



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT <b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	POLICY NO. <b>556.01</b>	EFFECTIVE DATE <b>07/11/2016</b>	PAGE <b>1 of 10</b>
APPROVED BY: <i>Robin Kay, Ph.D.</i> Acting Director	SUPERSEDES <b>500.39 04/20/2005</b>	ORIGINAL ISSUE DATE <b>04/20/2005</b>	DISTRIBUTION LEVEL(S) <b>1</b>

**PURPOSE**

- 1.1 To ensure the proper use of County Information Technology (IT) Resources within the Los Angeles County Department of Mental Health (LACDMH/Department).

**DEFINITION**

- 2.1 **Information Technology (IT) Resources:** Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information - including computers; ancillary equipment: software, firmware, and similar materials; services, including support services; and related resources.
- 2.2 **Malicious Software:** Collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of Malicious Software is the computer virus; other examples are Trojan horses and worms.
- 2.3 **System Managers/Owners:** Person responsible for the operation and use of a system.

For a more complete definition of terms used in this policy, see the LACDMH Information Security Glossary, Attachment 1 of LACDMH Policy No. 555.02, Information Technology and Security.

**POLICY**

- 3.1 Proper use of County IT Resources must be adhered to by each user and strictly enforced by management in accordance with LACDMH Policy No. 553.02,



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>2 of 10</b>

LACDMH Privacy and Security Compliance Program, County Fiscal Manual, and other County and LACDMH policies and procedures.

- 3.2 All users are required to sign the County of Los Angeles Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Attachment 1) and review this policy. The LACDMH Human Resources Bureau must ensure that each new user receives and signs the Agreement during the new hire orientation (or, for vendors, before work begins) and that each user (except vendors) completes the Agreement during the annual Performance Evaluation process. The signed Agreement will be filed in the user's official personnel folder (or vendor file).
- 3.3 LACDMH System Managers/Owners will ensure that all users with access to County IT Resources have signed the Agreement prior to providing access.
- 3.4 Responsibility
  - 3.4.1 Access to County IT Resources and accounts are privileges granted to individual users based on their job duties and may be modified or revoked at any time. Each user is responsible for proper use and protection of LACDMH's County IT Resources. Users must protect all information contained in the IT Resources as required by local, state, and federal laws and regulations. Each user must sign and abide by the Agreement as described in Section 3.2. Violation of this Acceptable Use for County IT Resources Policy may result in disciplinary action, up to and including, discharge, and possible civil and/or criminal liability.
  - 3.4.2 County IT Resources are the property of the County and are to be used for authorized business purposes only.
- 3.5 Workforce Member Privacy
  - 3.5.1 Workforce Members have no expectation of privacy with respect to their use of the County information system assets because at any time LACDMH may log, review, or monitor any data created, stored, sent, or



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>3 of 10</b>

received. LACDMH has and will exercise the right to monitor any information stored on a workstation, server, or other storage device; monitor any data or information transmitted through the LACDMH network; and/or monitor sites visited on the LACDMH intranet, Internet, chat groups, newsgroups, material downloaded or uploaded from the Internet, and e-mail sent and received by Workforce Members. The kinds of information that will be obtained through the monitoring include any information from any LACDMH computer system. Activities or communications or computer usage not related to County business are likely to be monitored. LACDMH may use manual or automated means to monitor use of its County IT Resources.

3.5.2 Use of passwords to gain access to County IT Resources or to encode particular files or messages does not imply any expectation of privacy in the material created or received. The requirement for use of passwords is based on LACDMH's obligation to properly administer IT Resources to ensure the confidentiality, integrity, and availability of information. Users are required to authenticate with a unique User ID so that all access may be auditable.

