

Outsourced Information Processing Policy

# Overview/Purpose

In order to fully leverage the advantages of the most up-to-date technology available, **<Utility Name>** may contract with outside sources to provide that technological advantage as opposed to developing solutions internally. This approach provides many advantages to include cost savings, faster implementation, and expertise often not available internally. While providing the aforementioned advantages, **<Utility 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 IT resources that are accessed, or provided, by third parties.

# Scope

This policy applies to all contractors, vendors and agents who may have a legitimate business-related need to connect to the 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 **<Utility 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.

# Policy

## Assessing Outsourcing Risks

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

## Contracts

* + 1. A formal contract between **<Utility Name>** and the outsourcer should exist.
    2. All contracts shall be submitted to **<person or group responsible for policy>** for accurate content, language and presentation.

## Hiring and training of employees

* + 1. Outsourced employees, contractors and consultants working on behalf of **<Utility Name>** may be subjected to background checks equivalent to those performed on employees.
    2. Companies providing contractors/consultants directly to **company** to outsourcers shall perform at least the same standard of background checks as those indicated above.
    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 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.

## Security audits

* + 1. If applicable, the outsourcer will provide SOC 1 and SOC 2 Reports, or agree to **<Utility Name>**’s right to audit.
    2. The frequency of audit shall be determined by **<person or group responsible for policy>.**

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to with 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.
* Adapted from ISO 27001 Security – “Information Security Policy on Outsourcing” ([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 |
| IT Manager | **CEO/GM** | **CFO**  **COO**  **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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |