Continuum Health Partners	***Information Technology***		
	ORIGINAL DATE: February 15, 2008	REVISED DATE: October 20, 2011	PAGE NUMBER: 1 of 6
POLICY NUMBER **IT-003**	SUBJECT: **Information Technology Access Management Policy**		APPROVAL: CIO

Purpose:

The Continuum Health Partners, Inc. (CHP), ***Information Technology Access Management Policy*** outlines a set of standards that must be followed to safeguard CHP's patients' information and CHP's internal data against unauthorized access; to promote availability of data; and, to safeguard the confidentiality and the integrity of the data that is entrusted to CHP.

This Policy applies to all information system users who create, distribute, access or manage information via CHP's information technology systems including personal, business unit, or corporate computers, and the networks and communication services by which they are connected. The Policy equally applies to individuals and enterprises that by nature of their relationship with CHP are entrusted with Company *Confidential* and *Internal Use Only* information. This Policy also applies to any device used to store, process, or communicate CHP's proprietary or other protected information.

Definitions:

Associate (Employee): A member of the CHP workforce that is paid via CHP Payroll.

Affiliate: A member of the CHP workforce that is not paid via CHP Payroll.

Credentialed Affiliate: A member of the CHP workforce that is not paid via CHP Payroll; whose role is to provide patient care and whose affiliation with CHP is managed via CHP's Credentialing Department.

Information System User: A CHP associate (employee), affiliate or credentialed affiliate that has been authorized by CHP to gain access to one or more of CHP's Information Systems for the purpose of performing his/her role based defined responsibilities.

Information System (Application) Owner: Individual assigned ultimate responsibility for a system to ensure that the program accomplishes the specified objective(s) or set of requirements established for that application, including appropriate security safeguards.

Confidential Data: Confidential Data is information protected by statute(s), regulation(s), CHP Policy(s) or contractual language.

Internal Data: Internal data is information that must be guarded due to proprietary, sensitive, ethical or privacy considerations; it is information that is restricted to personnel designated by CHP as having a legitimate business purpose for accessing such data.

Data Availability: Data/information is accessible and readily useable upon demand by an authorized information system user.

Data Confidentiality: Data/information that is private/sensitive is not accessible to or disclosed to unauthorized persons.

Data Integrity: Data/information that is not altered or destroyed in an unauthorized manner.

***System Security Incident*:** An event that poses a threat to or that has compromised the confidentiality, integrity or availability of an information system; examples include, but are not limited to: unauthorized system access, unauthorized changes to system configuration, events that are unusual for the CHP environment, etc.

Policy

ALL CHP Information System Users & People Managers:

All information system users must be issued a copy of this Policy by their Supervisor/Manager. Supervisors/Managers must document (using attached *Policy Acceptance Form*) that they have issued a copy of this Policy to each information system user for whom they have approved access.

It is the responsibility of the information system user's Manager to submit timely System Access Requests (SAR). As per CHP's *HR1002-Computer and Communication Security Policy,* when a workforce member no longer requires access or requires a different level of access to a CHP Information System the change in access requirement must be communicated to IT immediately.

SAR Processing Timeframes:
The IT Department will process each SAR as follows:

• New/Move/Update :	Within 3 business days of request
• Re-Enable:	Within 8 business hours of request
• Terminate:	Within 8 business hours of request

Requests for access to CHP's Information Systems are centrally managed by the IT Department. In instances where system access to a CHP Information System is not managed by IT, the access management process employed by the System Owner must be consistent with this Policy.

The '*requested for*' name documented on the SAR must be identical to the information system user's name as documented with CHP's Human Resources (HR) Department, as it appears on the credentialed information system user's license, or as it appears on the information system user's state/government issued identification.

Information system users will be assigned *a unique name and/or number (Access ID or User ID)* for identification and tracking of user activity within the system(s).

All SARs must identify the ***minimum*** system access required for the information system user to perform his/her assigned duties.

Access level requests that conflict with an information system's access security policy must be escalated to the administrator of the system for review and must be approved by a Vice President (VP).

All SARs require management level approval with the exception of access requests for Non-Credentialed Affiliates, which require Vice President approval (see Information System Access Requests for *Non-Credentialed Affiliates*).

When training is a pre-requisite for gaining access to an information system the information system user is responsible for scheduling and attending the required training.

To mitigate the threat of unauthorized access to CHP Information Systems:

- Access accounts that have not been used within 90 days will be disabled
- To re-enable a disabled account a *Re-Enable SAR* must be processed
- Access accounts that have not been used within 180 days, where feasible, are subject to removal from the application; where not feasible, account will remain in disabled status
- To re-create access for a workforce member whose account has been removed from the application a *New SAR* must be processed

Access IDs and Passwords cannot be shared as it is a violation of CHP Policy to disclose your Access ID and Password to another party (access ID may be disclosed to an IT Helpdesk Associate to complete the creation of a new Access ID or to reset the password that is linked to an existing Access ID).

Information system users must utilize their own Access ID and Password to establish a log-in session to access a device, information system and/or electronic data. It is against CHP Policy to utilize the *log-in session* of another information system user.

Information system users must lock or log-out of their workstation/device when not actively using their workstation/device or when leaving workstation/device unattended so as to be compliant with *CHP HR Policy: 1002 – Computer and Communication Security.*

It is recommended that information system users save CHP data to their assigned personal network share ("P" drive) or to a departmental network share ("H" drive) as data stored on the internal local memory of a device ("C" drive) is at risk of being lost (theft of device, accidental deletion, file corruption, etc.).

CHP Enterprise Screen Saver Configuration:
To mitigate the threat of unauthorized access to CHP Information Systems the following screen saver configuration has been implemented:

- *Clinical/Shared Workstations* that sit idle for a period extending beyond one (1) minute are configured to auto-display a screen saver

- *Non-Clinical/Individual Workstations* that sit idle for a period extending beyond two (2) hours a password protected screen saver will auto-activate. In order to use the workstation once the screen saver is displayed, user will have to enter network password to gain access.

This security measure does not override previous Policy statement; all workforce members are expected to lock/logout of their workstation when device is not in use or device is left unattended as per CHP HR Policy: 1002 – Computer and Communication Security.

CHP Standard Password Parameters:

- Password length must be a minimum of eight (8) characters
- Password must contain three (3) of the four (4) categories:
    1. English uppercase characters (A through Z)
    2. English lowercase characters (a through z)
    3. Base 10 digits (0 through 9)
    4. Non-alphabetic characters (for example, !, $, #, %)
- Password must be changed every 180 days
- Previous (8) passwords cannot be used
- Access ID lockout after four (4) failed log-in attempts

Password resets are handled by the CHP Helpdesk. Helpdesk Associates will ask information system users to respond to several key identity verifiers. In the event that a Helpdesk Associate feels that the information system user has not verified his/her identity in an accurate manner the Associate will direct the information system user to submit a *Confidential Information Form* to his/her Supervisor/Manager for processing.

Information System Access Requests for ***Non-Credentialed Affiliates:***

- Require Vice President (VP) approval

- VP signature serves as verification that this Policy has been shared with the information system user and that he/she has agreed to abide by the Policy

- Documentation of said agreement will be maintained by the VP or his/her designee

- Access is granted for only 1 year. To extend access beyond the 1 year period a *Renewal for CHP Affiliate SAR* must be submitted to IT at least three days in advance of account expiration date and the SAR must be approved by a VP.

ALL People Managers:

Are required to process a Service Request (SR) when re-allocating computing devices (desktops, laptops, PDAs, etc.) from one information system user to another as IT must sanitize the device.

Are required to process a SR when disposal of a computing device(s) is required as CHP must ensure that the device is sanitized prior to disposal.

Are to ensure that required data stored on the hard drive ("C" drive) is copied to a network share prior to scheduling device sanitization for re-allocation/removal.

Must assist Information System Owner(s) with annual access reviews to ensure that only information system users with an active employment status maintain system access.

ALL Information System Owners:

System Access Requests for the creation of Administrative System Accounts require Director-Level approval.

