Agency Wide Policy and Procedure

SECTION:	**Workplace Practice**	**ATTACHMENTS:**	**None**
SUBJECT:	**Use of Computers, Laptops and Electronic Equipment**	**APPROVAL DATE:**	**11/2020**
POLICY NUMBER: 2.08		**REVISION DATE:**	**10/2021, 2/2024**

Purpose: To provide employees with guidelines for appropriate use of First Resources laptops and computers.

Policy: All First Resources business must be done on First Resource's equipment to ensure compliance with privacy expectations; staff who have used personal phones/computers for FRC business have voluntarily designated their equipment as FRC's property and agree to the equipment being checked for policy violation.

The use of First Resources Corp.'s computers, laptops, networks, fax machines, electronic mail, and all forms of Internet access (collectively referred to as "automation systems") is for First Resources Corp. business and is to be used for authorized purposes only. Brief and occasional personal use of the automation systems is acceptable if it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense for First Resources Corp.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities.

All computer, electronic and telephonic documents and communications transmitted by, received from, or stored in First Resources Corp.'s equipment are the property of First Resources Corp. Employees are not to transmit material on First Resources Corp.'s equipment in violation of any state or federal law or government regulation. Employees do not use their company email for personal business.

Employees will not use code, access a computer or electronic file, retrieve any stored communication, or download any online document or software without authorization of the IT department or a supervisor. All pass codes are the property of First Resources Corp.

Employees using company computers away from First Resources Corp.'s premises are to use caution to protect their computers and the content of their computers from damage or theft. Because of the risk of theft of computers and files, employees are not to store on their computers hard drive away from First Resources Corp.'s premises sensitive or confidential information, or information that could be used by others to damage the Employer's interests.

Because of the risk of importing viruses into First Resources Corp.'s computer equipment or network, employees are not to import to First Resources Corp.'s computer equipment hard drives files or documents that are created outside of First Resources Corp.'s premises until the document or file is first scanned for viruses by the computer's anti-virus program.

The IT Department will assign all employees a temporary password or code to use when they are initially assigned computers, email, and the Internet in performing their job duties. Employees will immediately be prompted to change passwords at initial login in all appropriate applications. Employees are not to share their password or codes with anyone. From time to time, employees may be prompted to change their passwords automatically, or on a case-by-case basis. In the event this occurs, the employee will be required to initiate this change, or lose access to the system in which there is the prompt.

The IT department will assign employees who are issued a company telephone a passcode for the device. Employees are not to share the passcode with anyone. Employees will not be permitted to change the passcode assigned by the IT department.

An employee's computer file and electronic and telephonic communications are not private, and the Employer may inspect or monitor them at any time, at First Resources Corp.'s discretion.

All First Resources Corp. employees will follow the policies of the agency to keep the network secure and safe. Private Health Information will be sent via encrypted emails to external and third parties.

Employees who violate this policy may be disciplined, up to and including termination.

The IT department will be responsible to collect equipment from staff, clean files off computers and redirect equipment to other programs. All USB drives and hard drives of all laptops, desktops and servers will be "sanitized" using a software program designed to destroy all data without the possibility of recovery, before being either disposed of or sold.