Acknowledgements

This document and proposal was prepared by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee. The current sitting members of this committee are as follows:

Scott Gentry, Kenergy, Project Chairman and acting Vice President of the KAEC IT Association
Jonathan Grove, Cumberland Valley Electric Inc., acting President of the KAEC IT Association
Jim Petreshock, Owen Electric, acting Secretary of the KAEC IT Association
David Cox, Nolin Rural Electric Cooperative Corporation
Gregg Brown, CISSP, Jackson Purchase Energy Corporation
Tony Miller, Kenergy
Eddie McNutt, East Kentucky Power Cooperative
Bob Tegge, East Kentucky Power Cooperative
George H. Walker, Technical Research Analyst, National Rural Electric Cooperatives Association

These documents are provided for illustrative purposes only and may not be suitable for the individual needs of your company. The end user agrees to hold harmless the Kentucky Association of Electric Cooperatives IT Association from any claims arising out of misuse or the inappropriate use of these documents.
# Table of Contents

INTRODUCTION ......................................................................................................................... 1

INFORMATION & CYBER SECURITY POLICY ............................................................................... 3

IT RISK MANAGEMENT ................................................................................................................. 6

THIRD PARTY ACCESS .................................................................................................................. 8

OUTSOURCED INFORMATION PROCESSING ............................................................................... 12

ACCOUNTABILITY OF ASSETS ..................................................................................................... 15

PERSONNEL SECURITY ............................................................................................................... 18

PHYSICAL AND ENVIRONMENTAL SECURITY ....................................................................... 23

DOCUMENTATION PROCEDURES ............................................................................................... 27

SYSTEM PATCHING ..................................................................................................................... 30

INCIDENT MANAGEMENT ........................................................................................................... 33

SYSTEM LOGGING AND MONITORING ....................................................................................... 36

SYSTEM ACCEPTANCE AND CONFIGURATION ....................................................................... 39

MALWARE PREVENTION ............................................................................................................. 42

BACKUP AND RECOVERY ............................................................................................................ 46

NETWORK MANAGEMENT ........................................................................................................... 51

USER ACCOUNT MANAGEMENT ................................................................................................. 59

PASSWORD POLICY ...................................................................................................................... 63

REMOTE ACCESS ......................................................................................................................... 67

WIRELESS ACCESS ....................................................................................................................... 70

BUSINESS CONTINUITY AND DISASTER RECOVERY ................................................................ 73

COMPLIANCE REQUIREMENTS ................................................................................................... 76

ENCryption ................................................................................................................................... 79

ACCEPTABLE USE ....................................................................................................................... 82

EMAIL USE ................................................................................................................................... 88

INTERNET ACCESS ..................................................................................................................... 93

APPENDIX A: EXAMPLE BACKUP POLICY .............................................................................. 97

APPENDIX B: FINANCIAL SECURITY CHECK EXAMPLES ............................................................ 99

APPENDIX C: GENERAL PASSWORD CONSTRUCTION GUIDELINES ......................................... 100

APPENDIX D: ANTI-VIRUS AND MALWARE EXEMPTION FORM ................................................ 101

APPENDIX E: NETWORK MANAGEMENT EXEMPTION FORM .................................................. 102

Page ii
Introduction

The KAEC IT Association established the Cybersecurity Subcommittee specifically to address the concerns raised by the Kentucky Public Service Commission (KPSC) resulting from the final report of the “Cyber Security Risk Assessment & Risk Mitigation Plan Review” presented to the KPSC in December 2013. It quickly became apparent to the committee that addressing the specific concerns of the PSC would not be possible without a general consensus of what an up-to-date end-to-end cybersecurity plan for a cooperative should look like. With this in mind the Committee sat as its mission the creation of a “cybersecurity plan in a box”, that is to say, the production of document templates that provide a toolkit for all the state’s cooperatives to create, maintain, and verify a cybersecurity program that address industry standards and regulations as well as the concerns of the KPSC.

Each policy in this document is intended to be customized to fit the individual cooperative. With this in mind, the language has been kept deliberately generic. Every cooperative is encouraged to read and review each policy for possible adoption. Each policy includes sections that should be customized to fit that cooperative.

While the format of this template provides for an overarching policy at the board level and following individual policies set at the level of the CEO or Senior Management, the committee recognizes that this would not be appropriate for all cooperatives that might make use of this document.

How to Use This Document:

The template document is intended to be generic and easily customizable by the individual cooperatives.

<Cooperative Name> is used as a place holder in each policy for the legal name and/or identifier for the cooperative that is normally used in the cooperative’s policies.

<Person or Group Responsible for policy at Cooperative> is used as a place holder in each policy for the name or title of the member of management or department that is responsible for that policy. These persons or groups can be different for each policy if the cooperative so desires.

Because modern technology is subject to rapid change, and because social, cultural, and legal standards and expectations regarding technology are ever evolving, it is not possible for these policies to address every possible situation which might develop. Nonetheless, the philosophy, principles and procedures of these policies shall be used whenever possible to guide the development of, the compliance with, and the administration and enforcement of all matters relating to the effective acquisition and utilization of technology.

The term technology is intended to be defined broadly and includes all:

A. Electronic hardware, software, and services, including but not limited to desktops, laptops, rugged computers, tablets, workstations, monitors, printers, plotters, faxes, scanners, multifunction print devices, PDAs, smartphones, Blackberry devices, cellular phones, satellite phones, wireless broadband cards, pagers, servers, PBX equipment, telecommunications equipment, circuits, switches, routers, storage devices, recording devices, digital cameras, email,
Cyber Security Policy Framework

B. text messaging, instant messaging, Internet, firmware, operation systems, software, business applications, Software as a Service ("SaaS") applications, peripherals used in conjunction with the devices and software listed above, and all other electronic devices or software used to run software or create, record, store, transmit and/or received video, voice or data;

C. Electronic information, including but not limited to email addresses, phone numbers, IP addresses, email messages, text messages, instant messages, word processor documents, spreadsheets, presentations, drawings, images, photos, videos, music, voice, databases, application data, and all other electronic data; and

D. Electronic communications, including but not limited to voice, email, text messages, instant messages, voice messages, internet postings, facsimiles, and all other forms of electronic communications.
Information & Cyber Security Policy

1. Overview/Purpose

<Cooperative Name> Directors recognize the need to protect <Cooperative Name>, our members, and both cooperative and member data, and systems, from growing information and cybersecurity threats. This policy establishes an Information & Cyber Security Program within <Cooperative Name> to ensure adequate measures are taken and controls are in place to mitigate threats and protect those company resources.

[Explanatory Note: This policy draft is intended for establishment of an overall Information Security Program at the Board level with Policy and Procedure management handled at the executive staff/IT Management level. It should be noted that Information Security is not solely an Information Technology concern but touches all departments, all employees, and all types of informational transactions. This may be or may not be the hierarchy necessary at a particular cooperative and should be modified as needed.]

The purpose of this policy is to ensure that <Cooperative Name> technology assets are protected against all internal, external, deliberate and accidental threats. Information, in all its forms, written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorized modification, or destruction throughout its life cycle. Policies and Procedures are established and shall be administered to protect cooperative technology systems and data, member financial and protected information, and cooperative data acquisition and control systems across the enterprise.

[Explanatory Note: This policy draft is intended for establishment of an overall Information Security Program at and not just a Cyber Security program.]

2. Scope

All employees, contractors, consultants, temporary and other workers at <Cooperative Name> and its subsidiaries must adhere to all policies and procedures authorized and approved under this program. This applies to cooperative data sets and technology equipment that is owned, operated, or leased by <Cooperative Name>. The Information & Cyber Security Policies describe the technology and information assets that must be protected and identifies many of the threats to those assets. The equipment, software, and storage medium used to process, store, and transmit information will be protected by appropriate controls.

3. Policy

3.1. The Policies and procedures will ensure that:

3.1.1. Sensitive, protected, and/or privileged Information and technology systems will be safeguarded against any unauthorized access;
3.1.2. Confidentiality of sensitive, protected, and/or privileged information will be assured;
3.1.3. Integrity of information will be maintained;
3.1.4. Availability of information for business purposes will be maintained;
3.1.5. Legislative and regulatory requirements will be met;
3.1.6. Business continuity and disaster recovery plans will be developed, maintained and tested annually.

[Explanatory note: Cooperatives should feel free to alter this policy statement to include specific requirements within the cooperative and testing schedule they deem appropriate.]

3.1.7. All <Cooperative Name> employees will be provided information security and awareness training on a regular basis;
3.1.8. Any actual or suspected information security breaches will be reported to the designated <person or group responsible for policy at Cooperative>. All breaches will be investigated thoroughly and logged;

3.2. Policies and Procedures have been established to support this program, including appropriate controls and continuity plans.

3.3. Business requirements for availability of information systems will be met.

4. Compliance

4.1. Compliance Measurement

4.1.1. The designated <person or group responsible for policy at Cooperative> is responsible for maintaining the supporting Policies, Procedures and Controls and aiding managers in ensuring adherence to them.
4.1.2. Compliance with this Information & Cyber Security Program Policy is mandatory.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes

- Establishes a formal program to address the Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 14 of the accompanying PowerPoint presentation.

6. Definition of Terms

None.
7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<insert title of approver>

Date

<insert title of approver>

Date

<insert title of approver>

Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IT Risk Management

1. Overview/Purpose

To empower <person or group responsible for policy at Cooperative> to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2. Scope

Risk assessments (“RAs”) can be conducted on any entity within <Cooperative Name> or any outside entity that has signed a Third Party Agreement with <Cooperative Name>. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3. Policy

The execution, development and implementation of remediation programs is the responsibility of <person or group responsible for policy at Cooperative> and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Risk Assessment Team in the development of a remediation plan.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes

- Addresses Section 4.1 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 13 of the accompanying PowerPoint presentation.
6. Definition of Terms

None.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

_________________________________________________________ Date
<insert title of approver>

_________________________________________________________ Date
<insert title of approver>

_________________________________________________________ Date
<insert title of approver>

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Page 7
Third Party Access

1. Overview/Purpose

This policy covers third-parties such as software providers, hardware technical support personnel, or any other outside personnel who have a need to access cooperative-owned IT equipment in order to provide a service.

The purpose of this policy is to define standards for connecting to <Cooperative Name> networks from any host. These standards are designed to minimize the potential exposure to <Cooperative Name> from damages which may result from unauthorized use of <Cooperative Name> resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

2. Scope

This policy applies to all <Cooperative Name> contractors, vendors and agents with a <Cooperative Name> owned or personally owned computer or workstation used to connect to the <Cooperative Name> network. This policy applies to remote access connections used to do work on behalf of <Cooperative Name>, including reading or sending email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to VPN, SSH, or other means.

3. Policy

3.1. General Requirements

It is the responsibility of <Cooperative Name> contractors, vendors and agents with remote access privileges to <Cooperative Name>'s cooperative network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Cooperative Name>. General access to the Internet via <Cooperative Name>'s network for recreational use, or unrelated outside business interests, is not permitted. The <Cooperative Name> contractor, vendor and/or agent individually bears responsibility (as does the individual’s employer) for the consequences should the access be misused. Please review the following policies for details of protecting information when accessing the cooperative network via remote access methods, and acceptable use of <Cooperative Name>'s network:

- Acceptable Encryption Policy
- Wireless Communications Policy
- Acceptable Use Policy
3.2. Requirements

3.2.1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.

3.2.2. At no time should any <Cooperative Name> employee provide their login or email password to anyone, not even family members.

3.2.3. <Cooperative Name> contractors, vendors, or agents with remote access privileges to <Cooperative Name>‘s network must not use non-Cooperative email accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct <Cooperative Name> business, thereby ensuring that official business is never confused with personal business.

3.2.4. Reconfiguration of <Cooperative Name>’s equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

3.2.5. Third party connections must comply with requirements as stated in the Third Party Agreement.  **NOTE: Not included as part of this package.**

3.2.6. Personal equipment that is used to connect to <Cooperative Name>‘s networks must meet the requirements of <Cooperative Name>-owned equipment for remote access.

3.2.7. Organizations or individuals who wish to implement non-standard Remote Access solutions to the <Cooperative Name> production network must obtain prior approval from <person or group responsible for policy at Cooperative>.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 4.2 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 17 of the accompanying PowerPoint presentation.
- Adapted from SANS “Remote Access Policy” template @ https://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy
6. Definition of Terms

- **Dual Homing** - A computer with two or more network interfaces. A dual-homed host can act as a simple firewall on a small network as long as there is no direct IP traffic between the Internet and the internal network. In such a case, all Internet applications are run only on the dual-homed host.

