cfpb Consumer Financial Protection Bureau

Number	Date	Organization
CFPB-T&I-POLICY NUMBER TBC	07/22/2014	OFFICE OF TECHNOLOGY & INNOVATION

Policy on Information Governance at the CFPB

I. Overview & Scope

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the Act), Public Law No. 111-203, Title X, which created the Consumer Financial Protection Bureau (CFPB or Bureau), establishes that the Bureau "shall seek to implement and, where applicable, enforce Federal consumer financial law consistently for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that [such] markets ... are fair, transparent, and competitive."[1]

In the normal course of carrying out its statutory mandates, the Bureau collects information from consumers who seek the Bureau's help through the consumer response function and from the institutions involved in the complaints; from covered persons who are the subject of supervisory examinations or enforcement activity, as well as from whistleblowers and third parties who may have information relevant to an enforcement action; from individuals or third parties in the performance of market monitoring or research activities; and for other purposes authorized by law.

The policy contained in this document will set in place rigorous guidelines and processes, as well as recognize and account for existing procedures, which:

- Inform what information the Bureau can and should intake, and how that information intake shall occur in order to ensure compliance with applicable laws, contractual obligations, and Bureau policy requirements.
- Facilitate the assignment of a sensitivity level that may afford additional guidelines and policies on its access, use, and overall management.
- Ensure information is adequately secured and responsibly used in accordance with applicable laws, contractual obligations, and Bureau policy requirements.
- Inform what information can and should be disclosed by the Bureau and its program offices, subject matter experts, and data owners, either to the general public or to other government entities.
- Describe the rules, roles, and responsibilities related to the retention, archiving, and destruction of electronic and physical information and related assets.

A. Information Governance Documentation

Information-related activities at the CFPB are governed by a hierarchical collection of documents that provides increasingly specific requirements, guidelines, and rules for information-related behaviors within the Bureau.

[1] 12 U.S.C. § 5511, Pub. L. 111-203, Title X, § 1021 (July 21, 2010).

Policies

Policies describe the Bureau's broad rules and guidelines for particular stages in the information lifecycle (Intake, Management, Disclosure, and Disposition), and define the high-level boundaries of acceptable information-related behaviors. The Chief Information Officer (CIO) is responsible for developing Bureau-wide information governance policies for executive review and Director sign-off.

Standards

Standards provide specific guidance around components of the information lifecycle and are supported by specific procedures. The CIO is responsible for reviewing and approving information governance standards.

Procedures

Procedures describe the specific activities that the Bureau employs to execute information-related policies and standards, make decisions, and communicate with stakeholders. They also define the technical steps for executing components of information management. Procedures are developed by the operational bodies responsible for implementation.

B. Scope

All information received, created, stored, or disclosed by the Bureau or by a third party on behalf of the Bureau, regardless of format, is subject to this policy unless otherwise noted below. Information may be qualitative or quantitative. Information formats include but are not limited to structured databases, unstructured files, text / narratives, physical documents / media, and audio or video media. Subsets, extracts, aggregations, or other transformations of information that is subject to this policy are themselves subject to the policy.

Out of Scope

Bureau employees' electronic communications such as emails, voicemail, text messages, etc. are considered information transmission mechanisms, not covered information, and are generally not subject to this policy. To the extent that any electronic communication contains information that is in scope for this policy (e.g., an Excel spreadsheet attached to an email, an embedded table with account numbers, a discussion of statistics in an email, etc.), the transmission of that information may be a treated as an activity implicating the information lifecycle under this policy.

Any classified information received by the Bureau is not governed by this policy and will be handled in accordance with governing law.

Financial information related to Bureau operations is also considered outside the scope of this policy. This information is managed by the Office of the Chief Financial Officer.

The CIO will have final responsibility for determining what types and sources of information are subject to this policy, and may grant policy exceptions as deemed appropriate.

C. Bureau-wide, Office, or Division-Specific Policies

Existing Bureau-wide, office, or division-specific information governance policies that do not conflict with this policy will remain in effect, until and unless they are found to be in conflict with this policy, at which point they will be reviewed by the Data Governance Board ("DGB", defined below, or "Board") and CIO with input from the DGB.

