U.S. Department of Housing and Urban Development

Web Applications Policy

March 2023

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
Original	March 30, 2022	All	Final Draft policy prepared for clearance. Updated to include Program Office points of contact feedback. Initial Draft Version 1.0
Original	November 1, 2022	All	Incorporating OCIO clearance feedback.
Final ver. 1.0	March 28, 2023	Various	Incorporated and revised information to address Departmental clearance comments.

Table of Contents

1. Introduction

In computing, a native web application (or web app) is a client–server computer program that the client (including the user interface and client-side logic) runs in a web browser. Common web applications include webmail, online retail sales, online banking, and online auctions.

Within HUD, Web Applications fall into the following categories and are included under this policy:

- **A native web application** or **web app** is a client-server computer program that the client (including the user interface and client-side logic) runs in a web browser. Common web applications include webmail, online retail sales, online banking, and online auctions.
- **SharePoint web application** consists of a set of access mappings or URLs defined in the SharePoint central management console, which are replicated by SharePoint across every IIS instance (e.g. Web Application Servers) configured in the farm.
- **A mobile application** (also called a mobile app) is a type of application designed to run on a mobile device, which can be a smartphone or tablet computer.
- **Microservices** is an architectural style that structures an application as a collection of services that are highly maintainable and testable, loosely coupled, independently deployable, and organized around business capabilities.
- **Cloud Application** is an internet-based program where some, or all, of the processing logic and data storage, is processed in the cloud. The user interacts with the application via a web browser or a mobile application, and the data processing is managed by a combination of the local device and a cloud computing solution.
- **Software-as-a-Service (SaaS)** is a capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Microsoft SharePoint is provided as both a cloud-based service and as an on-premise server that is used to create web applications that store, organize, share, and access information from any device using a web browser**.** Further, web services are any software or application that provide web protocols to communicate and exchange data through the internet between users and web servers[1].

The U.S. Department of Housing and Urban Development (HUD) acknowledges the need to manage its web applications and associated information technology (IT) web-based assets throughout the five lifecycle stages (Initiation, Planning, Execution and Control, Operations and

[1] NIST SP 800-95, Guide to Secure Web Services further defines web services as a software component or system designed to support interoperable machine- or application-oriented interaction over a network. A Web service has an interface described in a machine processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

Maintenance, and Decommissioning). The web applications will be managed within a centralized IT asset repository that accounts for the assessment, security, and management of purchases of all related hardware and software.

2. Purpose

The Department's public web applications are important online information resources that are relied upon to deliver programmatic information or services to the public and our partners. These web applications reside across a variety of delivery platforms and devices and support the proper performance of HUD's mission. All HUD organizations planning, implementing, and using web applications to meet programmatic requirements will ensure compliance with the requirements of this policy.

This document establishes HUD's policy for identifying and managing HUD web applications, including:

- **Native web applications** or **web apps**
- **SharePoint web applications**
- **Mobile Applications** or **mobile apps**
- **Cloud Applications**
- **Microservices**
- **Software-as-a-Service (SaaS) applications**
- **Web Services:** A software component or system designed to support interoperable machine-oriented or application-oriented interactions over a network. A Web Service has an interface described in a machine-processable format.
- **Web Application Programming Interface** or **Web API:** A Web API is a set of software instructions and standards that allows machine-to-machine communication. Web APIs support sharing content and data between applications.

The scope of this policy encompasses the use and management of HUD's Web-based Applications (Web Apps), Cloud-based Applications, Web and Microservices, SaaS applications, Web APIs, and SharePoint application information and associated systems where the intent is to make information available to the public or a general audience within HUD ("hereinafter referred to as web applications").

3. Rescission

This policy does not rescind any other policy or document. This is HUD's Web Management Policy, version 1.0. This document will be reviewed annually, and rescission information will be updated as necessary.

4. Applicability

The Web Application Policy is applicable to all HUD organizations, HUD employees, IT contractors, and other stakeholders planning, developing, or implementing web applications to address business and operational requirements.

