CITADEL-IX
citadel information exchange

ANYWHERE
ANYTIME
ANY DEVICE

Citadel-IX VPDSS Compliance

Whitepaper

citadel group
MANAGING COMPLEXITY

What is the VPDSS?

The Victorian Protective Data Security Standards (VPDSS) V2.0 were released in October 2019 and outline 12 high level mandatory requirements to protect public sector information across all security areas including governance, information, personnel, Information Communications Technology (ICT) and physical security.

The VPDSS V2.0 are consistent with national and international standards and describe the Victorian Government's approach to protecting public sector information. They focus on the outcomes that are required to enable efficient, effective and economic investment in security measures through a risk-managed approach.

Citadel-IX VPDSS Compliance

The Citadel Group provides a suite of highly secure information management systems to support organisations with the VPDSS V2.0 compliance and other international standards for information security.

Citadel-IX is a secure information management system and is compliant with all 12 mandatory requirements of the VPDSS V2.0. Citadel-IX is also certified end-to-end to the Information Security Management ISO 27001 standards.

This paper provides an outline of the 12 standards within the VPDSS V2.0, and Citadel-IX's compliance against each of these standards.

Standard 1. Information Security Management Framework

An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.

The objective of this Standard is to clearly establish, articulate, support and promote the security governance arrangements across the organisation and manage security risks to public sector information.

Citadel-IX Compliance Statement

As part of the ISO 27001 certification, Citadel-IX has established an information security management system that sets out a foundation in which robust security measures have been implemented to mitigate the ever growing cyber threats posed to secure information management systems worldwide.

Standard 2. Information Security Value

An organisation identifies and assesses the security value of public sector information.

The objective of this Standard is to ensure an organisation uses consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity and availability.

Citadel-IX Compliance Statement

Citadel-IX provides a secure platform for its customers to use consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity and availability.

Standard 3. Information Security Risk Management

An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks.

The objective of this Standard is to ensure an organisation manages information security risks through informed business decisions while applying controls to protect public sector information.

Citadel-IX Compliance Statement

The Citadel Risk Management Framework governs the organisation's management of Citadel-IX information security risks, and assists in taking a

holistic approach to appropriately assessing individual risks, as well as applying correct treatment methods to lower the overall security risks posed to the Citadel-IX platform.

Standard 4. Information Access

An organisation establishes, implements and maintains an access management process for controlling access to public sector information.

The objective of this Standard is to formally authorise and manage the physical and logical access to public sector information.

Citadel-IX Compliance Statement

Access controls to the Citadel-IX environment follow industry best practices using modern authentication methods via a delegated authentication model, providing Citadel-IX customers full control over front-end access to the application. Back-end access to the system is protected by a multifactor authentication enforced remoted desktop gateway.

Standard 5. Information Security Obligations

An organisation ensures all persons understand their responsibilities to protect public sector information.

The objective of this Standard is to create and maintain a strong security culture by ensuring that all persons understand the importance of information security across all the security areas and their obligations for protecting public sector information.

Citadel-IX Compliance Statement

All Citadel-IX support staff must read and acknowledge our ISO 27001 certified information security policies, and successfully complete a police check and cyber threat awareness training prior to gaining access to the system. All administrative and management authentication events are logged and frequently monitored by the Citadel Security Operations Team.

Standard 6. Information Security Incident Management

An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

The objective of this Standard is to ensure a consistent approach for managing information security incidents in order to minimise harm or damage to government operations, organisations or individuals.

Citadel-IX Compliance Statement

Citadel follows industry best practices in relation to security incident management and response. Security events are triaged by a combination of automated and manual analysis activities. The Citadel team will identify the extent of the threat, and work with specialist technology and security staff to fully contain the threat. Once all containment activities are complete, the threat is eradicated and measures are implemented to help prevent the incident from recurring.

Standard 7. Information Security Aspects of Business Continuity and Disaster Recovery

An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans.

The objective of this Standard is to enhance an organisation's capability to prevent, prepare, respond, manage and recover from any event that affects the confidentiality, integrity and availability of public sector information.

Citadel-IX Compliance Statement

A mandatory component to the Citadel-IX ISO 27001 certification is to ensure security continuity is well integrated into the Business Continuity Plan and Disaster Recovery Plan. This ensures information security is maintained in disaster situations to safeguard the confidentiality, integrity and availability of Citadel-IX customer data.

Standard 8. Third Party Arrangements

An organisation ensures that third parties securely collect, hold, manage, use, disclose or transfer public sector information.

The objective of this Standard is to confirm that the organisation's public sector information is protected when the organisation interacts with a third party.

Citadel-IX Compliance Statement

"Keeping people and information safe" and "Secure Information Management" are core to the services and products Citadel provides to its customers. As a third party, Citadel is a trusted provider with a long history and proven track record of delivering high quality and innovative solutions to our customers from both the private and public sectors.

Standard 9. Information Security Reporting to OVIC

An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (VPDSS) and reports to the Office of the Victorian Information Commissioner (OVIC).

The objective of this Standard is to promote the organisation's security capability and ensure adequate tracking of its exposure to information security risks.

Citadel-IX Compliance Statement

As part of the Information Security Management System, Citadel conducts regular reviews of all security controls in place, ensuring they are aligned with the Victorian Protective Data Security Standards on an ongoing basis. Citadel will also meet any reporting requirements that the Office of the Victorian Information Commissioner has as a custodian of Victorian Government information.

Standard 10. Personnel Security

An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access public sector information.

The objective of this Standard is to mitigate an organisation's personnel security risks and provide a consistent approach for managing all persons with access to public sector information.

Citadel-IX Compliance Statement

All Citadel-IX support staff must read and acknowledge our ISO 27001 certified information security policies, and successfully complete a police check and cyber threat awareness training prior to gaining access to the system. Additionally, Citadel-IX staff are vetted by Citadel Group HR to ensure that they meet the suitable character profile and skillset required for their roles.

Standard 11. ICT Security

An organisation establishes, implements and maintains Information Communications Technology (ICT) security controls.

The objective of this Standard is to maintain a secure environment by protecting the organisation's public sector information through ICT security controls.

Citadel-IX Compliance Statement

Citadel-IX maintains a significant number of security controls covered under ISO 27001, ISO 27002, ISO 27017 & ISO 27018 to ensure the security of the platform is upheld at all times. Citadel also employs a dedicated 24/7 Security Operations Centre, enforces multifactor authentication, end-to-end encryption, regular penetration tests, and vulnerability assessments of the platform.

Standard 12. Physical Security

An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services.

The objective of this Standard is to maintain a secure environment by protecting the organisation's public sector information through physical security controls.

Citadel-IX Compliance Statement

Citadel-IX leverages global leading data centre security controls and third party certifications for the security of the networks, firewalls, databases, web application gateways, servers and storage arrays that reside in the data centres. Additionally, Citadel has a physical security policy that protects the physical security of the supporting systems and devices managing the Citadel-IX environments.

More Information

For more information about Citadel-IX, please contact us at info@citadelgroup.com.au or visit www.citadelgroup.com.au/citadel-ix