Information Security Policy

Version Number: ISP.v1a.23.5.01

Last Updated April 28, 2022

YieldRock Micro-Credit
45 10TH Avenue, Accra Ghana
+233 342 290 962; +233 303 935351
info@yieldrockgh.com

Table of Contents

Introduction 4

Purpose 4
Scope 4
Network Connectivity 5

Dial-up numbers shall be unlisted. 5
Dial Out Connections 5
Telecommunication Equipment 5
Permanent Connections 6
Emphasis on Security in Third Party Contracts 6
Firewalls 7
Malicious Code: 8

Antivirus Software Installation 8
New Software Distribution 8
Retention of Ownership 9
Encryption 10

Definition 10
Encryption Key 10
Installation of authentication and encryption certificates on the e-mail system 10
Use of WinZip encrypted and zipped e-mail 10
File Transfer Protocol (FTP) 11
Secure Socket Layer (SSL) Web Interface 11
Telecommuting 12

General Requirements 12
Required Equipment 13
Hardware Security Protections 13
Data Security Protection 14
Disposal of Paper and/or External Media 15
Disposal of External Media / Hardware 16

Disposal of External Media 16
Requirements Regarding Equipment 16
Disposition of Excess Equipment 16

Updates to Document

Date	User	Section	Content	Version
05/02/2023		All	Policy and Procedures	v1.0

YieldRock Micro-credit Enterprise	**Policy and Procedure**
Title: INTRODUCTION	**P&P #:** IS-1.0
Approval Date:	**Review: Annual**
Effective Date:	**Information Technology**

Introduction

Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at YieldRock Micro-credit Enterprise, hereinafter, referred to as YieldRock. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within YieldRock with policies and guidelines concerning the acceptable use of YieldRock technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all YieldRock employees or temporary workers at all locations and by contractors working with YieldRock as subcontractors.

Scope

This policy document defines common security requirements for all YieldRock personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of YieldRock, entities in the private sector, in cases where YieldRock has a legal, contractual or fiduciary duty to protect said resources while in YieldRock custody. In the event of a conflict, the more restrictive measures apply. This policy covers YieldRock network system which is comprised of various hardware, software, communication equipment and other devices designed to assist YieldRock in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any YieldRock domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by YieldRock at its office locations or at remote locales.

YieldRock Micro-credit Enterprise[1]	**Policy and Procedure**
Title: NETWORK CONNECTIVITY	**P&P #:** IS-1.3
Approval Date:	**Review: Annual**
Effective Date:	**Information Technology**

Network Connectivity

Access to YieldRock information resources through modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialing without passing through the access control system is prohibited.**

Dial-up numbers shall be unlisted.

Systems that allow public access to host computers, including mission-critical servers, warrant additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a department head with the submission of the Network Access Form and the approval of the Privacy Officer or appropriate personnel.

Dial Out Connections

YieldRock provides a link to an Internet Service Provider. If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the Privacy Officer or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place

Telecommunication Equipment

Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the Privacy Officer or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

- phone lines
- fax lines
- calling cards

- phone head sets
- software type phones installed on workstations
- conference calling contracts
- cell phones
- Blackberry type devices
- call routing software
- call reporting software
- phone system administration equipment
- T1/Network lines
- long distance lines
- 800 lines
- local phone lines
- PRI circuits
- telephone equipment

Permanent Connections

The security of YieldRock systems can be jeopardized from third party locations if security YieldRock's and resources are inadequate. When there is a need to connect to a third-party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of YieldRock systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

Emphasis on Security in Third Party Contracts

Access to YieldRock computer systems or corporate networks should not be granted until a review of the following concerns has been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of YieldRock Information Security Policy have been reviewed and considered.
- Policies and standards established in YieldRock information security program have been enforced.

- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the Business Associate Agreement.
- A description of each service to be made available.

- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to YieldRock computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.

- Because annual confidentiality training is required under the regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

Firewalls

Authority from the Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a YieldRock router or firewall.

