

Personnel Security Policy

# Overview/Purpose

Understanding the importance of cyber and personnel security via individual responsibilities and accountability is 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 updated and reinforced.

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

# Scope

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

# Policy

The **<HR Department Name>** is solely authorized to conduct and oversee the background check process pursuant to this policy on behalf of **<Utility 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 and shall develop a program for periodically following up on hired individuals to assure there have been no events requiring a revocation of privileges.

## Security Requirements

### Reference checks

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

### 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 **<Utility Name>**.

### Financial screening

Financial history check must be conducted for final applicants for positions that have access to any sensitive information.

### 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 Name>**. 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 Name>** will implement a program communicating **<Utility Name>** expectations relating to cybersecurity. This program shall include periodic training and formal acceptance of computer use polices.

## Training Requirements

* + 1. All new users must attend an **<Utility Name>** approved security awareness training class, prior to, or at least within 14 business days of being granted access to any information systems.
    2. All users must sign an acknowledgement stating they have read and understand **<Utility Name>** requirements regarding computer security policies and procedures.
    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 **<Utility Name>** information resources.
    4. **<person or group responsible for policy at Utility >** must prepare, maintain, and distribute one or more information security manuals that concisely describe **<Utility Name>** information security policies and procedures.
    5. All users must attend computer security compliance training annually, and pass the associated examination, if applicable.
    6. **<person or group responsible for policy at Utility>** must develop and maintain a process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy at Utility**> 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 at Utility**> 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

* Adapted from “Cyber Security Policy Framework”  
  (<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
  Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.
* 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](http://www.iso27001security.com/ISO27k_Model_policy_on_outsourcing.docx)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| HR | **CEO/GM** | **CIO**  **Legal Department** | **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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |