IM/IT Architecture & Standards Manual STANDARD **Office of the Chief Information Officer** **Province of British Columbia**	**Effective Date:** 2012-10-18 **Scheduled Review: Biannual** **Last Updated:** 2012-10-18 **Last Reviewed:** 2012-10-11
	Type: Technical

6.0 Information Technology Security (CPPM 12.3.6)

6.13 Network Security Zone Standard

Keywords: Network, datacenter

Description of Standard

The strategic aim of this standard is to support the Government's goals through improvements to IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support Province's business needs of the future.

This standard governs the separation and protection of government data networks according to zones that are based on the classification of the information assets that the zones and associated security controls are intended to protect.

Where to Apply This Standard

This standard applies where there is a need to isolate and segment the government's networks and and/or for the graduated protection of government applications and the data that those applications process. The zone required in any given network application is determined by business requirements, Security Threat Risk Assessment and Privacy Impact Assessment.

Authority and Exemptions

This standard has been issued by the Office of the CIO in accordance with the Core Policy and Procedures Manual Chapter 12.3.6, Information Technology Security and the Information Security Policy.

If there are compelling business reasons why an organization is unable to comply with this architecture or standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

Information owners define the information security classification of the assets that they are responsible for. The information owner in conjunction with the application or database administrator determines the appropriate zone placement. HP-AS defines firewall rules as requested by administrators. The information asset owner for the destination of firewall rule request is the approver and also responsible for ensure that firewall requests comply with this standard. The Information Asset owner is responsible to ensure that a periodic

validation of the configured firewall rule set is compared against the rules that have been requested for the application or database.

Terms and Definitions

See section 5 of the full standard for Terms and Definitions.

References

The full Network Security Zones standard is available by contacting ASB.CIO@gov.bc.ca or by visiting the OCIO Intranet What We Do page.

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca

Contact

Architecture and Standards Branch, OCIO

email: ASB.CIO@gov.bc.ca