- **Split Tunneling** - A computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of *Cooperative Name* is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The *person or group responsible for policy at Cooperative* shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All *Cooperative Name* personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

*Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.*

8. Approval

__________________________________________________________________________  
<insert title of approver>  
Date

__________________________________________________________________________  
<insert title of approver>  
Date

__________________________________________________________________________  
<insert title of approver>  
Date
## 9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Outsourced Information Processing

1. Overview/Purpose

In order to fully leverage the advantages of the most up-to-date technology available, <Cooperative Name> may contract with outside sources to provide that technological advantage as opposed to developing solutions internally. This approach provides <Cooperative Name> many advantages to include cost savings, faster implementation, and expertise often not available internally. While providing the aforementioned advantages, <Cooperative Name> must also be cognizant of the inherent risk involved in allowing third-party providers access to our internal systems and take the necessary precautions to safeguard confidential information.

This policy sets out principles and expectations pertaining to the security of <Cooperative Name> Technology resources that are accessed, or provided, by third parties.

2. Scope

This policy applies to all <Cooperative Name> contractors, vendors and agents who may have a legitimate business-related need to connect to the Cooperative network. This may include hardware/software support and maintenance staff, consultants; IT and/or business process outsourcing firms, or temporary staff hired for a specific project. This policy applies to remote access connections as well as on-site access used to do work on behalf of <Cooperative Name>, including reading or sending email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to, DSL, VPN, SSH, and/or remote web sessions.

3. Policy

3.1. Assessing Outsourcing Risks

Management shall nominate a suitable <Cooperative Name> owner for each business function/process outsourced. The owner, with help from the <person or group responsible for policy at Cooperative>, shall assess the risks before the function/process is outsourced, using <Cooperative Name>‘s standard risk assessment processes.

3.2. Contracts

3.2.1. A formal contract between <Cooperative Name> and the outsourcer should exist.

3.2.2. All contracts shall be submitted to <person or group responsible for policy at Cooperative> for accurate content, language and presentation.
3.3. Hiring and training of employees

3.3.1. Outsource employees, contractors and consultants working on behalf of <Cooperative Name> may be subjected to background checks equivalent to those performed on <Cooperative Name> employees.

3.3.2. Companies providing contractors/consultants directly to <Cooperative Name> or to outsourcers used by <Cooperative Name> shall perform at least the same standard of background checks as those indicated above.

3.3.3. Suitable information security awareness, training and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to <Cooperative Name> information security policies, standards, procedures and guidelines (e.g. privacy policy, acceptable use policy, procedure for reporting information security incidents etc.) and all relevant obligations defined in the contract.

3.4. Security audits

3.4.1. If applicable, the outsourcer will provide SOC 1 and SOC 2 Reports, or agree to <Cooperative Name>’s right to audit.

3.4.2. The frequency of audit shall be determined by <person or group responsible for policy at Cooperative>.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 4.3 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 10 of the accompanying PowerPoint presentation.
- Adapted from ISO 27001 Security – “Information Security Policy on Outsourcing” @ www.iso27001security.com/ISO27k_Model_policy_on_outsourcing.docx
6. Definition of Terms

None.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<insert title of approver>  
Date

<insert title of approver>  
Date

<insert title of approver>  
Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Accountability of Assets

1. Overview/Purpose

System and network documentation is one small part of IT documentation. Good system documentation enhances and validates security by documenting the configuration details and procedures that support a security policy. A reasonably complete inventory/register of the information assets can subsequently be risk assessed, classified and secured in accordance with other security policies. Complete System documentation also serves as an important part of backup and disaster recovery documentation, and an inventory/register serves a valuable guide to the creation of a backup and disaster recovery plan.

Good documentation must be thorough and must be kept current. Thus, updating documentation is a part of change management and many daily administration activities.

[Explanatory Note: Although configuration details are mentioned in the purpose of this policy, there are no recommendations for them included in the cybersecurity toolkit. The KAEC IT Association Special Committee feels that given the variety in systems and system configurations used by the state’s cooperatives, no recommendations can be made with any certainty that they would apply. Accordingly, the committee recommends that each cooperative develop their own configuration standards and either reference them in section 6 of this policy or attach them to this policy directly.]

The purpose of this policy is to ensure that all <Cooperative Name> information technology (IT) assets are accounted for, classified, inventoried, tracked, and managed throughout each IT asset’s lifecycle.

Through this policy, and its appendices, <Cooperative Name> is establishing the baseline standards by which the cooperative will manage, collect, and report information about the IT Assets under its control. <Cooperative Name> may establish additional written policies, standards, processes and procedures as necessary to accomplish its business objectives.

2. Scope

All employees, contractors, consultants, temporary and other workers at <Cooperative Name> and its subsidiaries must adhere to this policy. This policy applies to IT equipment that is owned, operated, or leased by <Cooperative Name> or registered under a <Cooperative Name> owned internal network domain.

3. Policy

3.1. General Requirements

3.1.1. Newly purchased technology, as defined in the Introduction herein, will be identified in the appropriate Technology Inventory.

3.1.2. Existing technology in the appropriate Technology Inventory will be physically inventoried on a periodic basis.

3.1.3. The <person or group responsible for policy at Cooperative> is responsible for establishing procedures to issue and inventory technology assigned to employees and contractors.
3.1.4. The Technology Inventory shall be available for audit.
3.1.5. The <person or group responsible for policy at Cooperative> will ensure that appropriate software licensing agreements for software used by cooperative employees are in place and that the cooperative is in compliance with those agreements.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will be responsible for conducting a physical inventory to reconcile Technology Inventory information on-hand for all technology on a periodic basis. A physical inventory reconciliation report will be reported to responsible parties as necessary. Discrepancies should be noted. Documentation support that a physical inventory has been taken, for all locations, should be retained in accordance with <Cooperative Name> retention policy.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 5.0 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 24 of the accompanying PowerPoint presentation.
- Audit Policy.  **NOTE: Not included as part of this package.**
- IT Risk Management Policy, see page 6 herein.
- See also, “Inventory of Authorized and Unauthorized Devices” @ [http://www.sans.org/critical-security-controls/control/1](http://www.sans.org/critical-security-controls/control/1) and “Inventory of Authorized and Unauthorized Software” @ [http://www.sans.org/critical-security-controls/control/2](http://www.sans.org/critical-security-controls/control/2)

6. Definition of Terms

- **Technology** – see definition in Introduction contained herein

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;insert title of approver&gt;</td>
<td>Date</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;insert title of approver&gt;</td>
<td>Date</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Personnel Security

1. Overview/Purpose

Understanding the importance of cyber security and personnel security via individual responsibilities and accountability are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific, training as well as personnel background verifications. The security awareness and training information needs to be continuously upgraded and reinforced.

The purpose of this Policy is to establish the background check requirements and processes for <Cooperative Name> prospective employees, current employees, volunteers and contractors in order to protect employees, membership, board members, and other associated parties. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users.

2. Scope

This Policy applies to all employees, vendors, contractors, partners, collaborators, interns, and any others, henceforth referred to as an Applicant, who will conduct business for, or research with, <Cooperative Name> that are in contact with financially sensitive information and/or security sensitive information.

3. Policy

The <HR Department Name> is solely authorized to conduct and oversee the background check process necessitated pursuant to this Policy on behalf of <Cooperative Name>.

<HR Department Name> may work with law enforcement or contract with outside agencies in executing any of the obligations set forth in this Policy. <HR Department Name> is responsible for making decisions regarding what type of background check is appropriate, interpreting background check records and information, determining whether an Applicant is eligible for employment, and for making personnel recommendations to the Hiring Authorities.

Notwithstanding this Policy, nothing precludes <HR Department Name> from conducting a background check on any individual when <HR Department Name>, in consultation with the Hiring Authority and Legal Counsel, determine that a background check is necessary.

Hiring Authorities are responsible for initiating the background check process by contacting <HR Department Name>.

Applicants must consent to a background check to be considered for a position. Any Applicant who refuses to consent to the background check, refuses to provide information necessary to conduct the background check, or provides false or misleading information will not be considered for the position for which s/he has applied. Any Applicant, or current employee, who is found to have provided false or
misleading information related to the background check, may be subject to disciplinary action, up to and including termination.

All <HR Department Name> employees are responsible for ensuring the integrity and confidentiality of the Background check process. The <HR Department Name> shall define all positions that meet the criteria for financial sensitivity, security sensitivity, or is in contact with vulnerable populations and shall develop a program for periodically following up on hired individuals to assure there have been no events requiring a revocation of privileges.

3.1. Security Requirements

3.1.1. Reference Checks

Reference checks must be completed for all final applicants. The <HR Department Name> is responsible for conducting reference checks.

3.1.2. Criminal Screening

A criminal history check must be conducted for all final applicants, unless a criminal history check has been conducted within the previous three years while employed with the cooperative.

3.1.3. Financial Screening

Financial history check must be conducted for final applicants for positions that have access to any <Cooperative Name> sensitive information. (Refer to Appendix B for examples)

3.1.4. Employee Self-Disclosure Requirements

Criminal Conviction or Felony Charge

Current employees are required to self-disclose criminal convictions or felony charges against them that occur on or after the effective date of this Policy within (2) two business days of the conviction or felony charges. This information should be reported to <HR Department>. Employees failing to self-disclose may be subject to disciplinary action, up to and including termination.

The <Person or Group Responsible for this Policy> in coordination with the <HR Department> will implement a program communicating <Cooperative Name> expectations relating to cyber security. This program shall include periodic training and formal acceptance of computer use polices.

3.2. Training Requirements

3.2.1. All new users must attend an <Cooperative Name> approved Security Awareness training class, prior to, or at least within 14 business days of being granted access to any <Cooperative Name> information resources.
3.2.2. All users must sign an acknowledgement stating they have read and understand <Cooperative Name> requirements regarding computer security policies and procedures.

3.2.3. All users (employees, contractors, interns, vendors, consultants, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect <Cooperative Name> information resources.

3.2.4. <Person or group responsible for policy at Cooperative > must prepare, maintain, and distribute one or more information security manuals that concisely describe <Cooperative Name> information security policies and procedures.

3.2.5. All users must annually attend computer security compliance training and pass the associated examination if applicable.

3.2.6. <Person or group responsible for policy at Cooperative > must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

4. Compliance

4.1. Compliance Measurement

The <Person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <Person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 6.0 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 18 of the accompanying PowerPoint presentation.
- Adapted from University of Colorado Boulder Background Check Policy
- ISO 27001 Outsourcing Security Policy Section 5.4 @ www.iso27001security.com/ISO27k_Model_policy_on_outsourcing.docx
6. Definition of Terms

- **Financially Sensitive** - Pertains to work that meets one or more of the following criteria:
  1. Responsibility for a handling, or having access to, cash, social security numbers, financial account information for either <Cooperative Name>, or associated members, vendors, or contractors, or;
  2. Access to financial account information for either <Cooperative Name>, or associated members, vendors, or contractors such as banking account information, credit/debit card information, etc.

- **Security Sensitive** - Pertains to work that meets one or more of the following criteria:
  1. Positions with information technology responsibilities that meet the criteria for Privileged Access.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The Person or group responsible for policy at Cooperative shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

---

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Physical and Environmental Security

1. Overview/Purpose

<Cooperative Name> is committed to protecting its employees, members and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This Physical Security Policy is to detail the requirements and guideline for the physical protection of <Cooperative Name> information, assets, and personnel.

2. Scope

This Policy applies to all <Cooperative Name> facilities, information, assets, and all personnel who are conducting work while on cooperative premises up to and including: employees, contractors, workforce members, vendors and agents with a computer/device connected to the <Cooperative Name> network.

3. Policy

3.1. Facility Security

- Sensitive exterior areas will be illuminated by security lighting from dusk to dawn. Lighting faults or failures should be reported to the <Person or group responsible for policy at Cooperative> in a timely manner.

- Sensitive facilities will be protected by an intrusion alarm system. <Person or group responsible for policy at Cooperative> will be responsible for designating which employees possess access to the alarm system. The alarm system will be tested on a recurring basis.

- Public areas will be accessible during normal business hours. Non-public areas of all buildings will be designated as sensitive areas. Only authorized personnel are allowed in sensitive areas.

- Access to sensitive areas will be controlled by an access control system, and will be recorded by video surveillance system.

- Lost access tokens/keys must be reported to the <person or group responsible for policy at Cooperative> immediately.

- Visitors will be escorted at all times in secured areas. Visitors will be required to sign in and a visitor log will be maintained at the main entrance.

[Explanatory note: Modify the visitor sign-in requirements to meet the particular cooperatives policies, or reference an existing visitor sign-in policy.]

