



COUNTY OF LOS ANGELES
DOWNEY DATA CENTER REGISTRATION
For L.A. COUNTY EMPLOYEES

S A M P L E

PROFILE INFORMATION — print or type completing boxes 1 – 9

(1) DATE OF REQUEST 3/14/07
(2) TYPE OF REQUEST (Check One) [X] ADD NEW LOGON ID
(3) LA COUNTY EMPLOYEE # 123456
(4) LAST NAME, FIRST NAME MI NEVERWRONG, SAMPLE A.
(5) E-MAIL ADDRESS SNEVERWRONG@LACDMH.ORG
(6) COUNTY DEPARTMENT NAME/DIVISION NAME COUNTYWIDE SRVCS/OUTWARD BOUND DIVISION/SMART
(7) COUNTY DEPARTMENT # 435
(8) WORK MAILING ADDRESS (STREET, CITY, STATE, ZIP) 2345 HAPPY STREET, CHERRY BLOSSOM, CA 90021
(9) WORK PHONE #

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

(10) LOGON ID
(11) 2-DIGIT MAJOR GROUP CODE HQ
(12) 2-DIGIT LSO GROUP CODE MH
(13) SECURITY AUTHORIZATION
[] TSO ACCESS — check box for access and complete fields 10, 11, 12 and 14. Fields with an asterisk are optional.
(14) 2-DIGIT TSO GRP CODE
(15) BIN NUMBER *
(16) SUG-GROUP 1 *
(17) SUB-GROUP 2 *
(18) SUB-GROUP 3 *
[] ONLINE ACCESS — check box for access and complete fields 10, 11, 12, 19, and 20. Fields with an asterisk are optional.
(19) SYSTEM APPLICATION
(20) GRP NAME / NATURAL PROFILE
(21) OLD GRP/NATURAL PROFILE *
DMV/JAI/APS APPLICATION COORDINATORS ONLY
APS A/O:
DMV SYSTEM CODE:
JAI SYSTEM LOCATION:

UNIX ENVIRONMENT ACCESS — complete for required access, as defined by your management.

(22) TYPE OF REQUEST (Check One) [] ADD NEW LOGON ID [] CHANGE LOGON ID ACCESS [] DELETE LOGON ID
(23) LOGON ID
(24) APPLICATION
(25) ACCESS GROUP
(26) ACCOUNT NUMBER

SECURID REMOTE ACCESS — complete each area as required. Your e-mail address is required, see box #5.

(27) ACCOUNT NUMBER for SecurID Token:
(28) DEVICE TYPE: [X] Standard Token [] Key Fob
[] VPN — Check the box if you are a VPN customer and read the security statement below. Your signature indicates that you have read and will comply with the statement:

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.

[X] WIRELESS ACCESS Check the box if you are requesting wireless access. Application: DMH E-MAIL

SIGNATURES — each signature entry must be completed in full.

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

(29) CUSTOMER'S SIGNATURE SIGNATURE REQUIRED
(30) MANAGER'S SIGNATURE AUTHORIZED MANAGER/DESIGNEE SIGNATURE 213-200-2001 SUSAN B. NEWHEAVEN 3/14/07
(31) PHONE #
(32) PRINT MANAGER'S NAME
(33) DATE
If you have indicated a need to access a system not owned by your department, concurrence from the other department(s) is required.
(34) APPLICATION COORDINATOR'S SIGNATURE
(35) PHONE #
(36) PRINT APPL COORDINATOR'S NAME JOYCE A. FANTROY
(37) DATE

[] PDF SUBMITTED: NAME (Print) JOYCE A. FANTROY SIGNATURE:

My signature above, stipulates that my department has setup a process to maintain the original form on file for a period of 7 years, and will make the original form available within 72 hours, upon request from ISD or those acting on the behalf of ISD, ie., internal or external Auditors.

WARNING: FAILURE TO FULLY COMPLETE & SIGN THIS FORM WILL CAUSE A DELAY IN PROCESSING. ORIGINAL SIGNATURES ARE REQUIRED. NO COPIES OR FAXES WILL BE ACCEPTED. PDF'S ACCEPTED.

