Vendor Access Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors, they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to ABC Company.

# II. Purpose

This policy establishes the rules for vendor access to ABC Company’s Information Resources and support services, vendor responsibilities, and protection of ABC Company information.

# III. Scope

This policy applies to all Staff that use ABC Company Information Resources.

# IV. Policy

Vendors must comply with all applicable ABC Company policies, procedures, and agreements including, but not limited to:

* Safety policies
* Privacy policies
* Security policies
* Auditing policies
* Software licensing policies
* Acceptable use policies

The IT Department shall implement and maintain a consolidated list of vendors with access to ABC Company’s Information Resources. Such list, as well as vendor agreements and contracts, must specify:

* The ABC Company resources the vendor to which the vendor has access.
* How ABC Company information is to be protected by the vendor.
* Acceptable methods for the return, destruction, or disposal of ABC Company information in the vendor’s possession at the end of the contract.
* The vendor must only use ABC Company information and Information Resources for the purpose of the business agreement.
* Any other ABC Company information acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes or divulged to others.

ABC Company will provide a point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with ABC Company policies.

Each vendor must provide ABC Company with a list of all Staff working on the contract. The list must be updated and provided to ABC Company within 24 hours of staff changes.

Each on-site vendor employee must acquire an ABC Company identification badge that will be displayed at all times while on ABC Company premises. The badge must be returned to ABC Company when the employee leaves the contract or at the end of the contract.

Each vendor employee with access to ABC Company sensitive information must be cleared to handle that information.

Vendor personnel must report all security incidents directly to the appropriate ABC Company personnel. If vendor management is involved in ABC Company security incident management the responsibilities and details must be specified in the contract.

Vendor must follow all applicable ABC Company change control processes and procedures.

Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate ABC Company management.

All vendor maintenance equipment on the ABC Company network that connects to the outside world via the network, telephone line, or leased line, and all ABC Company IT 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 ABC Company Password Policy. Vendor’s major work activities must be entered into the Third Party Service Provider Log Form and available to ABC Company management upon request. Log entries must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

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 ABC Company or destroyed within 24 hours.

Upon termination of contract or at the request of ABC Company, the vendor will return or destroy all ABC Company information and provide written certification of that return or destruction within 24 hours.

Upon termination of contract or at the request of ABC Company, the vendor must surrender all ABC Company identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized ABC Company management.

Vendors are required to comply with all State and ABC Company auditing requirements, including the auditing of the vendor’s work.

All software used by the vendor in providing service to ABC Company must be properly inventoried and licensed.

Third-party agreements that directly, or indirectly, impact Information Resources are required to -include explicit coverage of all relevant security requirements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Asset agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO09.05, APO10.05, APO12.02, APO13.07, BAI02.05-06, DSS01.05, DSS05.07

GDPR Article 25, 32

HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(b)(4)

ISO 27001:2013 8.3, A.5.1.1, A.9.2.6, A.11.1.2, A.13.2

NIST SP 800-37 3.3, 3.6, 3.7

NIST SP 800-53 AC-2, AC-21, CA-3, PA-4, PE-2-5, PS-4-6, SA-9

NIST Cybersecurity Framework ID.AM-4-6, ID.RA-4, ID.RM-1, ID.SC-2-4, PR.AT-3, DE.CM-6

PCI 2.5, 7.1-3, 8.1-2, 8.5-6, 8.8, 9.1-4