Commonwealth of Massachusetts

Massachusetts Office of Information Technology

# Enterprise Web Site Cookie Policy

**Reference #: ITD-SEC- 6.2 Revision Date: March 6, 2014
Issue #: 2**

## Table of Contents

[Table of Contents 1](#_Toc438559657)

[Executive Summary 1](#_Toc438559658)

[Whom this Policy Applies To 1](#_Toc438559659)

[Policy Statement 2](#_Toc438559660)

[Scope 4](#_Toc438559661)

[Roles and Responsibilities 4](#_Toc438559662)

[Related Documents 6](#_Toc438559663)

[Contact 6](#_Toc438559664)

[Appendix A: Terms 7](#_Toc438559665)

[Appendix B: Document History 8](#_Toc438559666)

## Executive Summary

Web site user privacy is of paramount concern to the Executive Department. This policy updates the provisions of the Executive Department’s “Requirements of Agency Web Site Privacy Policies” which pertain to use of cookies.

## Whom this Policy Applies To

All agencies and entities governed by the overarching Enterprise Information Security Policy must adhere to requirements of this supporting policy.

* Executive Department Agencies, [[1]](#footnote-2)
* Third parties with whom Executive Department Agencies contract for the provision of web services such as hosting and development services.
* Non-Executive Department entities whose sites become part of Mass.gov through portalization.

Other Commonwealth entities are encouraged to adopt, at a minimum, security and privacy requirements in accordance with this Enterprise Web Site Cookie Policy or a more stringent agency policy that addresses agency specific and business related directives, laws, and regulations

## Policy Statement

This policy articulates the requirements that agencies must adhere to when considering the use of either Session Cookies or Persistent Cookies as part of their web site or web-based application. The requirements articulated in this policy are in addition to all other applicable Enterprise Policies and Standards that govern an agency’s technical environment.

### General Requirements for Session Cookies and Persistent Cookies

Agencies must comply with all applicable security and privacy standards governing the collection and use of tracking information when using any type of cookie on their web sites for purposes of collecting visitor information.

Agencies must adhere to all relevant laws, regulations and policies including those designed to protect privacy governing the collection, use, retention, and safeguarding of any data gathered from users (web visitors), including but not limited to the following requirements as articulated in the Requirements for Agency Web-Site Privacy Policies:

* 1. Agencies must have an agency web site privacy policy posted prominently on their websites, and the policy itself must be written in clear, non-technical English (laymen’s terms) that is understandable to the ordinary reader.
	2. Agencies must disclose the purpose of cookie usage and the information collected via session cookies and/or persistent cookies whichever are used within an agency’s web site.
	3. Agencies must disclose their use of cookies, and the purpose for which they are using cookies, in their privacy policy and Terms of Use.
		1. An agency’s privacy policy and terms of use must identify any third party software that plants the cookies, and provide a link to the license and privacy policy associated with such software.
		2. Agencies must post clear and conspicuous notice on the Web site of the use of web tracking technologies.
		3. Agencies must provide a clear and understandable means for a user to opt-out of being tracked and not discriminate against those users who decide to opt-out in terms of their access to information.

### Requirements Specific to Persistent Cookies

The following requirements are specific to the use of persistent cookies:

* 1. Persistent cookies must be issued by a Commonwealth controlled domain.
	2. Persistent cookies must have a reasonable expiration date (for example, 2 years).
	3. Information/data collected via cookies stored on Commonwealth owned and managed systems must be destroyed when the purpose for which it was provided has been fulfilled unless required to retain for a longer period due to state or federal laws, regulations or policies of which the agency is subject.
	4. Information/data collected via cookies stored on third party managed systems must be subject to reasonable controls to protect users’ privacy.
	5. Permanent cookies issued by external parties other than software publishers providing contracted services are prohibited.
	6. Agencies must carefully review the legal terms related to any software that plants the cookies before using it, to ensure compliance with this policy and with the agency’s website privacy policy.
	7. Agencies are prohibited from using persistent cookies under circumstances that do not adhere to the requirements of this policy without first obtaining a waiver.

### Requirements for Seeking Waivers

Agencies with a business need to use persistent cookies in a manner that does not adhere to the requirements of this policy must seek a waiver from the Commonwealth Chief Information Officer. The waiver request must be sent to MassIT’s General Counsel, currently Linda Hamel, at linda.hamel@state.ma.us.

The waiver request must be submitted by the Secretariat’s Chief Information Officer (SCIO) and Portal Advisory Board (PAB) representative including a copy of the submission to the agency’s Information Security Officer (ISO). If the request is initiated by a specific agency within a secretariat, the agency must work through the SCIO and PAB representative to obtain the waiver. Waivers should not be sought if highly sensitive information, including but not limited to personal information, will be exposed through the use of persistent cookies.

The waiver must include sufficient background information to enable the reviewing body to determine:

* 1. The intended use and purpose of the non-compliant persistent cookies;
	2. Why the agency cannot meet its goals by complying with the policy.
	3. The results of the agency’s documented privacy/security review, including the agency’s privacy risk and mitigation recommendations.
	4. The Joint Privacy Policy Review Committee will make a recommendation to the Assistant Secretary for Information Technology for a final decision, who will sign all waiver grants.
		1. Waivers may be granted;
			1. For a limited period of time until agency comes into compliance with existing policy or;
			2. Permanently including a recommendation that specifics are incorporated into an updated enterprise policy as appropriate.

## Scope

A cookie is generated by software applications for purposes of performing an action. Therefore, this policy is intended to cover the requirements that are specific to the use of cookies. However, it is the [Enterprise Access Control Security Policies and Standards](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-access-control-policy.html)[[2]](#footnote-3) that articulate the specific security standards that must be adhered to for any public facing application. It is through the combination of these two documents that agency’s will best mitigate any known risks that could be introduced by the use of cookies.

## Roles and Responsibilities

All agencies and entities governed by the overarching [Enterprise Information Security Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html)[[3]](#footnote-4) are subject to the referenced roles and responsibilities in addition to those specifically stated within this supporting policy. In addition, the roles and responsibilities associated specifically with implementation and compliance with this policy follow:

Agency chief information officers, webmasters, and legal counsel are collectively responsible for ensuring adherence to this policy.

### Assistant Secretary for Information Technology

* The Assistant Secretary for Information Technology is responsible for the approval and adoption of the Enterprise Cookie Policy and its revisions.
* The Assistant Secretary for Information Technology is responsible for the final decision regarding requests for persistent cookie waivers.
* Granted persistent cookie waivers will be signed off by the Assistant Secretary for Information Technology.

### Secretariat Chief Information Officer (SCIO) and Agency Head

* SCIOs and Agency heads are responsible for exercising due diligence in adhering to the requirements contained in this policy.
* The SCIOs are responsible for submitting the persistent cookie waiver request and associated documentation.
* The Agency Heads are responsible for ensuring compliance with all applicable laws, regulations, and contractual obligations.
* The Agency Heads are responsible for signing and submitting the persistent cookie waiver request and associated documentation.

### Secretariat or Agency Information Security Officer (ISO)

* Ensure that the goals and requirements of this policy are implemented and met.

### Agency Legal Counsel

* Review the legal terms related to any software that plants the cookies before using it, to ensure compliance with this policy and with the agency’s website privacy policy.
* MassIT’s General Counsel is responsible for reviewing all persistent cookie waiver grants or denials prior to finalization and submitting her analysis to the Commonwealth Chief Information Officer for review and final signoff.

### Agency Web Masters

* Webmasters are responsible for conforming to this policy.

### Enterprise Security Board (ESB)

* Recommend revisions and updates to this policy and related guidance.
* Advise the Assistant Secretary for Information Technology in developing security policies, standards and guidelines.
* Act as a consultative body to the Assistant Secretary for Information Technology.

### Massachusetts Office of Information Technology (MassIT)

* Establish, adopt and implement the Enterprise-wide policies and standards for use of cookies on agency web sites:
	+ Continuous testing and monitoring of the enterprise environment.
	+ Requesting statements of compliance from Agency ISOs including additional information as required by the Assistant Secretary for Information Technology.
	+ Providing ongoing education and outreach.
* After review of any related recommendations of the Enterprise Security Board, issue revisions and updates to this policy and related standards.
* The Director of Mass.gov will enforce this policy.

### Third parties

* Ensure that all IT systems and applications developed by or for Executive Department agencies or servicing Mass.gov portalized sites conform to this and other applicable Enterprise Information Technology Policies, Standards and Procedures promulgated by the Assistant Secretary for Information Technology. Non-conforming cookies cannot be used unless the purchasing entity and their contractor have jointly applied for and received in writing from the Assistant Secretary for Information Technology or designee, notice that a specified deviation will be permitted.

## Related Documents

[Enterprise Access Control Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-access-control-policy.html) [[4]](#footnote-5)

## Contact

Standards@state.ma.us

## Appendix A: Terms

Key terms used in this policy have been provided below for your convenience. For a full list of terms please refer to the glossary of [Commonwealth Specific Terms](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html)[[5]](#footnote-6) on the Massachusetts Office of Information Technology’s website.

**Persistent Cookie(s) –** Also referred to as a ***permanent cookie***, or a stored cookie, a cookie that is stored on a user’s hard drive until it expires (persistent cookies are set with expiration dates) or until the user deletes the cookie. Persistent cookies are files that a Web site can place on a computer. A cookie file contains unique information that a Web site can use to track such things as the user’s password, lists of Web pages the user has visited, and the date when the user last looked at a specific Web page, or to identify a user’s session at a particular Web site. The file allows the Web site to recognize the user as they click through pages on the site and when the user later revisits the site. A Web site can use cookies to "remember" a user’s preferences, and to record a user’s browsing behavior on the Web. Although users can prevent Web sites from placing cookies on their computer by using the browser's preference menu, disabling cookies may affect a user’s ability to view or interact with some Web sites.

**Session Cookie(s) –** Also referred to as a ***transient cookie***, a cookie that is erased when the user closes the Web browser. A session cookie may be created when you visit a site or portion of a site. The cookie exists for the duration of your visit. The session cookie is stored in temporary memory and is not retained after the browser is closed. Session cookies do not collect information from the user’s computer. They typically will store information in the form of a session identification that does not personally identify the user. Cookies are files that a Web site can place on a computer. Depending on the settings in your browser, you may have the option to deny the session cookie; however, if you deny the cookie you may have trouble using the web site which relies on that cookie.

**Web Analytic / Web Tracking Tools –** Tools that measure, collect, analyze and report on the internet data for purposes of understanding and optimizing web usage. On-site web analytics measure a web visitor's journey once on the website and reports on web statistics and traffic. Such tools provide more robust reporting and collection of web usage data via the required use of permanent/persistent cookies.

## Appendix B: Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Action | Effective Date | Next Review Date |
| 11/17/2009 | Document Published | 11/17/2009 | 11/17/2010 |
| 1/23/12 | Reviewed | 1/31/12 | 1/23/13 |
| 1/17/14 | Updated | 3/6/14 | 1/1/15 |
| 1/5/15 | Reviewed | 1/6/15 | 2/1/15 |
| 2/5/15 | Reviewed | 2/6/15 | 2/1/16 |
| 12/22/2015 | Accessibility remediation – no content changes | 2/22/16 | 1/1/17 |

1. The Executive Department is comprised of the Executive Branch minus the Constitutional Offices, i.e., the State Auditor, State Treasurer, the Attorney General, and the Secretary of the Commonwealth. [↑](#footnote-ref-2)
2. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-access-control-policy.html [↑](#footnote-ref-3)
3. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-4)
4. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-access-control-policy.html [↑](#footnote-ref-5)
5. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html [↑](#footnote-ref-6)