Downey Data Center Registration Instructions

For L.A. COUNTY EMPLOYEES

Profile Information — print or type

1. Mandatory. Enter the current date.
2. Mandatory. Check appropriate type of request.
3. Mandatory. Enter your 6-digit County employee number.
4. Mandatory. Print your last name, first name and middle initial.
5. Mandatory. Enter your e-mail address.
6. Mandatory. Enter your organization name associated with the 3-digit department number.
7. Mandatory. Enter your 3-digit County department number.
8. Mandatory. Enter your complete business mailing address.
9. Mandatory. Enter your complete telephone number.

New logon ids will be created as follows: County Employee E and employee number (e.g. E222222)

You agree not to share your logon id and password with others.

IBM Data Center Access – N/A

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 your two-digit department major group code, as defined by your management.
12. Mandatory. Enter your two-digit local security group code, as defined by your management.
13. Optional. Complete if you have been designated as a Local Security Officer, by your management.

TSO Access — check box if this request applies to TSO access – N/A

14. Mandatory. Enter the two-digit identifier of your TSO group, as defined by your management.
15. Optional. Enter Downey bin number for report retrieval.
16. Optional. Enter the two-character identifier, as defined by your management.
17. Optional. Enter the two-character identifier, as defined by your management.
18. Optional. Enter the two-character identifier, as defined by your management.

Online Access — check box if this request applies to online access – N/A

19. Mandatory. Enter each CICS online or IMS system application you require for access, as defined by your management.
20. Mandatory. Enter the group name for each system application you require for access, as defined by your management.
21. Optional. Enter the old Natural group/profile name.

UNIX Environment Access — check box if this request applies to UNIX access – N/A

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

SecurID Remote Access — complete for access as required by your management.

27. Mandatory. Enter a valid 11-digit billing account number, as defined by your management. – N/A
28. Mandatory. Check box for device type.

Check box if you are a VPN customer and indicate your compliance with the security statement.

Anti-virus software and staying 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.). Check with your management if you need anti-virus and/or personal firewall software.

Check box if you are requesting wireless access.

Signatures — original signatures are required

29. Mandatory. Your signature indicates that you have read and will comply with the security statement.
30. – 33. Mandatory. Enter signature, phone # and date of authorizing manager (sign and print).
34. – 37. Mandatory. Enter signature, phone # and date of application coordinator (sign and print). -Systems Access Only
If you have indicated a need to access a system not owned by your department, concurrence from the other department(s) is required.

PDF SUBMITTED: The customer's manager must print his/her name and sign in the space provided, if a PDF is being submitted for processing, in lieu of submitting the original form. The department must maintain the original form on file for 7 years, and must provide the original form within 72 hours upon the request of ISD or those acting on behalf of ISD, ie., internal or external Auditors.

ISD Security, Mail Stop # 29, 9150 E. Imperial Hwy, Downey, CA 90242

**COUNTY OF LOS ANGELES
AGREEMENT FOR ACCEPTABLE USE AND
CONFIDENTIALITY OF
COUNTY'S INFORMATION TECHNOLOGY ASSETS,
COMPUTERS, NETWORKS, SYSTEMS AND DATA**

As a Los Angeles County employee, 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 (attached). 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 County computer, network, system or data. I will not disable or delete computer virus detection and eradication software on County 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, including the public Internet and other electronic mail systems, 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. Public Internet: I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be inadvertently exposed to such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.
8. Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will comply with County e-mail use policy and use proper business etiquette when communicating over e-mail systems.
9. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.

10. 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.

S
A
M
P
L
E

**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.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

<u>SAMPLE A. NEVERWRONG</u>	<u>REQUIRED</u>	<u>3/14/07</u>
Employee's Name	Employee's Signature	Date
<u>SUSAN B. NEWHEAVEN</u>	<u>REQUIRED</u>	<u>3/14/07</u>
Manager's Name	Manager's Signature	Date