IT1

Category: Information Technology

INFORMATION SYSTEMS ACCEPTABLE USE POLICY

I. PURPOSE

This policy provides useful tips and techniques to promote effective use of Pioneer Community Energy's (Pioneer) (agency) Information Systems. It applies to all agency systems located on or accessed from Pioneer property and systems provided by Pioneer for use in agency business.

II. DEFINITIONS

"Agency Business" shall mean carrying out the responsibilities and duties of the office or position held by the employee.

"Employee" or "Staff" shall mean those individuals who are employed for a salary or wage by Pioneer, not including members of the Board of Directors or individuals working under a contract for services unless specifically identified in said contract.

"Information Systems" shall mean an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.

III. Background

Information systems are a growing and important resource for staff, one that can provide critical competitive advantage to Pioneer in the form of information gathering, improved external communications, and increased customer responsiveness. As more and more of our staff use Information Systems to connect with our customers, suppliers and other key organizations, it is important that staff understand and agree on the appropriate procedures to protect Pioneer's assets.

Adopted: July 15, 2021
Resolution 2021-29

IV. Scope

This policy applies to all staff that have access to Pioneer's Information Resources.

V. POLICY

Pioneer utilizes sophisticated computer and communications systems to assist staff in performing their job functions. These technologies support Pioneer business activities by enabling closer, more effective and timely communications among personnel within Pioneer and with customers, partners and vendors. These guidelines advise all users regarding the access to and the disclosure of Information Systems. These guidelines establish Pioneer's expectations for all staff concerning the disclosure of information via agency Information Systems.

Pioneer maintains and uses many facilities, equipment, and communication systems, such as telephones, regular mail, special delivery services, E-mail, voice mail, fax machines, computers, etc., designed to make Pioneer's operations effective and efficient. Pioneer's Information Systems are provided to staff at agency expense to assist staff in carrying out day to day operations. Some of these systems permit staff to communicate with each other internally and with other parties externally. As with all agency assets, Pioneer's Information Systems are for official agency business only. Access to Pioneer's Information Systems is provided in conjunction with official agency business and individual job responsibilities. Use of Pioneer's Information Systems is subject to these policies and guidelines and other relevant policies and procedures.

A. Information Access, Content, and Use

Pioneer makes every effort to provide its staff with the best technology available to conduct Pioneer's official business. Pioneer

has installed, at substantial expense, Information Resources to conduct its official business.

This document addresses general Information Systems policies and guidelines, specific issues related to appropriate content, and staff use of Pioneer's Information Systems. All departments and staff are required to follow these general policies and guidelines. All staff with access to Pioneer's Information Systems are required to read, understand and comply with agency policies.

Pioneer's Information Systems are owned by Pioneer and are to be used for business purposes only in serving the interests of our customers and in the course of normal business operations.

The use of agency facilities, property, equipment, or communication systems is limited to Acceptable Use as defined in these policies and guidelines. Agency equipment and communications systems, including all hardware and software, may only be removed from Pioneer property as required to complete job duties and with authorization from Pioneer Management. Authorization could be in the form of a Supervisor approved telecommute schedule.

Personal equipment, including all computer hardware and software, may not be used for Pioneer's official business without prior Executive Director consent. Staff are not to use Pioneer's equipment to reach personal sites unless it is for business purposes, as determined solely by Pioneer management.

Pioneer encourages the use of Pioneer's Information Systems for business when such business can be accomplished consistent with approved policies. When using Information Systems, staff shall conduct official Pioneer business consistent with the approved policies. Official agency business shall comply with standards for integrity, accountability, and legal sufficiency. Thus, official agency business conducted via the Internet should meet or exceed the

standards of performance for traditional methods (e.g. meetings, use of telephone). Alternative meetings should be held only on well-known meeting/conference call platforms that maintain the security of Pioneer Information Systems. It is the responsibility of staff to ensure these meetings are held on adequate network systems, as to avoid meeting disruption and possible miscommunication.

Staff shall base decisions to use Pioneer's Information Systems on sound business practices. The conduct of business using Pioneer's Information Systems is particularly compelling where costs are reduced and/or the services provided by Pioneer are improved in measurable ways. When using Pioneer's Information Systems, staff shall promote and maintain a professional image.

Staff shall disseminate information that is current, accurate, complete, and consistent with Pioneer's policy. Information released via Pioneer's Information Systems is subject to the same official agency policies for the release of information, such as public records requests, via other media (such as printed documents). Information accuracy is particularly important.

