14.3. Web Applications

Objective

14.3.1. Access to Web content is implemented in a secure and accountable manner.

Context

Scope

14.3.2. This section covers information on Web browsers, plug-ins and active content including the development and implementation of appropriate use policies.

14.3.3. The requirements in this section apply equally to the Web accessed via the Internet as well as websites accessed on an agency intranet.

References

14.3.4. An example of open source software that manages allow lists for client-side JavaScript controls is available at:

Reference	Title	Publisher	Source
	NoScript Firefox extension	Inform Action	https://noscript.net/

Rationale & Controls

Web usage policy

14.3.5.R.01. **Rationale**

If agencies allow system users to access the Web they will need to define the extent of Web access that is granted. This can be achieved through the development, and awareness raising amongst system users, of a Web usage policy.

14.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1272]

Agencies MUST develop and implement a policy governing appropriate Web usage.

Web proxy

14.3.6.R.01. **Rationale**

Web proxies provide valuable information in determining if malicious code is performing regular interactions over Web traffic. Web proxies also provide usable information if system users are violating agency Web usage policies.

14.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1592]

Agencies SHOULD use a Web proxy for all Web browsing activities.

14.3.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1593]

An agency's Web proxy SHOULD authenticate system users and provide logging that includes at least the following details about websites accessed:

- address (uniform resource locator);
- time/date;
- system user;
- internal IP address; and
- external IP address.

14.3.6.C.03. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1594]

Agencies SHOULD NOT permit downloading of executable files from external websites unless there is a demonstrable and approved business requirement.

Applications and plug-ins

14.3.7.R.01. **Rationale**

Web browsers can be configured to allow the automatic launching of downloaded files. This can occur with or without the system user's knowledge thus making the workstation vulnerable to attack.

14.3.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1597]

Agencies SHOULD disable the automatic launching of files downloaded from external websites.

Inspection of TLS

14.3.8.R.01. **Rationale**

As TLS encrypted Web traffic travelling over HTTPS connections can deliver content without any filtering, agencies can reduce this security risk by using TLS inspection so that the Web traffic can be filtered.

14.3.8.R.02. **Rationale**

An alternative of using an allow list for HTTPS websites can allow websites that have a low security risk of delivering malicious code and have a high privacy requirement like Web banking, to continue to have end-to-end encryption.

14.3.8.R.03. **Rationale**

It is however, important to note that there are many recorded cases of websites generally considered to be a low security risk that have been compromised.

14.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1602]

Agencies permitting TLS through their gateways SHOULD implement:

- a solution that decrypts and inspects the TLS traffic as per content filtering requirements; or
- an allow list specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked.

Legal advice on the Inspection of TLS traffic

14.3.9.R.01. **Rationale**

Encrypted TLS traffic may contain personal information. Agencies should seek legal advice on whether inspecting such traffic is in breach of the Privacy Act or other legislation. User policies should incorporate an explanation of the security drivers and acknowledgement from users on the policy contents and requirements. Refer to Chapter 9 – Personnel Security and Chapter 15 – Email Security.

14.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1605]

Agencies SHOULD seek legal advice regarding the inspection of encrypted TLS traffic by their gateways.

Allow listing / Deny listing websites

14.3.10.R.01. **Rationale**

Defining an allow list of permitted websites and blocking all unlisted websites limits one of the most common data delivery and exfiltration techniques used by malicious code. However, if agency personnel have a legitimate requirement to access a numerous and rapidly changing list of websites, agencies will need to consider the practicality and costs of such an implementation. In such cases deny listing is a limited but none-the-less effective measure.

14.3.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1609]

Agencies SHOULD implement allow listing for all HTTP traffic being communicated through their gateways.

14.3.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1608]

Agencies using an allow list on their gateways to specify the external addresses, to which encrypted connections are permitted, SHOULD specify allow list addresses by domain name or IP address.

14.3.10.C.03.

Control System Classifications(s): All Classifications; Compliance: Should [CID:1610]

If agencies do not allow list websites they SHOULD deny list websites to prevent access to known malicious websites.

14.3.10.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1611]

Agencies deny listing websites SHOULD update the deny list on a frequent basis to ensure that it remains effective.

Client-side active content

14.3.11.R.01. **Rationale**

Software that runs on agency systems SHOULD be controlled by the agency. Active content delivered though websites should be constrained so that it cannot arbitrarily access system users' files or deliver malicious code. Unfortunately the implementations of Web browsers regularly contain flaws that permit such activity.

14.3.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1614]

Agencies SHOULD block client-side active content, such as Java and ActiveX, which are assessed as having a limited business impact.

14.3.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1615]

Agencies SHOULD:

- use client-side controls that allow JavaScript on a per website basis; and
- add JavaScript functions used only for malicious purposes to the agency Web content filter or IDS/IPS.

Web content filter

14.3.12.R.01. **Rationale**

Using a Web proxy provides agencies with an opportunity to filter potentially harmful information to system users and their workstations.

14.3.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1618]

Agencies SHOULD use the Web proxy to filter content that is potentially harmful to system users and their workstations.

Website Passwords

14.3.13.R.01. **Rationale**

Some websites require the use of a userID and password as the authentication mechanism. The management of passwords on these websites is often insecure and there are numerous examples of compromises where tens of thousands, and sometimes millions of passwords are compromised in a single incident. Where the same password is used on multiple websites, an incident can potentially compromise the user's account on every website using that password. It is important to treat these websites as insecure and manage passwords appropriately.

14.3.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1621]

Users MUST NOT use agency userID and login passwords as credentials for external websites.

14.3.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1622]

Users SHOULD NOT store web site authentication credentials (userID and password) on workstations, remote access devices (such as laptops) or BYO devices.

14.3.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1623]

Users SHOULD NOT use the same password for multiple websites.