

**CENTRAL STATE HOSPITAL  
Policy and Procedure**

SUBJECT: **COMPUTER POLICY AND PROCEDURES**

---

ANNUAL REVIEW MONTH: March

RESPONSIBLE FOR REVIEW: Director, Information Services and Performance Evaluation

LAST REVISION DATE: July 2009

---

**Purpose:**

To provide policy and procedure for Central State Hospital (CSH) employees who use computers, computer peripherals, computer software including the full array of LAN based services (including e-mail and the Internet) and to ensure the integrity, security, and confidentiality of all mission critical databases.

**Definitions:**

LAN	Local Area Network
Computer	Desktop PC 's, handheld PC 's, servers, and laptop PC 's.
Computer Peripheral	Printers, PDA 's, digital cameras, scanners, or any other device that attaches permanently or temporarily to a PC.
e-mail	Electronic mail received and sent via GroupWise or the internet
ISPE	Information Services and Performance Evaluation Department including CSH 's Data Management operations.
DHR-OIT	Department of Human Resources Office of Information Technology staff located at CSH. Currently only applications staff
Help Desk	A service entity, contacted via a toll free number or website, established to function as the clearing house for all end-user problems associated with computer equipment and software.
LAN Engineer	The head of the DELL OR IBM operations located at CSH
DDO	Division Chief, Department Head or Office Director
GAIT2010	Privatization of DHR OIT tech support, contract awarded to IBM and AT&T

## **POLICY:**

### **1. LAN Access: Internet and e-mail usage:**

- a. Staff Expectations:** CSH employees will only use e-mail and the internet for business related communication with other CSH/Department of Behavioral Health and Developmental Disabilities (DBHDD) staff and/or to improve job knowledge. If a CSH employee violates any of the provisions stated in this policy, access may be terminated, and (dependent upon the severity of the situation) disciplinary action could result.
- b. Restrictions:** CSH ' s e-mail and Internet resources are provided only for the use of CSH staff. E-mail and Internet activity is subject to all existing laws (federal, state and local) as well as DBHDD policies and procedures. Furthermore, CSH employs the use of software that enables the blocking of certain categories of Internet sites and the monitoring of all Internet usage. This monitoring includes a record of the user, physical location of the PC, the Internet site visited, and the time/date of the visit. Any requests for denial of Internet access must be routed to the Data Manager via the appropriate DDO. Denial will only allow access to CSH ' s site and certain business related sites.
- c. E-mail Accounts:** E-mail accounts will be provided only to staff that require this resource in the execution of their duties as defined by appropriate management staff. In order to protect the LAN from viruses, any known non-work related file received through e-mail should not be opened. If personal e-mail messages with attachments are received at work, the message should be forwarded to a personal e-mail address to be opened at home after hours and then immediately deleted.
- d. Specifically Prohibited E-mail activities:**
  - i. The use of vulgar, abusive or hateful language/images or any language that could cause the recipient distress, embarrassment or unwarranted attention.
  - ii. Personal attacks including those based on ethnicity, national origin, religion, sexual orientation or affiliation.
  - iii. Communications originated with anonymity.
  - iv. Impersonation, misrepresentation, or unauthorized disclosures by an individual claiming to be acting in an official capacity.
  - v. Using another individual ' s password to send or receive e-mail.
  - vi. Using e-mail to support or oppose political candidates or ballot measures.
  - vii. The generation of or forwarding of chain letters.
  - viii. Activities for the purpose of personal or commercial financial gain solicitation of business or services, sales of personal property, etc.

- ix. Use of e-mail in any manner that would violate DBHDD's client confidentiality policy.
- x. Use of e-mail in any manner that would violate any local, state or federal laws.