### 3.6 Prohibited Activities

3.6.1 Prohibited Uses: Users are prohibited from using County IT Resources for any of the following activities:

3.6.1.1 Engaging in unlawful or malicious activities;

3.6.1.2 Sending, receiving, or accessing pornographic materials;

3.6.1.3 Engaging in abusive, threatening, profane, racist, sexist, or otherwise objectionable language;

3.6.1.4 Misrepresenting oneself or the County;



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>4 of 10</b>

- 3.6.1.5 Misrepresenting a personal opinion as an official County position;
- 3.6.1.6 Defeating or attempting to defeat security restrictions on County systems or applications;
- 3.6.1.7 Engaging in personal or commercial activities for profit;
- 3.6.1.8 Sending any non-work-related messages;
- 3.6.1.9 Broadcasting unsolicited, non-work-related messages (spamming);
- 3.6.1.10 Intentionally disseminating any destructive program (e.g., viruses);
- 3.6.1.11 Playing games or accessing non-business-related applications;
- 3.6.1.12 Creating unnecessary or unauthorized network traffic that interferes with the efficient use of County IT Resources (e.g., spending excessive amounts of time on the Internet, engaging in online chat groups, listening to online radio stations);
- 3.6.1.13 Attempting to view and/or use another person's account(s), computer file(s), program, or data without authorization;
- 3.6.1.14 Using County IT Resources to gain unauthorized access to LACDMH or other systems;
- 3.6.1.15 Using unauthorized wired or wireless connections to LACDMH networks;
- 3.6.1.16 Copying, downloading, storing, sharing, installing, or distributing movies, music, and other materials currently by



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>5 of 10</b>

copyright, except as clearly permitted by licensing agreements or fair use laws;

- 3.6.1.17 Using County IT Resources to commit acts that violate state, federal, and/or international laws, including but not limited to laws governing intellectual property;
  - 3.6.1.18 Participating in activities that may reasonably be construed as a violation of National/Homeland security;
  - 3.6.1.19 Posting scams such as pyramid schemes and make money-quick schemes; and
  - 3.6.1.20 Posting or transmitting private, proprietary, or confidential information, including patient information, to unauthorized persons, or without authorization.
- 3.6.2 Misuse of software: At no time must users be engaged in software copyright infringements. LACDMH prohibits users from conducting the following activities without proper licensing and prior written authorization:
- 3.6.2.1 Copying County-owned software onto their home computers;
  - 3.6.2.2 Providing copies of County-owned software to independent contractors, clients, or any other third-party person;
  - 3.6.2.3 Installing software on any LACDMH workstation (e.g., desktops, personal computers, mobile devices, laptops) or server;
  - 3.6.2.4 Downloading software from the Internet or other online server to LACDMH workstations or servers;



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>6 of 10</b>

3.6.2.5 Modifying, revising, transforming, recasting, or adapting County-owned software; and

3.6.2.6 Reverse engineering, disassembling, or decompiling County-owned software.

### 3.7 Passwords

3.7.1 Users are responsible for safeguarding their passwords for access to the County IT Resources. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No user may access any County IT resource with another user's password or account unless such access is explicitly allowed by the accessing user's job description.

### 3.8 Security

#### 3.8.1 County IT Resources

3.8.1.1 Users are responsible for ensuring that the use of outside computers and networks, such as the Internet, do not compromise the security of County IT Resources. This responsibility includes taking reasonable precautions to prevent intruders from accessing County IT Resources.

#### 3.8.2 Malicious Software

3.8.2.1 Malicious Software can cause substantial damage or inconvenience to County IT Resources. Users are responsible for taking reasonable precautions to ensure that they do not introduce Malicious Software into County IT Resources. Users must not bypass or disable County Malicious Software protections. Users must only use or distribute storage media or email (including attachments) known to the user to be free from Malicious Software.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>7 of 10</b>

3.8.2.2 Any user who telecommutes or is granted remote access must utilize equipment that contains current County-approved antivirus software and must adhere to County hardware/software protection standards and procedures that are defined by the County and LACDMH.

3.8.2.3 LACDMH restricts access to the Internet or any other network via modem, Digital Subscriber Line, cellular wireless, or other telecommunication services. No user may employ any external inbound or outbound connections to LACDMH network resources unless explicitly authorized by the Departmental Information Security Officer or designee.