- Wiring closets and areas that contain vital IT infrastructure, systems, or confidential data will follow the principal of least privileged access. Employees, contractors, and
vendor staff will be granted access only to facilities and equipment necessary to fulfill their job function.

<Person or group responsible for policy at Cooperative> will be responsible for assigning access to secure areas as is appropriate. Access reviews will be conducted and removal of individuals that no longer require access will be completed.

- All employees are responsible for checking to ensure that doors, windows, and other access ways in their area of responsibility are locked and secure at close of business. Employees should report open or unlocked access ways to the <Person or group responsible for policy at Cooperative> immediately.

3.2. Device and Server Security

- All servers that host sensitive data and all critical IT resources will be placed in access controlled areas.
- Laptops, tablets, cell phones, and other portable equipment will be kept in a secured area such as a locked drawer, locked office, or secured to a permanent object when not in use, or be secured in place by rugged locking equipment.
- Backups, portable hard drives, and other removable media will be kept in a secure area such as a locked drawer or locked office when not in use.
- Employees shall consider the sensitivity of the information to which they have access, such as personally identifiable information (PII) and protected health information (PHI), and shall take appropriate steps to prevent unauthorized access.
- <Cooperative Name> will implement physical and technical safeguards for all devices that access sensitive information to restrict access to authorized users. Appropriate measures include:
  - Restricting physical access to devices to only authorized personnel.
  - Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
  - Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with <Cooperative Name> Password Policy.
  - Complying with all applicable password policies and procedures. See <Cooperative Name> Password Policy.
  - Ensuring devices are used for authorized purposes only.
  - Never installing unauthorized software on devices.
  - Storing all sensitive information, including personally identifiable information (PII) and protected health information (PHI) on appropriately secured systems.
  - Keeping food and drink away from servers, network equipment, and workstations in order to avoid accidental spills.
  - Securing laptops that contain sensitive information.
  - Arrange screens to limit visibility of sensitive data.
  - Ensuring devices are left on but logged off in order to facilitate after-hours updates.
  - Exit running applications and close open documents when leaving for the day.
4. **Compliance**

4.1. **Compliance Measurement**

The *person or group responsible for policy at Cooperative* will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. **Exceptions**

Any exception to the policy must be approved by the *person or group responsible for policy at Cooperative* in advance.

4.3. **Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. **Related Standards, Policies, and Processes (cross references to industry standards)**

- Addresses Section 7.0 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 21 of the accompanying PowerPoint presentation.

6. **Definition of Terms**

- **Access Controlled Areas** – Areas controlled by an access control system, limiting access to authorized individuals.
- **Sensitive Areas** – Areas subject to stricter access controls due to potential risk for access to, or unauthorized use of, restricted data and/or systems.

7. **Responsibilities**

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of *Cooperative Name* is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The *person or group responsible for policy at Cooperative* shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All *Cooperative Name* personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.
8. Approval

<insert title of approver>  Date

<insert title of approver>  Date

<insert title of approver>  Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Documentation Procedures

1. Overview/Purpose

This policy ensures that the policies, plans, procedures, records, and documents necessary to comply with the <Cooperative Name> Cyber Security Policy are captured and managed by <Cooperative Name>.

This policy applies to personnel responsible for management and support of cyber assets and systems at <Cooperative Name>.

2. Policy

2.1. A documented program shall be implemented to capture, manage, and retain records and documents to comply with <Cooperative Name> Cyber Security Policy.

2.1.1. Information owners and management are responsible for identifying records and documents necessary to comply with <Cooperative Name> Cyber Security Policy.

2.1.2. Information that is necessary to demonstrate compliance with <Cooperative Name> Cyber Security Policy, regardless of media type, shall be captured, managed, and retained. Documents including but not limited to event logs, screen shots, alert emails, and system generated reports shall be retained as evidence to be used for internal or independent audits of compliance.

2.1.3. Review of this document control and records management program shall be performed at least annually, the results documented, and the program updated as necessary.

2.2. Procedures related to ongoing operation of a cybersecurity program (system patching, change control, etc.) shall be documented in enough detail so that a competent individual with minimal knowledge of the organization or system could perform the procedures.

2.3. Records shall be retained for at least <N> calendar years unless specified by another regulatory or <Cooperative Name> policy.

3. Compliance

3.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

3.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.
3.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

4. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 8.1 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 14 of the accompanying PowerPoint presentation.

5. Definition of Terms

- Cyber Assets - programmable electronic devices and communications networks including hardware, software, and data

6. Responsibilities

6.1. Responsibilities for this policy are delineated as follows:

6.1.1 The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

6.1.2 The CEO/President shall be responsible for the overall administration of this policy.

6.1.3 The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

6.1.4 All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

7. Approval

__________________________________________  Date

<insert title of approver>

__________________________________________  Date

<insert title of approver>

__________________________________________  Date

<insert title of approver>
8. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
System Patching

1. Overview/Purpose

<Cooperative Name> is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. <Cooperative Name> has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

This document describes <Cooperative Name>'s requirements for maintaining up-to-date operating system security patches on all <Cooperative Name> owned and managed workstations and servers.

2. Scope

This policy applies to workstations or servers owned or managed by <Cooperative Name>. This includes systems that contain company or customer data owned or managed by <Cooperative Name> regardless of location. The following systems have been categorized according to management:

- *.nix servers managed by <person or group responsible for policy at Cooperative>
- Microsoft Windows servers managed by <person or group responsible for policy at Cooperative>
- Workstations (desktops, laptops, and tablets) managed by <person or group responsible for policy at Cooperative>

3. Policy

Workstations and servers owned by <Cooperative Name> must have up-to-date (as defined by <person or group responsible for policy at Cooperative> minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, tablets, desktops, and servers owned and managed by <Cooperative Name>.

3.1. Workstations

Desktops, laptops, and tablets must have automatic updates enabled for operating system patches when available. This is the default configuration for all workstations built by <Cooperative Name>. Any exception to the policy must be documented and forwarded to the <person or group responsible for policy at Cooperative> for review. See Section 4.2 on Exceptions.

3.2. Servers

Servers must comply with the minimum baseline requirements that have been approved by the <person or group responsible for policy at Cooperative>. These minimum baseline
requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the <Cooperative Name> asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the <person or group responsible for policy at Cooperative> for review. See Section 8.0 on Exceptions.

3.3. Roles and Responsibilities

- <Person or group responsible for policy at Cooperative> will manage the patching needs for the *.nix servers on the network.
- <Person or group responsible for policy at Cooperative> will manage the patching needs for the Microsoft Windows servers on the network.
- <Person or group responsible for policy at Cooperative> will manage the patching needs of all workstations on the network.
- <Person or group responsible for policy at Cooperative> is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.
- The <Person or group responsible for policy at Cooperative> is responsible for approving the monthly and emergency patch management deployment requests.

3.4. Monitoring and Reporting

Active patching teams noted in the Roles and Responsibility section (3.3) are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Information Security and Internal Audits upon request.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.
5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 8.2 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 23 of the accompanying PowerPoint presentation.
- Adapted from “Patch Management Policy” @http://www.sans.edu/student-files/projects/200905_01.doc

6. Definition of Terms

None.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

8. Approval

<insert title of approver>  
Date

<insert title of approver>  
Date

<insert title of approver>  
Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Incident Management

1. Overview/Purpose

Cyber incidents occur frequently. It is important to realize that having an incident response and management policy allows <Cooperative Name> to protect its information, as well as its reputation. This policy requires <person or group responsible for policy at Cooperative> to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover from a cyber-incident.

This policy defines the requirement for a baseline incident response and management plan to be developed and implemented by <Cooperative Name> that will describe the process to discover an attack and then effectively contain the damage, eradicating the attacker’s presence, and restore the integrity of the network and system.

2. Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have an incident response and management plan, it does not specify what goes into the plan or sub-plans.

3. Policy

3.1. The Incident Response and Management Plan shall:

- Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.
- Assign job titles and duties for handling computer and network incidents to specific individuals.
- Define management personnel who will support the incident handling process by acting in key decision-making roles.
- Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate legal or regulatory organizations.
- Provide instructions on how to report computer anomalies and incidents. Such information should be included in routine employee awareness activities.
- Conduct periodic incident handling drills.
- The plan should be reviewed on a periodic basis.
4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 8.3 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 26 of the accompanying PowerPoint presentation.
- Adapted from “Incident Response and Management” @ http://www.sans.org/critical-security-controls/control/18

6. Definition of Terms

- Cyber Security Incident - any malicious act or suspicious event that: Compromises, or was an attempt to compromise, the electronic or physical security perimeter of a computing system or asset or, disrupts, or was an attempt to disrupt, the operation of a computing system or asset.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]
8. Approval

____________________________________  __________________________
<insert title of approver>                  Date

____________________________________  __________________________
<insert title of approver>                  Date

____________________________________  __________________________
<insert title of approver>                  Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
System Logging and Monitoring

1. Overview/Purpose

Monitoring and logging is an essential information security control that is used to identify, respond to, and prevent operational problems, security incidents, policy violations, and fraudulent activity.

The purpose of this policy is to establish requirements and parameters for creating, maintaining, storing, and accessing <Cooperative Name> computer and communication device logs. The logs shall be used to assist in troubleshooting, monitoring changes to system performance, record the actions of users when necessary to properly maintain security, give the ability to track security instances, and provide data useful for investigating malicious activity. Additionally, logs may be used to assist in business recovery activities and in order to comply with federal, state, and local laws and regulations.

2. Scope

All employees, contractors, consultants, temporary and other workers at <Cooperative Name> and its subsidiaries must adhere to this policy. This policy applies to technology, as defined in the Introduction herein, that is owned, operated, or leased by <Cooperative Name> or registered under a <Cooperative Name>-owned internal network domain.

3. Policy

3.1. General Requirements

3.1.1. Timestamps of all systems generating log files will be synchronized using an application such as the Network Time Protocol (NTP) Service in order to construct and maintain a clear sequence of events.

3.1.2. The level of information detail contained in a log will be determined by the <person or group responsible for policy at Cooperative> based on the risks to the relevant technology and underlying data and shall be determined in accordance with the cooperative’s risk management policy.

3.1.3. Log files must be examined on a regular basis in order to protect cooperative technology. The frequency and nature of log monitoring and review depends on the risks to the relevant technology and underlying data and shall be commensurate with the cooperative’s risk management policy.

3.1.4. Log files may contain confidential data and must be handled in a manner that is consistent with the cooperative’s policy for such data.
3.1.5. Logging facilities and log information should be protected against tampering, modification, destruction, and unauthorized access. Wherever possible, system administrators should not have permission to erase, deactivate, or modify logs of their own activities.

3.1.6. Log files will be maintained only as long as is necessary to comply with the cooperative’s record retention policy or as required to support analysis of misuse, incident reconstruction, or other investigations.

4. Compliance

4.1. Compliance Measurement

4.1.1. The <person or group responsible for policy at Cooperative> will be responsible for configuring log facilities to comply with this policy and dedicating resources sufficient for the storage and review of log files as required by this policy. The <person or group responsible for policy at Cooperative> are responsible for documenting appropriate compliance with this policy in their areas of responsibility.

4.1.2. Documentation should be periodically reviewed to ensure continued compliance with this policy.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 8.4 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 25 of the accompanying PowerPoint presentation.
- Audit Policy. **NOTE:** Not included as part of this package.
- IT Risk Management Policy, see page 6.
- See also, “Maintenance, Monitoring, and Analysis of Audit Logs” @ [http://www.sans.org/critical-security-controls/control/14](http://www.sans.org/critical-security-controls/control/14) and “Account Monitoring and Control” @ [http://www.sans.org/critical-security-controls/control/16](http://www.sans.org/critical-security-controls/control/16)

6. Definition of Terms

None.
7. Responsibilities

7.1 Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<insert title of approver> Date

<insert title of approver> Date

<insert title of approver> Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cyber Security Policy Framework

System Acceptance and Configuration

1. Overview/Purpose

This policy establishes that security measures and configuration settings are applied to all devices connecting to the network, including new devices as well as vendor and contractor devices that physically or remotely connect to the network.

2. Scope

This policy applies to all technology resources owned or operated by <Cooperative Name>. All users <Cooperative Name> employees, contractors, vendors or others) of technology resources are responsible for adhering to this policy.

3. Policy

Devices such as workstations, servers, network components, and mobile devices, as well as standard software deployments, such web servers or databases, should each have a standard configuration baseline maintained by the <Person or Group Responsible for policy at Cooperative>.

The baseline configuration should be reviewed and updated when required due to a significant configuration change, such as an operating system upgrade or hardware change, or a demonstrated vulnerability; as part of a system component installation or upgrade; or at least on a yearly basis.

