DPC/S4.15

ACROSS GOVERNMENT POLICY

Web server security standards

Purpose

The purpose of these standards is to secure the web presence and information assets of the Government of South Australia.

The objectives of these standards are to ensure that:

- security controls are deployed to eliminate or minimise the existence of system vulnerabilities and other weaknesses
- a standard build is defined to ensure that web servers are deployed in a consistently secure manner
- security roles and responsibilities are established to ensure the ongoing effectiveness of security controls
- current industry and vendor best practice guidelines are referenced in the build, deployment and operation of web servers
- a whole-of-Government approach for building, deploying and maintaining secure web servers is established.

These standards are written to support the implementation of the AS/NZS ISO/IEC 27002 standard and the Government of South Australia Protective Security Management Framework (PSMF) versions 3.0 and later.

Background

The Government of South Australia has a large number of web servers that host web applications. These web applications provide critical services to the public and internal agency stakeholders.

These standards recognise that certain operating systems and web server software are prevalent. Accordingly, they provide guidance for the following web server platforms:

- Microsoft Windows Server running the Internet Information Services web server
- Red Hat Linux Enterprise Linux running the Apache web server.

These standards are related to Web Application Security Standards as they address the controls required to implement the supporting web server infrastructure.

Scope

Scope inclusions

These standards apply to all web servers that agencies or third parties build, procure, deploy, modify and maintain for SA Government business. This includes:

- all internal and public-facing web servers located within StateNet (on-Net)
- all public-facing web servers hosted by external providers (off-Net)
- all bespoke, customised, and off-the-shelf web servers that are bundled with applications, or embedded in devices or applications.

Scope exclusions

These standards do not apply to web servers that do not serve web content.

Terms, Abbreviations and conventions

Web server – The computer that provides world wide web services on the Internet. It includes the hardware, operating system, web server software, TCP/IP protocols and the website content (web pages). If a web server is used internally, and not by the public, it may be known as an 'intranet server'[1].

Public-facing – Web server that is accessible by the public from the Internet.

Network segmentation – Achieved by implementing physical or logical means, such as network firewalls, routers with access control lists that restrict or control access to a particular segment of a network.

Platform segmentation – Achieved by placing operating systems into physical or logical configurations that represent a similar risk profile or classification.

CGI	Common Gateway Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HIPS	Host-based Intrusion Prevention Software
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IPS	Intrusion Prevention System
PSMF	Protective Security Management Framework
ITSA	Information Technology Security Advisor
NFS	Network File System
NTP	Network Time Protocol
OS	Operating System
PCI DSS	Payment Card Industry Data Security Standard

[1] Definition according to the Australian Government Architecture Reference Models

SCP	Secure Copy
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer

Conventions

The terms used in this document are to be interpreted as described in Internet Engineering Task Force (IETF) RFC 2119 entitled *Key words for use in RFCs to Indicate Requirement Levels*. The RFC 2119 definitions are summarised in the following table.

Table 1 – keywords for the expression of requirement levels

Term	Description
Must	This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement.
Must not	This phrase, or the phrase “SHALL NOT”, means that is an absolute prohibition.
Should	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
Should not	This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label.
May	This word, or the adjective “OPTIONAL”, means that an item is truly optional.

Standards

The requirements analysis, data classification and risk assessment activities defined within Web Application Security Standards must be completed prior to deployment of a web server.

Agencies must adopt a defence-in-depth approach to minimise the security risks to web servers. Security controls must be applied at each layer of the web server to eliminate reliance on any single security control. Security controls must be selected based on the outcome of a risk assessment, and the classification of the information that will be processed by or stored on the web server.

These standards define a baseline of security controls that must be considered. They include a reference to the appropriate standard within the PSMF. Agencies should also note that particular requirements exist for public facing web servers installed within StateNet.

System build and maintenance

	Standard	References
1.	Servers may host a single system or component. Servers may host multiple systems or components when they have a similar risk profile and the same classification. Systems and components with different assessed risk profiles and/or classifications must be hosted on separate physical or logical servers as appropriate unless expressly authorised and formally documented by the agency. All shared web servers must have a responsible party nominated on behalf of all parties to coordinate change, incident and risk management activities.	ISMF Standard 19 AS/NZS ISO/IEC 27002 7.2.1
2.	Operating systems and application software installed on the web server must be security hardened with considerations for vendor recommendations and industry standards based upon role.	ISMF Standard 134 AS/NZS ISO/IEC 27002 15.2.2
3.	Application data (web content) must be located on a separate logical or physical partition to operating system files (web server software).	ISMF Standard 113 AS/NZS ISO/IEC 27002 12.4.1
4.	Disk volumes must use a file system type that supports access control and auditing capabilities.	ISMF Standard 113 AS/NZS ISO/IEC 27002 12.4.1
5.	Services should be running with the least privilege or authority necessary to carry out their tasks.	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2
6.	Remote monitoring and management services (such as SNMP, NTP, and Syslog) must be restricted with appropriate security hardening.	ISMF Standard 58 ISO 10.6.2
7.	Internet browsers running on web servers must be hardened by setting a high security level to untrusted sites/zones to prevent executable content from being downloaded. Internet browsers running on web servers should be used only for administrative purposes (e.g. downloading patches) from trusted sites, and not used for general “surfing”.	ISMF Standard 58 AS/NZS ISO/IEC 27002 10.6.2

8.	Any use of internet browsers on web servers must be performed from a non-administrative account, and only for defined business requirements as defined by the relevant agency security policy.	ISMF Standard 58 AS/NZS ISO/IEC 27002 10.6.2
9.	To support user authentication to the web server, authentication protocols that pass or store credentials must not do so in a form that can be easily recovered by a third party.	ISMF Standard 58 AS/NZS ISO/IEC 27002 10.6.2
10.	Apply file permissions and share permissions based on least privileges for critical or sensitive data (including log files). This includes: • authentication files • log files • backup files • sensitive app data • DR files	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2
11.	Log files must be located separately from system files to prevent file system exhaustion due to unbounded log file growth.	ISMF Standard 52 AS/NZS ISO/IEC 27002 10.3.1
12.	Log file maintenance (size and rotation settings) must take into consideration the number and frequency of records generated, as well as the business needs of the agency (e.g the logs may be required for forensic or transaction investigations).	ISMF Standard 52 AS/NZS ISO/IEC 27002 10.3.1
13.	Static IP addresses must be assigned to the web server rather than using a Dynamic Host Configuration Protocol (DHCP) server to obtain IP configuration details except where dynamic Domain Name System (DNS) technologies are employed for load balancing.	ISMF Standard 58 AS/NZS ISO/IEC 27002 10.6.2
14.	Web server supported services must be minimised to those required to support the server role and business requirements.	ISMF Standard 84 AS/NZS ISO/IEC 27002 10.4.1
15.	The TCP/IP stack must be hardened to protect the web server against denial of service attacks. This includes: • disabling ICMP redirect • SYN attack protection • disable IP source routing.	ISMF Standard 84 AS/NZS ISO/IEC 27002 10.4.1
16.	DNS settings should be applied to prevent against DNS poisoning attacks by using only trusted authoritative sources and where possible DNSSEC.	ISMF Standard 84 AS/NZS ISO/IEC 27002 10.4.1
17.	Access to removable media drives (floppy disk, CD-ROM, USB, etc.) must be restricted to only local administrators.	ISMF Standard 59 AS/NZS ISO/IEC 27002 10.7.1
18.	A login banner must be set to display a legal warning stating that unauthorised access is prohibited and that actions may be monitored. The login banner should not present a person with the ability to differentiate between standard or sensitive services.	ISMF Standard 86 ISMF Standard 131 AS/NZS ISO/IEC 27002 11.4.2

	The recommended text for a login banner is: Message Title: “WARNING: IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORISATION” Message Body: “This system is restricted to authorised Government of South Australia users. Individuals attempting unauthorised access will be recorded and prosecuted. If unauthorised, terminate access now.”	AS/NZS ISO/IEC 27002 15.1.5
19.	Web server specific lockdowns (both tools and processes as appropriate) must be applied to secure web server software whilst ensuring that it is able to operate correctly[2].	ISMF Standard 134 AS/NZS ISO/IEC 27002 15.2.2
	Web server specific analysis tools should be used to check the server state.[3]	ISMF Standard 134 AS/NZS ISO/IEC 27002 15.2.2
20.	Sample applications or scripts must not be installed on production servers. All default scripts or test files installed by vendor applications must be removed.	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2
21.	Externally-visible services must not reveal excessive information where possible. For example, do not advertise the name and version numbers of applications providing FTP or SSH services where possible to prevent fingerprinting of services.	ISMF Standard 119 AS/NZS ISO/IEC 27002 12.5.4
22.	Old or backup files must be removed when they are no longer required to support web server operations. For example, files belonging to a superseded application or temporary and backup files located on the server.	ISMF Standard 134 AS/NZS ISO/IEC 27002 15.2.2
23.	Ensure that deleted files are permanently removed at the operating system level. Windows systems must not send deleted files to the recycle bin.	ISMF Standard 134 ISO 15.2.2
24.	Encryption must be used to protect sensitive data in transit (including login credentials) on public-facing and agency-controlled networks. The minimum requirement for encryption algorithms defined within the Australian Government Information Security Manual, and referenced by the ISMF, should be used for all transmission of sensitive data.	ISMF Standard 58 AS/NZS ISO/IEC 27002 10.6.2
25.	Encryption must be used to protect sensitive data that is stored on the web server. Options include full disk, partial disk, data field or whole database encryption and determined by the assessed risk profile and data classification. The minimum requirement for encryption algorithms defined within the Australian Government Information Security Manual, and referenced by the ISMF, should be used for all storage of sensitive data.	ISMF Standard 109 AS/NZS ISO/IEC 27002 12.3.1

[2] Example hardening scripts are the 0x71 Apache Hardening Script for RedHat-based servers, or IISLockdown and URLscan for Microsoft-bases servers

[3] Example analysis tools include tools that assess servers against the Center for Internet Security Benchmarks for Red Hat-based servers, or the Microsoft Baseline Security Analyzer for Microsoft-based servers

26.	An accurate and authenticated time source such as Network Time Protocol (NTP) based time keeping must be maintained by web servers.	ISMF Standard 75 AS/NZS ISO/IEC 27002 10.10.6
27.	Physical devices that could facilitate a remote connection to the server (such as modems, faxes, wireless devices) must only be connected to the server after review and approval, except where the web server resides within StateNet, in which case connectivity of remote devices is subject to StateNet Conditions of Connection requirements and/or StateNet Manager approval.	ISMF Standard 86 AS/NZS ISO/IEC 27002 11.4.2
28.	Prior to the disposal or re-use of server hardware: • hard drives must be securely wiped using a low-level disk utility, demagnetiser or physically destroyed to prevent content reconstruction or retrieval • labels or classification tags must be removed or obscured.	ISMF Standard 45 AS/NZS ISO/IEC 27002 9.2.6
29.	Web servers must use secure command line protocols in place of clear-text protocols (for example SSH and SCP rather than TELNET and FTP), depending on data classification.	ISMF Standard 58 AS/NZS ISO/IEC 27002 10.6.2
30.	Servers must be configured with a password-protected screen saver and/or console timeout to activate after 10 minutes of inactivity.	ISMF Standard 58 AS/NZS ISO/IEC 27002 10.6.2
	All web server administration and configuration documentation must be adequately protected from unauthorised access.	ISMF Standard 62 AS/NZS ISO/IEC 27002 10.7.4

