Policy

The Department of Children and Families (DCF) Information Services Division and its information assets represent critical components necessary to support DCF's mission of working together with families and communities for children who are healthy, safe, smart and strong.

This policy establishes the DCF-wide strategies and responsibilities for ensuring the confidentiality, integrity and availability of the information assets that are accessed, managed; or controlled by DCF in support of the aforementioned mission.

Any person acting on behalf of DCF shall comply with all applicable federal, state and local laws and regulations, including but not limited to:

- The Health Insurance Portability and Accountability Act. P.L. 104-19, as amended HIPAA), with special attention to the safeguarding of Protected Health Information (PHI) as specifically defined by 45 CFR 160.103;
- the Family Educational Rights and Privacy Act, 20 USC §1232g; 34 CFR Part 99, (FERPA), with special attention to the safeguarding of education records;
- the Federal Information Security Modernization Act P.L. 113-283 (FISMA);
- the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA Technical System Security Requirements or TSSR);
- Connecticut General Statutes including but not limited to §17a-16(b) and §17-28 *et seq.*;
- the Automated Data Processing System Security Requirements, 45 CFR 95.621(f) (CCWIS); and
- the Criminal Justice Information Systems, 28 CFR 2 et *seq.* (CJIS).

To facilitate compliance with the above regulations and statutes, policy statements that follow have been categorized into 17 security control families, as defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, because the security requirements of the aforementioned regulations and statutes map directly to the security topics contained therein.

To achieve the directives outlined in this policy and subsequent policy statements, DCF shall adhere to the NIST Risk Management Framework (NIST SP 800-37) to categorize its information systems, select and implement applicable security controls (NIST SP 800-53 Rev4), assess security controls, authorize the information system(s) and monitor security controls (NIST SP 800-137). Categorization of a system shall be set to the high-water mark based on the highest security categorization of the information accessed, processed, transmitted or stored therein. In the event that implementation of a security control will interfere with DCF's ability to carry out its mission, appropriate compensating controls shall be assessed and implemented.

All security control baselines shall be continuously reviewed and evaluated. Baselines shall be updated as required to ensure that federal, state and local regulatory-compliant control capabilities are maintained. Supporting methodologies and procedures shall provide specific guidelines and instructions to ensure the effective implementation of required security controls and control enhancements. The methodologies, procedures and baselines shall be maintained in the "DCF Information Systems Practice Guide," which shall include specific references and mappings to NIST 800-53 control elements and control enhancements sufficient to meet regulatory requirements.

See also: "DCF Information Systems Practice Guide."

Definitions

Information asset means any data, information, system, computer, network device, document, contractual agreement or any other component of DCF's infrastructure, regardless of its medium or location, which is used by any authorized individual in the execution of DCF business.

Staff member means any DCF employee, contractor, intern, volunteer or any other person authorized to act on behalf of DCF.

Intersection with DAS Policies

The policies and procedures of the State of Connecticut Department of Administrative Services shall be incorporated into this policy.

Scope and Applicability

The scope of this policy includes all information assets governed by DCF, including information assets provided by DCF through contracts, subject to the terms therein. All staff members and any individuals or information systems granted access to or the use of DCF information assets shall comply with this and all related policies and procedures.

Tier Responsibilities

DCF Executive Leadership (Tier 1) shall be responsible for addressing risk from an organizational perspective and to provide the governance structure for implementation and maintenance of this policy and all related procedures.

DCF Management and Business Leadership (Tier 2) shall be responsible for defining the types of information needed to successfully execute mission and business processes and to provide strategic guidance for protection of information assets.

DCF Staff (Tier 3) shall implement the security controls necessary to protect information assets based on decisions and guidance from Tiers 1 and 2.

Senior Information Security Officer

DCF shall appoint a senior information security officer who shall be responsible, in conjunction with the Information Systems Division, the DCF Senior Management Team and the DCF Policy Unit, for the development and implementation of DCF's information security policies and procedures.

DCF Role-Based Access Control (AC-1)

DCF shall limit information system access to authorized users and processes acting on behalf of authorized users and authorized devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. To achieve this directive, Access Control processes defining baseline methodologies, guidelines and procedures for account management, access enforcement, separation of duties, least privilege, unsuccessful logon attempts, system use notification, session lock, session termination, permitted actions without identification or authentication, remote access, wireless access, access control for mobile devices, use of external information systems, information sharing, and publicly accessible content shall be established, approved, monitored and maintained across DCF for all information systems, operating systems, databases and network devices supporting the DCF business processes.

(Continued next page)

DCF Role-Based Access Control (AC-1)	**Note:** Enterprise secure remote access to DCF information systems and infrastructure shall be through systems implemented and managed by DAS-BEST. Identities and access privileges shall be provisioned by DCF and provided to DAS-BEST for functional management. Third parties who are not DCF employees shall not have access to DCF electronic information systems except as authorized pursuant to procedures developed by Information Systems and approved by the Commissioner, or as otherwise specifically permitted by state or federal law.
DCF Role-Based Identification and Authentication (IA-1)	DCF shall identify information system users, processes acting on behalf of users and authorized devices and authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to DCF information systems. To achieve this directive, Identification and Authentication processes defining baseline methodologies, guidelines and procedures for users (both organizational and non-organizational) and device identification and authentication, as well as identifier and authenticator management, authenticator feedback and cryptographic module authentication, shall be established, approved, monitored and maintained across DCF for all information systems, operating systems, databases and network devices supporting DCF business processes.
Security Engineering System and Communications Protection (SC-1)	DCF shall monitor, control and protect DCF communications (*e.g.*, information transmitted or received by DCF information systems) and the systems involved in any such communications. To achieve this directive, System and Communications Protection processes defining baseline methodologies, guidelines and procedures for application partitioning, information in shared resources, denial of service protection, boundary protection, transmission confidentiality and integrity, network disconnect, cryptographic key establishment and management, cryptographic protection, collaborative computing devices, public key infrastructure certificates, mobile code, voice over internet protocol, secure name/address resolution service including architecture and provisioning therefor, session authenticity, protection of information at rest and process isolation shall be established, approved, monitored and maintained across DCF.
Security Engineering System and Information Integrity (SI-1)	DCF shall ensure the integrity of its information assets. To achieve this directive, System and Information Integrity processes defining baseline methodologies, guidelines and procedures for flaw remediation, malicious code protection, information system monitoring, security alerts, integrity of software, firmware and information, spam protection, input validation, error and information handling and retention and memory protection shall be established, approved, monitored and maintained across DCF for all information systems, operating systems, databases and network devices supporting DCF business processes.

Physical Protection Media Protection (MP-1)

DCF shall protect information system media, both physical and digital, from unauthorized access, modification or destruction. To achieve this directive, Media Protection processes defining baseline methodologies, guidelines and procedures for media access, media marking, media storage, media transport, media sanitization and media use shall be established, approved, monitored and maintained across DCF.

Physical and Environmental Protection (PE-1)

DCF shall limit physical access to information systems, equipment and the respective operating environments to authorized individuals and protect information systems and supporting infrastructure from hazards to ensure the availability of mission-critical information assets. To achieve this directive, Physical and Environmental Protection processes defining baseline methodologies, guidelines and procedures for physical access authorizations, physical access control, access control for transmission medium and output devices, monitoring physical access, visitor access records, power equipment and cabling, emergency shutoff, power and lighting, fire protection, temperature and humidity controls, water damage protection, delivery and removal, and alternate work sites shall be established, approved, monitored and maintained across DCF.

DCF Personnel Security Awareness and Training (AT-1)

DCF shall:

- ensure that managers and users of DCF information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, regulations and procedures related to the security of DCF's information systems; and
- ensure that applicable personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

To achieve this directive, Awareness and Training processes defining baseline methodologies, guidelines and procedures for security awareness training, role-based security training and security training records shall be established, approved, monitored and maintained across DCF.

