COUNTY OF LOS ANGELES
PROBATION DEPARTMENT

DIRECTIVE

No.:	1431
Issued:	02/19/2020
Post Until:	03/19/2020

SUBJECT: INFORMATION TECHNOLOGY POLICY

This Directive supersedes and fully replaces Directives No. 1345, 1315, and 1127
Refer to Los Angeles County Board of Supervisors Policies 6.100-6.105

PURPOSE

This policy governs the use of Probation Department Information Technology (IT) resources.

SCOPE OF POLICY

This policy applies to all Probation Department workforce members, including employees, volunteers, interns, consultants, and contractors, and all aspects of the Probation Department's computing environment, including all Los Angeles County data networks, computer systems, and data, as well as all computing resources operated by other organizations and provided to Probation Department users in the course and scope of their employment (collectively "information assets").

The term "user" as used in this policy refers to all Probation Department workforce members, contractors, and others (e.g., interns) who use Probation Department or County information technology resources.

POLICY

Probation Department managers shall ensure that all workforce members are aware of and comply with this policy. Failure to comply may result in disciplinary action up to and including discharge.

Security Management Responsibilities

The Probation Departmental Information Security Officer (DISO) is responsible for managing IT security risk, promoting safe and secure computing, developing IT security policy, monitoring and promoting compliance, and managing response and containment of IT security incidents.

All workforce members have a duty to protect information assets that are in their care or made available to them.

Issuance of County Computers

The Probation Department provides no more than one personal computer per workforce member. Laptop users will not be issued a desktop computer. Upon request, a docking station will be provided to laptop users to support a full-size monitor and keyboard in the office environment. In cases where business needs cannot be met effectively with a single computer, an additional computer may be

provided with approval of the Deputy Director. Bureau Chiefs, Deputy Directors, and Chief Deputies will be issued a desktop and a laptop if they so request.

Acceptable Use
All users are bound by the *County of Los Angeles Agreement for Acceptable Use and Confidentiality of County Information Assets*, a copy of which is attached hereto. All terms of the agreement are hereby incorporated into this policy. All users must execute the *County of Los Angeles Agreement for Acceptable Use and Confidentiality of County Information Assets* upon joining the Probation Department workforce and annually thereafter.

Required Training
Users must complete IT Security Awareness Training annually and as otherwise directed by the DISO.

Users who have access to the Probation Electronic Medical Record System (PEMRS) or who otherwise have access to Protected Health Information (PHI) must complete Health Insurance Portability and Accountability Act (HIPAA) Privacy Training biennially and as otherwise directed by the DISO.

Additional Security Controls
Certain systems, projects, and job functions may require compliance with additional security controls beyond those specified in this document. Users may be required to acknowledge additional responsibilities and sign additional documents when their responsibilities include use of systems with additional security controls.

Duty to Protect Data
Users must protect data created and/or accessed in the course of their duties from unauthorized access, loss, destruction, and/or alteration.

Data stored on County servers (i.e., *network drives*, *home directories (h: drive)*, and *file shares* or *shared folders*) and on County-issued *OneDrive for Business* accounts are protected from data loss. All business documents must be stored on a County server or on a County-issued *OneDrive for Business* account.

Probation Department desktop computers, portable computers, smartphones, tablets, and data storage media must use disk encryption managed by the Information Systems Bureau.

Users must not store confidential data on portable computing equipment (e.g., laptops, phones, tablets) or removable media (e.g., flash drives, memory cards, CDs, DVDs) unless required by the user's duties. Users who store confidential data on portable computing equipment or removable media must ensure that all data are encrypted in accordance with Probation Department Information Systems Bureau standards. Examples of confidential data include but are not limited to PHI, Personally Identifiable Information (PII), and Criminal Offender Record Information (CORI).

Users may store confidential data on their County-issued OneDrive for Business account. Users are not to store confidential data on any other Internet-based website or file storage system or service, unless authorized by the DISO or her or his designee.

All outbound email sent to email addresses not ending in *lacounty.gov* and containing confidential or sensitive data, including, but not limited to, PHI, PII, and CORI data, must be encrypted by the user. As of the date of this directive, users can encrypt messages sent from their *probation.lacounty.gov* accounts by including *[SECURE]* in the subject line of the email, including square brackets.

Users shall not send email containing confidential data to their personal (non-County) email accounts. Users shall not automatically forward emails to their non-County email accounts.

Physical documents that contain confidential data must be stored securely.

Physical Security
Users shall exercise due care in ensuring the physical security of computer equipment and data storage media. Computer equipment installed or stored in an area that is not secure must be secured by means of equipment locks or secure storage.

Only authorized Information Systems Bureau technical staff shall perform hardware repairs and upgrades. Computer equipment must not be opened by users.

Computing equipment, including but not limited to desktop computers, monitors, and printers, may only be moved by authorized Information Systems Bureau technical staff.

Personally-owned computing equipment, including, but not limited to, desktop or portable computers, tablets, smartphones, printers, hard disks, flash drives, other removable media, hubs, routers, switches, and access points are not to be connected to the County network in Probation Department offices unless authorized by the DISO. For purposes of this paragraph, the County network includes wired networks and the WiFi networks that provide access to County computing resources such as servers, printers, and applications. As of the date of this directive, the *LACMOBILE* and *LACEMPLOYEE* WiFi networks provide access to County computing resources and are considered part of the County network. Use of the *LACGUEST* WiFi network is permitted for personal devices.