Staff shall protect confidential and proprietary information entrusted to Pioneer. Questions regarding confidential or proprietary information should be directed to Pioneer's management or his/her designee.

B. PROTECTING CONFIDENTIAL INFORMATION

Maintaining the confidentiality of sensitive information is crucial to Pioneer's success. Confidential information stored on or carried over Pioneer's Information Systems could become the subject of accidental or intentional interception, mis-delivery, hacking or even unauthorized internal review unless staff take the necessary precautions outlined in this policy.

Pioneer has developed specific procedures to ensure the protection of confidential information. Staff should exercise care when communicating any potentially confidential information outside of Pioneer, as all electronic communication may be vulnerable to being compromised.

Some directories in Pioneer's Information Systems contain sensitive or confidential data. Access to these directories is restricted. Unauthorized attempts to circumvent such access restrictions are violations of this Policy and may result in disciplinary action, up to and including termination of employment, and legal action.

Staff will respect the privacy of individuals who send them messages. Staff should protect voice mail, and E-mail accounts from unauthorized access. Appropriate protection procedures include ensuring proper password protection to these accounts, closing E-mail messages after reading them and deleting all messages when they are no longer needed.

Staff shall not place Pioneer material (e.g., internal correspondence) on any publicly accessible Internet computer without prior permission.

The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet is at risk of detection by a third-party. Staff must password protect or encrypt when transferring such material in any form.

C. COPYRIGHTED INFORMATION

Pioneer respects the intellectual property rights of other companies and individuals. Use of all copyrighted material, including literature, software, and graphics shall comply with relevant, valid license terms. Pioneer's Information Systems may provide access to materials protected by copyright, trademark, patent and trade secret and even export laws. Staff should not assume that merely

because information is available on an electronic information system such as the Internet, that it may be downloaded or further disseminated. No copyrighted material should be copied, transmitted, posted, or otherwise distributed without such compliance. If a question arises as to the propriety of downloading information, Pioneer's management should be consulted.

Pioneer licenses to use software is carefully set forth in legal agreements that Pioneer has with the developers and distributors of the software. Staff's use of software must follow those agreements. If Pioneer gives staff the opportunity to use certain software, copying of that software is strictly prohibited. Loading of software of a personal interest is prohibited unless staff are given prior express consent by Pioneer management. All Pioneer owned software, licenses, data and media will remain with Pioneer and access removed for terminated employees.

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, staff members are prohibited from downloading software and/or modifying any such files without permission from the copyright holder and Pioneer's IT department.

D. PRIVACY STATEMENT

Staff are to follow this policy in the performance of their duties. It is also intended to place staff on notice that staff should not expect Pioneer's Information Systems and their contents, to be confidential or private. All data, including any that is stored or printed as a document, is subject to audit and review.

No staff member has a reasonable expectation of personal privacy with respect to the use of any of Pioneer's facilities, property, equipment or communications systems. This includes anything created or received on Pioneer Information Systems even if used

for business purposes and in the normal course of business operations.

Pioneer reserves the right, but not the obligation, to monitor use of Pioneer's Information Systems including the Internet, E-mail, computer transmissions, and electronically stored information created or received by staff with Pioneer's Information Systems. All computer applications, programs, work-related information created or stored by staff on Pioneer's Information Systems, are Pioneer property.

E. Monitoring and Inspecting Information Systems

Pioneer's Information Systems are provided for official business. Pioneer's Information Systems are owned and controlled by Pioneer and are always accessible by Pioneer for maintenance, upgrades and other business or legal purposes.

All Information Systems, including the messages and data stored on the systems, are always and will remain the property of Pioneer, subject to applicable third-party intellectual property rights such as copyrights. By continued employment and use of Pioneer systems, all staff are considered to have consented to monitoring and other access by authorized agency personnel. Pioneer reserves the right to inspect a staff member's computer system for violations of Pioneer policies.

Pioneer reserves the right to access and conduct an inspection or search all directories, indices, files, databases, faxes, Pioneer computer hardware and software, voice mail, E-mail and communication systems or deliveries sent or received to any agency location, and other Information Resources no matter to whom it is addressed, with no prior notice. Pioneer may also cancel or restrict any staff's privilege to use any or all its facilities, equipment, property, or communication systems.

