Access Rights

Access rights to [company name] system components are limited to authorized personnel only, with all end-users being properly provisioned in accordance with stated access rights policies and procedures. This includes using all applicable provisioning and de-provisioning forms as necessary along with ensuring users' access rights incorporate Role Based Access Control (RBAC) protocols or similar access control initiatives.

Additionally, users with elevated and/or super user privileges, such as system administrators, I.T. engineers and other applicable personnel, are responsible for ensuring access rights for all users (both end users and users with elevated and/or super user privileges) are commensurate with one's roles and responsibilities within [company name].

Thus, the concepts of "separation of rights" and "least privileges" are to be adhered to at all times by [company name] regarding access rights to system components. Specifically, "separation of rights" implies that both the "functions" within a specified system component, for which there are many, should be separated along with the roles granted to end-users and administrators of these very system resources. "Functions" pertains to the actions a system component and its supporting components (i.e., the OS and applications residing on the server) can perform and the associated personnel who have authority over these functions. Thus, when permissible, functions (such as read, write, edit, etc.) should never be grouped together and end-users and administrators should not be granted access to multiple functions.

By effectively separating access rights to system components whereby only authorized individuals have access to the minimum rights needed to perform their respective duties, [company name] is adhering to the concept of "least privileges", a well-known and best practices rule within information technology.

Furthermore, passwords used by all users must meet or exceed all stated [company name] policies for password complexity requirements. Along with ensuring strong passwords, additional password parameters regarding account lockout policies and password resets are also to be enforced with appropriate system settings. Furthermore, only authorized personnel are allowed to make any changes to the password complexity rules and lockout policies to system components.

Methods of Authentication

Authentication to [company name] system components are to be enacted by utilizing one of or a combination thereof the following three (3) stated factors:

(1). Something a user knows: This method of authentication generally includes passwords, passphrases, numerical PINS or some other type of knowledge that is known by a user.

(2). Something a user has: This method of authentication generally includes some type of physical attribute provisioned to a user, such as a swipe card, badge reader, key fob, smart card, dynamically generated unique identifier or any other type of utility owned by the user.

(3). Something a user is: This method of authentication generally includes a unique physical attribute of the user, commonly known as biometrics. Many devices will read a user's biometrics for purposes of authentication, which may include, but is not limited to, the following:

- Iris Scanners
- Palm Scanners
- Fingerprint Readers
- Facial Recognition Utilities
- Voice Recognition Devices

Additionally, along with utilizing the above three (3) methods of authentication, all users are to invoke strong authentication measures (more commonly known as two factor authentication) at all times for ensuring access to [company name] system components are protected at all times. Two factor authentication is met by incorporating two (2) of the three (3) given methods of authentication, and must be used for accessing the following environments listed below:

Two Factor Authentication Matrix

System Components and Environments that Require "Two Factor Authentication"		Description of "Two Factor Authentication" measures used	Additional Comments
(1).			
(2).			
(3).			
(4).			
(5).			

Password Parameters

- User password parameters are set to require users to change passwords at least every ninety (90) days.
- Password parameters are set to require passwords to be at least seven (7) characters long.
- Password parameters are set to require passwords to contain both numeric and alphabetic characters.
- Password parameters are set to require that new passwords cannot be the same as the previous four (4) passwords used.
- Authentication parameters are set to require that a user’s account is locked out upon the sixth (6th) invalid logon attempt.
- Password parameters are set to require that once a user’s account is locked out, it remains locked for a minimum of thirty (30) minutes or until a system administrator resets the account.
- System configuration settings are set to require that system/session idle time out features have been set to and period of fifteen (15) minutes or less.

- For a user requesting a password reset that is not in the physical presence of appropriate and designated IT personnel, they must undergo a verification process, which consists of one of the following activities: (1). Verbal confirmation of vital statistical information to intended party who may reset their password. This verbal confirmation may consist of a date of birth, Social Security Number or some other unique identifier. (2). Verbal confirmation of employment data, such as length of employment, annual salary, etc. (3). Verbal confirmation of some other unique identifier developed by [company name].
- First-time passwords for new users, and reset passwords for existing users, are set to a unique value and changed after each use.