Access Control

	Standard	References
31.	Web server access and methods must be restricted to authorised users in accordance with business requirements and users must be restricted to authorised and appropriate activities only.	ISMF Standard 76 AS/NZS ISO/IEC 27002 11.1.1
32.	Users, including administrators, must log on using their personal user accounts to enforce accountability. Use of shared accounts must not be used unless approved by the Business Owner and formally documented.	ISMF Standard 94 AS/NZS ISO/IEC 27002 11.5.2
33.	Default administrator or root access accounts, and in-built accounts must be secured by the following means: • renamed to something other than default (Windows only) • disable the renamed account (Windows only) • create a secondary local administrator account • set with a long and complex password • default account description changed; and • used only when Domain or NFS accounts are unavailable.	ISMF Standard 94 AS/NZS ISO/IEC 27002 11.5.2
34.	The number of personnel that can gain access to the web server with administrator privileges (whether local or network-based) must be minimised.	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2
35.	Default, anonymous and guest accounts including default vendor accounts must be disabled and/or deleted.	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2
36.	All vendor default passwords must be changed to meet agency password requirements.	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2
37.	User accounts must be created and added to groups or security roles such that users are assigned the least privileges necessary to carry out their duties. User accounts and privileges should be regularly reviewed.	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2
38.	All console ports not required must be disabled to prevent unauthorised console connections.	ISMF Standard 90 AS/NZS ISO/IEC 27002 11.4.6
39.	Authentication controls must be in line with the classification of the information held and processed on the web server. Web servers housing data that is particularly sensitive may require greater protection.	ISMF Standard 17 AS/NZS ISO/IEC 27002 7.1.2
40.	Passwords must meet minimum agency password requirements. Where compliance is not possible, an exemption from policy must be granted and formally documented by the agency.	ISMF Standard 95 AS/NZS ISO/IEC 27002 11.5.3
41.	Server accounts must be reviewed regularly and accounts no longer required must be removed.	ISMF Standard 77

	(A server account is any account that support operating system or pre-installed middleware processes. This does not include regular logins and application logins, either individual or generic.)	AS/NZS ISO/IEC 27002 11.2.1
42.	Only specific authorised users or groups are allowed to manage user accounts as specified by agency security policy.	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2
43.	Remote access services must be authenticated and restricted to users or groups that have a need to access the service.	ISMF Standard 86 AS/NZS ISO/IEC 27002 11.4.2
44.	Servers must use strong encryption for remote management communications.	ISMF Standard 58 AS/NZS ISO/IEC 27002 10.6.2
45.	Two-factor authentication must be used for remote administrative access established over non-agency-controlled network links (e.g. the Internet).	ISMF Standard 86 AS/NZS ISO/IEC 27002 11.4.2
46.	Web server administration of StateNet hosted web servers must not be conducted via the browser (front end) over non-agency-controlled network links (e.g. the Internet). This does not apply to publicly hosted servers.	ISMF Standard 76 AS/NZS ISO/IEC 27002 11.1.1
47.	Access controls must take into account service and application account management/controls e.g. backup agent, SNMP community string (read, read/write), etc	

Backups and Recovery

	Standard	References
48.	The Business Owner is responsible for the development, maintenance and hosting of business continuity plans where business-critical functions are hosted on web servers.	ISMF Standard 124 AS/NZS ISO/IEC 27002 14.1.3
49.	Appropriate measures must be in place to support the implementation of a disaster recovery plan. This must include: • retaining system images that reflect the current state of the server configuration • retaining off-site copies of custom software relied upon by the server • retaining off-site backups of critical data.	ISMF Standard 124 AS/NZS ISO/IEC 27002 14.1.3
50.	Web servers must be accompanied by server build documentation that is accurate and up-to-date to facilitate a rebuild.	ISMF Standard 124 AS/NZS ISO/IEC 27002 14.1.3
51.	Backups of web servers must be tested regularly to ensure that data and operating systems can be recovered when required.	ISMF Standard 56 AS/NZS ISO/IEC 27002 10.5.1
52.	Backups must be secured to the same degree as the production data present on the server to preserve its integrity and confidentiality.	ISMF Standard 56 AS/NZS ISO/IEC 27002 10.5.1
53.	Backups should be stored in accordance with the disaster recovery plans.	ISMF Standard 56 AS/NZS ISO/IEC 27002 10.5.1

Change and Release Management

	Standard	References
54.	All changes to web servers must be reviewed and tested to ensure that there is no adverse impact on operation or security before being implemented on a production system.	ISMF Standard 117 AS/NZS ISO/IEC 27002 12.5.2
55.	Formal change control procedures must be established and documented, and evidence retained that the procedure is implemented and complied with.	ISMF Standard 116 AS/NZS ISO/IEC 27002 12.5.1
56.	All changes must be approved by the Business Owner or nominated delegate.	ISMF Standard 116 AS/NZS ISO/IEC 27002 12.5.1
57.	Systems must only be deployed on production and public-facing networks after final approval by the business owner.	ISMF Standard 48 AS/NZS ISO/IEC 27002 10.1.2
58.	When changes or enhancements to be made to a web server are assessed by the business owner as significant, a risk assessment must be performed to consider the security implications. Additional security testing should be undertaken where deemed necessary.	ISMF Standard 116 AS/NZS ISO/IEC 27002 12.5.1

