DCF PRIVACY PROGRAM PLAN

April 2024

Wisconsin Department of Children and Families

DCF-P-5743 (N. 04/2024)

Table of Contents

OVERVIEW OF PRIVACY PROGRAM

The National Institute of Standards and Technology (NIST) published updated security and privacy controls in September 2020. A new program management control is PM-18 Privacy Program Plan. The Program Management (PM) family of controls are designed to facilitate organizational compliance with applicable federal laws, executive orders, directives, policies, regulations, and standards[1].

This document serves as the Wisconsin Department of Children and Families (DCF) Privacy Program Plan, as described and required by IRS Publication 1075, and aligns with NIST Special Publication 800-53r5.

DCF Organizational Vision

"All Wisconsin children and youth are safe and loved members of thriving families and communities."

As DCF works toward this vision on a daily basis, protecting the privacy of these families is paramount, including following federally required standards to protect their information from privacy risks.

Privacy Program Plan Strategic Goals and Objectives

The strategic goals and objectives of DCF's privacy program plan are provided below:

1. Ensure compliance with applicable federal laws, regulations, and policies.
2. Streamline privacy policies and procedures for systems, programs, and operations.
3. Provide clear and easily accessible information about department-wide privacy policies, practices, and processes.
4. Collect and use personal information for the specified purposes and retain personal information for only as long as necessary.
5. Conduct risk assessments to manage privacy risks across the department.

DCF management and staff are collectively committed to meeting current and evolving privacy requirements and regulations through establishing clear policies, implementing robust processes, conducting regular risk assessments and fostering a culture of compliance within the organization through ongoing communication, training, and continuous improvement.

[1] Related controls include PM-19 Privacy Program Leadership Role and PM-20 Dissemination of Privacy Program Information

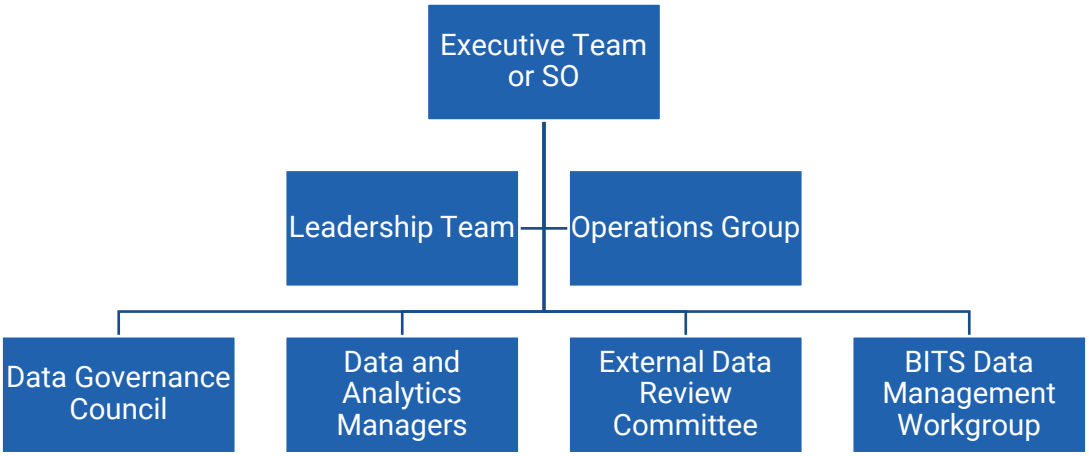
PRIVACY PROGRAM STRUCTURE

This section provides information regarding how DCF ensures the protection of personal information through security categorization and control efforts and describes how security or privacy related activities affecting systems are planned for and coordinated across the organization.

Data and Privacy Governance

DCF has a de-centralized privacy and data decision making structure. To ensure coordination across the department, privacy policies and procedures are addressed through councils, workgroups, and committees. The membership of decision-making bodies includes Senior Agency Officials for Privacy (SAOP) and other privacy officials across the department.[2] The agency utilizes a Data Governance Council, Data and Analytics Managers, an External Data Review Committee, and an Information Technology Data Management Workgroup which make recommendations to the DCF Operations or Leadership Teams on a wide variety of privacy-related issues. The Data Governance Council, External Data Review Committee and Data and Analytics Managers Workgroup include Senior Agency Officials for Privacy and other privacy officials. These groups incorporate the use of charters and reporting structures to further ensure alignment with DCF's organizational vision and avoid duplication of privacy efforts. See Figure 1.

Figure 1. DCF Privacy and Data Decision Making Structure



Executive Team – Includes the DCF secretary, deputy secretary, and assistant secretary and other executive leaders in the Secretary's Office (SO). The Executive Team leads the department vision and priorities, operations, policies and positions on issues related to all divisions and department programs.

Leadership Team – Includes SO and division administrators. The Leadership Team's role is to discuss high-level organizational strategies, establish and carry out agency must-do goals, effectuate cross-agency decision-making, and review high-level key performance indicators (KPI) impacting the organization, divisions, and other teams.

[2] System-level decisions flow to the DCF Privacy and Data Decision Making Structure.

Operations Group – Includes division leaders (primarily deputy administrators) and key agency operations areas, such as finance, information technology, regional operations, performance management, agency operations, human resources, budget, and legal. The Operations Group focuses on operational awareness, alignment and effective problem solving. This group also has primary decision-making authority around cross-agency operational issues.

Data Governance Council - Includes Senior Agency Officials for Privacy and other privacy officials. The Data Governance Council makes recommendations regarding the data governance structure, the process for vetting research and information requests, and a standardized process for data sharing agreements including a data sharing agreement template.

External Data Review Committee - Includes Senior Agency Officials for Privacy and other privacy officials. The External Data Review Committee is responsible for ensuring that the data found within DCF's publicly available data products are transparent, consistent, easily accessible, and meet all standards for privacy.

Data and Analytics Manager Workgroup - Includes Senior Agency Officials for Privacy and other privacy officials. The Data and Analytics Managers workgroup focuses on building a community of learning, championing data-informed decision making and promoting the concept of data as a valuable asset.

Bureau of Information Technology Services (BITS) Data Management Workgroup – Includes BITS Enterprise Data and Architecture (EDA) members, application and business intelligence technical leads and subject matter experts. The BITS Data Management Workgroup is responsible for developing BITS data management policies and procedures, establishing cross-section best practices and providing an avenue for data management peer reviews. The goal of the workgroup is to ensure uniformity, accuracy, stewardship and accountability for BITS data assets.

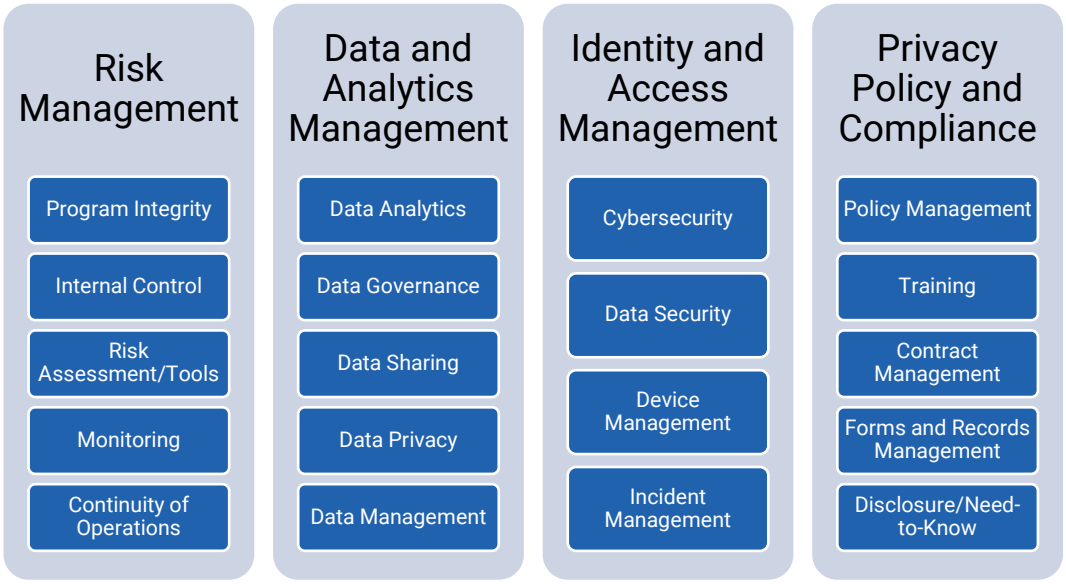
Privacy and Security Organizational Structure

