Print Form

LOS ANGELES COUNTY ISD INTERNAL SERVICES

COUNTY OF LOS ANGELES
DOWNEY DATA CENTER REGISTRATION
For Contractors/Vendors

SAMPLE

PROFILE INFORMATION — print or type completing boxes 1 – 9

(1) DATE OF REQUEST	(2) TYPE OF REQUEST (Check One)	(3) CONTRACT OR VENDOR NUMBER
03/01/2016	☐ REPLACE LOST/STOLEN SECUREID TOKEN ☑ ADD NEW LOGON ID ☐ CHANGE LOGON ID ACCESS ☐ DELETE LOGON ID	

(4) LAST NAME, FIRST NAME MI	(5) E-MAIL ADDRESS
NEVERWRONG, SAMPLE A.	SNEVERWRONG@SAMPLE.COM
(6) COMPANY/ORGANIZATION NAME	**(7) COORDINATING L.A. COUNTY DEPARTMENT NAME / NUMBER**
SAMPLE MHS	
(8) WORK MAILING ADDRESS (STREET, CITY, STATE, ZIP)	**(9) WORK PHONE NUMBER**
2345 HAPPY STREET, CHERRY BLOSSOM, CA 90021	213-201-2000

IBM DATA CENTER ACCESS — complete each area for required access, as defined by L.A. County management

(10) LOGON ID	(11) 2-DIGIT MAJOR GROUP CODE	(12) 2-DIGIT LSO GROUP CODE	
C	HQ	MH	

☐ **TSO ACCESS — check box and complete for required access, as defined by L.A. County management. Asterisks are optional data.**

(13) 2-DIGIT TSO GRP CODE	(14) SUB-GROUP 1 *	(15) SUB-GROUP 2 *	(16) SUB-GROUP 3 *	

☐ **ONLINE ACCESS — check box and complete for required access, as defined by County management. Asterisks are optional data.**

(17) SYSTEM APPLICATION	(18) GRP NAME / NATURAL PROFILE	(19) OLD GRP/NATURAL PROFILE *	DMV/JAI/APS APPLIATION COORDINATORS ONLY
IS			APS A/O:
			DMV SYSTEM CODE:
			JAI SYSTEM LOCATION:

UNIX ENVIRONMENT ACCESS — complete for required access, as defined by L.A. County management.

(20) TYPE OF REQUEST (Check One) ☐ ADD NEW LOGON ID ☐ CHANGE LOGON ID ACCESS ☐ DELETE LOGON ID

(21) LOGON ID	(22) APPLICATION	(23) ACCESS GROUP	(24) ACCOUNT NUMBER

SECURID REMOTE ACCESS — complete as defined by L.A. County mgnt., e-mail address is required, see box #5

(25) BILLING ACCOUNT NUMBER for SecurID Token: A20500 -

(26) ACCESS TYPE: SecurID VPN ☐ Adaptive Authentication VPN ☐

SECURITY STATEMENT

Before connecting to the County network you must install anti-virus software, and stay up-to-date with definitions, Microsoft patches (critical and security) and service packs. A Firewall, either a hardware firewall or personal firewall software, is required for those using broadband Internet access (DSL, ISDN, cable modem, etc.). You agree not to share your logon id, password and SecurID passcode with others.

SIGNATURES — each signature entry must be completed in full.

Your signature indicates that you have read and will comply with the above **security statement.**

(27) CUSTOMER'S S — *SIGN AND DATE*

PLEASE SIGN HERE

ANAGER'S SIGNATURE	(29) PHONE #	(30) PRINT COUNTY DEPARTMENT MANAGER'S NAME	(31) DATE
	213-201-2001	SUSAN B. NEHEAVEN	03/01/2016
(32) ISD/APPLICATION COORDINATOR'S SIGNATURE	(33) PHONE #	(34) PRINT ISD/APPLICATION COORDINATOR'S NAME	(35) DATE
	213-351-1335		

WARNING: FAILURE TO FULLY COMPLETE & SIGN THIS FORM WILL CAUSE A DELAY IN PROCESSING.

You may submit completed registration form to DMH/CIOB/SYSTEMS ACCESS UNIT, 695 South Vermont Ave, 7th Floor Los Angeles, CA 90005 Mail Stop # 29 to Process.

For any questions related to registration please call (562) 940-3305.

Revised: October 2015

SAMPLE

Downey Data Center Registration Instructions

For Contractors/Vendors

Profile Information — print or type

1. Mandatory. Enter the current date.
2. Mandatory. Check appropriate type of request.
3. Mandatory. Enter your contract or vendor number.
4. Mandatory. Print your last name, first name and middle initial.
5. Mandatory. Enter your e-mail address.
6. Mandatory. Enter your company/organization name.
7. Mandatory. Enter the coordinating L.A. County department name or number.
8. Mandatory. Enter your complete business mailing address.
9. Mandatory. Enter your complete telephone number.

