MANAGEMENT DIRECTIVE

DCFS INFORMATION SECURITY

Information Security Incident Reporting and Response

Management Directive #20-03

Date Issued:

☒ New Policy Release

☐ Revision of Existing Procedural Guide dated

Cancels: None

PURPOSE

To establish a policy to identify, detect, and report information security incidents adequately and promptly.

DEFINITIONS

EXHIBIT A – Information Technology and Security Definitions.

POLICY

General

The Department of Children and Family Services (DCFS) Information Assets are essential County resources that shall be protected at all times. While being vigilant, DCFS Workforce shall:

a. Follow and adhere to all applicable information security, privacy, and acceptable use policies, procedures, guidelines, protocols, standards, requirements, measures, best practices, and mandates;

b. Immediately report any violation of information security and privacy policies, protocols, or mandates, or any suspected, attempted or successful, intentional or accidental, natural or man-made events that may disrupt business continuity, endanger or adversely impact the privacy, confidentiality, integrity or availability of Information Assets and resources; and

c. Preserve evidence by avoiding the use of updating or modifying any potentially impacted or involved DCFS Information Asset (e.g., software, hardware) until official and written authorization is provided by the Departmental Information Security Officer (DISO).

Information Security Incident Reporting:

Information security incidents shall be reported using one of the following methods:

a. Phish Alert button in outlook to report suspicious emails

b. Internal Services Department (ISD) eService Portal via: DCFS LAKids Intranet site Home page or http://sms.isd.lacounty.gov/cherwellPortal.

c. Contact ISD Help Desk at: (562) 658-1606 or (562) 940-3305.

When reporting an event, it is critical to accurately provide as much information as possible, and at minimum:

a. Contact information;

b. Date and time of the event or incident;

c. Thorough description of the incident in chronological order;

d. Type of potentially compromised data and information (e.g., Personally Identifiable Information (PII), Protected Health Information (PHI), case information, or any other sensitive/confidential data or information); and

e. Potentially affected or impacted users, entities or organizations, software or hardware including, but not limited to, any system, application, or physical computing device that stores, accesses, processes or transmits data or information (e.g., LRS, CWS/CMS, laptop, desktop, mobile or satellite phone, CD/DVD, Flash/USB storage device, digital camera, printer, etc.).

Management Responsibilities:

DCFS managers and supervisors are responsible to ensure staff:

a. Follow and adhere to information security, privacy and acceptable use policies, procedures, guidelines, protocols, standards, requirements, measures, best practices, and mandates; and

b. Immediately and properly report violation of information security and privacy policies and mandates, events, and incidents set forth herein.

The DISO is a member of the Countywide Cybersecurity Emergency Response Team (CERT), leads and oversees the DCFS CERT, and has the authority including, but not limited to:

- Take all necessary actions to address information security threats and incidents;

- Communicate and coordinate all incident response activities with applicable entities and organizations (e.g., DCFS Executive Team, County Chief Information Office, Auditor-Controller, law enforcement, etc.); and

- Facilitate eDiscovery and investigations as needed including the prosecution of criminal acts.

Release of any information related to incidents to the media or public shall be coordinated by the DISO and provided through authorized DCFS representatives or official spokespersons (i.e., DCFS Public Relations or Information Office).

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

DCFS Management Directive (MD) 20-01 – Use of DCFS Information Assets