At minimum, the baseline configuration for each category of device shall include:

- Standard operating system/installed applications with current version numbers,
- Standard software load for workstations, servers, network components, and mobile devices and laptops, for each internal division
- Up-to-date patch level information,
- Security configuration including disabled services, ports, and etc.

The configuration baseline may be less formal for devices or systems of limited size and scope, such as cell phones and tablets.
Additionally, **<Person or Group Responsible for policy at Cooperative>** shall:

3.1.1. Monitor systems for configuration baseline and policy compliance. Automated tools should be used to efficiently identify when the system is not consistent with the approved baseline configuration and when remediation actions are necessary.

3.1.2. Reapply all baseline configurations to systems, as appropriate, when the system undergoes a material change, such as an operating system upgrade.

3.1.3. Modify individual system configurations or baseline configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning and/or security audits.

3.1.4. Before a system is entered into production, **<Person or Group Responsible for policy at Cooperative>** shall implement the baseline configuration settings; identify, document, and approve exceptions from the baseline configuration settings for individual systems based on explicit operational requirements; and certify that system complies with baseline security configurations.

4. **Compliance**

4.1. **Compliance Measurement**

The **person or group responsible for policy at Cooperative** will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. **Exceptions**

Any exception to the policy must be approved by the **person or group responsible for policy at Cooperative** in advance.

4.3. **Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. **Related Standards, Policies, and Processes (cross references to industry standards)**

- Addresses Section 8.5 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 16 of the accompanying PowerPoint presentation.

6. **Definition of Terms**

None.
7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<insert title of approver>                                          Date

<insert title of approver>                                          Date

<insert title of approver>                                          Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Malware Prevention

1. Overview/Purpose

This Anti-Virus and Anti-Malware policy is to detail the requirements and guideline for <Cooperative Name> to identify, quarantine and remove viruses and other malware. This is an essential information security control necessary for defense against cyber threats posed.

The purpose of this policy is to outline which technology systems are required to have anti-virus and/or anti-malware applications and establish base requirements for these systems.

2. Scope

This policy applies to all technology that is owned, operated, or leased by <Cooperative Name>. This policy will also determine which technology will have anti-virus and anti-malware applications installed on it and to deploy such applications as appropriate.

3. Policy

3.1. General

All computing systems, both physical and virtual, connected to the cooperative network shall have an anti-virus and anti-malware application installed, configured, activated and updated with the latest threat definitions. This software application must be capable of real-time scanning protection to files and applications running on the target system.

3.2. Guidelines

3.2.1. The <person or group responsible for policy at Cooperative> is/are responsible for creating and maintaining a document, <Cooperative Name> Anti-Virus and Anti-Malware procedures, that details procedures to ensure anti-virus software is run at regular intervals, and computers are verified as threat free.

- Employees shall be instructed NOT to trust any other source for virus protection patches.
- Ensure that the current version is installed with anti-virus updates as they become available. Updates shall be no more than four weeks out of date.
- The anti-virus and malware software should be configured so as to always scan a new removable media and devices attached to cooperative computer prior to use. If this is not an available option, this can be accomplished by opening the anti-virus client software and selecting the appropriate media and manually executing a scan.
- Whenever new threats are identified, and determined to be of sufficient concern to cooperative business, all corporate computer users will be notified about the new threat and appropriate measures to take, if any.
3.2.2. Any activities with the intention to create and/or distribute malicious programs into <Cooperative Name>’s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with <Cooperative Name>’s Acceptable Use Policy.

3.2.3. Virus or malware infected computers must be isolated from the cooperative’s network until they are verified as virus-free. Refer to <Cooperative Name>’s Anti-Virus and Malware Remediation Processes for more information. NOTE: This process document is not included as part of this package.

3.2.4. Employees will be educated about safe anti-malware practices such as, but not limited to;
- Opening unexpected attachments
- Downloading files from unknown sources
- Deleting spam, chain mails, junk emails

3.2.5. To expedite the recovery from any virus/malware threats the <person or group responsible for policy at Cooperative> shall ensure that all critical network data and system configurations are backed up in accordance with <Cooperative Name>’s Backup and Recovery Policy.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies. To ensure that the use of the Cooperative’s Information Systems and other electronic communications systems is consistent with the cooperative’s legitimate business interests, authorized representatives of the Cooperative may monitor the use of such equipment from time to time and without notice.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 8.6 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 27 of the accompanying PowerPoint presentation.
- Backup and Recovery Policy, Page 45.
- Acceptable Use Policy, Page 78.
- Anti-Virus and Malware Exemption form, see Appendix D.
- See also “Malware Defenses” @ http://www.sans.org/critical-security-controls/control/5
6. Definition of Terms

- **Malware** – a general term used to refer to a variety of forms of hostile or intrusive software such as; computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs
- **Virus** – a computer program or piece of code that is installed on, or executed by any computer without the knowledge of the owner and runs against the owner's wishes. Viruses are often destructive and malicious.
- **Spyware** – malware that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <*>Cooperative Name*> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <*>person or group responsible for policy at Cooperative*> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <*>Cooperative Name*> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

*[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]*

8. Approval

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;insert title of approver&gt;</td>
<td>Date</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;insert title of approver&gt;</td>
<td>Date</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Page 44
9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Backup and Recovery

1. Overview/Purpose

<Cooperative Name> is committed to protecting <Cooperative Name> employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. <Cooperative Name>'s intentions for publishing a Backup and Recovery Policy are not to impose restrictions that are contrary to <Cooperative Name>'s established culture of openness, trust and integrity.

The purpose of the Backup Policy is to establish rules and outline the use of media systems and network servers for storage, backup and recovery of electronic information in <Cooperative Name>'s Information Technology environment. Electronic backups are a business requirement to enable recovery of data and applications in the case of events such as natural disasters, system drive failures, espionage, data entry errors, or systems operations errors.

2. Scope

<person or group responsible for policy at Cooperative> personnel, in coordination with respective business owners, are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. These backup provisions will allow <Cooperative Name> business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of institutional data backups should be maintained.

Federal and state regulations pertaining to the long-term retention of data (e.g., financial records) will be met using separate archive policy and procedures, determined by the Business Owner (Department) of the information. Backups are not primarily intended to archive data for future reference, but rather system restoration. Data stored locally on desktop computers is not backed up, nor is data backed on systems that are not managed by <person or group responsible for policy at Cooperative>. Long-term archive requirements are beyond the scope of this policy.

3. Policy

<Cooperative Name> requires that computer systems be backed up on a regular basis and that the backup media is located/stored in a secure off-site location. The purpose of the systems backup is to provide a means to restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster and provide a measure of protection against human error or the inadvertent deletion of important files. Systems backups are not intended to serve as an archival copy or to meet records retention requirements.

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the <Cooperative Name> business owner.
• **<Cooperative Name>** Information Technology backup and recovery processes for each system and service should be annually reviewed by the responsible business owner and the **<person or group responsible for policy at Cooperative>** personnel.
• Backup procedures should be periodically tested to ensure that the IT resource is recoverable.
• Procedures for the offsite backup storage should be reviewed periodically.
• Backup media must be readily identified by appropriate labeling, and noted in a centralized log as to its physical storage location.
• All critical information used on workstations should be placed on networked file server drives for backup.

### 3.1. Network Storage Structure

**<Cooperative Name>** has network servers in place in **<Identified Locations>**. **<Cooperative Name>** management and staff have file storage folders allocated for their account on network servers. These storage areas are usually referred to as the users "X: drive", where X denotes a mapped storage area on a network server as described below;

**H: Drive** - Users personal folder on the network server

When the user successfully logs on to their workstation, network connections are established to these folders which can then be accessed as the "X: Drive" in Windows Explorer, Microsoft Word, Excel, and other software programs. Files can be copied from the user's workstation to their "X Drive", or software programs may be configured to save files directly to these mapped drives. These mapped drives are backed up to network storage and removable media. The removable media shall be rotated to an off-site storage facility and securely stored to provide for security and disaster recovery.

*Explanatory Note: This specific application of a network storage structure from cooperative to cooperative will vary. This information was provided only as a guide.*

### 3.2. Storage of User Data Files

In order to be able to recover lost data, management and staff should store essential data files requiring backup, to one of the network mapped drives. Data files on the user's local workstation may not be recoverable if the drive fails. Appropriate use of network storage will ensure ample capacity for archival storage of user data files. Users should store and maintain data files (or current copies), which are important to the company and which would be costly or impossible to recreate, on the network mapped drives. Users should not store non-business or non-essential data files on the network drives. Types of data files to be stored and their locations will be determined on a departmental level, and should be documented in a department level data backup guideline to be communicated with the **<person or group responsible for policy at Cooperative>**.
3.3. Backup Schedule

The systems backups will consist of regular full and incremental backups in accordance with Appendix A, "<Cooperative Name> Backup Schedule by System".

3.4. Documentation

<Cooperative Name> Information Technology backup and recovery processes for each system and service must be documented by the <person or group responsible for policy at Cooperative> with assistance from the business owner.

- Backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.
- Documentation of the restoration process must include procedures for the recovery from single-system or application failures as well as a total data center disaster scenario.
- Backup and recovery documentation will be reviewed and updated annually to account for new technology, business changes, and migration of application to alternative platforms. Recovery procedures will be tested on an annual basis where feasible.

3.5. Backup verification

Test restores from backup archives must be performed at least annually where feasible. This ensures that both the archive media and backup procedures work properly. It must at least once be proven that complete data restoration is possible. This ensures reliable testing as to whether:

- Data restoration is possible
- The data backup procedure is practical
- There is sufficient documentation of the data backup process, thus allowing a substitute to carry out a data restoration if necessary
- The time required for the data restoration meets the availability requirements

3.6. Offsite Storage

In order to provide disaster recovery capability, backup media are rotated to an offsite storage location from the backup source. Backup media are maintained in offsite storage according to the schedule outlined in Appendix A, <Cooperative Name> Backup Schedule by System".

3.7. File Recovery

In order to have a file restored from the backup archive, the user should contact <person or group responsible for policy at Cooperative> and provide the date of the last known good version of the file – this will help identify the set of backup media to use in attempting to restore the file.
Files can usually be restored within a few hours or less. The <person or group responsible for policy at Cooperative> cannot restore data files which were not archived on the network servers. As the media is rotated, users should request restoration of data files as soon as possible to prevent data being overwritten on the backup media.

3.8. Open Data Files

The backup server software is unable to archive data files which are open. Each user should ensure that all files that are to be archived are closed at the end of each business day.

3.9. Backup Failure

All backup failures will be logged and investigated as soon as practical upon detection.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Corporate Data Retention policy, Not a part of this documentation
- Corporate Risk Assessment policy, Not a part of this documentation
- Addresses Section 8.7 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 30 of the accompanying PowerPoint presentation.
- See also “Data Recovery Capability” @ http://www.sans.org/critical-security-controls/control/8
- <Reference to ISO 27000, NIST, CRN, if applicable. Make reference to Guernsey Report in Explanatory Notes>
6. Definition of Terms

None.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<insert title of approver>  
Date

<insert title of approver>  
Date

<insert title of approver>  
Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Management

1. Overview/ Purpose

<Cooperative Name> is committed to protecting its employees, members and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This Network Management Policy is to detail the requirements and guideline for <Cooperative Name> to address areas of Network Management of routers, switches, servers, etc. as an essential information security control to minimize the threat window for both internal and external cyber threats.

The purpose of this policy is to assure the availability, security, reliability, and integrity, of the network infrastructure at <Cooperative Name>. This policy documents practices and responsibilities associated with the administration, maintenance, configuration, expansion, and use of the <Cooperative Name> network. in order to:

   a. provide reliable Intranet and Internet communications to support corporate business;
   b. assure that network usage is authorized and consistent with the companies mission; and
   c. protect the confidentiality, integrity, and availability of corporate information that is transmitted through the <Cooperative Name> network.

2. Scope

This policy applies to all servers and computers that are owned, operated, or leased by <Cooperative Name> as well as any computers that are connected to the corporate network.

3. Policy

No individual, or <Cooperative Name> component, is permitted to independently deploy network devices that extend the <Cooperative Name> Network, or secure or isolate parts of the <Cooperative Name> Network, except as may be stipulated under the provisions of this policy. The <Cooperative Name> <IT Department Name> is charged with overall responsibility for proper deployment and management of a fully monitored and protected network communication service, including all infrastructure elements, network address assignments, and radio frequency (RF) spectrum usage.

No exceptions or exemptions to this policy shall be granted without the express written approval of the CEO/Manager/President of <Cooperative Name> or the <VP of IT or Related Department>.