The DCF Privacy Program Plan is delegated to the Division of Management Services (DMS). DMS is responsible for providing department-wide business services and functional support to the department. These supportive infrastructure services include, but are not limited to, information technology services and application development; data management; metric development; program evaluation; contract administration and monitoring; payment-issuance and other accounting-related services; and programmatic compliance. Additional functional support services by DMS include facilities management, staff change processes, forms, publications, management of DCF policies, and continuity-of-operations activities.

The DCF Privacy and Security Structure is comprised of four functional components that are dispersed across the department, with privacy and security functions coordinated by DMS (see Figure 2):

- Risk Management
- Data and Analytics Management
- Identity and Access Management
- Privacy Policy and Compliance

Figure 2. DCF Organizational Structures Supporting Privacy and Security



ROLE OF SENIOR AGENCY OFFICIALS FOR PRIVACY AND OTHER STAFF

DCF employs a distributed model for privacy which includes privacy officials across the department who ensure alignment with privacy program requirements and implement and monitor requirements within each respective program area. The following describes the roles of senior agency officials for privacy and other staff.

Secretary's Office

The Secretary's Office (SO) is ultimately responsible for DCF's Privacy Program, guides the organizational mission, and provides adequate resources. The Secretary's Office may, however, designate responsibility to other senior privacy officials within the agency. The SO has delegated responsibility for coordinating, developing and implementing requirements related to a wide variety of regulations, compliance, and managing risks across the department to DMS.

Senior Agency Officials for Privacy

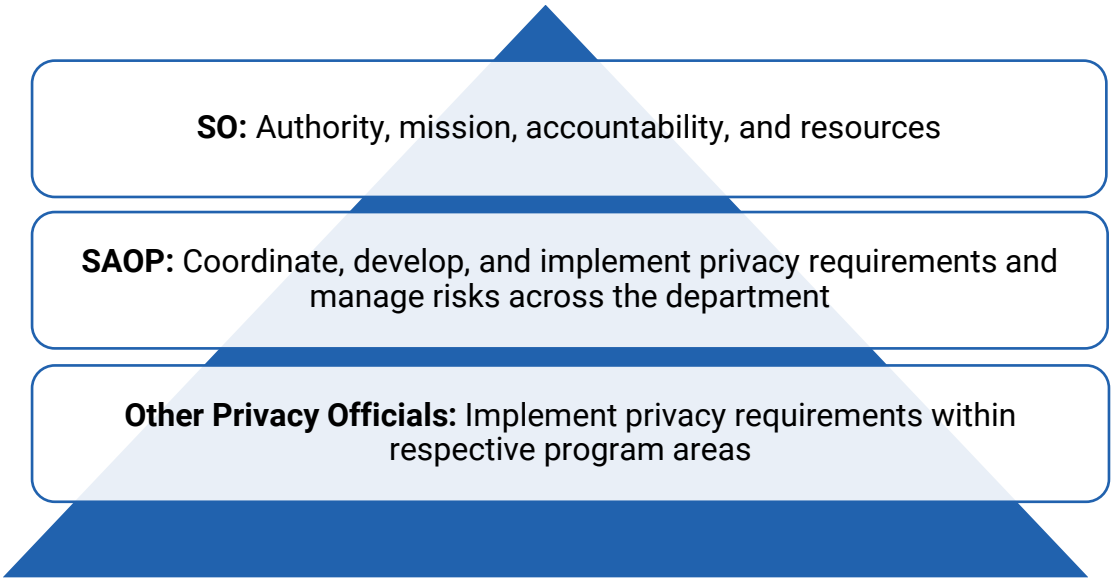
Within DMS, there are three senior agency officials for privacy (SAOP); these include the division's policy initiatives advisor (PIA), director of the Bureau of Performance Management (BPM), and the chief information security officer (CISO). These positions manage plan related activities and are responsible for the successful operation of the privacy program plan including relevant policy development, data governance, technical infrastructure, coordination of resources, ensuring protection of sensitive information, overseeing the implementation and coordination of the plan, and monitoring the plan for compliance and risk.

