IT7

Category: Information Technology

REMOTE ACCESS POLICY

I. PURPOSE

This policy applies to all Pioneer Staff with a computer used to connect to the Pioneer's network from a remote location. This policy applies to remote access connections used to conduct official Pioneer business, including reading or sending e-mail and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to, high speed Internet connectivity, Virtual Private Network (VPN), Secure Shell (SSH), Microsoft Azure and other cloud-based systems, and other forms of electronic connectivity to Information Systems.

II. SCOPE

This policy applies to all Staff that access Pioneer's Information Systems from a remote location.

III. DEFINITIONS

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

IV. POLICY

Staff shall contact the IT Department for approved methods to remotely connect to Pioneer's Information Systems. Staff shall review Pioneer's Securing Information Systems Policy for details on protecting information when accessing the corporate network via remote access methods. Staff shall review the Information Systems Acceptable Use Policy for the acceptable use of the Company's Information Systems.

It is the responsibility of Staff with remote access privileges to Pioneer's Information Systems to ensure that their remote access connection is given the same consideration as the user's on-site connection.

Adopted: January 20, 2022
Resolution 2022-1

Secure remote access is strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases. For information on creating a strong password/phrase see the Password Policy. At no time should any Pioneer Staff member disclose their login or e-mail password to anyone.

When accessing Pioneer's Information Resources from a remote location, Staff shall ensure:

- Pioneer's policies and procedures are followed.
- Friends and relatives do not have access to Pioneer's systems and assets.
- Staff do not connect to other networks (excluding the Internet, an in-house personal network, or a secure WIFI network) at the same time they are connected to Pioneer's systems.
- Only Pioneer e-mail accounts are used for business related communications.
- All computers, mobile devices, etc. use up-to-date anti-malware software and an activated firewall (if available). Please refer to the Anti-Malware Policy for more information.

Staff who wish to implement non-standard remote access solutions to Pioneer Information Systems must obtain prior written approval from the Executive Director.

V. ENFORCEMENT

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

VI. DISTRIBUTION

This policy is to be distributed to all Pioneer staff.