Personnel Security (PS-1)

DCF shall:

- ensure that individuals occupying positions of responsibility within DCF meet established security criteria for those positions;
- ensure that DCF information assets are protected during and after personnel actions such as terminations and transfers; and
- employ formal sanctions for personnel failing to comply with information security policies and procedures.

To achieve this directive, Personnel Security processes defining baseline methodologies, guidelines and procedures for position risk designation, personnel screening, termination and transfer, access agreements, third-party personnel security and personnel sanctions shall be established, approved, monitored and maintained across DCF.

Governance and Planning Contingency Planning (CP-1)

DCF shall establish, maintain and effectively implement plans for emergency response, backup operations and post-disaster recovery for DCF information systems to ensure the availability of mission-critical information resources and continuity of operations in emergency situations. To achieve this directive, Contingency Planning processes defining baseline methodologies, guidelines and procedures for information system contingency plans, contingency training, contingency plan testing, alternate storage and processing sites, telecommunication services, information system backup and information system recovery and reconstitution shall be established, approved, monitored and maintained across DCF.

Incident Response (IR-1)

DCF shall :

- establish an operational incident-handling capability for DCF information systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities; and
- track, document and report incidents to appropriate DCF officials and other authorities.

To achieve this directive, Incident Response processes defining baseline methodologies, guidelines and procedures for incident response training, incident response testing, incident handling, incident monitoring, incident reporting, incident response assistance and incident response plans shall be established, approved, monitored and maintained across DCF.

System Maintenance (MA-1)

DCF shall :

- perform periodic and timely maintenance on DCF information systems; and
- provide effective controls on the tools, techniques, mechanisms and personnel used to conduct information system maintenance.

To achieve this directive, System Maintenance processes defining baseline methodologies, guidelines and procedures for controlled maintenance, maintenance tools, non-local maintenance, maintenance personnel and timely maintenance methodologies and procedures shall be established, approved, monitored and maintained across DCF.

Security Planning (PL-1)

(SSPs) for DCF information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems. To achieve this directive, Security Planning processes defining baseline methodologies, guidelines and procedures for system security planning, rules of behavior and information system security architecture shall be established, approved, monitored and maintained across DCF.

See also “Use of Social Media” subsection below.

System and Services Acquisition (SA-1)

DCF shall:

- allocate sufficient resources to adequately protect DCF information systems;
- employ system development life cycle processes that incorporate information security considerations;
- employ software usage and installation restrictions; and
- ensure that third-party providers employ adequate security measures, through federal and state law and contractual language, to protect information, applications and services outsourced from DCF.

To achieve this directive, Systems and Services Acquisition processes defining baseline methodologies, guidelines and procedures for allocation of resources, system development life cycle (SDLC), acquisition process, information system documentation, security engineering principles, external information system services, developer configuration management and developer security testing shall be established, approved, monitored and maintained across DCF.

Continuous Diagnostics and Mitigation Audit and Accountability (AU-1)

DCF shall:

- create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate activity on DCF information systems; and
- ensure that the actions of individual information system users can be uniquely traced for all DCF information systems containing regulated data.

To achieve this directive, Audit and Accountability processes defining baseline methodologies, guidelines and procedures for auditable events, content of audit records, audit storage capacity, response to audit processing failures, audit review, analysis and reporting, audit reduction and report generation, time stamps, protection of audit information, audit record retention and audit generation shall be established, approved, monitored and maintained across DCF.

Security Assessment and Authorization (CA-1)

DCF shall:

- periodically assess the security controls in DCF information systems to determine if the controls are effective in their application;
- develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in DCF information systems;
- authorize the operation of DCF's information systems and any associated information system connections; and
- monitor information systems security controls on an ongoing basis to ensure the continued effectiveness of the controls.

To achieve this directive, Security Assessment and Authorization processes defining baseline methodologies, guidelines and procedures for security assessments, system interconnections, plans of action and milestones, security authorization, continuous monitoring and internal system connections shall be established, approved, monitored and maintained across DCF.

Configuration Management (CM-1)

DCF shall:

- establish and maintain baseline configurations and inventories of DCF information systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles; and
- establish and enforce security configuration settings for information technology products employed in DCF information systems.