Other Privacy Officials

Other privacy officials[3] work across the department to ensure alignment with requirements and implement and monitor activities related to privacy and security within the respective program areas. These privacy officials could include program area subject matter experts (SME) within the divisions, information systems data stewards, forms coordinators, the Office of Legal Counsel (OLC), Office of Inspector General (OIG) and Communications Office. Descriptions of these additional resources and staff dedicated to the success of DCF's privacy program are described in Figure 3.

[3] At DCF, "other privacy officials" are staff who work on privacy issues.

Figure 3. Role of Senior Agency Officials for Privacy at DCF



RESOURCES DEDICATED TO PRIVACY PROGRAM PLAN

The DMS administrator serves on the DCF Leadership Team and advocates for sufficient resources to implement department-wide privacy program governance. In partnership with the SO and divisions, coordination and staff resources are allocated as needed. The resources dedicated to DCF's privacy program plan are described below.

Privacy Program Plan Support

In addition to the SAOP, general job duties of other privacy staff who support the plan are provided below.

Program Area SMEs

- Reviews and aligns program privacy policies, procedures, and contract management with the DCF Privacy Program Plan.
- Ensures the implementation of privacy policies and procedures within their respective program areas and coordinates monitoring.
- Provides guidance and escalates program privacy policies and procedures to SAOPs.

Data Stewards and Data and Analytics Managers

- Staff within each division is responsible for overseeing the sharing of their division's administrative data with external parties.
- Follow the policy and process for sharing non-identifiable, aggregate data, identifiable data, data sharing that is statutorily required or federally mandated and data sharing that is part of a contract.
- Ensures that data assets are used appropriately and to their fullest capacity.

Data Governance Coordinator

- Chairs the Data Governance Workgroup.
- Maintains DCF policies related to performance management.
- Maintains the Data Sharing Manual.
- Maintains the Data Sharing Agreement Template.
- Answers questions relating to the data sharing process.
- Serves on the External Data Review Committee.

Data Governance Administrative Assistant

- Manages the procedural aspects of the data sharing program.
- Receives and directs data, and information requests to appropriate divisions.
- Documents the process of data sharing and finalizes and routes data sharing agreements.
- Serves on the Data Governance Workgroup.

Agency Communications Office

- Reviews and approves certain public records requests.
- Responsible for internal and external communication.
- Develops public information pieces including press releases, webpages, informational documents, infographics, etc.
- Reviews annual and quarterly reports required by state and federal governments.
- Maintains a central resource webpage on the DCF public website that serves as a central source of information about the DCF Privacy Program Plan.
- Serves on the Data Governance Workgroup.
- Serves on the External Data Review Committee.

Office of Legal Counsel

- Provides legal advice to DMS on existing and proposed department policies, procedures, rules, state and federal laws, contracts, and other legal matters affecting the administration of the DCF Privacy Program Plan.
- Manages and responds to DCF public records requests.
- Advises data stewards throughout the data sharing process.
- Reviews documentation related to data request denials to determine if the request should be granted according to the Wisconsin Open Records law.
- Serves on the Data Governance Workgroup.

Office of the Inspector General

- Conducts independent internal reviews and evaluations of a wide variety of DCF programs.
- Directs an annual operational risk assessment process across the organization to identify emerging risks to mission achievement through the identification of topic areas that would benefit from further independent and objective review.
- Determines, through various means, whether DCF's network of risk management, internal controls and governance processes as designed and represented by management, are adequate and functioning as intended and resources are being used efficiently.
- Provides recommendations to division or agency management related to operational improvements, lessons learned, highlights successes, and best practices.

Chief Information Security Officer

- Ensures compliance with state and DCF Cybersecurity policies and standards.
- Ensures the protection of sensitive information.
- Develops and administers the IT Security Program.
- Formulates any DCF-specific IT security standards.
- Provides guidance to management in interpreting federal, state, and local information security laws and requirements.
- Serves on the Data Governance Workgroup.

PROGRAM MANAGEMENT AND COMMON CONTROLS

The following section provides statements based on DCF policies that help to ensure compliance with privacy regulations and requirements across the organization.

