprehensive written notice should be given within 48 hours to Rick Holmes, Chief Security Officer at rholmes@up.com, or at (402) 544-3106, and Lori Lentsch, Deputy Chief Security Officer, lalentsc@up.com, or at (402) 544-6022. The notice must summarize in reasonable detail the nature and scope of the Data Incident (including each data element type that relates to an individual, if any) and the corrective action already taken or to be taken by Consultant. The notice must be timely supplemented to the level of detail reasonably requested by Railroad, inclusive of relevant forensic reports. Consultant must promptly take all necessary and advisable corrective actions, and must cooperate fully with Railroad in all reasonable efforts to investigate the Data Incident, to mitigate the adverse effects, and to prevent its recurrence. Such cooperation must include responding to Railroad's inquiries about the Data Incident in a timely fashion. In the event of a Data Incident, Railroad's point of contact at Consultant is: _____, [title], phone: _____, email: _____.

Consultant acknowledges that it is solely responsible for the confidentiality and security of Railroad Information in its possession, custody or control, or for which Consultant is otherwise responsible. Consultant must hold Railroad harmless from any suspected or actual Data Incident or other compromise of Railroad Information while in Consultant's possession, custody or control, or for which Consultant is otherwise responsible. The Parties must collaborate on whether any notice is required to be given to any person, and if so, the content of that notice. Railroad must designate signatory to the notice. Consultant must bear all costs of the notice. If Railroad reasonably determines that the Data Incident is likely to have substantial adverse impact on Railroad's relationship with its customers or associates or otherwise substantially harm its reputation, Railroad may suspend the services provided by the Consultant under the Agreement to which this Addendum is appended or any other contract.

E. Third Parties - Consultant must not share, transfer, disclose or otherwise provide access to any Railroad Information or systems to any third party unless Railroad has authorized Consultant to do so in writing. If Railroad so approves, in writing, Consultant must ensure that any third party to which it provides access to Railroad Information is obligated to have a Security Program equivalent to that required of the Consultant (which includes all terms of this Information Security Addendum). Further, regarding any Data Incident, Consultant must contractually preserve for itself - or Railroad - all such rights as Railroad has in section D above. Regarding audit rights, Consultant must contractually preserve for itself - or Railroad - all such rights as Railroad has in section G below. Consultant must not share Railroad Information with any other third party without prior written approval or, if required to comply with legal process, only after

notice to Railroad. Consultant must only retain third Parties that are capable of performing the delegated obligations in accordance with this Information Security Addendum.

F. Ownership and Usage - Any Railroad Information, including in any reconfigured format, must at all times be and remain the sole property of Railroad, unless agreed otherwise in writing by Railroad. Any usage of Railroad Information is limited to the sole purpose expressly authorized by this Addendum or the Agreement to which it is appended.

G. Security Review and Audit -

1. Railroad's Information Technology or Audit Groups may conduct a security review of Railroad's engagement with Consultant when determined reasonably required by Railroad ("Security Review").

2. At Railroad's request, Consultant must provide Railroad copies of its data privacy and security policies and procedures that apply to Railroad Information. Consultant also may be asked, upon Railroad's reasonable request, to submit written responses to questions regarding its privacy and information security practices that apply to Railroad Information. Such responses must be submitted within ten (10) days of receipt.

3. Consultant must provide Railroad's Information Technology or Audit Groups an opportunity to conduct a privacy and security audit of Consultant's Security Program and systems and procedures. Such audit may be conducted on-site by Railroad personnel or Railroad's contracted third party assessors or through surveys and interviews, at the option of Railroad. Such audit may be conducted no more than once per year, or more frequently in the event of any Data Incident. When an on-site audit is conducted, Railroad must provide Consultant with reasonable advance notice of not less than 15 days, except in the event of a Data Incident or if Railroad has a reasonable basis to believe Consultant may not be in compliance with this Addendum, in which case advance notice must be not less than 48 hours.

4. In the event Consultant has any security audits or reviews of its own systems, performed by Consultant or a third party, including vulnerability and penetration assessments, it must give Railroad notice of any current findings that are likely to adversely impact Railroad Information or systems, such as in the form of a written summary of the findings, and must keep Railroad timely informed of its remediation efforts.

H. Compliance - Consultant must comply with (i) all applicable legal requirements (federal, state, local and international laws, rules and regulations and governmental requirements) currently in effect and as they become effective, relating in any way to the privacy, confidentiality, integrity, availability, or security of Railroad Information, that includes, but is not limited to, the California Consumer Privacy Act; (ii) all applicable industry standards concerning privacy, data protection, confidentiality, integrity, availability, or security of information, and any other similar standards; (iii) applicable policies, statements or notices that are provided to Consultant in writing; and (iv) controls required by the Information Technology or Audit Groups Review, including secure coding standards, if applicable (collectively referred to as "Privacy and Security Requirements"). In addition, Consultant must take any actions necessary to ensure Railroad's compliance with applicable legal requirements, including, but not limited to, the deletion of personal information, and promptly providing to Railroad (in no case more than seven (7) days) the necessary information and or data to respond to a legal obligation.

I. Mobility and Transfer of Data -

1. Railroad Information that is classified as Private Data or Confidential Data must not be stored, transported or kept on a laptop or any other mobile device or storage media, including USB, "thumb drives," DVDs, CDs, unless encrypted using an encryption methodology approved in writing by Railroad. All electronic data transfers of Railroad Information classified as Private Data or Confidential Data must be

via secure FTP or other Railroad-approved protocol and/or in Railroad-approved encrypted form. Any physical removal or transfer of Railroad Information classified as Private Data or Confidential Data from Railroad's or Consultant's facilities must be conducted only according to controls developed or approved by Railroad's Information Technology or Audit Groups.