To the extent that any Bureau-wide or office or division-specific policy is found by the CIO to be in conflict with this policy, this policy governs. The CIO, with advice from the DGB, will be responsible for reviewing, clarifying, and/or revising said policies to bring them into alignment.

D. Applicable Law Controls

To the extent that this policy conflicts with any applicable law, that law governs over the policy.

E. Data Governance Board

The DGB is a committee chaired by the CIO. This Board has responsibility for assessing the benefits and risks associated with managing the Bureau's information. The DGB will advise the CIO on decisions regarding intake, management, disclosure, and disposition of information in accordance with this policy.

Responsibilities of the DGB

The responsibilities of the DGB include, but are not limited to, advising the CIO in making the following decisions:

1. Determining whether given information should be brought into the Bureau
2. Categorizing information as Public, Low, Medium, or High sensitivity
3. Developing and enforcing standards for managing Public, Low, Medium, and High sensitivity information
4. Reviewing and approving information governance standards
5. Reviewing and approving decisions to delegate authority to individuals or committees
6. Reviewing decisions made by delegated authorities
7. Reviewing policy exceptions granted by the CIO

Ultimately, it is the responsibility of the CIO to make all decisions regarding information governance, or to delegate those decisions to another authority.

F. Delegation of Responsibilities

The CIO may for operational purposes, and at his/her discretion, delegate any information governance oversight responsibilities to any Associate, Deputy Associate or Assistant Director in the various CFPB offices, the DGB, and/or operational committee established by the DGB.[2] The CIO (with the assistance of the DGB) will be required to specify criteria under which certain delegated information activities must be reviewed by the DGB or approved directly by the CIO.

[2] Unless specified otherwise, the CIO also retains the delegated authorities.

In cases where this responsibility is delegated, the responsible Associate, Deputy Associate or Assistant Director, DGB, or operational committee will be required to provide the CIO with a regular, detailed report on information-related activities.

All major decisions approved by a delegated authority (whether an individual or an operational committee) will be reviewed by the CIO and the DGB no less than once per year.

G. Definitions

Please refer to the *Information Governance Definitions* document for relevant definitions.

II. Information Intake

This section of the policy provides the principles that guide Bureau decision-making regarding information intake, describes the responsibility and authority of the CIO to oversee and approve information intake, and establishes the role of the Data Governance Board in assisting the CIO with these responsibilities.

A. Information Intake Guiding Principles

The ability to intake and analyze information is fundamental to the Bureau's mission. Analysis informs Enforcement and Supervisory decisions, guides policy development and rule-making, provides critical information about the condition of consumer financial markets, and supports decision-making about Bureau's internal policies and operations. In order to ensure that the Bureau is careful, consistent, and responsible in its intake of these critical information assets, the decision to intake information must be governed by several guiding principles:

1) Ensure Proper Authority – any information received by the Bureau must be acquired under authorities established in the Dodd-Frank Act and/or other applicable law.

2) Adhere to Applicable Law – the Bureau must at all times comply with existing law governing the intake and use of information.

3) Demonstrate Due Diligence – the Bureau should assess the reliability of a source before requesting or receiving information from it.

4) Avoid Undue Burden – the Bureau should seek to ensure that it does not place unnecessary burdens (technical, financial, etc.) on external parties in the course of requesting or receiving information.

5) Validate Reasonableness – the Bureau should request or receive only information that is likely to be reasonably necessary to fulfill the Bureau's responsibilities, and that has value in light of any risks of that collection to the consumers or entities to whom the information relates. Care should be taken to ensure that the volume and specific data elements requested are reasonable in light of the purposes that will be served.

6) Avoid Redundancy – the Bureau should, wherever reasonably possible, avoid requesting or receiving information (either through the same source or from different sources) that is duplicative.

7) Align With Bureau Goals & Objectives – any decision to receive information should align with the Bureau's purpose, objectives, and functions; its strategic goals; its responsibility to protect the privacy or confidentiality of consumers' and financial institutions' proprietary, personal, or confidential information; and its responsibility to maintain the public trust.