When feasible Information Systems must be configured to utilize CHP's standard based centralized authentication and access control architecture, currently, Active Directory (AD). Information Systems that cannot be configured to authenticate through Active Directory must be configured with the following Password Parameters:

- Password length must be a minimum of eight (8) characters
- Password must contain three (3) of the four (4) categories:
    1. English uppercase characters (A through Z)
    2. English lowercase characters (a through z)
    3. Base 10 digits (0 through 9)
    4. Non-alphabetic characters (for example,! $, #, %)

- Password must be changed every 180 days
- Previous (8) passwords cannot be used
- Access ID lockout after four (4) failed log-in attempts

Information Systems that cannot be configured with above mentioned password parameters must be documented as exceptions to this Policy via the CHP *IT Policy Exception Request Form.*

Information System Access Request for ***Vendor Support/Maintenance* Access IDs**:

- Must include access ID activation 'start' and 'end' date and time that correlates to the timeframe for which the vendor requires system access to complete required maintenance/support

- Should vendor require 24 x 7 access a Policy Exception Request must be processed

Must perform, document and manage annual user reviews of system access to affirm that only active authorized workforce members maintain access to CHP's Information System(s).

Must immediately report system security incidents to the IT Security Officer.

Policy Authority/Enforcement:

Continuum Health Partners, Inc.'s Information Security Officer has general responsibility for enforcement of this policy. Members of the Continuum Health Partners' staff who violate this policy will be subject to disciplinary action in accordance with Department of Human Resources *Policy-HR1002: Computer and Communications Security*. Violation of this policy may result in disciplinary action up to and including termination.

Related Policies and Procedures:

- HR Policy: 1002-Computer and Communication Security.
- HR Policy: 6001-Change of Name and Address
- HR Policy: 7005-Employment Transfer Process
- HR Policy: 9001-Termination and Sign Out Process and Form
- System Access Request Management Process
- IT Policy Exception Management Procedure

CHP Information Technology Department
Policy/Procedure Acceptance Form

Policy/Procedure Title:	**Policy #:**
Department or IT Team:	**Department Manager or IT Team Director:**

By signing below you are affirming that you understand and that you will comply with the aforementioned Policy/Procedure and that your Supervisor/Manager has informed you that failure to comply with said Policy/Procedure may result in disciplinary action up to and including termination of employment.

Workforce Member Name	Signature	Date
Workforce Member Supervisor/Manager Name	Signature	Date

Continuum
Health Partners

CHP IT Department Policy/Procedure Approval Document

Policy/Procedure Title: Information Technology Access Management Policy	**Policy #:** IT-003
Approval Requested For: Revisions to current version of published policy	**Date:** 07/25/11

REVISION SUMMARY (IF APPLICABLE):

- Revised Policy Format - Policy Statements were organized under the following sections: All *CHP Information Users & People Managers*; *All People Managers*; and *All Information System Owners*, in an effort to make the Policy more user friendly

- The following Policy Statements have been added:

    1. CHP Enterprise Screen Saver Standard Configuration

    2. Recommended methodology for the saving of data onto network drive(s) and relocation and disposal of computing devices

    3. Requirement concerning the processing of *Policy Exception Requests* in the event that compliance to one or more of the Policy Statements is not feasible

- The following Policy Statements have been modified:

    1. Policy Statement concerning user access reviews has been modified to reflect frequency of "annual"

    2. Policy Statement concerning disabling access account for workforce members that are on Leave of Absence (LOA) has been removed. Access accounts for workforce members that are on LOA will be disabled or removed from a system(s) according to account inactivity parameters described on page two (2) of the Policy

    3. Policy Statement concerning required password parameters has been modified to reflect current parameters implemented for Active Directory, which serves as the model for all CHP Information Systems.

Continuum
Health Partners

Your Approval of Referenced Policy/Procedure Confirms That:

1 – You agree to the policy statements and/or the procedural steps detailed in the referenced policy/procedure.

2 – You will ensure that Workforce Members under your leadership are aware of and that they comply with the referenced policy/procedure.

3 – You agree to notify the IT Audit & Compliance Administrator immediately of any changes in the IT Environment that relate to referenced policy statements/procedure steps.

Name & Title	Signature	Signature Date
Ross Macaluso, Director of IT Audit & Compliance	Ross J Macaluso	7/25/11
Eli Tarlow, Director of Service Delivery		7/26/11
Jill Wojcik, Director of Enterprise Distributed Architecture		7.28.11
Mark Moroses, Chief Information Officer		8/3/11