COUNTY OF LOS ANGELES
MAINFRAME, UNIX AND REMOTE ACCESS REGISTRATION FORM
For L.A. COUNTY EMPLOYEES and CONTRACTORS

LOS ANGELES COUNTY ISD INTERNAL SERVICES

PROFILE INFORMATION — complete boxes 1 – 9.

(1) DATE OF REQUEST	(2) TYPE OF REQUEST	(3) EMPLOYEE OR CONTRACTOR #
	☐ NEW LOGON ID ☐ UPDATE LOGON ID ☐ DELETE LOGON ID	

(4) LAST NAME, FIRST NAME, MI

(5) E-MAIL ADDRESS

(6) COUNTY DEPARTMENT NAME/ORGANIZATION NAME

(7) COUNTY DEPARTMENT NUMBER

(8) WORK MAILING ADDRESS (STREET, CITY, STATE, ZIP)

(9) WORK PHONE NUMBER

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

(10) LOGON ID	(11) 2-DIGIT MAJOR GROUP CODE	(12) 2-DIGIT LSO GROUP CODE	(13) SECURITY AUTHORIZATION

☐ **TSO ACCESS —** check box for access and complete fields 10, 11, 12 and 13 (see above).

(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, 13, 19, and 20.

(19) SYSTEM APPLICATION	(20) GRP NAME / NATURAL PROFILE	(21) OLD GRP/NATURAL PROFILE	DMV/JAI/APS APPLIATION 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	

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

☐ **(26a) NEW TOKEN**   ☐ **(26b) REPLACE LOST/STOLEN TOKEN**   ☐ **(26c) REPLACE DEFECTIVE TOKEN**   ☐ **(26d) RENEW TOKEN**

PLEASE SELECT YOUR REMOTE ACCESS TYPE:

Expiration Date:_____

Note: When selecting a RSA SecurID Hard Token or Software Token, a valid Billing Account Number is **REQUIRED**

☐ **(27a) TOKENLESS AUTHENTICATION VPN**
Uses Password - Does Not Expire

☐ **(27b) HARD TOKEN SECURID VPN**
Uses KeyFob - 3 Year Expiration

☐ **(27c) SOFTWARE TOKEN SECURID VPN**
Uses Mobile Device or Computer - 3 Year Expiration

Select Device Type Below:

(28) BILLING ACCOUNT NUMBER for SecurID Token: _____

☐ **IOS**   ☐ **ANDROID**   ☐ **COMPUTER**

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

SIGNATURES — Please sign, date and print name below.

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

(29) CUSTOMER'S SIGNATURE	(30) PHONE #	(31) NAME	(32) DATE
(33) MANAGER'S SIGNATURE	(34) PHONE #	(35) MANAGER'S NAME	(36) DATE
(37) DEPARTMENT COORDINATOR'S SIGNATURE	(38) PHONE #	(39) DEPTARTMENT COORDINATOR'S NAME	(40) DATE

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

You may submit completed registration form to ISDRegistration@isd.lacounty.gov or ISD Registration office at 9150 E. Imperial Hwy, Downey, CA 90242 Mail Stop # 29 **for processing**. For any questions related to registration please call (562) 940-3305.

Downey Data Center Registration Instructions
For L.A. COUNTY EMPLOYEES and CONTRACTORS

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 or Contractor number (If you have one).
4. Mandatory.   Print your last name, first name and middle initial.
5. Mandatory.   Enter your e-mail address.
6. Mandatory.   Enter your County Department name or Organization name
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: <u>County Employee</u> E and employee number (e.g. E222222) <u>Contractor</u> C and contractor number (e.g. C222222).   You agree not to share your Logon ID and password with others.

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 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
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
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. Mandatory.   Enter the old Natural group/profile name.

UNIX Environment Access — check box if this request applies to UNIX access
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.

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

26a. Mandatory. Check box for a New Token.

26b. Mandatory. Check box to replace a lost/stolen Token.

26c. Mandatory. Check box to replace a defective/malfunctioned Token.

26d. Mandatory. Check box to renew a Token.

27a. Mandatory. Check box for Tokenless, which is RSA Adaptive Authentication remote access to County-protected resources.

27b. Mandatory. Check box for RSA SecurID Hardware token, which is a KeyFob that is valid for 3 years.

27c. Mandatory. Check box for RSA SecurID Software token, which is a file for your device. Please also indicate device type.
> IOS/Android - You will receive a QR Code or Hyperlink for your mobile device
> Computer - You will receive a program (.stdid) file for your Windows/MacOS workstation. You need to install the RSA Software Token client.

Checking any of the boxes for 27. indicates 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. Check with your management if you need anti-virus and/or personal firewall software.

28. Mandatory.   Enter a valid 11-digit billing account number, as defined by your management.

Signatures — signatures are required

29. – 32. Mandatory.   Enter signature, phone # and date of county employee or contractor (sign and print).
33. – 36. Mandatory.   Enter signature, phone # and date of authorizing manager (sign and print).
37. – 40. Mandatory.   Enter signature, phone # and date of application coordinator (sign and print).

> If you have indicated a need to access a system not owned by your department, concurrence from the other department(s) is required.

