

System Acceptance and Configuration Policy

# Overview/Purpose

This policy establishes the requirement that security measures and configuration settings must be 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.

# Scope

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

# 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 for policy >**.

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 configuration 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, 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 >** shall:

* + 1. Monitor systems for configuration baseline and policy compliance. Automated tools should be used to apply initial configurations, and to efficiently identify when a system is not consistent with the approved baseline configuration and when remediation actions are necessary.
    2. Reapply all baseline configurations to systems, as appropriate, when a system undergoes a material change, such as an operating system upgrade.
    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.
    4. Before a system is placed into production, **<person or group responsible for policy >** 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.

# 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

* 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.

# Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **System Admin**  **Network Admin** | **IT Department** |

*[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) |
|  |  |  |
|  |  |  |