If a staff member refuses to cooperate with a search or inspection for business purposes that is based on reasonable suspicion that the staff is in possession of prohibited materials, Pioneer may take that refusal into consideration in determining appropriate disciplinary action. Discipline, including termination, will be based on all available information, including the information giving rise to the inspection or search.

Access to on-line services, the Internet, blogs, social media sites, or other communications networks is prohibited for personal use unless Pioneer has provided prior express consent. As such, no agency equipment, telephone lines, or on-line services may be used to view or download offensive, discriminatory or pornographic material. Employee use of these services may be monitored to include numbers called and the amount of time spent using the services. Pioneer reserves the right to inspect computer systems for viruses, offensive, discriminatory or pornographic material, personal software, etc.

Pioneer management may examine staff communications or files and such examination should be expected to occur in various circumstances, including, but not limited to:

- Ensuring that Pioneer systems are not being used to transmit discriminatory, harassing or offensive messages of any kind.
- Determining the presence of illegal material or unlicensed software.
- Ensuring that communication tools are not being used for unauthorized, disruptive, or improper uses.
- Investigating allegations or indications of impropriety.
- Locating, accessing and/or retrieving information in staff absence.
- Examine searches in response to Public Information Records requests.

- Responding to legal proceedings and court orders in the preservation or production of evidence.
- Pioneer reserves the right to review staff use of and to inspect all material created by or stored on Pioneer Information Systems. Pioneer reserves the right to monitor all use of Information Systems to access, review, copy, delete, or disclose messages and data derived from any use. All messages or data become property of Pioneer, subject to access, review, duplication, deletion, or disclosure by Pioneer management or by other personnel authorized by Pioneer. Staff should be aware that billing practices, firewall protections, and traffic flow monitoring programs often maintain detailed audit logs setting forth addresses, times, durations, etc. of communications both within and external to Pioneer. Staff should treat Pioneer's Systems with the expectation that communications will be available for review by authorized personnel of Pioneer at any time.

Pioneer reserves the right to access, review, duplicate, delete or disclose any communications, messages or data derived from use of Pioneer Information Systems.

F. Storing and Archiving Information

Pioneer has developed specific archival procedures to ensure the safe retention of electronic data. Most files are subject to routine back-up procedures. Copies of documents and electronic messages may be retained for long periods of time. By various archival practices employed by Pioneer, any messages or data stored, even temporarily, on Pioneer Information Systems may be copied to magnetic, cloud, or other storage without the specific knowledge of the individual creating the messages or data. Such archives are and remain agency property and may be used by Pioneer for any purpose. Simply deleting messages or data from these Information Systems does not provide privacy about such messages or data. Staff may be required to preserve their electronic data based on

pending litigation and/or investigations by Pioneer and adherence to State Statutes for record retention. Refer to the **Data Retention Policy** for more information on storing and archiving information.

G. Employee Usage

Each staff member has the responsibility of complying with Pioneer's policies provided in this document. Failure to do so may result in disciplinary action, up to and including termination of employment and legal action.

The use of Information Systems is restricted to official agency business. Personal use of or time spent for personal gain is strictly prohibited unless Pioneer gives prior express consent. Inappropriate personal use includes the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited. In addition, any Internet use that could cause congestion, disruption of normal service, or general additional agency expense is prohibited.

Hacking or unauthorized attempts or entry into any other computer is forbidden. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited. The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.

Staff should be aware that Pioneer's Information Systems and the World Wide Web are not censored and contain information some users may find offensive. Pioneer cannot accept responsibility for what the staff accesses. However, if offensive material is accessed, staff shall disengage from the material immediately.

Staff shall not copy or transfer electronic files without prior permission. Almost all software is subject to Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to the staff. When in doubt, consult Pioneer management. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on Pioneer Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights.

Downloading a file from the Internet can infect Pioneer's systems with malware. Staff shall not circumvent or disable standard virus prevention software and/or Information Resource security mechanisms.

Staff shall not send post or provide access to any confidential Company materials or information to anyone outside Pioneer.

Staff are obligated to cooperate with any investigation regarding the use of staff computer equipment and which Pioneer management has authorized.

Alternate Internet Service Provider connections to Pioneer's internal network are not permitted unless prior express consent has been given by the Executive Director or the IT department and properly protected by a firewall or other appropriate security device(s).

Pioneer has no control or responsibility for content on an external server not under the control of Pioneer. Information may be offensive and/or unsuitable for dissemination.

Staff should regularly save and/or archive any files staff wish to save.

Staff using Company accounts are acting as representatives of Pioneer. As such, staff should act accordingly so as not to damage the reputation of Pioneer.

H. Information Systems Awareness

The proper use of Pioneer Information Systems is the responsibility of each staff member. The practices listed below are not inclusive, but rather designed to remind each staff of the need to raise their Information Systems awareness.

- Protect equipment. Keep it in a secure environment and attempt to keep food and drink from electronic systems.
- Know where the fire suppression equipment is located and how to use it in an emergency.
- Protect areas. Keep unauthorized people away from equipment and data. Challenge strangers in the area.
- Protect passwords. Never write it down or give it to anyone. Don't use names, numbers or dates that are personally identified with the staff. Change the password immediately if it has been compromised. For more information see the **Password Policy**.
- Protect files. Don't allow unauthorized access to staff files and data. Never leave equipment unattended with the password activated – log off.
- Report security violations. Staff should tell their supervisor or management if staff see any unauthorized changes to staff data. Immediately report any loss of data or programs, whether automated or hard copy.

I. Electronic Mail (E-mail) and Etiquette

E-mail may be sent through each staff's computer. E-mail will be sent for official agency business only. No personal E-mail shall be sent or received via Pioneer Internet accounts.

Pioneer staff should not attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading. Management reserves the right, but not the obligation, to access all E-mail files created, received or stored on agency-funded systems and such files can be accessed without prior notification.

Pioneer staff are expected to maintain their E-mail accounts on a regular basis. This entails organizing emails into folders and deleting unnecessary emails from a long email chain.

E-mail requires extensive network capacity. Sending unnecessary E-mail, or not exercising constraint when sending very large files, or sending to many recipients consumes network resources that are needed for critical official agency business. When Pioneer grants an individual staff access to the network, it is the responsibility of staff to be cognizant and respectful of network resources.

E-mail users are to exercise good judgment and common sense when creating and distributing messages. E-mail is the property of Pioneer and is to be used exclusively for official agency business. No staff E-mail is considered private. Similarly, the accessing, reading or copying of E-mail not intended for a staff member's eyes is prohibited. staff are strictly prohibited from sending E-mail messages of a harassing, intimidating, offensive or discriminatory nature. Anonymous messages are not to be sent. Staff are prohibited from using aliases while connected to services. Pioneer retains the right to access a staff member's E-mail at any time for any reason without notice to the staff. Conduct in violation of this policy will subject staff to disciplinary procedures.

E-mail on the internet is not secure. Never include in an E-mail message anything private and confidential. E-mail is sent unencrypted and is easily read. If anything, but non-confidential

information is required to be sent in an E-mail, consult the IT department for alternatives.

State the subject of the message in the subject line.

Include a signature (an identifier that automatically appends to the E-mail message) that contains the method(s) by which others can contact staff (usually staff's E-mail address, phone number, faxes number, etc.).

Watch punctuation and spelling. It can reflect on staff's professionalism. Use automatic spell-checking programs.

Be careful when sending replies - make sure staff is sending to a group when intent is to send to a group and to an individual when staff intent is to send to an individual. It is best to address directly to a sender(s). Check carefully, the "To" and "From" before sending mail. It can prevent unintentional errors.

Never send angry messages. If staff receives and email that seems rude or insensitive, do not overreact, but instead remain professional in all communication. Remember that not everyone is polite. **DO NOT SEND MESSAGES ALL IN CAPITALS**. It looks like shouting. Use initial capitals or some other symbol for emphasis. For example: That IS what I meant. That *is* what I meant.

Please keep messages to the point without appearing terse or rude. It is good practice to re-read electronic correspondence before sending. Remember, it can be difficult to interpret tone through written communication and may require another staff members review.

The use of Information Systems should be consistent with Pioneer's core values when communicating with both staff and external

parties. Particularly, the values of honesty, integrity and mutual respect should govern staff's use of Information Systems. When using voice mail and E-mail systems for communicating with other individuals over Information Systems, staff should consider the following principles:

- Be courteous - Refrain from saying anything electronically that you would not say to the recipient face-to-face.
- Keep messages brief - Include only one topic per message and start the main point in the first sentence.
- Proofread messages - E-mail messages drafted in haste can be difficult to follow and easy to misinterpret. Do not ignore the basics of writing in E-mail correspondence.
- Use a descriptive subject line - When using E-mail, never leave a subject line blank. Remember to use brief but informative message headers.
- Properly prioritize - Do not overstate the urgency of the message simply to get attention. "Urgent" designations should be limited to messages that require immediate response from the recipient.
- Send messages only to appropriate individuals - Send E-mail on a need-to-know basis only. Unnecessary messaging should be avoided as it decreases the effectiveness of Pioneer systems.
- Identify the message sender - No E-mail or other electronic communication may be sent which attempts to hide the identity of the sender or represent the sender as someone else or from another organization.
- Be careful not to use "Reply all" unless you intend all other recipients to receive your response.
- Think before forwarding messages - Think of the sender's intentions before forwarding private communications.