To optimize their accessibility, usability, security, and privacy, all electronic and information resources developed or procured for use within the <Cooperative Name> network shall comply with the applicable provisions of cooperative mandates and policies dealing with the accessibility, usability, and compatibility.
3.1. Guidelines

3.1.1. All devices connected to the <Cooperative Name> network (wired or wireless) must be associated with, and in support of, the mission of the cooperative. The integrity, security, and proper operation of the <Cooperative Name> network require an orderly assignment of network addresses and the correct configuration of devices attached to the network. Network access, performance, and security are put at risk when devices are introduced into the network environment without appropriate coordination. To mitigate this risk, all connections to the <Cooperative Name> Network must be managed with due consideration for accessibility, performance, privacy, and security.

3.1.2. <IT Department Name> shall coordinate the connection and network address assignment of any and all devices on the <Cooperative Name> network. Other departments and individual users may not install, alter, extend or re-transmit network services in any way. Departments and individual users are prohibited from attaching or contracting with a vendor to attach equipment such as routers, switches, hubs, firewall appliances, wireless access points, virtual private network (VPN) servers, network address translators, proxy servers, and dial-up servers to the <Cooperative Name> network without prior authorization from <IT Department Name>. <IT Department Name> may disconnect and confiscate any unauthorized network device, including wireless routers and access points.

3.1.3. <IT Department Name> reserves the right to monitor and audit devices, systems, and general network traffic to ensure compliance with this and other <Cooperative Name> policies.

3.1.4. The use of all devices connected to the <Cooperative Name> network, including corporate issued and personal computers and wireless devices, is accompanied by certain responsibilities. Specifically, all users are required to perform timely updates of applications, services, operating systems, virus protection software and anti-malware software to minimize risks of system compromise. <IT Department Name> provides products and services for achieving such updates.

3.1.5. Server and application administrators that utilize this network to transmit sensitive or restricted, or confidential, information are responsible for the security of that information as it traverses the network. Examples of available protections include encrypted protocols such as SSL, IPSec, SSH, etc. Contact the <IT Department Name> for assistance in implementing the necessary protective measures.

3.1.6. All servers and capable network devices should be configured with time stamped logging and must be time synchronized against a common time source.
3.1.7. Appropriate network documentation must be maintained, updated, and secured as necessary for the network infrastructure.

3.1.8. A business owner shall be assigned responsibility for each network server and they shall collaborate with <IT Department Name> as necessary to:

- Protect server(s) against exploitation of known vulnerabilities. The <IT Department Name> will provide guidance for achieving such protection in its Server Management Standards and Procedures. Servers must comply with the provisions in this document anytime they are connected to the <Cooperative Name> network. These Standards and Procedures will evolve over time to address new and evolving threats, so server administrators should refer back periodically for updates. **NOTE: This standards and procedures document is not included in this package.**
- Address and resolve security problems identified with any device for which they are responsible. <IT Department Name> provides consulting and problem resolution services;
- Utilize the protection benefits available through the <Cooperative Name>‘s network edge protection mechanisms (e.g., firewall, intrusion prevention systems, network security appliances, etc.);
- Accommodate risk assessments, vulnerability scans, and penetration tests of their server(s) by <IT Department Name> takes steps to mitigate the risks identified by these procedures;
- Immediately report system compromises and other security incidents in a timely manner to <IT Department Name>.

3.1.9. DHCP (see definitions - Dynamic Host Configuration Protocol) is the standard and preferred method for assigning IP addresses to corporate network devices. Users desiring a static IP address may be asked to demonstrate why DHCP is inadequate for their purpose. <IT Department Name> reserves the right to change static IP addresses periodically to address new or modified corporate network infrastructure; users of static IP addresses shall be notified with a minimum of two (2) weeks advance notice of pending changes to those addresses.  

*[Explanatory note: Configure per your cooperative standard]*

3.1.10. Each network device must be configured, if applicable, with an unauthorized access banner similar to the following:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action,"
and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

3.1.11. The <IT Department Name> shall require minimum router configuration standards:

- No local user accounts are configured on the router. Routers and switches must use Terminal Access Controller Access Control System+ (TACACS+) for all user authentication,
- The enable password on the router or switch must be kept in a secure encrypted form.
  The router or switch must have the enable password set to the current production router/switch password from the device’s support organization,
- Two factor authentication system should be implemented for administrative access to production devices,
- The following services or features must be disabled:
  a. IP directed broadcasts,
  b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses (IPv4) or RFC 4193 (IPv6),
  c. TCP small services,
  d. UDP small services,
  e. All source routing and switching,
  f. All web services running on router,
  g. Cisco discovery protocol on Internet connected interfaces,
  h. Telnet, FTP, and HTTP services,
  i. Auto-configuration,
- The following services should be disabled unless a business justification is provided:
  a. Cisco discovery protocol and other discovery protocols,
  b. Dynamic trunking,
  c. Scripting environments, such as the TCL shell,
- The following services must be configured:
  a. Password-encryption,
  b. NTP configured to a corporate standard source,
- All routing updates shall be done using secure routing updates,
- Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems,
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself or can be routed through the device,
- Access control lists for transiting the device are to be added as business needs arise,
The router must be included in the corporate enterprise management system with a designated point of contact,

Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol,

Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported,

The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

  a. IP access list accounting,
  b. Device logging with synchronized time stamping,
  c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses (IPv4) or RFC 4193 (IPv6), or those that could be used to spoof network traffic shall be dropped,
  d. Router console and modem access must be restricted by additional security controls,
  e. Deny communications with known malicious IP addresses (blacklists), or limit access to trusted sites (whitelists).

4. Compliance

4.1. Compliance Measurement

The <Personnel or group responsible for information security> will verify compliance to this policy through various methods, including but not limited to, periodic facility inspections, video monitoring, business tool reports, internal and external assessments, and feedback to the policy owner.

4.2. Exceptions

Any exceptions to this policy must be documented on the Network Management Exemption form and authorized by the appropriate Department Head in coordination with the <Personnel or group responsible for information security> in advance.

4.3. Non-Compliance

Violations of this policy, excluding authorized exceptions, are subject to disciplinary action, up to and including discharge from employment. To ensure that the use of the Cooperative’s Information Systems and other electronic communications systems is consistent with the cooperative’s legitimate business interests, authorized representatives of the Cooperative may monitor the use of such equipment from time to time and without notice.
4.4. Compliance Scope

<Cooperative Name> cooperates fully with federal, state, and local law enforcement authorities in the conduct of criminal investigations. Users are reminded that the <Cooperative Name> will file criminal complaints against those who access or utilize the <Cooperative Name> Network in the conduct of any other criminal act.

5. Related Standards, Policies and Processes

- Addresses Section 8.8 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 15 of the accompanying PowerPoint presentation.
- Malware Prevention Policy, Page 40.
- Acceptable Use Policy, Page 78.
- Server Management Policy. NOTE: Not included with this package.
- Information Security Policy. NOTE: Not included with this package.
- Server Management Standards and Procedures. NOTE: Not included with this package.
- Network Management Exemption Form, Appendix E.

6. Definitions of Terms

- **Access Point** – an electronic device that serves as a common connection point for devices seeking to use radio frequency waves to connect to a wired network.
  Wireless access points provide shared bandwidth such that as the number of users connected to an access point increases, the bandwidth available to each user decreases.
- **Application Administrator** – an individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of a software application or service that is accessed by users over the <Cooperative Name> Network (may also be a Server Administrator).
- **Device** – any hardware component that can be attached to the <Cooperative Name> Network to process, store, or transmit information. Examples of devices include smart phones, MiFi devices, laptop computers, desktop computers, servers, and network devices such as routers, switches, wireless access points, and printers.
- **DHCP (Dynamic Host Configuration Protocol)** – facilitates the temporary assignment of a network address to a device from a pool of available addresses so that addresses can be reused when devices no longer need them. DHCP is the predominant alternative to permanent, static network address assignment.
- **Extend the Network** – connecting a device other than a single end-system to a segment of the <Cooperative Name> Network (most often a data jack). For these purposes, an end-system is defined as a device (e.g., a computer) that has no other network connections, physical or virtual, other than its physical link to the data jack. Devices that extend the network include but are not limited to hubs, bridges, switches, routers, firewalls, NATs, VPN servers, or computers configured to provide any of this functionality. Extending the network
does NOT include the use of software solutions such as Microsoft Windows Remote Desktop to connect to machines on the <Cooperative Name> network from remote locations.

- **Interference** – degradation of network communication signal due to electrical pulses or electromagnetic radiation from an external source.
- **Internet** – a standards-based, global system of interconnected networks that utilizes Transmission Control Protocol / Internet Protocol (TCP/IP) for data representation, signaling, authentication, and error detection.
- **Intranet** – a private computer network that uses Internet technologies and standards to securely share an organization’s information with the organization’s constituents; a generic name for the <Cooperative Name> network,
- **Network Address (aka Internet Protocol Address or IP Address)** – a unique identifier assigned to a network-connected device that is used to route network transmissions to their intended destinations on the Internet or Intranet.
- **Server** – a computer that provides a specific type of service on behalf of another computer or computer user (i.e., a client). Examples include a file server that stores and manages access to files, a Web server that facilitates access to Web sites and pages, and a name server that maps user and computer names to machine and network addresses.
- **Server Administrator** – an individual (including contractors and service providers) designated by the server owner as principally responsible for performing server management functions, including the installation, configuration, security, ongoing maintenance, and registration of the server.
- **SSID (Service Set Identifier)** – the name of a wireless network, or more specifically, a set of characters that identify a specific wireless network, as defined in the IEEE 802.11 standards.
- **System Compromise** – any device that is no longer entirely under its owner’s control. Two major sources of compromise are:
  a. infection by a worm, virus or Trojan horse; and
  b. exploitation of an operating system or application vulnerability by another user giving that user remote control of the computer.
- **User** – An individual who utilizes an information technology device or service.
- **Network** – the data and communications infrastructure at <Cooperative Name>. It includes the campus backbone, various local area networks (LANs), and all equipment connected to those networks including remote locations. It includes the wired network as well as both the secure (encrypted) and open (unencrypted) wireless networks
- **Wireless Network** – that part of the <Cooperative Name> Network infrastructure that uses electromagnetic waves (per IEEE 802.11 standards) instead of copper or fiber optic cable to connect computing and communication devices to the rest of the <Cooperative Name> Network infrastructure and beyond.
7. Responsibilities

8. Approval

President/CEO/General Manager _______________________________ Date

VP Operations and Technology _______________________________ Date

Manager of Technology _______________________________ Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Changes</th>
<th>Revised by</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
User Account Management

1. Overview\Purpose

User/Network accounts control access to the Cooperatives technology resources. They are critical to any IT security program, and the proper creation, control, and supervision of all User/Network accounts is vital.

The purpose of this policy is to establish a formal process to ensure timely action related to granting, modifying, or deleting user account access. This policy is necessary to safeguard the confidentiality and integrity of the Cooperative’s information.

2. Scope

This policy applies to all accounts on any system that is owned or leased by the Cooperative.

3. Policy

3.1. General

The <person or group responsible for policy at Cooperative> is responsible for ensuring that this policy is adhered to. All authorized users will be provided a unique User/Network account for their sole use. All accounts must be uniquely identifiable by an assigned user name. All accounts must have a password that complies with the Password Policy.

Individual Accounts

Individual accounts are the primary and preferred method of providing access to the Cooperatives IT resources. Users are accountable for their actions and can be audited by the systems to which they have access rights. Individual users must adhere to the terms and conditions of the Cooperatives Acceptable Use Policy.

Administration (Privileged) Accounts

IT Administrative staff can be granted privileged accounts that permit elevated access rights for specific system or application support and maintenance. Generic/built-in privileged accounts (e.g. Windows domain and local administrator, ect.) shall not be used for daily systems administration. Use a cooperative privileged account instead.

Application-Specific Accounts

An application-specific account controls access to individual applications. Access rights and privileges are programmed/configured within the application. These accounts must never be used for individual access to the network.
Guest Accounts

A guest account is associated with an account that has a generic ID rather than an individual User/Network ID. Such accounts are intended for temporary use by a visitor who has been authorized by a designated account administrator. Guest accounts must be kept to a minimum and their access limited to only what is needed. Guest accounts must be disabled when not in use.

Group Accounts

A group account identifies a functional group or organization. It provides a group of users with a shared User/Network ID to access a common application or system. Group accounts should provide the minimum access privilege required to meet business needs (e.g. read/write access is not given when read-only access will suffice).

