TABLE OF CONTENTS

1. STATEMENT OF PURPOSE

Pioneer **N**atural **R**esources USA, Inc. (PNR) respects the individual, community, and environment. PNR is committed to protecting the environment from damage and protecting its employees and those who work in or live near its areas of operations from injury and health risks.

PNR Technology Solutions Department is committed to the continual development and maintenance of relevant systems to maintain the highest standard of service including, but not limited to, those outlined below.

- Governance
- Security
- Service Management
- Business Continuity

As part of its business operations, PNR and its affiliates acquire, develop, secure, and maintain computers, software networks, security solutions, mobile devices, and operational technology systems. These resources include, but are not limited to, those outlined below.

- Tangible property in the form of hardware
- Intellectual property in the form of software, data, and other proprietary business or technical information of value
- PNR email system
- Internet access through PNR network(s)

These resources are intended for business related purposes, including direct and indirect support of PNR oil and gas exploration and production missions and administrative functions.

This policy applies to all users of PNR computing resources, whether a PNR employee or not, and to all uses of those resources, whether on PNR premises or remote locations. Additional documentation may govern computing resources provided or operated by specific affiliates of, or departments within PNR.

The right to use PNR computing resources comes with responsibilities, is limited, and is subject to the requirements of legal and ethical behavior.

This policy and subsequent PNR Standards and Best Practices will generally align to information security management systems standards published by the **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) and the **C**ybersecurity and **I**nfrastructure **S**ecurity **A**gency (CISA), as more specifically set forth in the Cyber Security Framework.

Verbal forms necessary to express provisions within this document are specified as being 'must' (requirement), 'should' (recommendation), 'may' (permission), and 'can' (possibility and capability). These terms are defined as listed below.

- **Must** used to indicate that a provision is mandatory.
- **Should** used to indicate that a provision is not mandatory, but recommended as good practice.
- **May** used to indicate that a provision is optional.
- **Can** used for statements of possibility or capability.

This document does not supersede any federal, state, or local laws or regulations.

In case of conflict between documents, notify PNR and clarification will be issued.

This document will be reviewed regularly, or every **3yr**, to ensure content and terms are current and representative of corporate and industry best practices.

2. POLICY STATEMENT

2.1 Users must not allow unauthorized persons to use the computer or password assigned to them by PNR without authorization from the Technology Solutions Department.

2.2 Users must not deliberately attempt to circumvent data protection or other security measures or to gain unauthorized access to or block others from access to the PNR computer network system.

2.3 Users must not install or use any software (including software downloaded from the internet) on the computer assigned to them by PNR except as authorized by employee leadership and the Technology Solutions Department.

2.4 Users must not copy any software or digital proprietary data, whether belonging to PNR or to a third party, without authorization from the Technology Solutions Department.

2.5 Remote access users are responsible for ensuring adherence to all PNR Security Standards and Procedures.

2.6 Illegal activities, and use of remote access for business interests other than those of PNR, are strictly prohibited.

2.7 All PNR employees must handle information in accordance with its defined classification.

2.8 Additional legal or regulatory protection measures may be prescribed for specific types of information (i.e., PII and HIPAA).

2.9 PNR employees must not publicly disclose internal PNR information via posting to any website, including blogs, newsgroups, chat groups, and social networking sites.

- Responses to specific customer electronic mail messages are exempt from this policy.

2.10 If a corporate computing resource is lost or stolen, users must report the loss to Technology Solutions Department as soon as possible.

2.11 Users must not travel with corporate computing resources to countries designed as 'Level 4: Do Not Travel' by the United States Department of State.

- The current list of travel advisories is available at the URL below. https://travelmaps.state.gov/TSGMap/

2.12 Users must not connect external storage devices to a corporate computing resource unless received from or approved by Technology Solutions and such devices must not have been connected to any non-Pioneer resources.

2.13 Any violation of this policy may result in disciplinary action up to and including termination of employment.

3. APPROVALS

Approval signatures below indicate that signatories have read, fully understand, and endorse this document and its contents.

/s/	10/10/2022
Signature	*Date*
Stephanie Stewart **VP, Chief Information Officer**	

/s/	10/10/2022
Signature	*Date*
Ron Schindler **VP, Legal & Chief Compliance Officer**	

/s/	10/10/2022
Signature	*Date*
Caroline Braich **Associate General Counsel**	