

# Information Systems Access Policy

## I. PURPOSE

The purpose of this policy is to maintain an adequate level of security to protect <COMPANY NAME> data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of <COMPANY NAME> information systems.

## II. POLICY

Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

Who is Affected: This policy affects all employees of this <COMPANY NAME> and its subsidiaries, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject disciplinary action up to and including termination.

Affected Systems: This policy applies to all computer and communication systems owned or operated by <COMPANY NAME> and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

Entity Authentication: Any User (remote or internal), accessing <COMPANY NAME> networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- Automatic logoff
- And Unique user identifier
- At least one of the following:
  - Biometric identification
  - Password
  - Personal identification number
  - A telephone callback procedure
  - Token

Workstation Access Control System: All workstations used for this <COMPANY NAME> business activity, no matter where they are located, must use an access control system approved by <COMPANY NAME>. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOS. Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly log out of all

applications and networks. Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 30 minutes). Users will then be required to re-log on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

Disclosure Notice: A notice warning that those should only access the system with proper authority will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and those unauthorized users should disconnect or log off immediately.

System Access Controls: Access controls will be applied to all computer-resident information based on its' Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

Access Approval: System access will not be granted to any user without appropriate approval. Management is to immediately notify the Security Administrator and report all significant changes in end-user duties or employment status. User access is to be immediately revoked if the individual has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job.

Limiting User Access: <COMPANY NAME> approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorized.

Need-to-Know: Users will be granted access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required performing their jobs.

Compliance Statements: User's who access to this <COMPANY NAME>'s information systems must sign a compliance statement prior to issuance of a user-ID. A signature on this compliance statement indicates the user understands and agrees to abide by these <COMPANY NAME> policies and procedures related to computers and information systems. Annual confirmations will be required of all system users.

Audit Trails and Logging: Logging and auditing trails are based on the Data Classification of the systems.

Confidential Systems: Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access
- All privileged commands must be traceable to specific user accounts

In addition logs of all inbound access into <COMPANY NAME> 's internal network by systems outside of it's defined network perimeter must be maintained.

Audit trails for confidential systems should be backed up and stored in accordance with <COMPANY NAME> back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs must be audited on a periodic basis. Audit results should be included in periodic management reports.

Access for Non-Employees: Individuals who are not employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use the <COMPANY NAME> computers or information systems unless the written approval of the Department Head has first been obtained. Before any third party or business partner is given access to this <COMPANY NAME> computers or information systems, a chain of trust agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization.

Unauthorized Access: Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. System privileges allowing the modification of 'production data' must be restricted to 'production' applications.

Remote Access: Remote access must conform at least minimally to all statutory requirements including but not limited to HCFA, HRS-323C, and HIPAA.

# Password Policy

## I. PURPOSE

The purpose of this policy is to ensure that only authorized users gain access to <COMPANY NAME>'s information systems.

## II. POLICY

To gain access to <COMPANY NAME> information systems, authorized users, as a means of authentication must supply individual user passwords. These passwords must conform to certain rules contained in this document.

Who is Affected: This policy affects all employees of this <COMPANY NAME> and it's subsidiaries, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject disciplinary action up to and including termination.

Affected Systems: This policy applies to all computer and communication systems owned or operated by this <COMPANY NAME> and it's subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

User Authentication: All systems will require a valid user ID and password. All unnecessary operating system or application user IDs not assigned to an individual user will be deleted or disabled.

Password Storage: Passwords will not be stored in readable form without access control or in other locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls.

Application Passwords Required: All programs, including third party purchased software and applications developed internally by this <COMPANY NAME> must be password protected.

Choosing Passwords: All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character. The use of control characters and other non-printing characters are prohibited. All users must be automatically forced to change their passwords appropriate to the classification level of information. To obtain a new password, a user must present suitable identification.

Changing Passwords: All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized

parties. All users must be forced to change their passwords at least once every sixty- (60) days.

Password Constraints: The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. After three unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three minutes, or (c) if dial-up or other external network connections are involved, disconnected.