3.2. Account Creation

A <person or group responsible for this at Cooperative> must summit a request for the creation of a new account to <person or group responsible for policy at Cooperative>. A user is not permitted, under any circumstances, to inherit the User/Network ID that was originally assigned to another user. Before access is given to an account, all users should be provided with the Cooperatives Acceptable Use Policy. (Or any other policy that might pertain to using the Coop’s IT resources) The account administrator shall create the user ID, the privileges for the account, and a temporary password and retain the accounts associated request and approval documentation.

3.3. Account Deletion

A user’s manager must immediately notify IT or H.R. of changes in a user’s employment status (departure, extended leave). The account administrator will then disable or remove all associated User/Network accounts.

3.4. Account Management

The account administrator will:

- Ensure that disabled User/Network IDs are not re-issued to another user.
- Leave the associated Network account disabled for 30 days to facilitate auto reply indicating that a person has left the company. (Remove the Network account after 30 days.)
- Modify user accounts in response to events like name changes, accounting changes, permission changes, or office transfers,
- Remove, after consultation with a user’s manager, redundant User/Network accounts that are no longer required.
- Periodically review existing accounts for validity.
Supervisors may be granted access to an account if an individual is involuntarily removed from a position to ensure continuity of communication for business purposes. Also upon special request, a supervisor will be granted access to the account after an employee voluntarily leaves.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 9.1 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 9 of the accompanying PowerPoint presentation.
- See “Account Monitoring and Control” @ http://www.sans.org/critical-security-controls/control/16, “Controlled Use of Administrative Privileges” @ http://www.sans.org/critical-security-controls/control/12, and “Controlled Access Based on the Need to Know” @ http://www.sans.org/critical-security-controls/control/15

6. Definition of Terms

None.
7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<insert title of approver>  

Date

<insert title of approver>  

Date

<insert title of approver>  

Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. Overview/Purpose

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of <Cooperative Name>'s resources. All users, including contractors and vendors with access to <Cooperative Name> systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any <Cooperative Name> facility, and has access to the <Cooperative Name> network.

3. Policy

3.1. Password Creation

3.1.1. All user-level and system-level passwords must conform to the Password Construction Guidelines.

3.1.2. Users shall never use the same password for <Cooperative Name> accounts as for other non-<Cooperative Name> access (for example, personal ISP account, option trading, benefits, and so on).

3.1.3. Excluding single sign on, users must not use the same password for various <Cooperative Name> access needs.

3.1.4. User accounts that have administrator/system-level privileges must have a unique password from all other accounts held by that user.

3.1.5. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

3.2. Password Change

3.2.1. All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on a reasonable periodic basis.

3.2.2. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every 90 days.

3.2.3. Password cracking or guessing may be performed on a periodic or random basis by the <person or group responsible for policy at Cooperative>. If a password is guessed or
Cyber Security Policy Framework

cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

3.2.4. Passwords may be required to be changed upon identification or notification of a cybersecurity incident or threat.

3.3. Password Protection

3.3.1. Passwords must not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, IT, and/or family members.

3.3.2. Passwords must not be inserted into email messages or other forms of electronic communication.

3.3.3. Passwords must not be revealed over the phone to anyone.

3.3.4. Do not reveal a password on questionnaires or security forms.

3.3.5. Do not hint at the format of a password (for example, "my family name").

3.3.6. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) in clear text.

3.3.7. Do not use the "Remember Password" feature of applications (for example, web browsers).

3.3.8. Any user suspecting that his/her password may have been compromised must report the incident to <person or group responsible for policy at Cooperative> and change all passwords.

3.4. All of the rules above that apply to passwords apply to passphrases.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 9.2 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 11 of the accompanying PowerPoint presentation.
Cyber Security Policy Framework

- Password Construction Guidelines, see Appendix C.
- Adapted from “Password Protection Policy” @ http://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

6. Definition of Terms

- **Simple Network Management Protocol (SNMP)** - is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.
- **Single Sign On** - a session/user authentication process that permits a user to enter one name and password in order to access multiple applications.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of `<Cooperative Name>` is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The `<person or group responsible for policy at Cooperative>` shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All `<Cooperative Name>` personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

*[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]*

8. Approval

---

<insert title of approver>  
Date

---

<insert title of approver>  
Date

---

<insert title of approver>  
Date
9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Remote Access

1. Overview/ Purpose

The purpose of this policy is to define standards for connecting to <Cooperative Name>’s network from any host. These standards are designed to minimize the potential exposure to <Cooperative Name> from damages which may result from unauthorized use of <Cooperative Name> resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical <Cooperative Name> internal systems, etc.

2. Scope

This policy applies to all <Cooperative Name> employees, contractors, vendors and agents with a <Cooperative Name>-owned or personally-owned computer or workstation used to connect to the <Cooperative Name> network. This policy applies to remote access connections used to do work on behalf of <Cooperative Name> including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to VPN and SSH.

3. Policy

It is the responsibility of <Cooperative Name> employees, contractors, vendors and agents with remote access privileges to <Cooperative Name>’s cooperative network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Cooperative Name>.

Remote access by non-corporate persons is prohibited. The <Cooperative Name> employee bears responsibility for any misuse.

Please review the following policies for details of protecting information when accessing the cooperative network via remote access methods, and acceptable use of <Cooperative Name>’s network:

- Encryption Policy
- Wireless Access Policy
- Acceptable Use Policy

3.1. Requirements

3.1.1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

3.1.2. At no time should any <Cooperative Name> employee provide their login or email password to anyone, not even family members.

3.1.3. All hosts that are connected to <Cooperative Name> internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal
computers. Third party connections must comply with requirements as stated in the Third Party Access Policy.

3.1.4. Organizations or individuals who wish to implement non-standard Remote Access solutions to the <Cooperative Name> production network must obtain prior approval from <person or group responsible for policy at Cooperative>.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Third Party Access, Page 8
- Password Policy, see page 60
- Wireless Access Policy, Page 67
- Encryption Policy, Page 75.
- Acceptable Use Policy, Page 80.
- Addresses Section 9.3 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 19 of the accompanying PowerPoint presentation.
- Adapted from “Remote Access Policy” @ [http://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy](http://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy)
- <Reference to ISO 27000, NIST, CRN, if applicable. Make reference to Guernsey Report in Explanatory Notes>

6. Definition of Terms

None.
7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

__________________________________________________________ Date

__________________________________________________________ Date

__________________________________________________________ Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Wireless Access

1. Overview/ Purpose

Insecure wireless configuration can provide an easy open door for malicious threat actors.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to <Cooperative Name> network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the <Information Security Department> are approved for connectivity to a <Cooperative Name> network.

2. Scope

All employees, contractors, consultants, temporary and other workers at <Cooperative Name>, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of <Cooperative Name> must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a <Cooperative Name> network or reside on a <Cooperative Name> site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

3. Policy

All wireless infrastructure devices that reside at a <Cooperative Name> site and connect to a <Cooperative Name> network, or provide access to information classified as <Cooperative Name> Confidential, or above must:

- Be installed, supported, and maintained by an <Approved Support Team>.
- Use <Cooperative Name> approved authentication protocols and infrastructure.
- Use <Cooperative Name> approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.
4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 9.4 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 22 of the accompanying PowerPoint presentation.
- Adapted from “Wireless Communication Policy” @ http://www.sans.org/security-resources/policies/network-security/pdf/wireless-communication-policy
- See also “Wireless Access Control” @ http://www.sans.org/critical-security-controls/control/7

6. Definition of Terms

- **MAC Address** - Short for Media Access Control address, a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub-layers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]
8. Approval

_________________________________________  ____________________________
<insert title of approver>  Date

_________________________________________  ____________________________
<insert title of approver>  Date

_________________________________________  ____________________________
<insert title of approver>  Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Business Continuity and Disaster Recovery

1. Overview/ Purpose

Since disasters happen so rarely, disaster recovery planning process is often overlooked. It is important to realize that having a contingency plan in the event of a disaster gives <Cooperative Name> a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan should be part of the Business Continuity Plan.

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by <Cooperative Name> that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a disruption to business processes or access to critical data and IT services.

2. Scope

This policy is directed to the <Person or Group Responsible> Staff who are accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan; it does not provide requirements around what goes into the plan or sub-plans.

3. Policy

3.1. General Requirements

The following contingency plans must be created to include at a minimum:

3.1.1. Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
3.1.2. Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
3.1.3. Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
3.1.4. Criticality of Service List: List all the services provided and their order of importance.
3.1.5. Explain the order of recovery in both short-term and long-term timeframes.
3.1.6. Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
3.1.7. Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
3.1.8. Mass Media Management: Who is in charge of giving information to the mass media? Also provide some guidelines on what data is appropriate to be provided.
3.2. **Exercise Requirements**

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

3.3. **Review Schedule**

The plan, at a minimum, should be reviewed and updated on an annual basis.

4. **Compliance**

4.1. **Compliance Measurement**

The `<person or group responsible for policy at Cooperative>` will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. **Exceptions**

Any exception to the policy must be approved by the `<person or group responsible for policy at Cooperative>` in advance.

4.3. **Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. **Related Standards, Policies, and Processes (cross references to industry standards)**

- Addresses Section 10.0 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 28 of the accompanying PowerPoint presentation.

6. **Definition of Terms**

- **Disaster** - a sudden calamitous event bringing great damage, loss, or destruction that disables a system component and caused a major outage.
7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

_____________________________________________ Date

<insert title of approver>

_____________________________________________ Date

<insert title of approver>

_____________________________________________ Date

<insert title of approver>

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Compliance Requirements

1. Overview/ Purpose

There are many external compliance requirements which <Cooperative Name> must adhere to from a regulatory standpoint as well as all internal policies that <Cooperative Name> has developed and implemented. These policies must be periodically reviewed and internal cooperative practices modified as necessary to insure compliance with all applicable policies.

The purpose of this policy is to delineate those policies, both internal and external, which <Cooperative Name> has determined to be a requirement for a strong overall cyber security program.

2. Scope

This policy applies to the senior management staff at <Cooperative Name> who are responsible for determining the overall cyber security program and to the <person or group responsible for policy at Cooperative> who provide Information Security guidance to the management staff, implement those policies that are approved by the appropriate authority, and insure that all policies are kept up-to-date with current guidelines/best practices.

3. Policy

<Cooperative Name> will comply with all external policies to include:

- Health Insurance Portability and Accountability Act (HIPAA)
- The Sarbanes–Oxley Act (SOX)
- The Gramm–Leach–Bliley Act (GLBA)
- The Payment Card Industry Data Security Standard (PCI DSS)
- Fair and Accurate Credit Transactions Act of 2003 (FACT Act Red Flags Rules)

<Cooperative Name> senior management and legal counsel will determine those compliance requirements to be appropriate as well as any internal policies developed by <person or group responsible for policy at Cooperative> the combination of which comprise the overall cyber security plan.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.
4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Addresses Section 11.0 of Cyber Security Risk Assessment and Risk Mitigation Plan Review for the Kentucky Public Service Commission, December 9, 2013. See also page 29 of the accompanying PowerPoint presentation.

6. Definition of Terms

None.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

__________________________________________  _______________________
<insert title of approver>  Date

__________________________________________  _______________________
<insert title of approver>  Date

__________________________________________  _______________________
<insert title of approver>  Date
## 9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Encryption

1. Overview/ Purpose

Encryption makes data unreadable to anyone without some secret information --the key. Encryption can provide many benefits to an electric cooperative:
- Properly encrypted data is safer to transport securely.
- Properly encrypted data is easier to delete securely.
- Properly encrypted data can be safely backed up to a third party.

While encryption is a powerful tool for preventing unauthorized access and modification of data, it is also implicated in some business risks:
- Cryptography can be used to conceal the unauthorized use or exfiltration of data.
- Properly encrypted data is not recoverable in the event of key loss.
- Broken cryptography conveys a false sense of security.

This policy sets usage guidelines for the use of encryption to ensure that <cooperative name> can leverage cryptographic software to safeguard our member data and our operations, while mitigating the attendant risks.

2. Scope

This policy shall apply to all appropriate applications for encryption.

3. Policy

It is the responsibility of <Cooperative Name> employees, contractors, vendors and agents with remote access privileges to <Cooperative Name>'s cooperative network to ensure that confidential <Cooperative name> data should be encrypted at rest and in transit whenever practical. Confidential <Cooperative name> data shall be encrypted when it leaves <Cooperative name> premises. This includes:

- <Cooperative name> laptops and other mobile devices
- Portable data storage devices.
- Off-site backup.

3.1. Transport layer security

The use of Transport Layer Security is strongly encouraged for all employee and contractor web browsing and for use on <Cooperative name> web servers.

<Cooperative name> web servers should be configured to use TLS 1.0 or later, and shall not fall back to Secure Socket Layer 3.0 or earlier.
3.2. Full disk encryption

Every <Cooperative name> workstation, laptop and mobile device should have full disk encryption enabled and configured according to best practices for that platform.

