User Privilege 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

This policy defines the privileges various users on the organizational network are allowed to have, specifically defining what groups of users have privileges to install computer programs on their own or other systems. This policy defines the users who have access to and control of sensitive or regulated data. This policy defines Internet access to specific sites for some users or other ways they may or may not use their computer systems.

# II. Purpose

This policy is designed to minimize risk to organizational resources and data by establishing the privileges of users of data and equipment on the network to the minimum allowable while still allowing users to perform job functions without undue inconvenience.

# III. Scope

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

# IV. Policy

A. Types of users

Main categories of users on a computer or network include:

* Restricted user – can operate the computer and save documents but can't save system settings.
* Standard user (power user) – can change many system settings and install programs that don't affect Windows system files.
* Administrators – have complete access to read and write any data on the system and add or remove any programs or change system settings. The majority of users on most common networks should be restricted users on their local computers. Only users with special training or a need for additional access should be allowed to change system settings and install programs that are not operating system programs. This is because many viruses and adware or spyware may be installed in a subtle manner by tricking the user or the installation may be completely transparent to the computer user. If the user does not have the ability to install programs or change settings to a more vulnerable setting, most of these potential security problems can be prevented. Therefore only users that demonstrate a need and ability for power user or administrator access on local machines shall permitted to have this level of access. Upon demonstration of a special need for additional access, the IT Director must approve the access before it can be made effective. Examples of users with special privileges include domain administrators, help desk personnel, and application developers.

B. Network resources

Most network users will have access to the following types of network resources.

* E-mail – most users will have full access to their own e-mail. They will not be able to transfer ownership to someone else.
* A mapped drive on a networked file server – a folder on a drive that only the primary user of this drive can read and write exclusive of domain administrators. The user will not be able to transfer ownership to someone else.
* A shared group or organizational division's drive – a folder that members of specific groups or divisions in the organization may access. Access may be read or write and may vary by organizational requirements.
* Access to databases – databases stored on a shared drive or other resource. Most databases will have a standard user level which gives users appropriate permissions to enter data and to see report information. However only the database administrators shall have full access to all resources on a database. Database administrators will only have full access to the database that they administer.

Groups that may be allowed additional access include:

* Backup operator – allowed to read data on the domain for the purpose of saving files to backup media. This group cannot write all data on the domain.
* Account operator – can manage and view information about user accounts on the domain.
* Server operator – has full privileges on servers including reading and writing of data, installing programs, and changing settings.
* Domain administrator – has full privileges on all computers in the domain including servers and workstations. Privileges include reading and writing data, installing programs, and changing settings.

C. Security Considerations

The Chief Security Officer shall ensure:

* The organization shall implement administrative, physical, and technical safeguards to protect sensitive information confidentiality, integrity, and availability. The organization shall ensure that any agent, including a subcontractor, agrees to implement reasonable and appropriate safeguards.
* Electronic mechanisms corroborate that sensitive information has not been altered or destroyed in an unauthorized manner. Information Systems that contain sensitive information shall automatically check for data integrity (e.g. check sums verification, digital signature).
* Third party service providers and business associates (e.g. billing services, hardware and software vendors, external consultants, lawyers) have been identified. The organization has established written contracts or other arrangements with business contacts and third party service providers that meet security requirements. Contracts are in place with third party service providers to ensure security requirements are addressed. Before sensitive information is disclosed, the organization shall receive assurances from third party service providers and each associate that they appropriately safeguard information. Refer to the Third Party Service Providers Policy for more information.
* The organization shall be provided with a report if the third party service provider or business associate experiences a security incident. Procedures shall specify the process to terminate the contract with the third party service provider or business associate if they have violated a material term of the contract or experienced a material breach.

# 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 APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(3)(ii)(A), 64.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.310(b)

ISO 27001:2013 5.3, 6.1.3, A.6.1.2, A.7.2.1, A.8.1.3, A.9.1.2, A.9.2.2-3, A.9.4.1, A.9.4.4

NIST SP 800-37 3.3, 3.6, 3.7

NIST SP 800-53 AC-2-3, AC-5-6, AC-24, CM-5, PL-4, PS-6, PS-7, SA-9

NIST Cybersecurity Framework PR.AC-1, PR.AC-4, PR.AT-2, DE.CM-1-3, DE.DP-2, RS.RP-1

PCI 7.1-2, 8.1, 10.2, A1.1-2, A3.4.1