14.5. Web Application Development

Objective

14.5.1. Security mechanisms are incorporated into all Web applications by design and implementation.

Context

Scope

14.5.2. This section covers the deployment of agency Web applications and websites.

Protecting Web servers

14.5.3. Even though Web servers may contain only information authorised for release into the public domain, there still remains a need to protect the integrity and availability of the information. As such, Web servers are to be treated in accordance with the requirements of the classification of the system they are connected to.

Web application components

14.5.4. Web application components at a high level consist of a Web server for presentation, a Web application for processing and a database for content storage. There can be more or fewer components, however in general there is a presentation layer, application layer and database layer.

References

14.5.5. Further information on Web application security is available from the Open Web Application Security Project at:

Reference	Title	Publisher	Source
	The Open Web Application Security Project (OWASP) - Reference	OWASP	https://owasp.org/
	NZ Digital Government - Security and Privacy assurance	DIA	https://www.digital.govt.nz/standards-and-guidance/governance/managing-online-channels/security-and-privacy-for-websites/designing-for-security-and-privacy/security-and-privacy-assurance/
	Web Design and Applications	W3C	https://www.w3.org/standards/webdesign/
	Web Development – Patterns and Practices	Microsoft	https://msdn.microsoft.com/en-us/library/ff921348.aspx

Rationale & Controls

Agency website content

14.5.6.R.01. **Rationale**

Reviewing active content on agency Web servers will assist in identifying and mitigating information security issues.

14.5.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1661]

Agencies SHOULD review all active content on their Web servers for known information security issues.

Segregation of Web application components

14.5.7.R.01. **Rationale**

Web applications are typically very exposed services that provide complex interactions with system users. This greatly increases the security risk of being compromised. By segregating components, the impact of potential application flaws or attacks is limited.

14.5.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1664]

Agencies SHOULD minimise connectivity and access between each Web application component.

Web applications

14.5.8.R.01. **Rationale**

The Open Web Application Security Project guide provides a comprehensive resource to consult when developing Web applications.

14.5.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1667]

Agencies SHOULD follow the documentation provided in the Open Web Application Security Project guide to building secure Web applications and Web services.