MANAGEMENT DIRECTIVE

DCFS INFORMATION SECURITY

Use of DCFS Information Assets

Management Directive #20-01

Date Issued:
☒ New Policy Release
☐ Revision of Existing Procedural Guide dated
Cancels: None

PURPOSE

To establish a policy for proper and secure use of County and DCFS Information Assets.

DEFINITIONS

EXHIBIT A – Information Technology and Security Definitions.

POLICY

General

DCFS Information Assets are essential County resources and a privilege provided at the discretion of the Department and management, and shall be:

a. Adequately and accurately documented, inventoried, tracked, and accounted for throughout the lifecycle of the asset;

b. Properly labeled, and clearly identified as the property of the County of Los Angeles;

c. Utilized for County business purposes, as intended and authorized, ethically, and professionally; and

d. Safeguarded and protected (physically and logically) against all forms of accidental or intentional, natural, or manufactured unauthorized access, view, use, disclosure, exposure, modifications, processing, transmission, deletion,

destruction, tampering, damage or theft, or events that may potentially disrupt, endanger or adversely impact business continuity or services.

DCFS Workforce shall:

a. Acknowledge, comply, adhere and follow applicable federal, state, County and DCFS information security, privacy and acceptable use policies, procedures, guidelines, protocols, standards, measures, best practices, mandates and record retention requirements including the Acceptable Use Agreement (AUA) of Los Angeles County, (attached to the Board of Supervisors Policy No. 6.101) and annually thereafter;

b. Obtain prior, formal, and written management authorization and approval to possess, access, use, transmit or store any DCFS Information Asset;

c. Use Department provided or approved computing devices, equipment, systems, software, or solutions (e.g., computers, tablets, USB flash drives, email, Cloud services) to transfer or store DCFS Information Assets;

d. Ensure personally owned devices have adequate malware protection software (e.g., antivirus), are up-to-date with all software patches, have firewall enabled before as applicable, before remotely accessing or using County Information Assets;

e. Protect and preserve the accuracy, privacy, confidentiality, integrity, and availability of County Information Assets and resources for which they are entrusted;

f. Connect County provided computing devices or endpoints to LA County Network (LANet) every 30 days, and not to exceed 45 days, to receive the latest security and software updates;

g. Encrypt all Non-public data and information (e.g., information which is exempt from public disclosure in specific legislation or which is identified as personal, sensitive, or confidential, such as Personally Identifiable Information (PII), individually identifiable health information, Protected Health Information (PHI), medical records (MI), employment and education records) according to DCFS requirements and standards set by the Departmental Information Security Officer (DISO);

h. Use proper measures and safeguards to secure paper documents and ensure access and disclosure of information is restricted to authorized individuals with legitimate business needs only. Paper documents that are no longer required must be securely disposed, shredded, or placed in locked containers;

i. Successfully complete the required and mandatory Information Security Awareness trainings;

j. Wear DCFS issued identification badge in a fashion that picture and information on the badge are clearly visible when entering all DCFS restricted areas at all times; and

k. Immediately and properly report all information security and privacy events or incidents in accordance with DCFS Management Directive - Information Security Incident Reporting and Response.

No entitlement or expectation of privacy is conveyed to DCFS Workforce concerning their activities when obtaining or utilizing County or DCFS Information Assets, including, and without limitation, anything they possess, access, use, view, create, store, or transmit (send, receive or share). Such activities are also subject to litigation and electronic discovery (eDiscovery).

The Department has the right to administer, modify, revoke and/or restrict, monitor, log, store, make public, investigate, put a litigation hold, audit and/or review all activities of DCFS Workforce related to use or access of DCFS Information Assets and resources via authorized personnel at any time without notice or consent, including, and without limitation, internet usage and activities, electronic communications (e.g., email sites, instant messaging sites, chat groups, newsgroups), data downloaded from or uploaded to the Department, files, data sets, databases, applications or systems.

Management Responsibilities:

DCFS managers and supervisors shall:

a. Ensure staff is informed, aware, up-to-date, adequately trained, acknowledge and adhere to County and DCFS information security, privacy and acceptable use policies, procedures, guidelines, protocols, standards, requirements, measures, best practices, and mandates including the AUA and annually thereafter;

b. Monitor, review, verify, validate and accordingly adjust staff access, authentication and authorization levels and permissions to DCFS Information Assets including access to restricted information technology areas based on business requirements; need to know; need to have; and principle of least privilege while preserving and maintaining separation of duties, at a minimum, quarterly and upon a change in business needs (e.g., changes in roles, responsibilities, duties, or when access is no longer needed) or changes in employment status (e.g., resignation, termination, transfer, promotion); and

c. Adhere to, follow, and implement County Fiscal Manual (CFM) requirements and maintaining effective internal controls, and perform ongoing monitoring of all internal control processes to ensure they are designed appropriately and operating as intended, and any weaknesses or non-compliance are promptly identified and corrected.