New logon ids will be created as follows:

Contractor/Vendor LOGON ID will be assigned and you will be notified by phone (e.g. Cxxxxxx).

IBM Data Center Access

10. Mandatory. Enter your existing logon id. If this is a new request, your logon id will be assigned as described above.
11. Mandatory. Enter the two-digit department major group code, as defined by L.A. County management.
12. Mandatory. Enter the two-digit local security group code, as defined by L.A. County management.

TSO Access — check box if this request applies to TSO access

13. Mandatory. Enter the two-digit identifier of your TSO group, as defined by L.A. County management.
14. Optional. Enter the two-character identifier, as defined by L.A. County management.
15. Optional. Enter the two-character identifier, as defined by L.A. County management.
16. Optional. Enter the two-character identifier, as defined by L.A. County management.

Online Access — check box if this request applies to online access

17. Mandatory. Enter each CICS online or IMS system application required for access, as defined by L.A. County management.
18. Mandatory Enter the group name for each system application, as defined by L.A. County management.
19. Optional. Enter the old Natural group/profile name.

UNIX Environment Access — complete for required access as defined by L.A. County management

20. Mandatory. Check appropriate type of request.
21. Mandatory. Enter your existing Logon ID. If this is a new request, your logon id will be assigned as described above.
22. Mandatory. Enter the application you require for access, as defined by L.A. County management.
23. Mandatory. Enter your UNIX access group.
24. Optional. Enter a valid 11-digit billing account number.

SecurID Remote Access — complete for required access as defined by L.A. County management.

25. Mandatory. Enter a valid L.A. County 11-digit billing account number.
26. Mandatory. Check box for device type.

    VPN customers must check the box and indicate compliance. Anti-virus software and stay up-to-date with definitions, patches and service packs applies to everyone. A Firewall, either a hardware firewall or personal firewall software, is required for those using broadband Internet access (DSL, ISDN, cable modem, etc.).

Signatures — original signatures are required

27. Mandatory. Your signature indicates that you have read and will comply with the security statement.
28. – 31. Mandatory. Enter signature, phone # and date of authorizing L.A. County department manager (sign and print).
32. – 35. Mandatory. Enter signature, phone # and date of ISD manager or application coordinator (sign and print).

COUNTY OF LOS ANGELES
AGREEMENT FOR ACCEPTABLE USE
AND
CONFIDENTIALITY OF
COUNTY INFORMATION TECHNOLOGY RESOURCES

ANNUAL

As a County of Los Angeles (County) employee, contractor, subcontractor, volunteer, or other authorized user of County information technology (IT) resources, I understand that I occupy a position of trust. Furthermore, I shall use County IT resources in accordance with my Department's policies, standards, and procedures. I understand that County IT resources shall not be used for:

- For any unlawful purpose;
- For any purpose detrimental to the County or its interests;
- For personal financial gain;
- In any way that undermines or interferes with access to or use of County IT resources for official County purposes;
- In any way that hinders productivity, efficiency, customer service, or interferes with a County IT user's performance of his/her official job duties;

I shall maintain the confidentiality of County IT resources (e.g., business information, personal information, and confidential information).

This Agreement is required by Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, which may be consulted directly at website http://countypolicy.co.la.ca.us/6.101.htm.

As used in this Agreement, the term "County IT resources" includes, without limitation, computers, systems, networks, software, and data, documentation and other information, owned, leased, managed, operated, or maintained by, or in the custody of, the County or non-County entities for County purposes. The definitions of the terms "County IT resources", "County IT user", "County IT security incident", "County Department", and "computing devices" are fully set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, which may be consulted directly at website http://countypolicy.co.la.ca.us/6.100.htm. The terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information, which may be consulted directly at website http://countypolicy.co.la.ca.us/3.040.htm.

As a County IT user, I agree to the following:

1. Computer crimes: I am aware of California Penal Code Section 502(c) – Comprehensive Computer Data Access and Fraud Act (set forth, in part, below). I shall immediately report to my management any suspected misuse or crimes relating to County IT resources or otherwise.

2. No Expectation of Privacy: I do not expect any right to privacy concerning my activities related to County IT resources, including, without limitation, in anything I create, store, send, or receive using County IT resources. I understand that having no expectation to

any right to privacy includes, for example, that my access and use of County IT resources may be monitored or investigated by authorized persons at any time, without notice or consent.