YieldRock Micro-credit Enterprise[1] **Policy and Procedure**	
Title: MALICIOUS CODE	**P&P #:** IS-1.4
Approval Date:	**Review: Annual**
Effective Date:	**Information Technology**

Malicious Code:

Antivirus Software Installation

Antivirus software is installed on all YieldRock personal computers and servers. Virus update patterns are updated daily on YieldRock servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration - The antivirus software currently implemented by YieldRock is McAfee VirusScan Enterprise. Updates are received directly from McAfee which is scheduled daily at 5:00 PM.

Remote Deployment Configuration - Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

Monitoring/Reporting – A record of virus patterns for all workstations and servers on YieldRock network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

New Software Distribution

Only software created by YieldRock application staff, if applicable, or software approved by the Privacy Officer or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained in Appendix C. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on YieldRock computers and networks. These precautions include determining that the software does not, because of faulty design, "misbehave" and interfere with or damage YieldRock hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a YieldRock computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate YieldRock personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a YieldRock computer or network.

Computers shall never be "booted" from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not "bootable".

Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of YieldRock are the property of YieldRock unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging YieldRock ownership at the time of employment. Nothing contained herein applies to software purchased by YieldRock employees at their own expense.

Encryption

Definition

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text*;* encrypted data is referred to as cipher text**.**

Encryption Key

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, YieldRock shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. YieldRock employs several methods of secure data transmission.

Installation of authentication and encryption certificates on the e-mail system

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user by contacting the Privacy Officer or appropriate personnel. Once verified, the certificate is installed on each recipient workstation, and the two may safely exchange secure e-mail.

Use of WinZip encrypted and zipped e-mail

This software allows YieldRock personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any YieldRock staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

File Transfer Protocol (FTP)

Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

Secure Socket Layer (SSL) Web Interface

Any system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form (found in Appendix A) and have appropriate approval from the supervisor or department head as well as the Privacy Officer or appropriate personnel before any access is granted.

Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. YieldRock considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of YieldRock office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to YieldRock network from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to YieldRock's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as customer data to risks not present in the traditional work environment.

General Requirements

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

- **Need to Know:** Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
- **Password Use:** The use of a strong password, changed at least every 90 days[27], is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

Required Equipment

Employees approved for telecommuting must understand that YieldRock will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

YieldRock Provided:

YieldRock supplied workstation.

A cable lock to secure the workstation to a fixed object.

If using VPN, a YieldRock issued hardware firewall is required.

If printing, a YieldRock supplied printer.

If approved by your supervisor, a YieldRock supplied phone.

Employee Provided:

Broadband connection and fees,

Paper shredder,

Secure office environment isolated from visitors and family,

A lockable file cabinet or safe to secure documents when away from the home office.

Hardware Security Protections

Virus Protection: Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all YieldRock personal computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.

VPN and Firewall Use: Established procedures must be rigidly followed when accessing YieldRock information of any type. YieldRock requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.

Security Locks: Use security cable locks for laptops at all times, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock Screens: No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be

protected by or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 15[29] minutes of inactivity.

Data Security Protection

Data Backup: Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established or if you have external media that is not encrypted, contact the appropriate YieldRock personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to YieldRock: Transferring of data to YieldRock requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to YieldRock.

External System Access: If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-YieldRock Networks: Extreme care must be taken when connecting YieldRock equipment to a home or hotel network. Although YieldRock actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, YieldRock has no ability to monitor or control the security procedures on non-YieldRock networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of customer level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces. If your laptop has not been set up with an encrypted work space, contact the Privacy Officer or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or customer level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside YieldRock: All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any customer level information to anyone outside YieldRock without the written approval of your supervisor.

Disposal of Paper and/or External Media

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-YieldRock work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- External media must be wiped clean of all data. The Privacy Officer or appropriate personnel has very definitive procedures for doing this – so all external media must be sent to them.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

YieldRock Micro-credit Enterprise **Policy and Procedure**	
Title: DISPOSAL OF EXTERNAL MEDIA / HARDWARE	**P&P #:** IS-1.10
Approval Date:	**Review: Annual**
Effective Date:	**Information Technology**

Disposal of External Media / Hardware

Disposal of External Media

It must be assumed that any external media in the possession of an employee is likely to contain either protected health information ("PHI") or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

Disposition of Excess Equipment

As the older YieldRock computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.