Vulnerability and Threat Management

	Standard	References
59.	Existing agency vulnerability identification and patch management procedures must be followed to ensure that security vulnerabilities are identified and addressed.	ISMF Standard 121 AS/NZS ISO/IEC 27002 12.6.1
60.	All software, including operating systems and third-party applications, must be protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Agencies should adopt a risk-based approach to prioritise patching of web servers. Patches applicable to high-risk servers should be installed as soon as possible, but within one month of release.	ISMF Standard 121 AS/NZS ISO/IEC 27002 12.6.1
61.	Vulnerability identification and patch management procedures must include review of external security alerting services such as AusCERT and vendor security bulletins to identify new vulnerabilities.	ISMF Standard 121 AS/NZS ISO/IEC 27002 12.6.1
62.	Threat protection software must be configured to: • update scan engine and virus definitions at least daily • perform real-time and regular full scans at least once per week.	ISMF Standard 54 AS/NZS ISO/IEC 27002 10.4.1

Monitoring and Audit Logging

	Standard	References
63.	Capacity planning and monitoring must be performed to ensure the adequacy of processing and storage capabilities for the web server.	ISMF Standard 52 AS/NZS ISO/IEC 27002 10.3.1
64.	Host-based intrusion prevention software (HIPS) should be installed on web servers. HIPS will assist to prevent modification of system files and potentially malicious behaviour occurring on the server.	ISMF Standard 54 AS/NZS ISO/IEC 27002 10.4.1
65.	Monitoring for security breaches (malware, IPS alerts, etc.) must occur with policies configured to allow for alerting of critical events to security administrators.	ISMF Standard 71 AS/NZS ISO/IEC 27002 10.10.2
66.	Audit logging must be configured to record the following events: • privileged actions • access to sensitive resources, e.g. a particular file/folder (success and failure) • security events, including: o successful and failed login attempts o clearing of audit logs o account management events, including changes to membership of privileged/administrative user groups o system start up and shutdown o system time changes o system backup or restoration o changes to audit policy settings.	ISMF Standard 71 AS/NZS ISO/IEC 27002 10.10.1
67.	The integrity of audit logs must be secured and preserved.	ISMF Standard 32 AS/NZS ISO/IEC 27002 13.2.1
68.	Audit logs must be reviewed[4] regularly (at least weekly) for anomalous behaviour and events. At a minimum this should include: • failed login attempts • unusual login/logout times • failed services • security configuration changes • access violations to sensitive resources.	ISMF Standard 71 AS/NZS ISO/IEC 27002 10.10.1
69.	All audit events must record: • date and time of the event	ISMF Standard 71 AS/NZS ISO/IEC 27002 10.10.1

4 The reviewing and alerting function can be automated where appropriate.

	• event type identification/description • subject identity (e.g. user identification) • success or failure of the event.	
70.	Audit logs must be retained and stored in a manner that allows their integrity and authenticity to be verified for a period required to meet all legal and regulatory requirements. No users are to have update or delete access to the location where the log files are stored.	ISMF Standard 71 AS/NZS ISO/IEC 27002 10.10.1
71.	Audit log collection and storage should be on an agency-approved log server.	ISMF Standard 71 AS/NZS ISO/IEC 27002 10.10.1
72.	Security incidents must be reported according to the agency's incident management procedures.	ISMF Standard 30 AS/NZS ISO/IEC 27002 13.1.1

Assurance

	Standard	References
73.	Where deemed applicable by the risk assessment, specific security testing (e.g. vulnerability assessment and penetration testing) must be performed on completion of web server builds to validate that controls operate as designed. Additional testing should be performed when major or key system controls are changed, e.g. login pages are rewritten, database queries are changed.	ISMF Standard 134 AS/NZS ISO/IEC 27002 15.2.2
74.	Security testing must be performed by individuals other than the server operating system build team. Testing must be performed by individuals with qualifications that are deemed appropriate by the agency Business Owner.	ISMF Standard 118 AS/NZS ISO/IEC 27002 12.5.3
75.	Security vulnerabilities found during testing must be handled through the risk management methods of correct, mitigate, accept or transfer prior to implementation of any web server. Any uncorrected security vulnerabilities must be documented, and the documentation reviewed by the agency ITSA, the infrastructure provider's ITSA, and the ITSA of any other agency using the same web server and approved by the Business Owner.	ISMF Standard 121 AS/NZS ISO/IEC 27002 12.6.1
76.	The Business Owner should organise periodic security testing of the web server to ensure the ongoing effectiveness of security controls as new threats emerge.	ISMF Standard 134 AS/NZS ISO/IEC 27002 15.2.2

Physical and Environmental Security

	Standard	References
77.	Any web server that resides in an offsite facility, such as an ISP or hosting co-locate, must be subject to appropriate levels of control. Security controls must be implemented based on the established risk profile and must include physical and logical segmentation from other systems not used for SA Government business.	ISMF Standard 51 AS/NZS ISO/IEC 27002 10.2.1

Compliance

	Standard	References
78.	The Business Owner is responsible for identifying, documenting and notifying web server provider of all additional regulatory requirements that may require security controls or extended server log retention periods.	ISMF Standard 127 AS/NZS ISO/IEC 27002 15.1.1
79.	The requirements of PCI DSS must be implemented for web servers that store, process or transmit payment card data. Consideration should be given to segregation of systems that store, process or transmit payment card data to minimise the scope of PCI DSS compliance requirements.	ISMF Standard 127 AS/NZS ISO/IEC 27002 15.1.1

Implementation

Implementation Considerations

SA Government agencies, or external parties that develop, procure or operate web servers on behalf of the Government of South Australia, must implement the requirements of these standards.

The majority of agency web applications are hosted within the SA Government enterprise network StateNet, which has a specific role-based network segment for hosting public facing web applications. This segment includes a number of specific security functions including intrusion prevention, auto-vulnerability assessment and application security management technologies. The conditions of use that apply to agency web servers deployed in the DMZ are covered in a separate document.

Exemptions

Exemptions from these standards must adhere to existing cross-government ICT exemption policies (https://dpc.sa.gov.au/digital/exemption).

Responsibilities

The following responsibilities are defined.

Role	Responsibility
Chief Information Officers	Chief Information Officers are responsible for ensuring that these standards are implemented across web servers used for the agency's business.
Agency IT Security Advisers (ITSA)	Agency IT Security Advisers are responsible for advising on this standard across their agency.
Business Owners	Business Owners are responsible for conducting risk assessments and establishing and documenting risk profile prior to development being undertaken. They are also responsible for classifying information stored and processed by web servers.
Server Teams	Server Teams are responsible for the build, deployment and maintenance of web servers in line with the standards.

References, links and additional information

- Protective Security Management Framework
- Web Application Security Standards
- Guidelines on Securing Public Web Servers, National Institute of Standards and Technology
- *Information Technology – Security techniques – Code of practice for information security management*, AS/NZS ISO/IEC 27002:2006, Standards Australia, Sydney
- *Information Technology – Security techniques – Information security management systems – Requirements*, AS/NZS ISO/IEC 27001:2006, Standards Australia, Sydney
- *Key words for use in RFCs to Indicate Requirement Levels*, Harvard University

Document Control

ID	DPC/S4.15
Version	1.3
Classification/DLM	Public
Compliance	Required
Original authorisation date	July 2014
Last approval date	March 2019
Next review date	March 2020

Appendix A – IIS Specific Checklist

The following checklist provides specific requirements for Internet Information Services-based web servers[5] [6] [7]. The requirements directly reference the benchmarks published by the Center for Internet Security.

Basic Configuration

	Requirement		Reference	Check
A1	Ensure web content is on non-system partition.	Required	CIS Benchmark 1.1.1	
A2	Remove or rename well-known URLs.	Required	CIS Benchmark 1.1.2	
A3	Disable directory browsing.	Required	CIS Benchmark 1.1.4	
A4	Set default application pool identity to least privilege principal.	Required	CIS Benchmark 1.1.5	
A5	Ensure application pools run under unique identities.	Required	CIS Benchmark 1.1.6	
A6	Ensure unique application pools for sites.	Required	CIS Benchmark 1.1.7	
A7	Configure anonymous user identity to use application pool identity.	Required	CIS Benchmark 1.1.8	
A8	Require host headers on all sites.	Recommended	CIS Benchmark 1.1.3	

Authentication

	Requirement		**Reference**	**Check**
A9	Configure global authorisation rule to restrict access.	Required	CIS Benchmark 1.1.1	
A10	Ensure access to sensitive site features is restricted to authenticated principals only.	Required	CIS Benchmark 1.2.1	
A11	Require SSL in forms authentication.	Required	CIS Benchmark 1.2.2	
A12	Configure cookie protection mode for forms authentication.	Required	CIS Benchmark 1.2.3	
A13	Ensure password format credentials element not set to clear.	Required	CIS Benchmark 1.2.5	

[5] Note that the checklist covers server specific requirements. A completed checklist does not indicate conformance with the requirements of the standards described in this document.

[6] Note that public facing web servers with internal connections to StateNet (eg database connection) carry the highest risk and accordingly should be afforded a higher level of security hardening.

[7] Note that on-Net web servers located in the StateNet DMZ will be afforded a level of security assurance through integrated StateNet security systems. Non-compliant on-Net web servers will be treated under the Conditions of Connection. Off-Net web servers will require separate risk assessment.

A14	Configure forms authentication to use cookies.	Recommended	CIS Benchmark 1.2.4	
A15	Lock down encryption providers.	Recommended	CIS Benchmark 1.2.7	

ASP.NET Configuration

	Requirement		Reference	Check
A16	Set deployment method to retail.	Required	CIS Benchmark 1.3.1	
A17	Ensure cookies are set with HttpOnly attribute.	Required	CIS Benchmark 1.3.6	
A18	Configure machinekey validation encryption.	Required	CIS Benchmark 1.3.7	
A19	Configure global .NET trust level.	Required	CIS Benchmark 1.3.8	
A20	Turn debug off.	Recommended	CIS Benchmark 1.3.2	
A21	Ensure custom error messages are not off.	Recommended	CIS Benchmark 1.3.3	
A22	Ensure failed request tracing is not enabled.	Recommended	CIS Benchmark 1.3.4	
A23	Configure use cookies mode for session state.	Recommended	CIS Benchmark 1.3.5	

Request Filtering and Restrictions

	Requirement		Reference	Check
A24	Ensure double-encoded requests will be rejected.	Required	CIS Benchmark 1.4.5	
A25	Disallow unlisted file extensions.	Required	CIS Benchmark 1.4.6	
A26	Configure MaxAllowedContentLength request filter.	Recommended	CIS Benchmark 1.4.1	
A27	Configure maxURL request filter.	Recommended	CIS Benchmark 1.4.2	
A28	Configure maxquerystring request filter.	Recommended	CIS Benchmark 1.4.3	
A29	Do not allow non-ASCII characters in URLs.	Recommended	CIS Benchmark 1.4.4	

IIS Logging Recommendations

	Requirement		Reference	Check
A30	Move default IIS web log location.	Required	CIS Benchmark 1.5.1	
A31	Enable advanced IIS logging.	Required	CIS Benchmark 1.5.2	

FTP Requests

	Requirement		Reference	Check
A32	Encrypt FTP requests.	Required	CIS Benchmark 1.6.1	

Appendix B – Apache Specific Checklist

The following checklist provides specific requirements for Apache-based web servers running on Red Hat Enterprise Linux[8]. The requirements directly reference the benchmarks published by the Center for Internet Security.

