

Cybersecurity Awareness Training Policy

# Overview/Purpose

**<Utility Name>** recognizes that properly educated employees are an important means of cybersecurity defense. This document establishes a formal program for ongoing cybersecurity awareness training within **<Utility Name>**.

# Scope

On an annual basis, all **<Utility Name>** employees will receive cybersecurity awareness training.

# Policy

The Information Security Steering Committee (ISSC) defines the content of the cybersecurity awareness training, which must be updated at least yearly to account for changes in threats and industry best practices.  
  
Training topics shall meet the following requirements:

* PCI DSS 12.6
* Red Flag Rule
* NERC CIP (if applicable)
* RUS ERP

Training should be provided in a format appropriate to the **<Utility Name>**, preferably in short segments (no longer than 10 minutes each ), in the form of Computer Based Training, which should support mobile devices.

Cybersecurity Awareness training can be created in-house by **<Utility Name>** or can make use of external, commercially available content. The training shall include reporting features to ensure that employees attended and satisfactorily complete training.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> 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.

## Exceptions

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

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* PCI DSS Requirements 12.6  
  (<https://www.pcisecuritystandards.org/document_library>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **HR** | **All employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |