Los Angeles County - Department of Health Services
DHS Workforce Member / Client VDI Access Form

rev. 12/2017

SUBJECT: VDI ACCESS CONTROL - VDI Client Access

PURPOSE: The purpose of this policy is to ensure that Technology Support and Operations take the necessary steps to secure the network, and to fully document all requests for access to the DHS network. This policy covers remote access to the DHS Network using a VDI client connection by a County entity.

POLICY: DHS must implement policies and procedures to limit physical access to electronic information systems and the Facilities in which they are housed, while ensuring that properly authorized access is allowed. These policies and procedures must be consistent with DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).

All requests for access to the DHS network County entities must be accompanied by the DHS Non-Disclosure Agreement (NDA), the Los Angeles County Acceptable Use Agreement.

The form must be filled out completely, reviewed by the Facility Security Officer, and approved by the Facility CIO/Designee before any connection to the DHS network can take place. After completion, DHS Technical Services group will process the request.

DEFINITIONS:

ACCESS: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.

INFORMATION TECHNOLOGY (IT): A term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, personal health information, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).

SAFEGUARDS: Administrative, Physical and Technical actions or measures, and policies and procedures to protect Protected Health Information (PHI) and other confidential information.

APPROVED BY: Approval by CTO/CIO (Signature on File) Date:

Chief Technology Officer/Chief Information Officer

Approval by Security Operations Manager (Signature on File) Date:

Security Operations Manager

PURPOSE: To help DHS' IT define a process for ensuring the physical protection for DHS's information systems and infrastructure.

- **Customer can obtain VDI Access Form at:** https://intranet.ladhs.org/isb/vpn.htm **NOTE:**

Please submit this completed form to the DHS Enterprise Help Desk Support for processing. PROCEDURE:

This form consists of 5 sections, please fill out all questions. If modifying/deleting an existing connection, please utilize the existing form and check the appropriate box in section A. Make the necessary modifications and resubmit the form. Please keep form for future modifications and your records.

1) The DHS Workforce Member will open a service request with DHS Enterprise Help Desk by any of the following steps:
   A. Email the VDI form to helpdesk@dhs.lacounty.gov. The DHS Enterprise Help Desk will reply with a service request #. (Please include Facility Name and "County VDI Form" on the subject line).
   B. Fax documents to DHS Enterprise Help Desk at **323-441-8056** (Please include Facility Name and "County VDI Form" on the subject line).
   C. Call DHS Enterprise Help Desk at 323-409-8000.
2) DHS Enterprise Help Desk will verify the completeness of the form.
   A. If complete, DHS Enterprise Help Desk will assign to Security Compliance for Review.
   B. If not complete, DHS Enterprise Help Desk will contact customer for re-submittal.
3) Technical Services Group will review and process request.
   A. Create user accounts.
   B. Send Log-in information to customer.
4) Technical Service Group will contact customer to notify customer of process completion.
5) If there are any issues, Technical Service Group will work with customer to resolve and close service request.

Note: Please retain completed form for future reference and use.

Los Angeles County - Department of Health Services
DHS Workforce Member / Client VDI Access Form

rev. 12/2017

GENERAL INFORMATION FOR DHS ENTERPRISE HELP DESK USE: Service req #:_____

LAC-DHS ENTITY INFORMATION

A. DHS Requesters Information

1. Facility Information (Employee): Facility Name: _____ Facility Department: _____ Division/Section: _____	Employment Type: ○ Full Time Employee (FTE) ○ Contractor Service type: ○ New ○ Update ○ Terminate

2. Requestor Information for DHS Contact(s):

Name: _____ Employee/Contractor ID #: _____

Function/Title: _____ Phone Number: _____

Email Address: _____ Fax Number: _____

Facility Address: _____
Street Room/Location City Zip

B. Purpose Statement/Business Needs for Requested Access.

1. Customer must provide a justification/business case for purposed connection. (Please attach a separate sheet if needed)

C. VDI Access Requirement

1. Please select your Role:

○ Clinician

○ Executive

○ Administrative

D. Los Angeles County Acceptable Use Agreement

1. For VDI Client connection, we require requestor to read, sign, and understand the County of Los Angeles Agreement for Acceptable Use on **Appendix A** , pages 4-5. **E.** Facility Approvals:

	Name	Signature	Date
Applicant			
Supervisor			
FACILITY INFORMATION SYSTEMS			
Facility CIO/Designee			

*** Note: Local Facility IT Approval is required ***

Appendix A

COUNTY OF LOS ANGELES

AGREEMENT FOR ACCEPTABLE USE OF LA COUNTY'S INFORMATION TECHNOLOGY ASSETS

As a Los Angeles County contractor, vendor or other authorized user of County Information Technology (IT) assets including computers, networks, systems and data, I understand that I occupy a position of trust. I will use County IT assets for County management approved business purposes only and maintain the confidentiality of County's business and Citizen's private data. As a user of County's IT assets, I agree to the following:

1. Computer crimes: I am aware of California Penal Code 502(c) - Comprehensive Computer Data Access and Fraud Act (**Appendix A.1**). I will immediately report any suspected computer misuse or crimes to my Management.

2. Security access controls: I will not subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. I will not share my computer identification codes (log-in ID, computer access codes, account codes, ID's, etc.) or passwords.

3. Approved business purposes: I will use the County's Information Technology (IT) assets including computers, networks, systems and data for County management approved business purposes only.

4. Confidentiality: I will not access or disclose any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.

5. Computer virus and malicious code: I will not intentionally introduce any computer virus, worms or malicious code into any computer, network, system or data. I will not disable or delete computer virus detection and eradication software on computers, servers and other computing devices I am responsible for.

6. Offensive materials: I will not access or send any offensive materials, e.g., sexually explicit, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.

7. Disciplinary action for non-compliance: I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including my suspension, discharge, denial of service, cancellation of contracts or both civil and criminal penalties.

DHS SYSTEM SECURITY REQUIREMENTS

The Department of Health Services (DHS) network is protected by a variety of hardware and software systems, but viruses and other forms of attack constantly evolve and change so no network is completely safe. In order to reduce risk to the DHS network, **company IT managers** must secure the PCs of remote users, especially those using VDI accounts to attach to the DHS network.

1. It is your responsibility to have an up-to-date antivirus and anti-spam program installed on your computers;
2. Assure that all antivirus definitions are up-to-date on your computers by configuring your antivirus software to update automatically;
3. Assure that all operating system service packs, security patches and updates are applied regularly; (Go to www.windows.com and go to 'Product Resources', 'Windows Update' to obtain the latest security patches);
4. If using broadband access (DSL, ISDN, cable modem, etc), have either a hardware or software firewall;
5. Install the provided VDI client, assist users to set up/enter user Security Questions and logon using the AD password;
6. You must manage users and ensure that they not share login ID, password or AD password with others. **Some information on Viruses**

Viruses are programs that cause an unexpected, usually negative, event. Viruses are often disguised games, screen savers or images. They may even enter a network from an infected work-related file from a system that does not have up-to-date antivirus software.

Computer Worms are viruses that reside in the active memory of a computer and have the ability to duplicate themselves. Worms can send copies of themselves to infect other computers, such as through email or Internet Relay Chat (IRC).

Along with antivirus hardware and software, most private networks restrict user ability to load screen savers, games, backgrounds and other non-work files in order to reduce the chance of virus infections.

Some of the better known anti-virus products are Symantec's Norton Antivirus, Trend Micro's PC-cillin, or McAfee VirusScan; but there are other good quality products on the market. Please contact the Enterprise Help Desk at 323-409-8000, if you need assistance in selecting an appropriate antivirus software package for your computers.

Appendix A.1

CALIFORNIA PENAL CODE 502(c) - "COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"

Below is a section of the "Comprehensive Computer Data Access and Fraud Act" as it pertains specifically to this Agreement. California Penal Code 502(c) is incorporated in its entirety into this Agreement by reference and all provisions of Penal Code 502(c) apply. For a complete copy, consult the Code directly at website www.leginfo.ca.gov/.

502.(c) Any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

YOUR SIGNATURE BELOW INDICATES THAT YOU HAVE READ AND WILL COMPLY WITH THE ABOVE ACCEPTABLE USE AND NETWORK/DESKTOP SECURITY REQUIREMENTS

Print Name	Date
Title	Phone#
Signature	
Company	Email Address