Cyber Security - Employee Awareness Training Program
Cyber Security Employee Awareness Training Program

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

Acknowledgements

Table of Contents

Introduction

Cyber Security Employee Awareness Training Program

Overview/Purpose

Scope

Standards and Legislative Requirements

Program

Roles and Responsibilities

Training Needs Assessment

Awareness Training

Security Training

New Employee Orientation Training

Related Standards

Definition of Terms

Revision History
Effective Cyber Security begins with awareness. A comprehensive Cyber Security program not only focuses on physical and technical security practices and methods, but also on the human aspects of cyber security threats and common methods employed by malicious parties to take advantage of the inherent weaknesses that humans with inadequate awareness and training represent.

This document was prepared to provide resources to the individual cooperatives to aid in the development of an Employee Awareness Training Program. Each individual cooperative should seek to develop a policy and program that meets their individual needs and structure. Wherever possible, the documentation provided herein is open source without restriction on its use.
Cyber Security
Employee Awareness Training Program

Overview/Purpose
<Cooperative Name> recognizes the need to protect <Cooperative Name>, our members, employees and cooperative data, and systems, from growing cybersecurity threats. This document establishes a formal program for ongoing Employee Awareness Training within <Cooperative Name> to ensure employees are adequately trained to recognize, appropriately act upon, and mitigate threats and protect those member, employee and company resources.

Scope
All full time and temporary employees and other workers at <Cooperative Name> and its subsidiaries must receive identified introductory and ongoing Cyber Security Awareness Training.

Standards and Regulatory Requirements
A formal Cyber Security Training program is required for compliance with many standards, regulatory requirements, and Cyber Security Best Practices. Requirements applicable to <Cooperative Name> are listed below, along with NERC CIP standards. <Cooperative Name>, at this time, is not bound by NERC CIP standards but they are included herein for reference and consideration of use. Other standards and regulations may be developed and/or implemented subsequent to this program acceptance and should be adopted and implemented as necessary.

ISO/IEC 27001 & 27002 §8.2.2 - All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

PCI DSS §12.6 - Make all employees aware of the importance of cardholder information security.

• Educate employees (for example, through posters, letters, memos, meetings and promotions).

• Require employees to acknowledge in writing that they have read and understood and will comply with the company’s security policy and procedures.

Health Insurance Portability and Accountability Act (HIPPA) §164.308.(a).(5).(i) - Implement a security awareness and training program for all members of its workforce (including management).

Red Flag Rules §16 CFR 681.1(d)-(e). Employees should be trained about the various red flags to look out for, and/or any other relevant aspect of the organization’s Identity Theft.
Prevention Program.

RUS Emergency Restoration Plan (ERP) – Note relevant cyber security regulations.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standard. §CIP-004-3(B)(R1) - The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

(Note: The cyber security CIP standards will be changing to Version 5 and likely 6 prior to forthcoming compliance dates of April 1, 2016 for high and medium category assets and April 1, 2017 for low category assets. Additional, under Version 3, CIP-002-3 must also be addressed by co-ops included in the NERC compliance registry.)
Program

Roles and Responsibilities

1. **Manager of Technical Services** (and similar functions) – Ensures that high priority is given to effective security awareness training for all employees. This will include implementation of a viable IT Cyber Security program with a strong awareness and training component. The Manager of Technical Services will:
   - Assign responsibility for IT Security;
   - Ensure that a `<Cooperative Name>` wide IT Cyber Security program is implemented, is well-supported by resources and budget, revised on a periodic basis (annually or a different basis) to reflect lessons learned, actual events, and available technology, and is effective; and
   - Ensure that `<Cooperative Name>` has enough sufficiently trained personnel to protect its IT resources;
   - Establish the overall strategy for the IT security awareness and training program;
   - Ensure that the Board of Directors, President and CEO, Senior Vice Presidents, Managers, system and data owners, and others understand the concepts and strategy of the security awareness and training program, and are informed of the progress of the program’s implementation;
   - Ensure Board of Director meeting minutes reflect the ongoing discussion of cyber security issues;
   - Promote the development and certification of the IT security program staff, full-time- or part-time security officers, and others with significant security responsibilities;
   - Ensure that `<Cooperative Name>`’s IT security awareness and training program is funded and staffed;
   - Ensure that all users are sufficiently trained in their security responsibilities and only have access to the systems and information they need to perform their job; and
   - Ensure that effective tracking and reporting mechanisms are in place.