J. Securing Information Systems With Passwords

Prior express consent for Information Systems access must be obtained through Pioneer management. Staff of contractors shall

only be given access to the network after written communication and approval by Pioneer management. Once Pioneer provides prior express consent, staff shall be responsible for the security of their account password and will be held responsible for all use or misuse of his or her account. No other password or security device shall be used without approval by Pioneer management.

Pioneer Information System's require staff to set and change their password. Guidelines for choosing and setting passwords should be obtained from the **Password Policy**. Periodic password changes keep undetected intruders from continuously using the password of a user. After logging on, the computer will attribute all activity to a staff member's user id. Therefore, never leave workstations without logging off -- even for a few minutes. Always log off or otherwise inactivate the workstation so no one could perform any activity under staff's user id when away from the area. staff should safeguard sensitive information from disclosure to others.

Staff must maintain secure passwords and never use an account assigned to another user.

Pioneer reserves the right to override the user's password and other security features when it has a need to do so. Should a time come when staff terminates, or at any other appropriate time, Pioneer will replace staff's password with another of Pioneer's choosing.

K. Protecting Information Systems From Malware

Pioneer provides malware protection software to help safeguard Information Systems. These systems are not foolproof. As such, be particularly cautious when opening any E-mail with an attachment.

Staff shall not disable or remove anti-virus software. Malware can infect executable files, disk boot sectors, documents, etc. If malware is received from a sender, that sender should be notified

that the file was infected and if possible, the type of virus should be identified.

L. Encrypting Data

Only Pioneer authorized encryption tools (both software and hardware) may be used in connection with Information Systems. Except with the prior written consent of management, all encryption tools must permit Pioneer to access and recover all encrypted information.

M. Securing Mobile Computing Devices

Staff who use agency mobile computing resources (laptops, handheld devices, etc.) must take adequate precautions to ensure that proprietary information contained in such devices is secure and not available to third parties, particularly during travel. Staff are responsible for taking adequate precautions against theft of their mobile computing devices.

N. Acceptable Use

- Authorized Use. The authorized use of Pioneer systems is limited to official agency business. Pioneer provides Information Systems and communication tools to facilitate business communication and enhance productivity. Pioneer reserves the right to prohibit or restrict use of agency systems for any other purpose and at any time.
- Incidental Personal Use. Personal use of Pioneer systems is permitted so long as it is not excessive as determined by Pioneer, does not interfere with job performance, consume significant resources, or interfere with the activities of other staff.

O. Unacceptable Use

- Unauthorized Use. Excessive personal and other use of Information Systems inconsistent with this or any other

Pioneer policy is unauthorized. Under no circumstances are Pioneer's Information Systems to be used for personal financial gain or to solicit others for activities unrelated to official agency business, such as solicitations for personal, political, or religious causes. Installation of software without approval from management is unauthorized.

- Disruptive Use. Use that may reasonably be considered offensive or disruptive to any individual or organization, or to harmony within the workplace is prohibited. Such disruptive use includes, but is not limited to, transmission, retrieval, storage, or display of defamatory, obscene, offensive, politically motivated, slanderous, harassing, or illegal data, or messages that disclose personal information without authorization. Grossly indiscriminate or "broad band" distribution of E-mail would clearly constitute a disruptive use.
- Prohibited use. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights. When in doubt about the existence or scope of a license or about appropriate use of copyrighted, patented, or otherwise proprietary third-party data or software code, staff should contact management. Staff are expressly prohibited from using Pioneer's Information Systems to store or access pornography.

Only the IT Department and other approved persons are authorized to install software on servers, storage, and other related Information Resources.

VI. ENFORCEMENT

Any staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VII. DISTRIBUTION

This policy is to be distributed to all Pioneer staff who use Information Resources.