Organizational Enterprise Structure

- The department continuously updates its technical and business procedures in order to further the DCF mission. All privacy system requirements are considered in the evaluation and approval process.
- Applications and an end user computing environment fulfilling agency program needs are provided.
- Activities pertaining to security and privacy that impact systems require planning, coordination with authorized agency staff, and approval by the designating official and/or authorized representative prior to plan implementation.
- At DCF, information is secured in accordance with NIST special publication 800-53r5 – Minimum Security Controls (Moderate-Impact Baseline).
- Access is granted based on principles of least privilege and is granted only upon approvals of supervisor and in some case data owner approval. Requirements for usernames, passwords, and passwords used to grant authorized users access to DCF's network are defined.

Constituent System Components

- Authorized personnel review requests for access to data. Authorized personnel will approve and assign the access, deny the access request, or send the request back for additional information. These requests must contain at least:
    - Identification of the data to which access is needed, the level of access required, and the reason why access is required.
    - Manager's approval.
- Privacy requirements are included in the DCF enterprise architecture.
    - Fundamental system components include, but are not limited to:
        - Network
        - Routers
        - Switches
        - Firewalls
        - Servers
        - Desktops
        - Mobile devices
        - Phones
        - Smart video/chat

Information Types Processed, Stored or Transmitted

- Information types processed, stored, and transmitted by the system (public, sensitive or confidential information, Federal Tax Information, etc.) are identified.

- Confidential data is encrypted with minimum 128-bit cryptography while in transit and at rest. This includes data stored on DCF systems. No confidential data is stored on mobile computing devices, or any personal devices used to access DCF systems.
    - No confidential data is stored on systems outside of DCF control (e.g., cloud storage) without signed Data Sharing Agreements, Memorandums of Understanding, Service Agreements, and/or any other required documentation.
- DCF will not disclose Personal Identifiable Information (PII) or Federal Tax Information (FTI) of individuals except as required for DCF business operations and allowed by DCF policies and as allowed or required by applicable law.

Security and Privacy System Overview

- Specialized system security and privacy measures include system access forms, lock screens, encryption and multi-factor authentication (MFA).
- DCF's privacy efforts protect individuals from unauthorized access to, alteration, disclosure or destruction of information that DCF holds. As part of DCF's privacy efforts, many of the services are protected by:
    - Encrypting information.
    - Using multifactor authentication to access DCF systems.
    - Reviewing information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems or data.
    - DCF personnel and agents are subject to strict contractual and other confidentiality requirements. DCF personnel and agents have access to PII only for DCF business purposes.
    - All system access requests include a confidentiality component. Staff must sign a form acknowledging the confidentiality component.

Specific Threats of Concern to the Organization

- Specific threats to the system that may be of concern to the organization (i.e., phishing, ransomware attacks, malware, user error, insider threats) are monitored and assessed.
- Breach procedures in various scenarios are periodically tested (i.e., phishing simulations and/or assessments).
- The United States Computer Emergency Readiness Team security alerts and advisories are monitored for alerts that may lead to the potential compromise of applicable systems (i.e., phishing attacks or messages that contain harmful software/applications).

Privacy Risk Assessment for Systems Processing FTI

- At least once every three (3) years or whenever there are significant changes to the information system or environment, a thorough examination is conducted of applications, servers, and networks to assemble a record. The record will be used to analyze risk and measure the current state to ensure electronic data and information systems are sustainable and compared against industry standards established by the National Institute of Standards and Technology (NIST).

    - Each applicable item is checked for risk vulnerability to ensure any such identified risks are proactively resolved. Once the critical set of risks are thoroughly analyzed, the evaluator is better able to determine the best course of action to mitigate those risks by considering what options are available and the associated costs, benefits, tradeoffs, and impacts of each option.

- In addition, ad-hoc risk assessments for any system processing FTI can be conducted at any time by request from DCF divisions/programs.
- DCF personnel must safeguard protected or confidential data such as FTI or PII. Such data shall not be emailed or stored in an inbox or on a mobile device, unless encrypted or protected in some other legally acceptable manner.