2. **Computer Systems Analyst** – Functions in the role of Information Technology Security Manager and has tactical level responsibility for the IT security and awareness training program. The Computer Systems Analyst will:
• Ensure that awareness and training material developed and presented is appropriate and timely for the intended audiences;
• Ensure that awareness and training material is effectively deployed to reach the intended audiences;
• Ensure that users and managers have an effective way to provide feedback on the awareness and training material and its presentation;
• Ensure that awareness and training material is reviewed periodically and updated when necessary; and
• Assist in establishing a tracking and reporting strategy.

3. Managers – Have responsibility for complying with IT security awareness and training requirements established for their users. Managers will:
   • Work with the Manager of Technical Services and Computer Systems Analyst to meet shared responsibilities;
   • Serve in the role of system/data owner, where applicable;
   • Consider developing individual development plans (IDP’s) for users in roles with significant security responsibilities;
   • Ensure that all users (including contractor’s) of their systems (i.e., general support systems and major applications) are appropriately trained in how to fulfill their security responsibilities before allowing them access;
   • Ensure that users (including contractor’s) understand specific rules of each system and application they use; and
   • Work to reduce errors and omissions by users due to lack of awareness and/or training.

4. Users – Users comprise the largest audience and are the single most important group of people that can help reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, other agency personnel, visitors, guests, and other collaborators or associates requiring access. Users must:
   • Understand and comply with <Cooperative Name> security policies and procedures;
   • Be appropriately trained in the rules of behavior for the systems and applications to which they have access;
   • Work with management to meet training needs;
- Be aware of actions they can take to better protect <Cooperative Name>'s information. The actions include, but are not limited to: strong password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and rules to deter spread of spam or viruses and worms.

[Explanatory Note:] The cooperative should modify roles and responsibilities, and titles to match their structure.
Training Needs Assessment

1. A needs assessment will be conducted to determine <Cooperative Name>’s awareness and training needs. As a minimum, the following roles will be involved and addressed to identify any special training needs:

- Executive Management – Identify directives and laws (including data breach) that form the basis of the security program. Ensure comprehension of leadership roles in effecting full compliance by users within their departments;
- Identified Security Personnel – Ensure cooperative staff and individuals who are acting as consultants to <Cooperative Name> are well educated on security policy and accepted best practices;
- System Owners – Ensure a broad understanding of security policy and a high degree of understanding regarding security controls and requirements applicable to the systems they manage;
- System Administrators and IT Support Personnel – Ensure a high degree of technical knowledge in effective security practices and implementation;
- Operational Managers and System Users – Ensure a high degree of security awareness and training on security controls and rules of behavior for systems they use to conduct business operations.
Cyber Security Employee Awareness Training Program

Awareness Training

1. IT security awareness will be used to focus attention on security and should not be confused with Security Training. Various methods will be utilized to promote awareness of security to include, but not be limited to the following methods:
   - Utilization of security awareness posters and banners throughout all <Cooperative Name> campus;
   - Targeted email’s with an Awareness message appropriate to the group;
   - All employee emails with an appropriate message to the group;
   - Presentations by IT security managers at employee meetings; and
   - Scheduled online security awareness training.

Security Training

1. All Technical Services staff involved with IT systems will attend security basics and literacy training courses relative to their areas of oversight and level of security responsibility.
2. <Cooperative Name> will seek to hire and/or to provide education for IT staff who hold, or to obtain, degrees from accredited universities, or industry recognized certifications in IT Security. Examples of such include but are not limited to:
   - Bachelor’s/Master’s Degree in Information Systems Security
   - Certified Information Systems Security Professional (CISSP)
   - Certified Ethical Hacker (CEH) Certification
   - Global Information Assurance Certification (GIAC)

New Employee Orientation Training

Newly hired full-time and part-time employees, contractors and consultants, will be provided Cyber Security orientation training to consist of the following:
1. Overview of <Cooperative Name> employed computing technology.
2. Provision of <Cooperative Name> IT Cyber Security Policies Packet. This should include covering of major aspects of the policies with a signed acknowledgment that the employee has read and understood <Cooperative Name>’s security policies and procedures.
Related Standards

Definition of Terms

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>