Suspend-to-ram (S3 or “sleep”) shall be disabled for platforms which hold encryption keys in memory while suspended. This includes Windows, Linux and Android operating systems, and excludes Apple OS X and iOS devices as well as Google Chromebooks.

3.3. Procuring secure encryption software

All encryption software used at <Cooperative name> must be approved for use by <person or department responsible for this policy>.

Encryption software must be actively supported and audited for security to be eligible for approval. The <person or department responsible for this policy> is responsible for determining whether a piece of cryptographic software meets these criteria, and for maintaining a list of approved encryption software.

3.4. Key Management

All secret key material (keys, passphrases, etc.) used by <Cooperative name> employees and contractors must be stored securely and redundantly. Employees and contractors must submit secret key information to the IT security manager or their designee, for storage in an offline key repository.

Keys shall be stored offline, in a secure location, such as a safe. Offline key repository may not be accessed from an internet connected computer.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.
5. Related Standards, Policies, and Processes (cross references to industry standards)

6. Definition of Terms

- **Actively supported** - A trusted vendor or open source community is actively maintaining the software, such that security issues may be addressed when they are found.
- **Audited for security** - The software specification and its code base have undergone security review by a third party.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of **Cooperative Name** is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The **person or group responsible for policy at Cooperative** shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All **Cooperative Name** personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]
Acceptable Use

1. Overview/ Purpose

<Cooperative Name> is committed to protecting <Cooperative Name> employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet Web browsing, and FTP, are the property of <Cooperative Name>. These systems are to be used for business purposes in serving the interests of the company, and our customers in the course of normal operations. <Cooperative Name>’s intentions in publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Cooperative Name>’s established culture of openness, trust and integrity.

Effective security is a team effort involving the participation and support of every <Cooperative Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment and Information Technology (IT) infrastructure at <Cooperative Name>. These rules are in place to protect the employee’s and <Cooperative Name>’. Inappropriate use exposes <Cooperative Name> to risks including computer virus attacks, compromise of network systems and services, and legal issues. The policy balances the employee’s ability to benefit fully from information technology with the company’s need for secure and effectively allocated IT resources.

2. Scope

This policy applies to employees, contractors, consultants, temporaries and other workers at <Cooperative Name>, including all personnel affiliated with third parties. This policy applies to all equipment, software and/or applications that is owned or leased by <Cooperative Name>.

3. Policy

3.1. General Use and Ownership

3.1.1. While <Cooperative Name>’s network administration desires to provide a reasonable level of privacy, users should be aware that data they create on the corporate systems remains the property of <Cooperative Name>. Because of the need to continually monitor the internal network (Intranet) in order to protect <Cooperative Name>’s IT resources and information, management cannot guarantee the confidentiality of personal information stored on any network device belonging to <Cooperative Name> or in files on the <Cooperative Name> Intranet.

3.1.2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies <Cooperative Name> owned IT
equipment and computers and related services may be used for incidental personal use purposes provided that:

- Usage is reasonable and does not interfere with work productivity.
- Does not directly or indirectly interfere with <Cooperative Name> business operations, IT facilities or electronic mail services.
- Burden <Cooperative Name> with noticeable incremental cost.
- If there is any uncertainty as to what constitutes acceptable personal use, employees should consult their supervisor or manager who will make the determination.

3.1.3. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy.

3.2. Security and Proprietary Information

3.2.1. Users may not encrypt any emails without obtaining written permission from their supervisor and <Cooperative Name>’s <person or group responsible for policy at Cooperative>. If approved, the encryption key(S) must be made known to <Cooperative Name>’s <person or group responsible for policy at Cooperative>.

3.2.2. Data residing on <Cooperative Name> corporate IT systems may be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, and customer lists. Employees should take all necessary steps to prevent unauthorized access to this information.

3.2.3. For security and network maintenance purposes, authorized individuals within <Cooperative Name> may monitor equipment, systems and network traffic at any time, per <Cooperative Name>’s System Logging and Monitoring Policy.

3.2.4. <Cooperative Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2.5. Employees must use extreme caution when opening e-mail attachments received from unknown senders which may contain viruses, e-mail bombs, or Trojan horse code. <Cooperative Name> utilizes Anti-Virus software on each workstation and server as well as filtering all inbound email through an outside security firm, but some unsafe attachments may still find their way through the defenses. If there are ever any questions or if an individual is unsure, please contact <person or group responsible for policy at Cooperative> prior to opening the attachment.

3.2.6. Because information contained on portable and laptop computers is especially vulnerable, special care should be exercised to protect both the computer and its information.

3.2.7. Employees shall not use <Cooperative Name> e-mail, or other facilities to post to news groups, message boards, or websites unless the posting is in the course of business duties.
3.3. Passwords

Please refer to the <Cooperative Name> Password Policy.

3.4. Anti-Virus Protection And Prevention

For complete information please refer to the <Cooperative Name> Malware Prevention Policy.

3.5. Unacceptable Use

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

3.5.1. System and Network Activities

- Under no circumstances is an employee of <Cooperative Name> authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing <Cooperative Name> owned resources.
- Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by <Cooperative Name>.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Cooperative Name> or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)
- Using <Cooperative Name> computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
- Making fraudulent offers of products, items or services originating from any <Cooperative Name> account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee in not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service (DOS), and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to <person or group responsible for policy at Cooperative> is made.
Cyber Security Policy Framework

- Executing any form of network monitoring which will intercept data not intended for the intercepting employee, unless the activity is a part of the employee’s normal job/duty.
- Circumventing user authentication or security of any computer, network or account.
- Interfering with or denying service to any user other than the employee’s computer (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind with the intent to interfere with, or disable, a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, <Cooperative Name> employees to parties outside <Cooperative Name> without Human Resources Department approval.

3.5.2. Email and Communications Activities

The e-mail system is the property of <Cooperative Name> and as such shall not be misused in any of the following manner:

- Sending unsolicited email messages, including the sending of “junk e-mail” or other advertising material to individuals who did not specifically request such material (e-mail spam), unless part of a corporate approved targeted marketing campaign.
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages
- Send or forward e-mails including any of the following: disruptive or offensive messages, still images, audio, or video images, including but not limited to offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. If you receive an email of this nature, promptly notify your immediate supervisor or manager.
- Forge or attempt to forge e-mail messages.
- Disguise or attempt to disguise your identity when sending e-mail.
- Send e-mail messages using another person’s e-mail account unless authorized to do so.
- Copy a message or attachment belonging to another user without permission of the originator.
- Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of Usenet Newsgroups, or message boards.

*For additional information please refer to the <Cooperative Name> E-Mail Use Policy*

3.5.3. Internet Access Activities

The following uses of the Internet, either during working hours or personal time, using <Cooperative Name> equipment or facilities, are strictly prohibited:

- Access, retrieve, or print text and graphics information, which exceeds the bounds of generally accepted standards of good taste and ethics.
- The Internet may not be used to access other systems for which the user has no authorization.
- The Internet or Internet connections shall not be used to access or transfer information that is in violation of Local, State, Federal, or copyright laws, or that contradicts the intent or spirit of these policies and procedures.
- Engage in personal commercial activities on the Internet, including offering services or merchandise for sale.
- Engage in any activity which would compromise the security of any <Cooperative Name> computer or system.
- Endorse any product or services, participate in any lobbying activity, or engage in any active political activity. The prohibition against engaging in any political activity or fundraising activity does not apply to employees that have <Cooperative Name> authorization.
- Employees and contractors, working for <Cooperative Name>, are prohibited from initiating non-work-related Internet sessions using <Cooperative Name> information resources from remote locations. That is, employees shall not connect into <Cooperative Name> resources from home or other non-<Cooperative Name> locations for the purpose of participating in non-job-related Internet activities.
- Employees and contractors working for <Cooperative Name> shall not engage in the transmittal of <Cooperative Name> information or data for non-business purposes and/or personal gain or benefit.

*For additional information please refer to the <Cooperative Name> Internet Access Policy*

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)


6. Definition of Terms

- **Spam** – Unauthorized and/or unsolicited electronic mass mailings
- **Chain Letter** – Chain letter (email) is a term used to describe emails that encourage you to forward them onto someone else
Cyber Security Policy Framework

- **Ponzi** – A Ponzi scheme is a fraudulent investment operation that involves paying returns to investors out of the money raised from subsequent investors
- **Pyramid Scheme** – A fraudulent scheme in which people are recruited to make payments to the person who recruits them while expecting payments from the persons they recruit

7. **Responsibilities**

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. **Approval**

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;insert title of approver&gt;</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. **Revision History**

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Email Use

1. Overview/ Purpose

<Cooperative Name> is committed to protecting <Cooperative Name> employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This email Policy defines proper use of the <Cooperative Name> electronic mail system, and to make users aware of what <Cooperative Name> deems as acceptable and unacceptable use of it. Users shall make every effort to prevent tarnishing the public image of <Cooperative Name> and themselves. When email goes out from <Cooperative Name> the general public will tend to view that message as an official policy statement from the company. <Cooperative Name>’s intentions in publishing an Electronic Mail (Email) Use Policy are not to impose restrictions that are contrary to <Cooperative Name>’s established culture of openness, trust and integrity.

2. Scope

This policy is intended to detail the rules of conduct for Email sent from a <Cooperative Name> Email address or through <Cooperative Name>’s email server and applies to all employees, contractors, consultants, temporaries and other workers at <Cooperative Name>, including all personnel affiliated with third parties.

3. Policy

3.1. Prohibited Use:

The <Cooperative Name> Email system referenced in this policy is the property of <Cooperative Name> and shall not be used for the creation or distribution of any of the following:

- Send or forward Emails consisting of any of the following: disruptive or offensive messages, including but not limited to offensive comments about race, gender, color, disabilities, age, sexual orientation, pornography, obscenity, religious beliefs and practice, political beliefs, or national origin. If you receive an Email of this nature, notify your immediate supervisor.
- Forge or attempt to forge Email messages.
- Disguise or attempt to disguise your identity when sending Email.
- Send Email using another person’s account unless authorized.
- Sending chain letters and offensive joke emails from a <Cooperative Name> Email account is prohibited.
- Forwarding of company confidential messages to external locations.
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.
- Accessing copyrighted information in a way that violates the copyright.
- Breaking into the company’s or another organization’s system or unauthorized use of a password/mailbox.
- Transmitting unsolicited commercial or advertising material unless part of a <Cooperative Name> approved targeted marketing campaign.
Cyber Security Policy Framework

- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus or malware into the corporate network.

Email generated and sent from a corporate Email account should be limited to business content only. Emails shall not contain content, signature lines, or images promoting unsolicited personal views on social, political, religious or other non-business related matters.

3.2. Best Practices

<Cooperative Name> considers Email as an important means of communications and recognizes the importance of proper Email content and speedy replies in conveying a professional image and delivering good customer service.

Users should take the same care in drafting an Email as they would for any other communication. Therefore <Cooperative Name> requests that users adhere to the following guidelines.

3.2.1. Writing Emails:

- Write well-structured Emails and use short descriptive subjects.
- <Cooperative Name>’s Email style is informal. Use of common salutations is acceptable such as “Hi” or “Dear” and the name of the person, and ending with “Best Regards”.
- Signatures should include pertinent information relative to your job classification such as your name, job title, company name, and company logo’s only. A disclaimer will be added underneath your signature. Signature lines shall not contain statements conveying religious, political, or other such references.
- Users should spell check all emails prior to transmission. This can be set to be performed automatically by most Email clients.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending.
- Do not write in ALL CAPITAL LETTERS.
- Do not use Blind Carbon Copy (bcc :) fields unless the bcc: recipient is aware you will be copying a mail to him/her and knows what action, if any, to take. The recipient should be aware that they were copied without other recipient’s knowledge.
- If you forward Emails, state clearly what actions you expect the recipient to take.
- Only send Emails of which the content could be displayed publicly. If they cannot be displayed publicly in their current state, consider rephrasing the Email or using another means of communication.
- Only mark Emails as important if they really are important.
- Don’t set every Email to require a read receipt, only those that really require it.

3.2.2. Replying to Emails:

- Emails should be answered in a timely manner. Users should endeavor to answer priority Emails as soon as possible. Priority Emails are Emails from customers and business partners.
3.3. Personal Use

<Cooperative Name> electronic mail services may be used for incidental personal purposes provided that:

- Usage is reasonable and does not interfere with work productivity.
- Non-work related Email is saved in a separate folder from work related Email.
- Does not directly or indirectly interfere with <Cooperative Name> business operations, IT facilities or electronic mail services.
- It is recommended that anyone using Email for personal reasons have a separate Internet Email account such as Google Gmail, Yahoo Mail, or Hotmail. This will put fewer burdens on the <Cooperative Name> Email servers allowing the system to work more efficiently.