**e. Specifically Prohibited Internet Activities:**

1. Use of the Internet for non-work related activities. Explicitly prohibited is the access or attempted access of adult/explicit sites, hate sites, gambling sites, sites advocating violence/criminal activities, video/audio streaming sites, and chat or "pager" sites.
2. Activities for the purpose of personal or commercial financial gain, solicitation of business or services, sales of personal property, etc.
3. Use of the Internet for unauthorized transfer of or entry into a file.
4. Using the Internet to gain unauthorized access into any computer system.
5. Use of the Internet to engage in illegal copying of software protected by U.S. copyright law (may also result in civil damages and criminal penalties).
6. Use of any log-in ID/Password other than your own.

**f. Other specifically prohibited LAN activities, e.g., access to "J" drive or other common drives:**

Any use of the LAN is restricted to work related activities. Explicitly prohibited is the posting of files on various drives that could cause another employee unwarranted attention including personal attacks (inclusive of those based on national origin, ethnicity, religion, sexual orientation or affiliation) and the posting of images that could be considered offensive to others.

1. Use of the LAN in any manner that would violate DBHDD's client confidentiality policy.
2. Use of the LAN in any manner that would violate any local, state or federal laws.
3. Use of any log-in ID/Password other than your own.

**2. Computer/Computer Peripheral Hardware:**

*Use of computers in the facility workplace are for work related tasks only*

- a. **Purchase and Distribution:** Requests for computers and computer peripherals must be generated via a "Request for Information Technology Products" form CSH 1619 (Attachment II) routed through the appropriate DDO to the Data

Manager. The Data Manager, with the counsel of the CSH IT Review Committee, will coordinate the purchase, distribution and issuance of computer hardware throughout the facility. Funds for the purchase of equipment will typically come from budgeted sources administered by the Data Manager; however, exceptions to this may be arranged by the DDO and financial services staff.

- b. **Intra-facility Equipment Transfer:** No computer equipment will be transferred (one room to another) without the appropriate notification of the Data Manager. When computers or peripherals are transferred, the form “Relocation of Computer Equipment” CSH 1617 (Attachment III) must be completed by the DDO or designee and forwarded to the Data Manager. Any other required notifications/forms should be handled per existing CSH Property Control procedures. If assistance is required in relocating computer equipment, contact the Help Desk, and a DELL OR IBM technician will respond subject to the following conditions:
1. New Equipment: DELL OR IBM will deliver the equipment to site, install the equipment and complete the necessary inventory paperwork.
  2. Replacement Equipment: DELL OR IBM will deliver the replacement equipment, install the equipment, return the replaced equipment for repair or surplus, and complete the necessary inventory paperwork.
  3. Relocation of Equipment: Staff should follow existing procedures for relocating state equipment. The responsibility for the physical move and resulting inventory paperwork resides with DDO staff. In general, DELL OR IBM staff will not be made available to assist in movements of this nature unless specifically requested via the Help Desk.
  4. Surplus Equipment: DDO staff will cause the equipment to be moved to the Data Management area and complete the “Relocation of Computer Equipment” form CSH 1617 (Attachment III). DELL OR IBM staff will then determine whether the equipment is salvageable or should be placed in surplus. If the equipment is to be placed in surplus, CSH Property Control staff will facilitate the paperwork necessary to remove it from the CSH equipment inventory (not the computer equipment inventory maintained by the Data Manager). Property Control staff will pick up the equipment from DELL OR IBM and deliver it to the appropriate surplus area.
- c. **Inventory:** Periodically, DDO 's shall be required to reconcile their computer inventory with reports submitted by the Data Manager to the CSH Leadership Team. Any discrepancies must be resolved and reported to the Data Manager within ten working days of receipt of the inventory.
- d. **Equipment Allowed Off Campus:** Only individually assigned laptop computers, handheld computers, and PDAs may be taken off campus, with the following exception: the LAN Engineer or the Data Manager may authorize removal of computer equipment for repairs by an appropriately contracted repair entity.