8) Standardization – whenever reasonably possible, information should be brought on board with formats, field names, and definitions consistent with pre-existing usage and standards that have been set across the Bureau.

B. Responsibility for Information Intake Decisions

All decisions to intake information must be approved by the Bureau's CIO (or by parties to whom the CIO has delegated responsibility for intake activities in accordance with Section 1.F) in accordance with the guiding principles listed above.

C. Responsibility for Information Intake Standards and Procedures

The Bureau's CIO (or by parties to whom the CIO has delegated responsibility for intake activities in accordance with Section I.F) shall, at a minimum, determine the following at the time of intake of information:

1) The sensitivity level for that information (See *Information Sensitivity Leveling Standard*)
2) The owner of the information asset, for High Sensitivity information
3) Any restrictions on use or disclosure for that information as defined by applicable law and/or contractual obligations

III. Information Management

This section of the policy, concerning information management, is comprised of three primary subsections:

- Information Storage: Establishes guidelines regarding the storage of information (Public, Low, Medium, or High sensitivity) within the CFPB data environment; and

- Intra-Bureau Information Sharing & Information Access: Establishes guidelines regarding access to information by CFPB employees and contractors; and

- Information Use: Establishes guidelines regarding acceptable use of CFPB information.

A. Information Storage

1. Centralized Storage

Regardless of the sensitivity of any information or the authority under which it was received, all Bureau information shall be properly secured, tracked for performance and usage, updated, and stored consistently.

Care will be taken to design a storage system where records subject to federal laws such as the Privacy Act of 1974, 5 U.S.C. § 552a, or other relevant laws, are identified and managed in accordance with those laws.

Medium and High Sensitivity information should not be stored locally on user laptops or desktop computers, or other non-centralized physical media (such as CD/DVDs, external hard drives, or non-CFPB-issued thumb drives), and CFPB information (regardless of sensitivity) shall *never* be stored on non-CFPB computers or computers that have not been approved by the CFPB for this purpose.

When Medium or High Sensitivity information is received on non-encrypted physical media, it shall be moved to a secure, centralized location (or to a CFPB-approved, encrypted device if this is not possible). Once copied over, the original physical media shall be properly sanitized, returned to the originator, or securely stored per Bureau records retention rules. In the event that a computer or storage device containing information is lost or stolen (or there is suspicion of a potential loss or theft), the CFPB Service Desk must be notified immediately (see *Information Security Program Policy* and *Privacy Incident Response Procedures* for additional detail on information leaks and breaches).

2. Local Storage Exceptions for High Sensitivity Information

When local storage of high sensitivity information is unavoidable (e.g., when performing an on-site examination where access to the Bureau's central information storage locations is unavailable), exception approval must be granted by the CIO and relevant Associate Director (AD) in writing. While exceptions may be granted for certain categories of information, these exceptions must be reviewed and approved by the CIO and relevant AD at least annually.

In the event that a local storage exception has been granted, information will be moved to an approved storage location and removed from the non-secure media/location as soon as practicable.

3. Information Protection/Encryption

Information stored in centralized, secure, access-restricted locations will not be required to be encrypted. All medium or high sensitivity information held (even temporarily) in non-secure locations must be password-protected and/or encrypted when not in use. This must be accomplished by using CFPB-approved devices such as CFPB-issued laptops and CFPB-issued thumb drives. All medium or high sensitivity physical information (including paper files) shall be stored in an access-restricted location.

4. Source Masking

In the course of its supervisory, enforcement and other activities, the Bureau receives certain information the existence of which is confidential and may not be disclosed either to the general public or to other individuals within the Bureau. In order to ensure this confidentiality, this information may be 'masked' (e.g., by using numeric identifiers to name folders instead of institution names, etc.) when it is received by the Bureau, or as soon as practicable after such receipt. The CIO, with the advice of the DGB, shall be responsible for reviewing and approving standards and procedures for properly masking data.

5. Information Restrictions

In the event that the Bureau receives information that contains data elements (e.g., social security numbers), the internal access to which is restricted by applicable law, including but not limited to Section 1022(c)(4)(C) of the Dodd-Frank Act; by contractual agreement; or by Bureau policy; the information shall be treated in accordance with such restrictions.