Prohibited Use:

DCFS Information Assets, including without limitation, internet services, and electronic communication shall not be utilized for:

- Any unlawful purpose;
- Any purpose detrimental to DCFS or its interests;
- Personal financial gain;
- Undermining or interfering with access to or use of DCFS Information Assets for official DCFS purposes;
- Hindering productivity, customer service, or interferes with a DCFS Workforce performance of their official job duties;
- Transfer or storage on non-Department provided or approved device, equipment, system, software, or solution including but not limited to personal or public computers, tablets, USB flash drives, emails, and Cloud providers;
- Expressing or implying sponsorship or endorsement by DCFS, except as approved in accordance with departmental policies, standards, and procedures;
- Personal purpose where activities are for private benefit, gain or advantage, or an outside endeavor not related to DCFS business purposes. Personal purpose does not include incidental and minimal personal use of DCFS Information Assets including internet usage;
- Representing themselves as someone else, real, or fictional, or sending information anonymously unless specifically authorized by Department management and the DISO;
- Sending, disseminating, storing, or otherwise disclosing non-public, confidential, personal information or medical records including without limitation, information that is protected under the Health Insurance Portability and Accountability Act, Health Information Technology for Economics and Clinical Health Act, or any other confidentiality or privacy legislation;
- Downloading, using, accessing, storing, displaying, or distributing software, unless approved by the DISO;
- Downloading, using, accessing, storing, displaying, viewing, or distributing material (e.g., movies, music, software, or books) in violation of copyright laws;
- Downloading, using, accessing, storing, displaying, viewing, or distributing pornography or other sexually explicit material;
- Soliciting participation in, or advertising scams (e.g., spamming, pyramid schemes, and "make-money-fast" schemes) to others;
- Posting or transmitting false, defamatory, fraudulent, or confidential information;

- Operating a personal business, or a non-County or DCFS business related web site;
- Posting or transmitting to unauthorized persons any material deemed to be non-public, confidential, personal, or otherwise protected from disclosure;
- Participating in soliciting political activities;
- Attempting unauthorized access to the account of another person or group on the internet, or attempting to circumvent County or DCFS security measures, or security measures taken by others connected to the internet, regardless of whether or not such attempts are successful or resulting in corruption or loss of data or other information (e.g., password stealing, phishing, or whaling);
- Disabling, modifying, or deleting managed security software or computer settings;
- Knowingly or carelessly introducing any malicious device or software to County or DCFS Information Assets; and
- Downloading, accessing, creating, sharing, or distributing offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County or DCFS Information Assets (e.g., over County or DCFS 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 such DCFS Workforce assigned job function.

APPLICABILITY

This policy applies to all DCFS Workforce.

COMPLIANCE

DCFS Workforce who violate this directive may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-DCFS Workforce, including, and without limitation, contractors, in violation may be subject to termination of contractual agreements, denial of access to County or DCFS resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

There are no exceptions to Information Security Management Directives and policies.

RESPONSIBLE DEPARTMENT

Department of Children and Family Services.

REFERENCE

July 13, 2004, Board Order No. 10 – Board of Supervisors — Information Technology and Security Policies

Board of Supervisors Policy No. 3.041 – Protection of Records Containing Non-Public Information

Board of Supervisors Policy No. 3.040 – Protection Records Management and Archive of County Records

Board of Supervisors Policy Manual Chapter 6 - Information Technology

Board of Supervisors Policy No. 9.015 – County Policy of Equity

Board of Supervisors Policy No. 9.040 – Investigations Of Possible Criminal Activity Within County Government

Agreement for Acceptable Use and Confidentiality of County Information Assets (Acceptable Use Agreement)

Comprehensive Computer Data Access and Fraud Act, California Penal Code Section 502

Health Insurance Portability and Accountability Act (HIPAA) of 1996

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

California Civil Code Section 1798.29

Los Angeles County Fiscal Manual (CFM)

November 21, 2017 Board Order No. 19