- e. **Help Desk:** Any malfunctions or other problems with computer equipment must be reported to the Help Desk. If the Help Desk cannot solve the problem, the Help Desk personnel will create a ticket regarding the problem and forward it to the DELL OR IBM staff.
- f. **Equipment Configurations:** Configurations, settings, and parameters shall be set by DELL OR IBM staff only. This includes, but is not limited to, the setting of Windows default fonts, screen colors, backgrounds, screen savers, etc. Unauthorized alteration of these configurations can potentially cause serious LAN issues, including problems with mission critical applications such as Avatar.

### 3. Computer Software:

*Unlicensed software is not permitted on CSH computers; consequently, software shall not be copied or reproduced in any manner for personal, private, or business use unless specifically allowed by the license.*

- a. **Purchase and Distribution:** The Data Manager, with the counsel of the CSH IT Review Committee, will coordinate the purchase, distribution and issuance of computer software throughout the facility. Funds for the purchase of software will typically come from budgeted sources administered by the Data Manager; however, exceptions to this may be arranged by the DDO and Financial Services staff. **Computer Games:** The DBHDD has mandated that all computer games (including those furnished with the Windows Operating System) be removed from all facility computers and that, subsequently, no game software be installed on facility computers. The only exception is the allowance in designated training rooms, and by certain staff who are demonstrating or providing assistance to clients for the purpose of developing client computer skills (in both of these situations the Data Management shall be made aware of the necessity for such software). Each DDO shall work with the Data Manager and DELL OR IBM staff to ensure compliance.
- b. **Software Installation:** Installation/de-installation of software shall be by DELL or IBM staff only, with the exception of certain pre-approved programs, e.g., software, etc. Exceptions to this restriction are available from the Data Manager. The Data Manager shall maintain all original software and software licenses purchased by CSH.
- c. **Help Desk:** Any problems with supported software must be communicated (phone/website) to the Help Desk. Software lists supported via this procedure are available from the Data Manager.
- d. **Personal Software:** Personal software purchased by an employee must be clearly work related and approved by the DDO and the Data Manager prior to installation. Original personal software media must be kept with the computer on which it is installed. Neither the Data Manager or DELL OR IBM staff will support personal software problems. If personal software precipitates any LAN problems it will be removed. Personal software must be removed when an employee ends his/her employment.
- e. **Downloading Software:** All software restrictions apply to downloads from any

source. Additionally, downloaded software shall be checked for viruses prior to installation. Requests for assistance in virus checking should be directed to the Help Desk.

#### 4. Confidentiality and Security:

*Access to client information using computers and computer software is subject to the policy and procedures in CSH Policy 4.29 on Confidentiality.*

- a. **Storage of Confidential Data:** Confidential information will be stored on computers in such a manner so as to restrict access by unauthorized personnel. Confidential information stored on desktop computers or the LAN will be secured by password access to the directory, application or file. Under no circumstances shall confidential data be placed on the “J” shared drive.
- b. **Off-Site Usage of Data:** If data are required to be used off of the hospital campus, it will be kept secure and confidential by the employee. Under no circumstances should hospital data reside on an employee’s home PC that other family members access.
- c. **E-mailing Confidential Data:** Information transmitted via e-mail to GroupWise recipients is encrypted with industry standard 128-bit encryption methods; however circumstances may require that appropriate management staff be given access to an employee’s e-mail files. Information e-mailed to non-GroupWise recipients is not considered secure, and confidential information should not be attached without some form of encryption, e.g., password protection via a word processing document, etc.
- d. **Passwords:** Passwords allowing access to restricted information systems will be approved by the DDO and the Data Manager as appropriate.
- e. **Backup:** Users are responsible for backing up their mission critical data either locally or to the LAN.
- f. **Login/Logoff:** Users are responsible for the confidentiality of their login information. Certain usage of the LAN and Internet is tracked via a permanent record of the login data; consequently, users are considered to be the sole owners of their login ID’s and passwords. Users should logoff PC’s that are left unattended in areas accessible to others.
- g. **External Data Storage:** Users are responsible for insuring that data brought into CSH from external sources, e.g., zip<sup>8</sup> disks, floppy disks, USB drives, etc., are scanned for possible virus content.
- h. **Modem Usage:** Users responsible for downloading or uploading data via a PC based modem must make the Data Manager aware of these activities.

#### PROCEDURES:

A. **Access to Electronic Data:**

To access data through a PC connected to the LAN, you must log into the network utilizing a Novell user name and password.

<b><u>Responsibility</u></b>	<b><u>Action</u></b>
<b>End User</b>	<ol style="list-style-type: none"><li>1. Complete "Local Area Network (LAN) Security Application" CSH 1618 (Attachment 1). <b>This form must be filled out completely and legibly. Latest version of form may be found on CSH's web site.</b></li><li>2. Read CSH Computer Policy 1.13. <b>Latest version of policy may be found on CSH's web site.</b></li></ol>
<b>DDO</b>	<ol style="list-style-type: none"><li>1. Review form for completeness and validity.</li><li>2. Sign form.</li><li>3. Send form to Data Manager, Wilkes Building.</li></ol>
<b>Data Manager</b>	<ol style="list-style-type: none"><li>1. Review form for completeness.</li><li>2. Sign form.</li><li>3. Initiate Help Desk ticket for DELL OR IBM.</li><li>4. Give copy of signed form to LAN Administrator for Processing.</li></ol>
<b>DELL OR IBM LAN Administrator</b>	<ol style="list-style-type: none"><li>1. Create or modify user account.</li><li>2. Notify DDO and/or requestor when account is ready.</li></ol>

B. **Requests for Hardware, Software, or LAN Drops:**

Requests for any software, computers, printers, monitors, or other peripherals (anything that connects or installs on a PC) must be made on a Request for Technology Products form using the following procedure.

<b><u>Responsibility</u></b>	<b><u>Action</u></b>
<b>End User</b>	<ol style="list-style-type: none"><li>1. Complete "Request for Technology Products" CSH 1619 (Attachment II).</li></ol>
<b>DDO</b>	<ol style="list-style-type: none"><li>1. Review form for completeness and validity.</li><li>2. Sign form.</li><li>3. Send form to Data Manager, Wilkes Building.</li></ol>
<b>Data Manager</b>	<ol style="list-style-type: none"><li>1. Examine form for completeness.</li><li>2. Resolve any unanswered questions about the request.</li><li>3. Present the request to the IT Review Committee at next scheduled meeting (2<sup>nd</sup> Tuesday of each month).</li></ol>

**IT Review  
Committee**

1. Evaluate the request based on its merit, funding, and resources available.
2. Approve or deny the request.

**Data Manager**

1. Send a copy of the request back to the DDO indicating, the status. Indicate whether the request was approved or denied.
2. If the request was approved, submit EDP request to the DBHDD contact person in Atlanta (required on all software and many hardware products).
3. When all approvals are received, order product from approved vendor.
4. When item is received, make appropriate inventory entries.
5. Initiate request for DELL OR IBM to install item for user.

**C. Movement of Computer Equipment:**

An inventory of all computer equipment is maintained in the ISPE Department. Any movement of computer equipment must be reported to ISPE for inclusion and modification to the computer inventory database.

**Responsibility**

**Action**

**Person Who Moves  
Equipment**

1. Complete "Computer Equipment Relocation" CSH 1617 (Attachment III).
2. Submit form to DDO Property Control Office, Central Property Control and Data Manager in Wilkes Building.

