DEPARTMENT: Information Systems	**POLICY NUMBER: 0012**
DISTRIBUTION: All Staff	**EFFECTIVE DATE:**
SUBJECT: User Account Control Policy	**REVISION DATE:**

POLICY:

User accounts allowing access to Equinox Inc. private network will be issued to employees at the discretion of the Supervisor as required to complete job duties. Additionally, the Information Technology (IT) Department will facilitate access to 3rd party applications (*i.e.*, _____, and any other applications owned by a 3rd party) required to complete job duties.

PROCEDURE:

Person(s) Responsible:	**Procedures:**
Supervisors	1. Submit electronic form to request new user accounts or to revoke existing user accounts. Submit an email to the Help Desk to request changes to existing accounts. Periodically review accounts to make sure necessary and appropriate access is in place, employees are maintaining confidential passwords and taking care to keep information confidential. Employees should have the minimum access necessary to complete job duties. Notify the tech@equinoxinc.org email immediately upon separation of an employee, or when appropriate for any change in job responsibilities.
Information Technology (IT) Department	2. Issue a confidential username and password and provide access to requested network resources. Facilitate access to, and end user support within, 3rd party applications as directed by 3rd party application policies. Comply with any responsibilities or requirements of 3rd party application agreements. Disable user accounts as requested by supervisor, upon receiving employee separation documentation, or as otherwise directed by supervisors, or the Corporate Compliance Officer, or at the discretion of the Coordinator of IT. See **User**

Person(s) Responsible:	Procedures:
	Separation or Change of Duties Checklist attached. Report password or account sharing to Program Director for follow up.
All Employees	3. Maintain confidential passwords for all named user accounts assigned to you, including changing passwords at least every three (3) months or whenever you believe someone has learned your password. Refer to employee handbook for appropriate use of network and 3rd party accounts.
Program Directors/Designee	4. Address any incidents of password or account sharing with the user directly and instruct IT Department to re-enable account when appropriate.