6. 3rd-party Information Storage

Information held by 3rd parties on behalf of the CFPB is generally subject to all of the same rules and restrictions as information held directly by the CFPB. When a 3rd party is a government contractor, the contract should include the requirements regarding information storage and related topics. Because authority to issue and make changes to the contract lies with the Contracting Officer, the CIO will coordinate with the Contracting Officer on any concerns or issues that arise. With respect to other types of 3rd party agreement, the CIO may, as authorized by law, approve exceptions to specific information management provisions as appropriate.

B. Intra-Bureau Information Sharing & Information Access

Access to information will be consistent with the sensitivity level of the information (see *CFPB Information Sensitivity Leveling Standard*), the authority under which the information was received, the Bureau's ininformation sharing standards, and applicable law or contractual obligations. This policy will be documented by information access standards and procedures that will clearly define which Offices/Divisions may access information based on the above factors.

1. Intra-Bureau Information Sharing

Sharing of information across business areas within the Bureau is governed by specific rules based on the sensitivity level of the information and the authority under which the information was received.

In the event that neither office or division-specific policies nor the established Bureau information sharing standards cover an instance of desired information sharing, the issue will be referred to the DGB which will be responsible for both resolving the immediate instance and amending, as necessary, the standards to cover the situation in the future.

2. Information Access Permissions Rules

a. Public and low sensitivity information may be shared internally without restriction or acquired through request without additional approval(s).

b. Medium sensitivity information access will be granted to users with certain roles.

c. Access to high sensitivity information will require demonstrated business need.

The CIO, with the advice of the DGB, shall have the responsibility for reviewing and approving standards and procedures that provide detailed information access rules, requirements and processes.

Note that in the event that a user is acting as a service provider for another office or division, that user will be deemed to be a member of the group they are supporting for purposes of access permissions.

3. Access Permissions Request Escalation

In the event that the permissibility of access for an individual is unclear or contested, the request will be referred to the CIO with advice from the DGB for review and clarification.

4. Information Read/Write Privileges

The CIO and any delegated authorities will calibrate the level of read/write/modify privileges it grants to individuals requesting information based upon the nature and extent of the need that the requesting individual demonstrates in his or her request, as well as the user's role. In general, the CFPB will provide the minimal level of privilege necessary to perform assigned duties.

5. Revocation of Information Access Rights

Information access rights shall be reviewed, suspended and/or revoked in a number of cases, including:

- When the business or role-based need that justified access to the medium or high sensitivity information no longer exists
- When an employee/contractor leaves the CFPB
- When there is a real or suspected risk of breach, or the need for fuller investigation of information activities
- In response to certain disciplinary actions
- In response to certain ethics opinions

6. Information Access Audit

Periodic audits of access rights related to High Sensitivity information will be performed in order to ensure that appropriate access has been granted, and that information access rights have been revoked timely and appropriately. These audits will include review with information owners.

C. Information Use

The CIO and delegated authorities will determine permissible use of information primarily by taking into account the sensitivity level of the information, the authority under which the information was received,

applicable laws, contractual obligations, and the applicable information sharing standards. Permissible use of information may also be informed by other factors, such as the input of information owners.

Note that in the event that a user is acting as a service provider for another office or division, that user will be deemed to be a member of the group they are supporting for purposes of identifying permissible uses.

This policy will be documented by a *Permissible Information Use Matrix* that will clearly define how information may be used based on the above factors.

1. **Identifying Permissible Uses**
Identifying the permissible use(s) for information occurs at the time of intake and is the responsibility of the CIO with advice from the DGB, operational bodies charged by the CIO and/or DGB with information intake oversight, and/or divisional or office representatives to whom the CIO has delegated authority. Additional acceptable uses may be evaluated after intake, but must comply with this policy and may require review and/or approval from the CIO.

2. **Desired Use Escalation**
In the event that the permissibility of the desired use of given information is unclear or contested, the request will be referred to the CIO who will, with advice from the DGB, review and clarify. The outcome of this review should be used to amend the *Permissible Information Use Matrix* in order to inform similar requests going forward.

