Vendor Management Policy

Purpose

The purpose of the (District/Organization) Vendor Management Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to (District/Organization), its business partners, and its stakeholders from any of its vendors.

Audience

The (District/Organization) Vendor Management Policy applies to any individuals that interacts, set up or manage any (District/Organization) vendors.

Contents

[Assessments](#_Access)

[Management](#_Access_1)

Policy

### Assessments

* Vendors granted access to (District/Organization) **Information Resources** must sign the (District/Organization) Vendor Non-Disclosure Agreement/Business Associate Agreement.
* Vendors must be evaluated prior to the start of any service and thereafter on a bi-annual basis.
* A vendor risk assessment must be performed on vendors with access to **confidential information** and/or critical vendors.
* Vendors with PCI DSS compliance requirements must have their status reviewed on an annual basis.

### Management

* Vendor agreements and contracts must specify:
  + The (District/Organization) information the vendor should have access to,
  + How (District/Organization) information is to be protected by the vendor,
  + How (District/Organization) information is to be transferred between (District/Organization) and the vendor,
  + Acceptable methods for the return, destruction or disposal of (District/Organization) information in the vendor’s possession at the end of the contract,
  + Minimum information security requirements,
  + Incident response requirements,
  + Right for (District/Organization) to audit vendor.
* If a vendor subcontracts part of the information and communication technology service provided to (District/Organization), the vendor is required to ensure appropriate information security practices throughout the supply chain.
* The vendor must only use (District/Organization) **Information Resources** for the purpose of the business agreement.
* Work outside of defined parameters in the contract must be approved in writing by the appropriate (District/Organization) point of contact.
* Vendor performance must be reviewed annually to measure compliance to implemented contracts or SLAs. In the event of non-compliance with contracts or SLAs regular meetings will be conducted until performance requirements are met.
* Vendor’s major IT work activities must be entered into or captured in a log and available to (District/Organization) IT management upon request. Logs must include, but are not limited to, events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
* Any other (District/Organization) information acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes or divulged to others.
* Vendor personnel must report all security incidents directly to the appropriate (District/Organization) IT personnel.
* (District/Organization) IT will provide a technical point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.
* New vendors must provide (District/Organization) a list of key personnel working on the contract.
* Vendors must provide (District/Organization) with notification of key staff changes within 24 hours of change.
* Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to (District/Organization) or destroyed within 24 hours.
* Upon termination of contract, vendors must be reminded of confidentiality and non-disclosure requirements.
* Upon termination of contract or at the request of (District/Organization), the vendor must surrender all (District/Organization) badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized (District/Organization) IT management.

Definitions

See Appendix A: Definitions

References

* ISO 27002: 7, 13, 15, 16
* NIST CSF: DE.CM

Waivers

Waivers from certain policy provisions may be sought following the (District/Organization) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Modified Date | Approved Date | Approved By | Reason/Comments |
| 1.0.0 | February 2018 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |