MANAGEMENT DIRECTIVE

DCFS INFORMATION SECURITY
Information Security Awareness Training

Management Directive #20-02

Date Issued:

☒ New Policy Release

☐ Revision of Existing Procedural Guide dated

Cancels: None

PURPOSE

To establish a policy to train and raise awareness on information security and privacy matters, requirements, protection measures, and responsibilities.

DEFINITIONS

EXHIBIT A – Information Technology and Security Definitions.

POLICY

The Department of Children and Family Services (DCFS) information security awareness trainings are formulated to:

a. Cultivate and raise DCFS knowledge and awareness on current and evolving information security and privacy matters (e.g., policies, procedures, legal mandates, safeguards, attack vectors, risks, threats, best practices); and

b. Empower DCFS Workforce to stay vigilant and timely identify, prevent, detect, respond to security incidents, and protect County Information Assets.

Information security awareness trainings are provided at new hire orientation sessions, followed by annual mandatory trainings, and ongoing refresher courses thereafter.

Supplemental and specialized information security awareness trainings and simulations are conducted continuously via various means (e.g., symposiums, seminars, management meetings, webinars, videos, newsletters, e-mail reminders, notifications, alerts, table-top exercises, and phishing simulations).

DCFS Workforce shall:

a. Timely enroll and successfully complete the mandatory information security awareness trainings and refreshers including new hire orientation sessions as applicable; and

b. Continuously and actively participate in information security awareness training programs, activities, and sessions.

Management Responsibilities:

DCFS managers and supervisors shall:

a. Monitor and ensure staff successfully and timely enroll and complete all mandatory information security awareness training courses;

b. Encourage continuous and active participation of staff in additional security awareness trainings and activities (e.g., Cybersecurity Awareness Month, presentations, webinars);

c. Ensure staff abide by County and DCFS information security policies and procedures, and as needed, request and coordinate additional trainings from DCFS Information Security Office; and

d. Track and keep record of staff who participated in trainings as applicable (e.g., sign-in sheet, list of attendees).

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.

RESPONSIBLE DEPARTMENT

Department of Children and Family Services

REFERENCE

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