3. **User Acknowledgement**
Users may be required to provide affirmative acknowledgement of information usage restrictions. In these cases, the need for affirmative acknowledgement will also be determined at the time of information intake by the person or governance body with applicable oversight responsibilities.

4. **Use of Transformed Information**
In certain cases information that is, in its raw form, restricted from particular uses may be appropriate for those uses when transformed. This transformation may be achieved through a number of methods, including aggregation, sampling, removal of certain data elements, etc. Transformed information should be evaluated against all information use criteria (e.g., the implied sensitivity level of the resulting transformed information, the authority under which the information was received, applicable laws, contractual obligations, and the applicable information sharing standards) to determine if additional uses are permissible. In cases where permissible uses of the transformed information are unclear, users should consult with the CIO or the appropriate delegated authority for review and approval.

IV. Information Disclosure

This section describes the responsibility and authority of the CIO to oversee and approve disclosures[3] within the scope of the CIO's authority, and establishes the role of the Data Governance Board in assisting the CIO with these responsibilities. It provides the principles that guide the CIO decision-making regarding discretionary disclosures of information to the public or other external entities.[4]

A. Disclosure Guiding Principles

The ability to disclose information, whether in its raw form, in aggregation, or as part of reports, studies, or other analytical outputs, is fundamental to the CFPB's mission. In order to ensure that the Bureau is careful, consistent, and responsible in its disclosure of information, the decision to disclose must be governed by several guiding principles:

1) Ensure Proper Authority – any information disclosed by the CFPB must be disclosed under or for the purpose of exercising authorities established in the Dodd-Frank Act and/or other applicable law.

2) Adhere to Applicable Law – the Bureau must at all times comply with existing law governing the disclosure of information.

3) Comply with Contractual Restrictions – the CFPB shall comply with all restrictions on disclosure specified in any contract, agreement, MOU, or other legally-binding document that governed the receipt of the information.

4) Risk-Benefit Analysis – when deciding whether to disclose information, the CFPB should weigh the benefits of disclosure against any potential risks to consumers or to other entities.

5) Align With Bureau Goals & Objectives – any decision to disclose information should align with the Bureau's purpose, objectives, and functions; its strategic goals; its responsibility to protect the privacy of consumers' and financial institutions' proprietary, personal, or confidential information; and its responsibility to maintain the public trust.

B. Public, Inter-governmental, and other 3rd-Party Disclosures

Special considerations may exist depending on whether an anticipated disclosure is to the general public, to other governmental entities, or to other non-governmental 3rd parties.

Public Disclosures

When disclosing information to the general public, the CFPB shall evaluate the risk that individual consumers or their financial information may be identified by the disclosure of information. This risk

[3] Disclosure is defined as transmission of information outside the Bureau. Transmission of information from one Bureau office or division to another is considered information sharing, not disclosure.

[4] Nothing in this policy shall be construed to modify the delegations of authority made in 12 C.F.R. Part 1070 that pertain to decision-making related to the disclosure of information.

evaluation must take into account not only the specific information being disclosed by the Bureau, but any existing publicly available information that, when combined with the disclosed data, could result in increased consumer identification risk.

In addition to individuals' privacy interests, any decision to disclose information should protect institutions' commercially sensitive or proprietary information, and the identities of persons to whom "confidential information" pertains (e.g., the identities of supervised institutions when the information is received under supervisory authority).

Inter-Governmental Disclosures

Any disclosures of Medium or High Sensitivity information between the CFPB and another governmental entity shall be governed by appropriate legal sharing documentation (e.g., Memorandum of Understanding, Access Request, etc.) that defines who may have access to the information, how the information may be used, and any restrictions on further disclosure by the receiving entity.

In addition, any agreement to disclose information to another entity must include assurances that the receiving entity will treat the information as described in the governing legal documentation.

Other 3rd Parties

Any agreement between the CFPB and other non-governmental 3rd parties under which the CFPB discloses information shall be governed by appropriate legal sharing documentation (e.g., contracts, etc.) that defines who may have access to the information, how the information may be used, and any restrictions on further disclosure by the receiving entity. Agreements that are Federal Government Contracts may be subject to additional requirements and should be evaluated in consultation with the Procurement Office and/or assigned Contracting Officer.