2. Consultant may not transfer individually identifiable information about a natural person out of the jurisdiction where it is presently located without Railroad's prior written approval.

J. Notice of Process - In the event Consultant receives a governmental or other regulatory request for, or legal process requesting, any Railroad Information, it agrees to immediately notify Railroad's Legal Department in order that Railroad may have the option to defend such action. Consultant must reasonably cooperate with Railroad in such defense.

K. Security Certification - Consultant must maintain a level of security certification or assessment consistent with best practices and by a qualified third party reasonably acceptable to Railroad. Such certifications must be provided to Railroad as reasonably requested by Railroad.

L. Segregation - Consultant warrants that all Railroad Information is maintained so as to preserve logical segregation of Railroad's Information from data of others, but especially any Railroad competitor.

M. Secure Return or Disposition; Termination of Access; Survival - Consultant must return or dispose of Railroad Information in its possession, custody or control: (i) if no longer needed for Railroad's business or legal purposes or upon termination of the Agreement to which this Addendum is appended, whichever is longer or (ii) upon Railroad's direction which may be given at any time. Notwithstanding the foregoing, Consultant must be permitted to retain Railroad Information for a longer period if such retention is strictly necessary to meet Consultant's legal compliance obligations, is done pursuant to Consultant's fully implemented and documented records management program, and is limited to the minimum Railroad Information and minimum retention period needed to meet these obligations. Any disposal must ensure that Railroad Information is rendered permanently unreadable and unrecoverable. Upon reasonable notice and if requested by Railroad, Consultant must provide Railroad with a certification by an officer attesting to Consultant's compliance with this section. To the extent Consultant accesses or has contact with Railroad's information systems, Consultant must ensure that such access is discontinued upon termination of the Agreement. The provisions of this Addendum survive until such time as Consultant has fully complied with the provisions of this section.

N. Location of Railroad Information – Unless otherwise authorized by Railroad in writing, Consultant must not transfer, transmit, share, maintain, store, or authorize any of the foregoing, any Railroad Information outside of the United States.

O. Prohibition Against Sale of Railroad Information -- Consultant shall not: (i) sell (or, effective January 1, 2023, share) Railroad Information as the terms sell and share are defined under Privacy Laws (as defined below); (ii) retain, use, or disclose UP Data for any purpose other than for the specific purpose of performing the Services; (iii) retain, use, or disclose Railroad Information for a commercial purpose other than providing the Services; (iv) retain, use, or disclose Railroad Information outside of the direct business relationship between Consultant and UP; or (e) effective January 1, 2023, combine Railroad Information that Consultant receives with personal information Consultant receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that Consultant may combine such information to perform any business purpose as that term is defined under Privacy Laws. Consultant certifies that it understands the restrictions in this paragraph and will comply with them. As used herein, "**Privacy Laws**" means any applicable privacy or data protection laws or regulations, including, without limitation the California Consumer Privacy Act of 2018 California Civil Code § 1798.100 et seq. ("California Consumer Privacy Act" or "CCPA"), the California Privacy Rights Act ("CPRA"), the

Virginia Consumer Data Protection Act ("CDPA"), and other analogous federal, state, or local privacy, data protection, information security, or related laws or regulations.

P. Cyber Liability Coverage: Consultant must, at its own cost and expense, obtain and maintain during the Term of this Agreement, and for a period of two (2) years following expiration or termination, Cyber Liability Coverage with a limit of not less than $5,000,000 each occurrence and an aggregate limit of not less than $5,000,000. Coverage includes, but not limited to, providing protection against liability for system attacks, loss of service attacks, spread of malicious software code, crisis management and customer notification expenses, and liability arising from the loss or disclosure of confidential data.

Q. Artificial Intelligence –

1. Consultant acknowledges and agrees that neither Consultant, nor any of its authorized subcontractors, employees, analysts, agents, consultants or representative may utilize Robotic Process Automation ("RPA"), Artificial Intelligence ("AI") or any other similar automation tools, software, technology or processes (hereinafter collectively referred to as "Automation Processes") to access, interface with, or use Railroad Information, without Railroad's express prior written consent. Railroad reserves the right to revoke the authorization to utilize any Automation Processes. Consultant shall be fully responsible for acts, services and functions performed by such Automation Processes to the same extent as if such acts, services and functions were performed by Consultant employees, and for purposes of this Addendum such acts, services and functions will be deemed work performed by Consultant. Consultant will remain fully liable for any and all use of such Automation Processes and shall indemnify and hold Railroad harmless from and against any and all claims, suits, actions, proceedings (formal and informal), investigations, judgments, deficiencies, damages, settlements, and liabilities, arising out of, based upon or in connection with any use of the Automation Processes.

2. To the extent Railroad agrees to permit Consultant to utilize Automation Processes, Consultant shall: (i) employ industry best practice encryption techniques for information stored on, accessed on or transmitted to or from the Automation Processes (at a minimum Consultant's encryption processes for "data at rest" and "data in transit" shall comply with the NIST Special Publication 800-111 standards); (ii) provide for and implement at a minimum, industry standard, security procedures, which will be subject to Railroad's audit and review, for all facilities (including equipment, software and network) used to transfer, transmit or access Railroad Information; (iii) ensure Automation Processes operate strictly in accordance with the terms and conditions set forth in this Addendum; (iv) not use Railroad Information to train, develop or tune generative AI models and/or functionality; and (v) upon the earlier to occur, expiration or termination of this Addendum or Railroad revoking its consent to use of the Automation Processes, immediately terminate the ability of the Automation Processes to access Railroad Information. Railroad's revocation of its consent to use the Automation Processes is effective immediately upon delivery of notice to Consultant.