3. Activities related to County IT resources: I understand that my activities related to County IT resources (e.g., email, instant messaging, blogs, electronic files, County Internet services, and County systems) may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall not either intentionally, or through negligence, damage, interfere with the operation of County IT resources. I shall neither, prevent authorized access, nor enable unauthorized access to County IT resources responsibly, professionally, ethically, and lawfully.

4. County IT security incident reporting: I shall notify the County Department's Help Desk and/or Departmental Information Security Officer (DISO) as soon as a County IT security incident is suspected.

5. Security access controls: I shall not subvert or bypass any security measure or system which has been implemented to control or restrict access to County IT resources and any related restricted work areas and facilities. I shall not share my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards).

6. Passwords: I shall not keep or maintain any unsecured record of my password(s) to access County IT resources, whether on paper, in an electronic file, or otherwise. I shall comply with all County and County Department policies relating to passwords. I shall immediately report to my management any compromise or suspected compromise of my password(s) and have the password(s) changed immediately.

7. Business purposes: I shall use County IT resources in accordance with my Department's policies, standards, and procedures.

8. Confidentiality: I shall not send, disseminate, or otherwise expose or disclose to any person or organization, any personal and/or confidential information, unless specifically authorized to do so by County management. This includes, without limitation information that is subject to Health Insurance Portability and Accountability Act of 1996, Health Information Technology for Economic and Clinical Health Act of 2009, or any other confidentiality or privacy legislation.

9. Computer virus and other malicious devices: I shall not intentionally introduce any malicious device (e.g., computer virus, spyware, worm, key logger, or malicious code), into any County IT resources. I shall not use County IT resources to intentionally introduce any malicious device into any County IT resources or any non-County IT systems or networks. I shall not disable, modify, or delete computer security software (e.g., antivirus software, antispyware software, firewall software, and host intrusion prevention software) on County IT resources. I shall notify the County Department's Help Desk and/or DISO as soon as any item of County IT resources is suspected of being compromised by a malicious device.

10. Offensive materials: I shall not access, create, or distribute (e.g., via email) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless authorized to do so as a part of my assigned job duties (e.g., law enforcement). I shall report to my management any offensive materials observed or received by me on County IT resources.

11. Internet: I understand that the Internet is public and uncensored and contains many sites that may be considered offensive in both text and images. I shall use County Internet services in accordance with my Department's policies and procedures. I understand that my use of the County Internet services may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall comply with all County Internet use policies, standards, and procedures. I understand that County Internet services may be filtered, but in my use of them, I may be exposed to offensive materials. I agree to hold County harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive materials.

12. Electronic Communications: I understand that County electronic communications (e.g., email, text messages, etc.) created, sent, and/or stored using County electronic communications systems/applications/services are the property of the County. All such electronic communications may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time, without notice or consent. I shall comply with all County electronic communications use policies and use proper business etiquette when communicating over County electronic communications systems/applications/services.

13. Public forums: I shall only use County IT resources to create, exchange, publish, distribute, or disclose in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) in accordance with Department's policies, standards, and procedures.

14. Internet storage sites: I shall not store County information (i.e., personal, confidential (e.g., social security number, medical record), or otherwise sensitive (e.g., legislative data)) on any Internet storage site in accordance with Department's policies, standards, and procedures.

15. Copyrighted and other proprietary materials: I shall not copy or otherwise use any copyrighted or other proprietary County IT resources (e.g., licensed software and documentation, and data), except as permitted by the applicable license agreement and approved by designated County Department management. I shall not use County IT resources to infringe on copyrighted material.

16. Compliance with County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements: I shall comply with all applicable County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements relating to County IT resources. These include, without limitation, Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, Board of Supervisors Policy No.

6.101 – Use of County Information Technology Resources, and Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

17. Disciplinary action and other actions and penalties for non-compliance: I understand that my non-compliance with any provision of this Agreement may result in disciplinary action and other actions (e.g., suspension, discharge, denial of access, and termination of contracts) as well as both civil and criminal penalties and that County may seek all possible legal redress.

CALIFORNIA PENAL CODE SECTION 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 Section 502(c) is incorporated in its entirety into this Agreement by reference, and all provisions of Penal Code Section 502(c) shall apply. For a complete copy, consult the Penal 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) wrongfully 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 any 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 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.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

SAMPLE A. NEVERWRONG	SIGN AND DATE
County IT User's Name	County IT User's Signature
NONE	03 / 01 / 2016
County IT User's Employee/ID Number	Date
SUSAN B NEWHEAVEN	PLEASE SIGN HERE
Manager's Name	Manager's Signature
PROGRAM MANAGER	03 / 01 / 2016
Manager's Title	Date