In addition, any agreement to disclose information to another entity must include assurances that the receiving entity has information governance policies and procedures as described in the governing legal documentation.

C. Disclosure of Transformed Information

In certain cases information that is restricted from disclosure in its raw form may be disclosed when transformed. This transformation may be achieved through a number of methods, including aggregation, sampling, removal of certain data elements, etc. In all cases, however, the disclosure of transformed information must adhere to the rules laid out in section D below.

D. Responsibility for Disclosure Decisions

All decisions to disclose information within the CIO's scope of authority must be approved by the Bureau's CIO (or by parties to whom the CIO has delegated responsibility for Disclosure activities in accordance with Section I.F) in accordance with the guiding principles and rules listed above.

Bureau Clearance

Nothing in this policy shall be construed to modify or ameliorate the requirement that work product that discloses information adhere to the clearance procedures in effect at the Bureau.

V. Information Disposition

This section of the policy, concerning information disposition, provides the principles that guide Bureau decision-making regarding the retention, archiving, and destruction of information; describes the responsibility and authority of the CIO related to information disposition; and establishes the role of the Data Governance Board in assisting the CIO with these responsibilities.

This information disposition policy considers the important distinction between official Bureau 'records', and non-record information. While many of the requirements and restrictions defined for records and non-records may be similar or identical, the legal impetus, underlying policy goals, and detailed operational processes may differ in significant ways.

A. Responsibility for Information Disposition Decisions

The CFPB Records Management Office has primary responsibility for decisions related to disposition of information, as directed by applicable laws. The CIO will have the responsibility to support, and where applicable, enforce these decisions, and will be assisted in these responsibilities by the Data Governance Board.

B. Bureau Records vs. Non-Records

In accordance with the Federal Records Act of 1950, Federal Records are,

"...all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them." (44 U.S.C. § 3301, Definition of Records).

All other information received, created, stored, or disclosed by the Bureau or by a third party on behalf of the Bureau is considered non-record information and is subject to corresponding disposition policy requirements.

Employees and 3rd parties (other than Federal Government contractors) should consult with the CFPB Records Management Office to determine the appropriate classification of information. For Federal Government contractors, the status of the records will be determined by the terms of the contract, applicable provisions of the Federal Acquisition Regulation, and the Federal Records Act if applicable.

C. Bureau Record and Non-Record Disposition

The rules around identification, classification and scheduling of official records are defined and enforced by the CFPB Records Management Office. These rules are set forth in the Bureau's *Agency File Code Policy*, and are consistent with Federal law and National Archives and Records Administration (NARA) directives.

When possible, retention (archival and disposal) requirements for records and non-records should be identified at the time of information intake or creation, and should be maintained as part of related information metadata.

Additional details concerning the retention, archiving and/or destruction of non-record information may be found in the Bureau's *Agency File Code Policy*.

D. 3rd-Party Record and Non-Record Retention

All legal agreements with 3rd parties should provide disposition requirements where applicable. The Bureau shall document any contractual disposition requirements and adhere to those requirements wherever practicable. For Federal Government contractors, disposition of records will be addressed by the contract, applicable guidance specified in the Federal Acquisition Regulation, and the Federal Records Act if applicable.

E. Disposition of Physical Information Assets

Physical information assets (whether paper or electronic assets such as external hard drives or thumb drives) are subject to the same policy considerations as their electronic counterparts. In the event that information held on a physical electronic device is to be destroyed, the device shall be completely erased to ensure that information cannot be reconstructed at a later date. In the event that medium or high sensitivity information contained on paper is to be destroyed, the paper shall be placed in a secure shred bin for proper disposal.

VI. Revision History

Action	Date	Approval Authority
Initial version	June 10, 2014	Richard Cordray, Director, CFPB
Technical corrections	July 22, 2014	Richard Cordray, Director, CFPB

VII. EFFECTIVE AND EXPIRATION DATES

This Policy will become effective on September 30, 2014.

VIII. DIRECTOR SIGNATURE & DATE

Richard Cordray
Director

July 31, 2014
Date