

Vendor/Third-Party Access Policy

Purpose

The purpose of the %ORGANIZATION% Vendor Access Policy is to establish the rules for vendor access to %ORGANIZATION% Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of %ORGANIZATION% information. Vendor access to %ORGANIZATION% Information Resources is granted solely for the work contracted and for no other purposes.

Audience

The %ORGANIZATION% Vendor Access Policy applies to all individuals that are responsible for the installation of new %ORGANIZATION% Information Resource assets, and the operations and maintenance of existing %ORGANIZATION% Information Resources, and who do or may allow vendor access for support, maintenance, monitoring and/or troubleshooting purposes.

Policy

- Vendors must comply with all applicable %ORGANIZATION% policies, practice standards and agreements, including, but not limited to:
 - Safety Policies
 - Privacy Policies
 - Security Policies
 - Auditing Policies
 - Software Licensing Policies
 - Acceptable Use Policies
- Vendor agreements and contracts must specify:
 - The %ORGANIZATION% information the vendor should have access to
 - How %ORGANIZATION% information is to be protected by the vendor
 - Acceptable methods for the return, destruction or disposal of %ORGANIZATION% information in the vendor's possession at the end of the contract
 - The Vendor must only use %ORGANIZATION% information and Information Resources for the purpose of the business agreement

- Any other %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
- %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.
- Each vendor must provide %ORGANIZATION% with a list of all employees working on the contract. The list must be updated and provided to %ORGANIZATION% within 24 hours of staff changes, wherever possible.
- Each vendor employee with access to %ORGANIZATION% Confidential Data must be approved to handle that information at a level commensurate with its classification level.
- Vendor personnel must report all security incidents directly to the appropriate %ORGANIZATION% IT personnel.
- If vendor management is involved in %ORGANIZATION% security incident management, the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable %ORGANIZATION% change control processes and procedures.
- If appropriate, regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate %ORGANIZATION% IT management.
- All vendor maintenance equipment on the %ORGANIZATION% network that connects to the outside world via the network, telephone line, or leased line, and all %ORGANIZATION% Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the %ORGANIZATION% Password Policy and Admin/Special Access Policy.
- Vendor's major work activities must be entered into a log and available to %ORGANIZATION% IT management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times, wherever possible.
- 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 %ORGANIZATION% or destroyed within 24 hours.
- Upon termination of contract or at the request of %ORGANIZATION%, the vendor will return or destroy all %ORGANIZATION% information and provide written certification of that return or destruction within 24 hours.
- Upon termination of contract or at the request of %ORGANIZATION%, the vendor must surrender all %ORGANIZATION% badges, access cards, equipment

and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized %ORGANIZATION% IT management.

- Vendors are required to comply with all regulatory and %ORGANIZATION% auditing requirements, including the auditing of the vendor's work.
- All software used by the vendor in providing service to %ORGANIZATION% must be properly inventoried and licensed.
- Each vendor granted access to any %ORGANIZATION% Information Resource must sign the %ORGANIZATION% Information Security Policy Acknowledgement Form which stipulates that he/she:
 - Has read and understands the security policies
 - Understands his/her responsibilities to comply
 - Understands the consequences of an infraction.

Version History

Version Number	Date	Reason/Comments
V1.00.00	November, 2006	Document Origination