Minimise Apache Modules

	Requirement		Reference	Check
B1	Enable only necessary authentication and authorisation modules.	Required	CIS Benchmark 1.2.1	
B2	Enable the log config module.	Required	CIS Benchmark 1.2.2	
B3	Disable WebDAV modules.	Required	CIS Benchmark 1.2.3	
B4	Disable status and info modules.	Required	CIS Benchmark 1.2.4	
B5	Disable Autoindex module.	Required	CIS Benchmark 1.2.5	
B6	Disable proxy modules.	Required	CIS Benchmark 1.2.6	
B7	Disable user directories modules.	Required	CIS Benchmark 1.2.7	

Restricting OS Privileges

	Requirement		Reference	Check
B8	Run the Apache web server as a non-root user.	Required	CIS Benchmark 1.3.1	
B9	Give the Apache user account an invalid shell.	Required	CIS Benchmark 1.3.2	
B10	Lock the Apache user account.	Required	CIS Benchmark 1.3.3	
B11	Apache directory and file ownership.	Required	CIS Benchmark 1.3.4	
B12	Apache directory and file permissions.	Required	CIS Benchmark 1.3.5	
B13	Core dump directory security.	Required	CIS Benchmark 1.3.6	
B14	Lock file security.	Required	CIS Benchmark 1.3.7	
B15	PID file security.	Required	CIS Benchmark 1.3.8	
B16	ScoreBoard File Security	Required	CIS Benchmark 1.3.9	

[8] Note that the checklist covers server specific requirements. A completed checklist does not indicate conformance with the requirements of the standards described in this document.

Apache Access Control

	Requirement		Reference	Check
B17	Deny access to OS root directory.	Required	CIS Benchmark 1.4.1	
B18	Allow appropriate access to web content.	Required	CIS Benchmark 1.4.2	
B19	Restrict override for the OS root directory.	Required	CIS Benchmark 1.4.3	
B20	Restrict override for all directories.	Required	CIS Benchmark 1.4.4	

Minimise Features, Content and Options

	Requirement		Reference	Check
B21	Restrict options for the OS root directory.	Required	CIS Benchmark 1.5.1	
B22	Restrict options for the web root directory.	Required	CIS Benchmark 1.5.2	
B23	Minimise options for other directories.	Required	CIS Benchmark 1.5.3	
B24	Remove default HTML content.	Required	CIS Benchmark 1.5.4	
B25	Remove default CGI content.	Required	CIS Benchmark 1.5.5	
B26	Limit HTTP REQUEST methods.	Required	CIS Benchmark 1.5.6	
B27	Disable HTTP TRACE method.	Required	CIS Benchmark 1.5.7	
B28	Restrict HTTP protocol versions.	Required	CIS Benchmark 1.5.8	
B29	Restrict access to .ht* files.	Required	CIS Benchmark 1.5.9	
B30	Restrict file extensions.	Recommended	CIS Benchmark 1.5.10	

Operations – Logging, Monitoring and Maintenance

	Requirement		Reference	Check
B31	Configure the error log.	Required	CIS Benchmark 1.6.1	
B32	Configure the access log.	Required	CIS Benchmark 1.6.2	
B33	Log monitoring.	Required	CIS Benchmark 1.6.3	
B34	Log storage and rotation.	Required	CIS Benchmark 1.6.4	
B35	Monitor vulnerability lists.	Required	CIS Benchmark 1.6.5	
B36	Apply applicable patches.	Required	CIS Benchmark 1.6.6	

Use SSL/TLS

	Requirement		Reference	Check
B37	Install mod_ssl and/or mod_nss.	Required	CIS Benchmark 1.7.1	
B38	Install a valid trusted certificate.	Required	CIS Benchmark 1.7.2	
B39	Protect the server's private key.	Required	CIS Benchmark 1.7.3	
B40	Restrict weak SSL protocols and ciphers.	Required	CIS Benchmark 1.7.4	
B41	Restrict insecure SSL renegotiation.	Required	CIS Benchmark 1.7.5	

Information Leakage

	Requirement		Reference	Check
B42	Limit information in the server token.	Required	CIS Benchmark 1.8.1	
B43	Limit information in the server signature.	Required	CIS Benchmark 1.8.2	
B44	Information leakage via default Apache content.	Required	CIS Benchmark 1.8.3	

Miscellaneous Configuration Settings

	Requirement		Reference	Check
B45	Denial of service mitigation.	Required	CIS Benchmark 1.9.1	
B46	Buffer overflow mitigation.	Recommended	CIS Benchmark 1.9.2	
B47	Restrict listen directive.	Recommended	CIS Benchmark 1.9.3	