

Agency Wide Policy and Procedure

SECTION: Compliance
SUBJECT: Usage and Security of Electronics
POLICY NUMBER: 7.15

ATTACHMENT:
APPROVAL DATE: 1/2025
REVISION DATE: 11/25

Policy: First Resources Corp will ensure systems and processes are in place to secure electronic equipment and to maximize cyber security.

Procedures:

Systems Access:

1. First Resources Corp staff have access to various software programs and systems.
2. Staff are designated to oversee certain programs/systems. System access roles are as follows:

Software/Program	Primary Staff	Back Up
ISolved	HR Administrator	CHRO
Credible EHR	Accounting Specialist	Credible Help Group
Staff Portal	Digital Marketing Specialist	Marketing Director QA Auditor (someone will need to notify of the need)
Share Point/One Drive Emails Folder Access	IT Technician IT Technician IT Technician	CFO/Access CFO/CHRO CFO/Access
IMPA	CFO	COO Director of Compliance
Cell Phones	IT Technician	COO/CFO
True Link	Office Assistant	Director of Compliance COO
IBHRS Portal	Billing Specialist	CFO
Waystar	Billing Specialist	CFO
MCO Portals	Billing Specialist	CFO
Relias	HR Trainer	CHRO
Personalized Accessibility Programs (ie Dragons)	IT Technician	CHRO
Gateway Entrance Code	IT Technician	Director of Maintenance

3. Emails will be sent to the DLemployeechanges@firstresources.us email when a person is being hired. The designated staff will set the person up in the system.

4. Emails will be sent to the DLemployeechanges@firstresources.us when a person is terminated. The designated staff will immediately shut off access to systems to ensure data is secure.
5. Emails will be sent to DLemployeechanges@firstresources.us for transfers, promotions, or demotions. The designated staff will review and change access as needed.

Agency Cell Phones

1. Agency Cell Phones will be distributed to staff whose positions require staff to have a cell phone for agency emails, on-call responsibilities, client pictures, direct client contact, etc.
2. Requests for cell phones will be approved by the COO and CFO.
3. The IT department will distribute cell phones to the employee/supervisor. Staff must set up their voice mail.
4. The IT Department will maintain an inventory of all cell phones, who they are assigned to and passwords.
5. The IT Department/COO will maintain a cell phone directory.
6. The IT Department will approve any apps that are added to company cell phones.
7. Upon termination of the employee, the cell phone is returned to the IT Department for redistribution. The cell phone # will remain with the position when appropriate.

Agency Computers

1. The IT Department will maintain an inventory of all agency computers and equipment.
2. Multifactor Authentication (MFA) is utilized to secure access to the system.
3. Other systems are to be accessed only after staff has logged into their First Resources Corp Microsoft 365 system.
4. Single Sign On (SSO) is utilized to secure the payroll and client electronic health records systems.
5. Computers will be programmed to automatically lock a user out after 5 failed log in attempts.
6. Requests for computers and IT equipment will be processed through the IT Ticket system. It is approved by the IT Department, CFO and COO as needed.
7. Upon notification of a staff needing a computer, the IT Department will:
 - a. Set up a Microsoft One Drive account for the staff.
 - b. Give permissions to necessary folders
 - c. Set up an email account and add applicable email groups or DL lists.
8. Upon notification of a staff termination, the designated staff will immediately deactivate access to Microsoft One Drive.