The Federal Government relies extensively on Web-based information technology applications and information, some of which are managed, hosted, provided and used by third parties to assist in Government operations. All web applications are at increased risk of unauthorized access due to unresolved security vulnerabilities and a lack of proper application implementation. Unauthorized access can lead to many problems for Federal agencies, such as a breach of sensitive data, the unavailability of the application for authorized use, and providing the basis for launching additional attacks. Therefore, the Web Application policy establishes the framework for ensuring that HUD's web applications comply with federal IT regulations and guidance.

5. Effective Implementation Date

This policy is effective immediately upon the date of approval.

6. Policy

This policy expands upon the following guidance:

- OMB M-15-13, A Policy to Require Secure Connections across Federal Websites and Web Services
- OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services
- OMB M-23-3, Fiscal Year 2-23 Guidance on Federal Information Security and Privacy Management Requirements
- EO 14028, 'Improving the Nation's Cybersecurity, May 2021
- NIST 800-44, Guidelines on Securing Public Web Servers
- NIST 800-95, Guide to Secure Web Services
- NIST 800-207, Zero Trust Architecture
- HUD Policy for IT Management Framework, HUD Handbook 3400.1
- HUD Policy for IT Project Planning and Management (PPM), HUD Handbook 3410.1

To ensure the confidentiality, integrity, and availability of HUD systems, all web applications must comply with the Web Application policy requirements. All web applications that were deployed prior to the effective date of this policy, must take steps to comply.

A. General

1. The Department shall have a single authority for the approval of minor web applications and associated assets throughout the five lifecycle stages (i.e. Initiation, Planning, Execution and Control, Operations and Maintenance, and Decommissioning).
2. The Department shall have a single web application inventory repository used to list and manage web applications and associated assets, sites, or pages.
3. All web applications must adhere to the following:
    a. All web applications and web services development projects shall adhere with the Project Planning and Management (PPM) policies and procedures for building secure information systems that includes undergoing threat modeling assessments, submitting to security testing processes and solutions to avoid exploitable vulnerabilities, and complying with security and privacy assessment policies and procedures prior to

deployment into enterprise environment;

b. Use HUD's product standards and solutions for building secure information systems;
c. Apply HUD's secure development life cycle (SDLC) requirements for building secure applications; and
d. Implement web applications using the DOTGOV (.gov) domain, administered by the Cybersecurity and Infrastructure Security Agency (CISA), to allow the public to quickly identify the web application as a trusted government source and increase security.[2]
    1) Multifactor authentication is enforced on all accounts in the .gov registrar.
    2) DOTGOV domains require browsers to use only a secure HTTPS connection.
    3) Allows adding a security contact for each requested DOTGOV domain, making it easier for the public to identify a potential security issue with the web application.

4. All web applications will prioritize alignment with zero trust (ZT) principles and HUD's associated policies and architecture framework.
5. No web page shall be used to gather information from the public or monitor public use of the HUD Internet without prior Paperwork Reduction Act (PRA) approval.
6. Prior to implementation:
    a. Major web applications shall receive an Authority to Operate (ATO) prior to implementation and this authority will be maintained per the security assessment and authorization process defined in the HUD IT Security Policy Handbook 2400.25 Rev 5 or as prescribed by the Chief Information Security Officer (CISO).
    b. All other Web applications shall undergo a security assessment based on inherited controls and capabilities and receive a Risk Based Determination.

B. Security/Terms of Use

1. The CISO establishes Information Technology Security policies and procedures (and its subsequent revisions) and is the authority on all Information Technology security requirements for web applications, information, and associated systems security. The CISO's authority includes Security Configuration Management (SecCM) and compliance with federal guidance.
2. A standard Security Statement (or banner) shall be applied HUD-wide and shall be readily accessible from all top-level, or entry point HUD web pages, or as deemed necessary by the CISO.
3. All web applications, web services, and web servers will comply with federal regulations, guidance, and best practices established by the National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), Department of Homeland Security (DHS), etc. for the implementation of zero trust strategies, HTTPS, HSTS, TLS, XML Encryption and Signature, web server hardening, and secure coding within the environment. As new regulations are released or updated, HUD will ensure thorough implementation strategies occur to maintain compliance.
4. Web applications are scanned for security vulnerabilities and configuration deficiencies in

[2] https://www.cisa.gov/sites/default/files/publications/DOTGOV_Domain_Fact-Sheet_508_0.pdf

adherence to the Vulnerability Management (VM) procedures[3].

5. All web applications must comply with HUD IT Security Policy, Handbook 2400.25, and Program Offices/System Owners are required to ensure that access controls are established for all web applications and access is reviewed as required. To review authorized users of web applications, a Help Desk ticket must be submitted by the application owner requesting a list of users with access to the application. The application owner must review the list and compare with internal application documentation. Any users found that should not have access to the web application will have their access revoked.

C. Privacy

1. The HUD Chief Privacy Officer (CPO) establishes policies and guidance that comply with the Privacy Act of 1974 and is the authority on privacy matters relating to web applications.
2. All web applications and associated information and data shall comply with the Privacy Act of 1974 and other applicable laws, regulations, and privacy policies.
3. A standard privacy statement shall be applied Departmentwide and shall be readily accessible from all top-level, or entry point HUD web pages.
4. Information gathered, used, or disseminated by a web application shall comply with HUD's stated Privacy Policy. The Chief Privacy Officer must approve exceptions based on the Privacy Act Exception Information Disclosure Guidance.
5. HUD personnel (employees, contractors, etc.) do not have a right, nor should they have an expectation, of privacy while using web applications when accessed via Government computers or networks. All such web activities are subject to monitoring at all times.

D. Operations and Maintenance

1. The OCIO Infrastructure and Operations Office (IOO) has authority over Operational Configuration Management, which includes application testing, release management, and infrastructure operational monitoring.
2. The IOO is responsible for compliance with the U.S. Department of Homeland Security (DHS) Continuous Diagnostic and Mitigation (CDM) Program and the operational scanning of all web applications.

E. Accessibility

1. The HUD Chief Information Officer (CIO) is the authority on accessibility matters relating to web applications.
2. All web applications and information shall comply with the information and communication technology (ICT) regulations covered by Section 508 of the Rehabilitation Act and Section 255 of the Communications Act, as well as all other applicable usability standards and guidance.
3. The policies and authorities prescribed in Section 508 of the Rehabilitation Act should be referenced when making accessibility determinations.

[3] The Vulnerability Management Procedures are located on the OCIO Operations and Security website at http://hudatwork.hud.gov/HUD/cio/po/i/it/opsec.

F. Configuration Management

1. Web applications will maintain baseline configuration documentation and undergo configuration assessments as a requirement of the configuration change control process.
2. System owners and web managers are required to adhere to this policy unless a waiver is submitted and approved. All web application changes must pass through the change control process for disposition prior to implementation.

G. Non-Compliance

1. Web applications that do not adhere to this policy may be taken offline until such time that a formal risk assessment and determination can be performed at the discretion of the CIO.
2. The CIO can recommend that the web application(s) remain offline until identified risks are successfully addressed.

7. Inventory

A. A web application inventory is established in the Web Application Inventory SharePoint site and will be used to manage, track, audit, and verify all web applications. The inventory shall contain, at a minimum, the following items:

1. Application Owner
2. Application Program Area
3. Application Program
4. Application Description
5. Public-facing[4] or Private (Internet, Intranet, or Extranet)
6. Major or Minor Application
7. Contains Personally Identifiable Information (PII) or Agency Sensitive Data
8. System Interfaces/Interconnections
9. Hostname (the name used to identify the component on a network)
10. System ID

B. Annual Inventory Validation

1. Web Managers are required to work with System Owners, Technical Points of Contact, and other appropriate staff to review and validate the web application inventory each Fiscal Year.
2. Web Managers ensure that any contractor system (i.e., hosted, operated, or maintained web applications on behalf of HUD, deployed within the HUD environment) has gone through the proper approval processes.
3. Formal, written certification is required to be submitted annually to the Configuration Control Management Board (CCMB) that the information contained in HUD's inventory is accurate and complete. Certification will be required within the first quarter of each Fiscal Year.

[4] Public-facing: Web content that is accessible by the public over an internet browser. No additional log-in or access is required.

8. Roles and Responsibilities

HUD web management is divided into three distinct disciplines:

- Management of web information,
- Management of associated systems, and
- Management of security.

Accordingly, the responsibilities and authorities for each discipline are assigned to an appropriate official. Within the discipline of information management, different officials and entities have disparate responsibilities.

A. The Chief Information Officer (CIO) shall:

1. Provide overall policy implementation and procedural guidance for the web applications and associated web-based systems.
2. Ensure adherence to policies, laws, regulations, and guidance including those regarding accessibility, privacy, and security.
3. Establish and enforce technical standards.
4. Enforce the authorization of all HUD websites and web applications.
5. Provide technical guidance for establishing and maintaining HUD Web Applications.

B. Chief Information Systems Security Officer (CISO) shall:

1. Provide governance and compliance of information system security requirements for Web Applications.
2. Ensure that HUD web information and associated systems adhere to laws, regulations, policies, and guidance regarding information system security.
3. Review and approve the System Security Plans (SSP) for Web-based Applications.
4. Conduct security assessments to support the determination of the authorization of all web applications. All web application authorizations will be documented and maintained in accordance with NIST SP 800-37 Rev 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy and HUD's security assessment and authorization (SS&A) process.

C. Chief Privacy Officer shall:

1. Assure that web services and service arrangements meet privacy policies regarding the protection, dissemination, and disclosure of information.
2. Review web application Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) and providing approval as appropriate.
3. Maintain HUD Privacy Policy and enforce its compliance.

D. Infrastructure and Operations Office (IOO) shall:

1. Establish and manage Operational Configuration Management, which includes application testing, release management, and infrastructure operational monitoring.
2. Manage and operate the CDM Program and conduct scanning of web applications.
3. Monitor all web applications to ensure they follow established operations and management procedures.
4. Initiate appropriate CCMB procedures to remove web applications and associated assets from the production environment.

E. Chief Technology Officer shall:

1. Appoint a Web Application Product Manager who is authorized to act as the IT Project Management (IT PM) for all Web applications.
2. Conduct an annual web application inventory verification and validation process.
3. Issue and maintain web application policies and procedures to meet federal IT regulations and guidance.

F. Configuration Control Management Board (CCMB) within the Chief of Technology Officer (CTO) shall:

1. Implement and exercise oversight of HUDs configuration management (CM) program.
2. Manage the change process for web applications.
3. Manage the exception, waiver request process for web applications.

G. Technical Review Subcommittee (TRC) within the CTO shall:

1. The TRC shall monitor web application projects and infrastructure services and provide analysis to the Chief Information Officer (CIO) and Customer Care Committee (CCC).
2. The TRC acts as a control gate in the Project Planning and Management (PPM) Life Cycle to ensure that necessary deliverables are produced and that all web applications comply with all technical standards and procedures.
3. Review technical risk associated with web application requests for exceptions and waivers.
4. Develop and manage the web application lifecycle.

H. Software License Manager (SLM) shall:

1. The Software License Manager shall have authority over software licensing related to web applications, which shall include commercial and commercial-off-the-shelf (COTS) software licenses (perpetual and term licenses) and maintenance (maintenance contracts, software assurance, upgrades, patches, and limited helpdesk support).
2. Implementing processes that ensure the web application processes and guidelines include alternative analyses in a technology-neutral manner that is merit-based and considers such factors as performance, the total cost of ownership, security, privacy, Section 508 compliance, interoperability, ability to share or re-use, and availability of quality support.

I. Office of Public Affairs (OPA) shall:

1. Ensure that the style, message, and content on the Internet conforms to the direction and vision set by the Secretary.
2. Provide and publish content describing HUD's mission, statutory authority, organizational structure, and Strategic Plan as required by the E-Government Act of 2002, as amended.

J. HUD Organization Heads shall:

1. Ensure that any initiative including web applications within their respective areas of responsibility adhere to policies, laws, regulations, and guidance including those regarding accessibility, privacy, and security.
2. Comply with established web application processes and procedures for publishing information to the web that accommodates the requirements of this policy and applicable authorities.
3. Develop and maintain content for the web applicable to their specific areas of responsibility, as they deem necessary.

4. Respond to certification and reporting requirements for their web information and associated systems.
5. Designate a Web Manager for their organization to participate on the Web-Based Application Working Group (WBAG). Such members will represent all agency components within the organization.

K. Web Managers shall:

1. Work with the WBAG Chairman and Web Application Product Manager to manage and monitor web applications and associated data and information within their area of responsibility.
2. Ensure that web applications within their area of responsibility adhere to laws, regulations, policies, and guidance including those regarding accessibility, privacy, and security.

L. Web Application System Owners shall:

1. Plan, develop, and implement web applications in compliance with established policies and procedures and in coordination with appropriate Web Manager(s).
2. Adhere to laws, regulations, policies, and guidance, including those regarding accessibility, privacy, and security.

9. Authorities and References

This policy is governed by numerous Public Laws and Authorities, that include:

A. Public Law 113-283, Title III, Federal Information Security Management Act (*FISMA*) of 2014.
B. Public Law 114-210, the ‘‘Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016’’ or the ‘‘MEGABYTE Act of 2016’’
C. The Freedom of Information Act, as amended, 5 U.S.C. § 552.
D. Section 508 of the Rehabilitation Act of 1973 and implementing policy and guidance.
E. The Privacy Act of 1974, as amended, (P.L. 93-579), December 1974
F. OMB Circular No. A-130, Managing Information as a Strategic Resource
G. Project Planning and Management (PPM)
H. HUD’s Web Application Security Plan (ASP)
I. Software Configuration Management Procedures
J. HUD Information Technology Security Policy Handbook 2400.25 Rev 5
K. NIST SP 800-37 Rev 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
L. NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations
M. NIST 800-44, Guidelines on Security Public Web Servers
N. NIST 800-95, Guide to Secure Web Services
O. NIST 800-145, The NIST Definition of Cloud Computing

10. Glossary - Abbreviations and Acronyms

For purposes of this policy, the following definitions apply.

A. ***Content:*** Information of any kind published to the web (includes text, graphics, symbols, retrievable data, and presentation concepts).
B. ***CISO***: Chief Information Security Officer
C. ***Extranet***: Any private network that uses the Internet protocol and the public telecommunication networks to securely connect to HUD Intranet and associated systems.
D. ***OCIO***: The Office of the Chief Information Officer
E. ***Internet***: The publicly accessible web presence of HUD. The top-level (home) page URL is https://www.hud.gov/.
F. ***IOO:*** Infrastructure Operation Office
G. ***Intranet***: The HUD web presence only accessible via authorized access to HUD networks. Note that various non-HUD personnel may at times have access to the HUD Intranet.
H. ***Personal Use***: Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.
I. ***Special Use Application***: HUD business software that uses the web as all or part of its communications network. Generally, has a limited audience and restricted access via user identification/password. The fact that a particular application may have a vast audience (for example, a Human Resources application accessible by all employees) does not exempt it from this category. Special Use Applications are not subject to this policy.
J. ***The Web***: Refers to the Internet, Intranet, and Extranet collectively.
K. ***Vulnerability Assessment***: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. This should be planned for and resourced within the programs Test Plan and executed within execution and control phase. (NIST SP 800-39)
L. ***Web Application***: is a client–server computer program that the client (including the user interface and client-side logic) runs in a web browser. Common web applications include webmail, online retail sales, online banking, and online auctions.
M. ***Web Content Manager***: Any individual designated to manage web content for an organizational element of HUD. The duties of the Web Content Manager include ensuring compliance with accessibility standards for persons with disabilities. This individual is the organization's primary point of contact for web issues.
N. ***Web Content Provider***: Any individual who authors content for publication to HUD websites.
O. ***Web Page***: Any single document posted to the web.
P. ***Web Site***: A group or system of web pages generally related by their content or ownership.