Risk Determinations for Security and Privacy Architecture

- Results of assessments conducted are recorded in a Risk Assessment Report which identifies gaps compared to the industry standards; impacts; likelihood of risk; and mitigation strategies to reduce the impact of any such risk.
- Risk vulnerability scanning which incorporates best practices and regulatory requirements for safeguarding data integrity is conducted.
    - Risk scanning also offers vulnerability guidelines to guarantee that data and IT resources are protected from loss and unauthorized access. As part of DCF's regular business of providing client service, the department safeguards assets, and maintains daily operations.
    - The level of vulnerability criticality is established by the United States Computer Emergency Readiness Team (US-CERT). The vulnerability assessment is completed in a non-invasive or low impact manner to the DCF network.
- Risk plans are documented considering the unique attributes of each system (application, server, etc.)
    - As an example, larger projects or those with high levels of uncertainty will benefit from detailed and formal risk management plans that record all aspects of risk identification: assessment; analysis; planning; allocation; as well as information systems, documentation, and reports.

Dependencies on Other Systems

- DCF creates policies and standards deemed necessary to meet security and compliance requirements and adopts the policy and standard language as documented in the Department of Administration, Division of Enterprise Technology's (DOA-DET) security policies and standards wherever DCF does not have corresponding policies and standards. DCF policies and standards will take precedence in situations of overlap.

Security and Privacy Controls

- If applicable, requirements for accessing FTI from a remote worksite align with requirements imposed by IRS publication 1075 for any DCF employee (permanent, project, and limited term) with access to FTI at a remote worksite.
- Controls are in place for meeting security and privacy requirements including virtual desktop infrastructure (VDI), authorized applications, principle of least privilege, data life cycle policies, and activity logging and monitoring.

- Prohibited activities, such as peer-to-peer file sharing when not directly related to official state business or without signed Data Sharing Agreements, Memorandums of Understanding, Service Agreements and/or any other required documentation are defined.

➢ Individual standards, procedures, and responsibilities for the proper use, security, and protection of DCF computers and information assets when using mobile storage devices and/or removable flash media are defined.

- The DCF Privacy Statement must be included on all external forms. The DCF Social Security Disclosure Statement must be included on all forms collecting an individual's social security number.

Media Sanitization and Disposition

- DCF data, including sensitive or confidential data, is properly disposed. Media or devices containing DCF data and information are wiped and/or destroyed before disposal. Sensitive printed materials (including documentation, backup media, or old storage devices) are shredded. This includes any data and information at telework locations. Any documents containing FTI must be disposed of by burning or shredding.
- Staff should only use authorized sources of images. Staff taking photos or videos as part of official duties must obtain a release in order for the photo to be used. Photos of children in out-of-home care cannot be used, with the exception of public events.

Privacy and Policy Compliance

Privacy Program Plan Management and Communication

- Policies and procedures related to privacy and security and included in this plan are reviewed every three years.
    - The designated SAOPs will review the plan annually and assess for changes to the system, environment of operations, problems found during the plan implementation, changes to federal privacy laws or organizational changes impacting the privacy program plan.
- Updated plans will be posted on the external website and changes will be shared in a department-wide communication.
- DCF will share its privacy program plan on the external website for public viewing. The plan will be posted as a PDF or other format which allows authorized individuals to lock the document preventing changes by unauthorized individuals.
- The privacy program plan metric will be the percent of DCF staff and contractors who complete the privacy training each calendar year. This metric will be used to track compliance.

Privacy Training Activities

- The Department of Administration (DOA) determines the appropriate content of security and privacy awareness training. DCF works with DOA to ensure the training fulfills the specific requirements of DCF and the information systems to which DCF personnel have authorized access. The organization's security awareness program is consistent with industry best practices.

- Trainings are regularly updated a minimum of once/year to reflect new or updated policies and/or other requirements relating to privacy.
- Trainings may be delivered through webinars, seminars, vendor presentations and/or independent study.
- Training needs are evaluated as part of continuous improvement efforts and/or as emerging risks related to privacy and/or security are identified.
- Records of completed training for information system security activities, including those for basic security awareness (including privacy) and specific information system security will be maintained and available for review.

- All DCF personnel are required to complete security and privacy awareness training within 60 days of hire, annually thereafter, and complete additional trainings for security and privacy awareness as determined necessary.
- Any significant changes to the privacy plan will be reflected in and training materials will be updated as necessary. The changes may include script, graphics or process descriptions, and plan statements.