COUNTY OF LOS ANGELES
AGREEMENT|FOR ACCEPTABLE USE
AND CONFIDENTIALITY OF
COUNTY INFORMATION ASSETS

As a County of Los Angeles (County) Workforce Member, and as outlined in Board of Supervisors Policy 6.101 "Use of County Information Assets", I understand and agree:

- That I occupy a position of trust, as such I will use County Information Assets in accordance with countywide and Departmental policies, standards, and procedures including, but not limited to, Board of Supervisors Policy 9.015 "County Policy of Equity" (CPOE) and Board of Supervisors Policy 9.040 "Investigations Of Possible Criminal Activity Within County Government".

- That I am responsible for the security of information and systems to which I have access or to which I may otherwise obtain access even if such access is inadvertent or unintended. I shall maintain the confidentiality of County Information Assets (as defined in Board of Supervisors Policy 6.100 – Information Security Policy).

- That County Information Assets must not be used for:
  o Any unlawful purpose;
  o Any purpose detrimental to the County or its interests;
  o Personal financial gain;
  o In any way that undermines or interferes with access to or use of County Information Asset for official County purposes;
  o In any way that hinders productivity, efficiency, customer service, or interferes with other County Workforce Members performance of his/her official job duties.

- That records, files, databases, and systems contain restricted, confidential or internal use information (i.e. non-public information) as well as Public information. I may access, read or handle Non-public information to the extent required to perform my assigned duties. Although I may have access to Non-public information, I agree to not access such information unless it is necessary for the performance of my assigned duties.

- Not to divulge, publish, share, expose or otherwise make known to unauthorized persons, organization or the public any County Non-public Information. I understand that:
  o I may divulge Non-public Information to authorized County staff and managers as necessary to perform my job duties;
  o I may divulge Non-public Information to others only if specifically authorized to do so by federal, state, or local statute, regulation or court order, and with the knowledge of my supervisor or manager;
  o I may not discuss Non-public Information outside of the workplace or outside of my usual work area;
  o To consult my supervisor or manager on any questions I may have concerning whether particular information may be disclosed.

- To report any actual breach of Information Security or a situation that could potentially result in a breach, misuse or crime relating to County Information Assets whether this is on my part or on the part of another person following proper County and Departmental procedures. I understand that I am expected to assist in protecting evidence of crimes relating to Information Assets and will follow the instructions of, and cooperate, with management and any investigative response team.

- I have no expectation of privacy concerning my activities related to the use of, or access to, County Information Assets, including anything I create, store, send, or receive using County Information Assets. My actions may be monitored, logged, stored, made public, and are subject to investigation, audit and review without notice or consent.

- Not possess a County Information Asset without authorization. Although I may be granted authorization to possess and use a County Information Asset for the performance of my duties, I will never be granted any ownership or property rights to County Information Assets. All Information

1

Assets and Information is the property of the County. I must surrender County Information Assets upon request. Any Information Asset retained without authorization will be considered stolen and prosecuted as such.

- Not intentionally, or through negligence, damage or interfere with the operation of County Information Assets.

- Neither, prevent authorized access, nor enable unauthorized access to County Information Assets.

- To not make computer networks or systems available to others unless I have received specific authorization from the Information Owner.
  o Not share my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric logons, and smartcards) with any other person or entity. Nor will I keep or maintain any unsecured record of my password(s) to access County Information Assets, whether on paper, in an electronic file.
  o I am accountable for all activities undertaken through my authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric logons, and smartcards).

- Not intentionally introduce any malicious software (e.g., computer virus, spyware, worm, key logger, or malicious code), into any County Information Asset or any non-County Information Systems or networks.

- Not subvert or bypass any security measure or system which has been implemented to control or restrict access to County Information Assets and any restricted work areas and facilities.
  o Disable, modify, or delete computer security software (e.g., antivirus, antispyware, firewall, and/or host intrusion prevention software) on County Information Assets. I shall immediately report any indication that a County Information Asset is compromised by malware following proper County and Departmental procedures.

- Not access, create, or distribute (e.g., via email, Instant Messaging or any other means) any offensive materials (e.g., text or images which are defamatory, sexually explicit, racial, harmful, or insensitive) on County Information Assets, unless authorized to do so as a part of my assigned job duties (e.g., law enforcement). I will report any offensive materials observed or received by me on County Information Assets following proper County and Departmental procedures.

- 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 countywide and Departmental policies and procedures. I understand that County Internet services may be filtered, however, my use of resources provided on the Internet may expose me 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 material.

- That County electronic communications (e.g., email, instant messages, etc.) created, sent, and/or stored using County electronic communications services are the property of the County. I will use proper business etiquette when communicating using County electronic communications services.

- Only use County Information Assets to create, exchange, publish, distribute, or disclose in public forums and social media (e.g., blog postings, bulletin boards, chat rooms, Twitter, Instagram, Facebook, MySpace, and other social media services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) in accordance with countywide and Departmental policies, standards, and procedures.

- Not store County Non-public Information on any Internet storage site except in accordance with countywide and Departmental policies, standards, and procedures.

- Not copy or otherwise use any copyrighted or other proprietary County Information Assets (e.g., licensed software, documentation, and data), except as permitted by the applicable license

2

agreement and approved by County Department management. Nor will I use County Information Assets to infringe on copyrighted material.

- That noncompliance may result in disciplinary action (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.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

_____
County Workforce Member's Name

_____
County Workforce Member's Signature

_____
County Workforce Member's ID Number

_____
Date

_____
Manager's Name

_____
Manager's Signature

_____
Manager's Title

_____
Date