**Data Manager**

1. Examine form for completeness.
2. Enter information into database.

**Approved:**

**This policy was approved by the CEO and CMO in September 2009.**

**Attachments:**

Attachment I: LAN Security Application form (CSH 1618)  
Attachment II: Request for Technology Products form (CSH 1619)  
Attachment III: Computer Equipment Relocation form (CSH 1617)

## Central State Hospital

### Local Area Network (LAN) Security Application Form

New Account     
  Revise Existing Account     
  Delete Account  
 Username: \_\_\_\_\_

Complete the following information ( <b>please print clearly</b> ):	
<b>Last Name:</b>	
<b>First Name:</b>	
<b>Middle Initial (required):</b>	
<b>Office Phone:</b>	
<b>Title:</b>	
<b>Division/Department/Office:</b>	
<b>Building/Floor/Room:</b>	

Check all Software applications needed:		
<b>GroupWise</b>	<input type="checkbox"/>	
<b>PeopleSoft</b>	<input type="checkbox"/>	Requires additional application - contact HR Manager for HR access - contact Financial Services Manger for FN access
<b>Avatar</b>	<input type="checkbox"/>	Requires additional application - contact Data Manager
<b>Go Screen</b>	<input type="checkbox"/>	Requires additional application - contact Data Manager
<b>Other (Specify)</b>	<input type="checkbox"/>	

**I have reviewed the CSH computer policy (1.13). I understand that my User ID and password are my responsibility and are not to be shared.**

\_\_\_\_\_ Employee – Printed Name     
 \_\_\_\_\_ Employee Signature     
 \_\_\_\_\_ Date

\_\_\_\_\_ Supervisor – Printed Name     
 \_\_\_\_\_ Supervisor – Signature     
 \_\_\_\_\_ Date     
 \_\_\_\_\_ Supervisor - E-mail  
 GroupWise User ID

\_\_\_\_\_ Division/Dept./Office Dir. – Printed Name     
 \_\_\_\_\_ DDO Signature     
 \_\_\_\_\_ Date

\_\_\_\_\_ Data Manager – Signature     
 \_\_\_\_\_ Date

**Return completed form to Data Manager, Wilkes Building**

**Request for Technology Products  
Central State Hospital**

<b>Name of Requestor/User:</b>		<b>Date:</b>	
<b>Location</b> (Bldg/Unit/Ward):		<b>Room #:</b>	<b>Phone #:</b>

Hardware	Software	LAN Drop
Personal computer	Manufacturer:	
Printer, black and white laser		New User
Printer, color inkjet	Title:	Additional Drop
Printer, network		
Monitor	Version:	Equipment to be connected:
Keyboard	Price:	PC
Memory upgrade	Source:	Printer
Other		

**Description of request:**

---



---

**Justification for request:**

---



---

**How is this need currently being met?**

---



---

**Authorization**

**DDO:** \_\_\_\_\_ **Date:** \_\_\_\_\_

*Print Name*

\_\_\_\_\_

*Signature*

**For CSH Management Use Only**

**Approved:** \_\_\_\_\_ **Date:** \_\_\_\_\_

*Signature*

**Status:** \_\_\_\_\_

*Please send completed form to Data Manager, Wilkes Building, fax # 0926*

**Central State Hospital  
Computer Equipment Relocation Form**

<b>The following computer equipment has been relocated:</b>	
<b>From:</b> Releasing Department	<b>To:</b> Receiving Department
Budget / Org #	Budget / Org #
Building	Building
Floor /Room #	Floor /Room #
Primary User	Primary User
Phone #	Phone #
Auth. Signature/Date	Auth. Signature/Date

	<b>CPU</b>	<b>Monitor</b>	<b>Printer</b>	<b>Other (Scanner, Laptop, etc) Please List:</b>
<b>Manufacturer</b>				
<b>Model #</b>				
<b>EDP #</b>				
<b>CSH #</b>				
<b>Serial #</b>				
<b>Port #</b>				

Comments: \_\_\_\_\_

Completed By: \_\_\_\_\_

\_\_\_\_\_  
(Please  
Print)

\_\_\_\_\_  
Date

**Please send completed form to your designated Property Control person, Central Property Control, AND Data Manager, Wilkes Building (Fax # 0926)**

---