To achieve this directive, Configuration Management processes defining baseline methodologies, guidelines and procedures for baseline configurations, configuration change control, security impact analysis, access restrictions for change, configuration settings, least functionality, information system component inventory, configuration management plans, software usage restrictions and user-installed software shall be established, approved, monitored and maintained across DCF.

Risk Assessment (RA-1)

DCF shall periodically assess the risk to DCF operations (including mission, functions, image and reputation), DCF assets and individuals resulting from the operation of DCF information systems and the associated processing, storage or transmission of DCF information. To achieve this directive, Risk Assessment processes defining baseline methodologies, guidelines and procedures for security categorization, risk assessment and vulnerability scanning shall be established, approved, monitored and maintained across DCF.

Business Associate Agreements

Any person or organization that performs or assists in the performance of a function or activity on behalf of DCF which involves the use or disclosure of ePHI, or any function or activity regulated by HIPAA, must comply with the terms and conditions of the HIPAA regulations section of the State of Connecticut Human Service Contract Part I.

Functions include, but are not limited to, the provision of the following services of ePHI:

- legal;
- actuarial;
- accounting;
- consulting;
- data aggregation;
- management;
- administrative;
- accreditation; or
- financial.

Cross-reference: Grants and Contracts subsection of DCF Policy 2-2, “Fiscal Services Division."

Use of Social Media

DCF staff may use social media (*e.g.,* Facebook, Twitter, MySpace, Craigslist, LinkedIn, YouTube, DCF-created websites) to:

- communicate with adult and child clients, foster parents and relative caregivers;
- provide general education about DCF to the public;
- search for relatives or for children on runaway status; and
- gather publicly-available information.

Social media use through state equipment is limited to DCF business purposes only. All relevant DCF and DAS-BEST policies shall strictly apply.

No confidential client information shall be posted to a social media site by a DCF employee in any manner or for any reason.

DCF employees shall not "friend" or otherwise contact DCF adult and child clients through personal social media accounts without the written permission of a DCF manager.

DCF staff may not discuss or comment on clients, relatives or foster families on their personal social media accounts.

Each social media account or website created using state equipment shall be approved in advance by the Information Services Division, which may, in turn, be required by state policy to seek permission from BEST.

Any DCF staff member who creates an account or otherwise accesses social media using state equipment shall:

- first submit a written statement to DCF Human Resources acknowledging that he or she has read the policies cited in this section;
- conform to the Terms of Service specific to the individual social media site;
- identify themselves clearly and accurately (pseudonyms shall not be permitted);
- comply with applicable law regarding copyrights and plagiarism;
- not post someone else's work, including photographs, without permission and proper attribution (other than short quotes that constitute legal "fair use"); and
- not post libelous or defamatory information to the internet.

DCF reserves the right to filter internet and social media sites accessed through state equipment. There is no expectation of employee privacy when using state equipment and DCF may monitor and review employee use at its discretion. Failure to adhere to this policy and the associated state policies may result in disciplinary action up to and including dismissal.

Proper Use of FBI Criminal Information

DCF employees who have been granted access to the FBI criminal information database through COLLECT shall adhere to all federal regulations pertaining to such use.

Cross-reference: DCF Policy 2-4-1, "Proper Use of FBI Criminal Information."

Loss Reporting Procedures

When the loss or theft of state equipment occurs, staff shall follow the procedures and timeframes set forth in this policy. The purpose of this policy is to promulgate mandatory agency reporting requirements to:

- respond properly and timely to the loss or theft of confidential or restricted state information; and
- respond properly to the loss of state assets or controllable items in conformance with state policy and/or statute.

See: Attachment A, "Loss Reporting Procedure Steps."

Policy Enforcement and Sanctions

DCF may temporarily suspend or block access to any individual or device when it appears necessary to do so in order to protect the integrity, security or functionality of DCF information assets.

Anyone who fails to comply with DCF, State of Connecticut or federal security policies and procedures shall be subject to discipline up to and including termination of employment. In addition, civil and criminal legal penalties may apply.