3.8.2.4 Each user is responsible for notifying the Department's Help Desk as soon as a device is suspected of being compromised by a virus.

3.9 E-Mail

3.9.1 Access to County e-mail services is a privilege that may be wholly or partially restricted without prior notice and without consent of the user. E-mail messages are the property of the County and subject to review by authorized County personnel.

3.9.2 E-mail messages are legal documents. Statements must not be made on e-mail that would not be appropriate in a formal memo. Users must endeavor to make each electronic communication truthful and accurate. Users are to delete e-mail messages routinely in accordance with both the LACDMH and County E-mail policies.

3.9.3 Protected Health Information (PHI) and other confidential and/or sensitive information can be sent or received only if it is encrypted or safeguarded in accordance with LACDMH Policy No. 508.01, Safeguards for Protected Health Information.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>8 of 10</b>

3.9.4 Internet-based e-mail services accessed with County IT Resources must only be used for County purposes.

3.10 Use of the Internet

3.10.1 Use of the Internet must be in accordance with LACDMH and County Internet and privacy policies.

3.10.2 LACDMH is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide public network that is uncensored and contains sites that may be considered offensive. Users accessing the Internet do so at their own risk and LACDMH shall not be liable for inadvertent exposure to any offensive materials.

3.10.3 Users shall not allow another user to access the Internet using their authorized account.

3.10.4 Internet access is provided to the user at the discretion of each LACDMH Manager/Program Head.

3.11 Incident Reporting (Theft, Loss, or Damage of County Resources, Data, or Computing Equipment)

3.11.1 If a County Resource, Data or Computing equipment is lost, stolen, or damaged:

3.11.1.1 The workforce member must immediately notify Chief Information Office Bureau (CIOB) Helpdesk and provide a detailed statement about the accident or incident (When, Where, What, Who, How). CIOB Helpdesk will initiate necessary data security measures to mitigate any risks and will notify the responsible authorities accordingly. This may include service deactivation if applicable.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>9 of 10</b>

3.11.1.2 The workforce member must notify his/her management immediately who then must complete an Accident/Incident Investigative Report (AIIR) via the Service Catalog.

- Upon completion, the AIIR will automatically be forwarded to the responsible parties such as DMH Information Security, DMH Privacy, and Procurement Units, which upon receipt will take appropriate action to mitigate introduced risks.

3.11.1.3 Law Enforcement Report:

- If lost or stolen, the workforce member must file a police report within thirty (30) days of the incident. The report shall be emailed to DMH Helpdesk and also attached to the AIIR.
- If damaged, it will be up to the discretion of CIOB to determine if the workforce member must provide a police report within thirty (30) days of the incident. If required, the police report shall be emailed to DMH Helpdesk and also attached to the AIIR.

3.11.1.4 Whether lost, stolen, or damaged, if carelessness or negligence is determined to be the cause, the workforce member may be financially responsible for the full or partial cost of replacing the device.

3.11.1.5 If the required police report is not provided within thirty (30) days of the incident, the workforce member will automatically be considered responsible for reimbursing the Department for the full or partial cost of replacing the device.



**LAC  
DMH**  
LOS ANGELES COUNTY  
DEPARTMENT OF  
MENTAL HEALTH

**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>ACCEPTABLE USE FOR COUNTY INFORMATION TECHNOLOGY RESOURCES</b>	<b>556.01</b>	<b>07/11/2016</b>	<b>10 of 10</b>

**AUTHORITY**

1. Code of Federal Regulations Title 45 Part 164 Subpart C § 164.308(a)(3)(ii)
2. Board of Supervisors Policies 6.101, Use of County Information Technology Resources; 6.102, Countywide Antivirus Security Policy; 6.104, Electronic Communications; and 6.105, Internet Usage Policy
3. LACDMH Policy No. 1200.05, Networked Information Systems Usage

**ATTACHMENT (HYPERLINKED)**

1. [County of Los Angeles Agreement for Acceptable Use and Confidentiality of County Information Technology Resources](#)

**RESPONSIBLE PARTY**

LACDMH Chief Information Office Bureau