3.4. Email Retention

- User Email is directly retained on the Microsoft Exchange server in a user mailbox for an unrestricted period of time. The retention period of any particular mail article on the server is subject to change by the associated mailbox user making modifications to his/her mailbox through either deleting mail articles or moving mail articles to a storage source external to the Exchange server, or by maintenance efforts to the Email system requiring purging of system data. In the latter case, when the maintenance is planned, notification of such maintenance events will be sent to the user base and <person or group responsible for policy at Cooperative> will coordinate with the user base to avoid loss of Email. In particular cases Email loss may be unavoidable.

- Email contained within system backups is retained for an indefinite period of time, subject to available resources and/or other policies and procedures.

3.5. Expectation of Privacy

The computers and computer accounts given to <Cooperative Name> users are to assist them in the performance of their jobs. Users should not have expectation of privacy while using <Cooperative Name>’s Email system.

3.6. Encryption

Users may not encrypt any Emails without obtaining written permission from their supervisor and <Cooperative Name>’s <person or group responsible for policy at Cooperative>. If approved, the encryption key(s) must be made known to <person or group responsible for policy at Cooperative>.

3.7. Disclaimer

The following disclaimer will be added to each outgoing email:
Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review,
4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.

5. Related Standards, Policies, and Processes (cross references to industry standards)

- Adapted from “Email Policy”@ http://www.sans.org/security-resources/policies/general/doc/email-policy

6. Definition of Terms

- Email - The electronic transmission of information through a mail protocol such as SMTP or IMAP
- Forwarded Email - Email re-sent from an internal network to a different outside or inside point
- Chain Email or Letter - Email sent to successive people. Typically the body of the note has directions to send out multiple copies of the note and promises good luck, money or some other reward if the direction is followed.
- Encryption - 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

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.
7.1.2. The CEO/President shall be responsible for the overall administration of this policy.
7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.
7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<insert title of approver>  
Date

<insert title of approver>  
Date

<insert title of approver>  
Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cyber Security Policy Framework

Internet Access

1. Overview/ Purpose

<Cooperative Name> is committed to protecting <Cooperative Name> employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This Internet Access Policy defines acceptable use of the Internet by employees, contractors, consultants, temporaries and other workers at <Cooperative Name>, including all personnel affiliated with third parties, while using <Cooperative Name>-owned or leased equipment, facilities, Internet addresses, or domain names registered to <Cooperative Name>. <Cooperative Name>’s intentions for publishing an Internet Access Policy are not to impose restrictions that are contrary to <Cooperative Name>’s established culture of openness, trust and integrity.

2. Scope

This policy is intended to detail the rules of conduct for Internet use from a <Cooperative Name> computer or through <Cooperative Name>’s corporate network and applies to all employees, contractors, consultants, temporaries and other workers at <Cooperative Name>, including all personnel affiliated with third parties.

3. Policy

Access to the Internet is available to employees, contractors, subcontractors, and business partners, whose duties require it for the conduct of company business. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy. Internet access may also be limited by user, to specific domains and websites or during predetermed hours, at management discretion.

3.1. Acceptable Use:

<Cooperative Name> provides Internet access to facilitate the conduct of company business. Occasional and incidental personal Internet use is permitted if it does not interfere with the work of personnel, the company’s ability to perform its mission, does not directly or indirectly interfere with <Cooperative Name>’s business operations, IT facilities or electronic mail services, and meets the conditions outlined in official company directives.

3.2. Prohibited Use:

Prohibited Internet activities, whether during normal working hours or on personal time, using <Cooperative Name> equipment include but are not limited to, the following:

- Browsing explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that the company has determined to be off-limits.
- Access, retrieve, or print text and graphics information, which exceeds the bounds of generally accepted standards of good taste and ethics.
3.3. User Responsibilities

Use of computer equipment and Internet access to accomplish job responsibilities will always have priority over incidental personal use. To avoid capacity problems and to reduce the susceptibility of <Cooperative Name> information technology resources to computer viruses, Internet users shall comply with the following guidelines.

- Files obtained via the Internet may only be stored on individual PC hard drives, or on file server shares, after they have been scanned for viruses.

  For additional information please refer to the <Cooperative Name> Malware Prevention Policy

- Video and voice files may not be downloaded from the Internet except when they will be used to serve an approved <Cooperative Name> business function.
• Streaming Video and Music greatly impact corporate network bandwidth and access speeds and may not be initiated except when they will be used to serve an approved <Cooperative Name> business function.

• Users shall follow existing security policies, and procedures in the use of Internet services shall refrain from any practices, which might jeopardize <Cooperative Name> computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.

• It is suggested that users learn about, and adhere to Internet etiquette, customs, and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.

• Users shall conduct themselves in a way that reflects positively on <Cooperative Name>, since they are identified as <Cooperative Name> employees on the Internet.

3.4. Expectation of Privacy

The computers and computer accounts provided for <Cooperative Name> users are to assist them in the performance of their jobs. Users should not have expectation of privacy anywhere they go on the Internet while using <Cooperative Name>’s computer system. Users of the Internet should be aware that most sessions on the Internet are not private.

3.5. System Monitoring

<Cooperative Name> has the right, but not the duty, to monitor any and all aspects of its computer systems, including but not limited to, adherence to the Internet Access policy. Circumvention of any monitoring software or tools is prohibited and is subject to the same penalties as any other violation of the Internet access policy.

4. Compliance

4.1. Compliance Measurement

The <person or group responsible for policy at Cooperative> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the <person or group responsible for policy at Cooperative> in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with cooperative HR policies.
5. Related Standards, Policies, and Processes (cross references to industry standards)


6. Definition of Terms

None.

7. Responsibilities

7.1. Responsibilities for this policy are delineated as follows:

7.1.1. The Board of Directors of <Cooperative Name> is responsible for the content of this policy and its implementation.

7.1.2. The CEO/President shall be responsible for the overall administration of this policy.

7.1.3. The <person or group responsible for policy at Cooperative> shall direct and monitor the implementation of appropriate practices/procedures in accordance with this policy.

7.1.4. All <Cooperative Name> personnel are responsible for following the guidelines and procedures laid out in this policy as well as for reporting known violations of the policy.

[Explanatory Note: Cooperatives should feel free to alter section to reflect the specific responsibility requirement determined by Cooperative management.]

8. Approval

<insert title of approver>  Date

<insert title of approver>  Date

<insert title of approver>  Date

9. Revision History

<table>
<thead>
<tr>
<th>Date of Change(s)</th>
<th>Revised by</th>
<th>Summary of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix A: Example Backup Policy

<Cooperative Name> Backup Schedule by System

Enterprise Servers

- One incremental backup set for each weekday. This backup media shall be retained offsite for the greatest period of; one week or that specified in the <Cooperative Name> data retention policy.

- Three weekly global backup sets, archived after close of business each Friday evening. This backup media shall be retained offsite for the greatest period of; two weeks or that specified in the <Cooperative Name> data retention policy.

- 12 monthly global backup sets, archived after close of business on the last Friday of each month. This backup media shall be retained offsite for the greatest period of; eleven (11) months or that specified in the <Cooperative Name> data retention policy.

CIS Servers

- One incremental backup set for each weekday. This backup media shall be retained offsite for the greatest period of; one week or that specified in the <Cooperative Name> data retention policy.

- Three weekly global backup sets, archived after close of business each Friday evening. This backup media shall be retained offsite for the greatest period of; two weeks or that specified in the <Cooperative Name> data retention policy.

- 12 monthly global backup sets, archived after close of business on the last Friday of each month. This backup media shall be retained offsite for the greatest period of; eleven (11) months or that specified in the <Cooperative Name> data retention policy.

MDM server

- 2 monthly global backup sets, archived after close of business on the last Friday of each month. This backup media shall be retained offsite for the greatest period of; one month or that specified in the <Cooperative Name> data retention policy.

GIS Server(s)

- Three weekly global backup sets, archived after close of business each Friday evening. This backup media shall be retained offsite for the greatest period of; two weeks or that specified in the <Cooperative Name> data retention policy.

Mail Server

- Drive duplication completed once a month. This backup media shall be retained offsite for the greatest period of; one month or that specified in the <Cooperative Name> data retention policy.
DA Servers

- Monthly global backup sets, archived after close of business on the last Friday of each month. This backup media shall be retained offsite for the greatest period of; one month or that specified in the <Cooperative Name> data retention policy.

SCADA

- Ignite Recovery backup for each system annually in January. This backup media shall be retained in coordination with <Cooperative Name> data retention policy.

- Global backup from /Root for each system annually in January. This backup media shall be retained in coordination with <Cooperative Name> data retention policy.

- Backup from /home bi-annually in January and July. This backup media shall be retained in coordination with <Cooperative Name> data retention policy.

- Backup from /DB quarterly in January, March, June, and September. This backup media shall be retained in coordination with <Cooperative Name> data retention policy.

PBX & Voice Mail Servers

- Global backup bi-annually in March and September. This backup media shall be retained in coordination with <Cooperative Name> data retention policy.
Appendix B: Financial Security Check Examples

A Financial History Check must be obtained for Final Applicants as outlined below.

<table>
<thead>
<tr>
<th>Required</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Officer and Executive Administrative positions at or above the level of Vice President.</td>
<td>CEO/President, Executive Assistant, Sr. Vice President, Vice President.</td>
</tr>
<tr>
<td>Leadership positions at or above the level of Supervisor.</td>
<td>Managers, Supervisors, Accounting personnel with access to check printing materials (software, or check paper).</td>
</tr>
<tr>
<td>All positions within the cooperative having a primary responsibility for handling cash.</td>
<td>Member Service Representatives, Billing Clerks, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Not Required</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrequent or incidental access to cash. Restricted access to finance system for purposes of conducting cooperative business.</td>
<td>Access to petty cash in a department. Administrative Assistant responsible for accepting occasional payments in the form of cash. Accounting personnel responsible for entering data in the accounting system.</td>
</tr>
</tbody>
</table>
Appendix C: General Password Construction Guidelines

Passwords are used for various purposes at <Cooperative Name>. Some of the more common uses include: user-level accounts, web accounts, email accounts, screen saver protection, and router logins. Since very few systems have support for one-time tokens (i.e. dynamic passwords which are only used once), everyone should know how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or Foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words “<Cooperative Name>”, “<Cooperative City Location>”, or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g. secret1, 1secret)

Strong passwords have the following characteristics:

- At least eight alphanumeric characters long.
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+=\[\]{}|~\<\>)
- Not a word in any language, slang, dialect, jargon, etc.
- Not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create a password that can be easily remembered. One way to do this is create a password based on a song title, affirmation or other phrase. For example, the phrase might be: “This may be one way to remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.

NOTE: Do not use either of these examples as passwords.
Appendix D: Anti-Virus and Malware Exemption Form

In accordance with <Cooperative Name> Malware Prevention Policy all exemptions to this policy must be approved by <person or group responsible for policy at Cooperative> in advance. This form serves as a record of requests and the approval status. The original copy shall be filled in accordance with <person or group responsible for policy at Cooperative> practices and a copy shall be provided to the requesting employee for their records.

All details pertaining to the requested exemption shall include; Hardware/Software information (name, location, etc.), Cooperative ID, Policy sections to be exempted, and justification for the request.

Requesting Employee Information

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Signature ___________________________ Date ___________________________

Exemption Request Information

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Authorization: ______ Approved ______ Declined

Requesting Employee’s Department Head

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Signature ___________________________ Date ___________________________

Technology Department

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Signature ___________________________ Date ___________________________
Appendix E: Network Management Exemption Form

In accordance with <Cooperative Name> Network Management Policy all exemptions to this policy must be approved by <person or group responsible for policy at Cooperative> in advance. This form serves as a record of requests and the approval status. The original copy shall be filled in accordance with <person or group responsible for policy at Cooperative> practices and a copy shall be provided to the requesting employee for their records.

All details pertaining to the requested exemption shall include; Hardware/Software information (name, location, etc.), Cooperative ID, Policy sections to be exempted, and justification for this request.

Requesting Employee Information

____________________________________________________________________________________
Last Name First Name
____________________________________________________________________________________
Signature Date

Exemption Request Information

____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________

Authorization: _____ Approved _____ Declined

Requesting Employee’s Department Head

____________________________________________________________________________________
Last Name First Name
____________________________________________________________________________________
Signature Date

Technology Department

____________________________________________________________________________________
Last Name First Name
____________________________________________________________________________________
Signature Date