Secure System Configuration
In collaboration with the Director of Infrastructure and Operations, Information Systems, the DISO shall establish standards for secure system configuration. Standards shall include but not be limited to inactivity timeout; password complexity, expiration, and reuse; multifactor authentication; port control; and encryption. Information Systems Bureau systems administrators shall implement the required controls in collaboration with the DISO.

User Access Controls
Access to computing resources must be specifically requested and granted based on the user's business need. Access to computing resources must be removed promptly when a user no longer has a business need for the access.

System Access Provisioning
The DISO shall establish standards for approving access to computer systems. System access must be authorized according to business need, using procedures established by the Information Systems Bureau. All system access requires approval by the user's management as well as the system owner.

System Access Deprovisioning
Users shall notify the Probation Department IT Service Desk when their job duties no longer require all the existing access rights to a system for which they have a user account. Managers and Special Assistants shall ensure that the IT Service Desk has been notified when a change in a user's job duties results in a change to their system access requirements.

System Access Review
All user accounts for systems containing PHI, PII, or CORI data shall be reviewed periodically on a schedule established by the DISO. Bureau Chiefs shall evaluate user accounts and permission levels, indicate accounts no longer required, indicate changes in permission levels required, and attest to the continuing need for access for all users whose accounts are to remain active. Accounts not verified by the appropriate manager or supervisor within the review and attestation time frame established by the DISO will be disabled.

Leave and Separation from Service
Managers and Special Assistants are responsible to ensure the IT Service Desk is notified to request that system access be disabled or terminated when an employee is on long-term leave or separates from employment with the Probation Department.

Inactive System Accounts
For systems containing PHI, PII, or CORI data, the DISO shall provide Deputy Directors with regular reports of accounts that have been inactive for an extended period. Deputy Directors shall indicate which users' job duties require continued access for infrequent use and which users' access is no longer required.

Reporting Security Incidents
Any user who becomes aware of a breach of information security or a situation that could potentially result in a breach, misuse, or crime relating to County information technology resources must contact the Probation Department IT Service Desk at (866) 607-3171 or ITService@probation.lacounty.gov to report the incident or situation.

Email Retention
The Probation Department retains email for five (5) years from the date a message is received or sent. Upon request by Internal Affairs or Civil Litigation, email will be retained until an investigation has been completed or legal hold has been lifted.

Access to Another User's Files or Email
Release of a user's files or emails to a supervisor or manager by Internal Services Department or Information Systems Bureau staff requires approval by the Internal Affairs Bureau Chief, Chief of Staff, or Chief Probation Officer.

Software License Compliance
Personally-owned copies of software shall not be installed on any Probation Department computer unless authorized by the Probation Department Chief Information Officer or his or her designee.

All software developed by or for the Probation Department is property of the County of Los Angeles.

Management Responsibilities
Managers and supervisors are responsible to ensure that workforce members under their supervision comply with this policy and to take appropriate corrective action, which may include discipline up to and including discharge, in the event of a policy violation. Managers and supervisors who become aware of violations of this policy by workforce members not under their supervision must promptly report the violation to the supervisor or manager of workforce member.

REVIEW DATE
The DISO shall review this policy annually and update as needed.

ASSISTANCE AVAILABLE
For questions or assistance regarding this Directive, contact the Probation Department DISO at (562) 940-2843 or ITSecurity@probation.lacounty.gov.

ATTACHMENTS
Attachment I: Agreement for Acceptable Use and Confidentiality of County Information Assets (AUA)
Attachment II: Confidentiality of CORI Information (CORI)

Ray Leyva
Interim Chief Probation Officer

ATTACHMENT I

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:
  - Any unlawful purpose;
  - Any purpose detrimental to the County or its interests;
  - Personal financial gain;
  - In any way that undermines or interferes with access to or use of County Information Asset for official County purposes;
  - 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:
  - I may divulge Non-public Information to authorized County staff and managers as necessary to perform my job duties;
  - 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;
  - I may not discuss Non-public Information outside of the workplace or outside of my usual work area;
  - 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 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.
- To 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.
  - 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.
  - 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).
- To 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.
- To 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.
  - 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.
- To 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 and that 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, and other social media services) in accordance with County-wide 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 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

ATTACHMENT II

CONFIDENTIALITY OF CORI INFORMATION

Criminal Offender Record Information (CORI) is that information which is recorded as the result of an arrest, detention or other initiation of criminal proceedings, including any consequent proceedings related thereto. As an employee of the Probation Department, in the course of your duties you will have access to CORI relative to persons referred for probation services. The Probation Department has a policy of protecting the confidentiality of Criminal Offender Record Information.

Copies of longhand drafts of court reports, official case notes, and miscellaneous case data are confidential probation records. These documents should be retained in the case file and are not to be removed or copied outside your normal duties. You are required to protect these confidential records against disclosure to all individuals who do not have a right to know the information.

The use of any information in probation files or the use of any information to make non-probationary contacts with probationers or their relatives, which has not been expressly approved by the Probation Department, is a breach of confidentiality, inappropriate, and unauthorized. Any employee engaging in such activities is in violation of the Probation Department's confidentiality policy and will be subject to appropriate disciplinary action and/or criminal action pursuant to Section 11142 of the California Penal Code.

I have read and understand the Probation Department's policy concerning the confidentiality of CORI records.

_____
(Signature)

_____
Name (Print)

_____
Classification

_____
Date

Copies: Personnel File, Employee
(Rev. 10/2019)