Int Tec Solutions

Cybersecurity and the Victorian Protective Data Security Framework (VPDSF)

What is the Victorian Protective Data Security Framework (VPDSF)?

The Victorian Protective Data Security Framework (VPDSF) was established under Part 4 of the *Privacy and Data Protection Act of 2014* and took effect on 1 July 2016. This framework, created by the Office of the Victorian Information Commissioner, provides information to Victorian organisations operating in the public sector about requirements that are specific to this sector. There are 3 components to the framework, including the Victorian Protective Data Security Standards (VPDSS), the Assurance Model, and supplementary security guides and supporting resources.

This framework was developed as a means to help public sector organisations improve their data security practices and policies, manage risk and promote innovation that can lead to increased productivity. On a very broad scale, the VPDSF emphasises a cultural change that moves information security from being an autonomous activity to one that is incorporated in every aspect of the organisation's operations. It builds in security measures related to the people, the buildings, the systems and the processes of the organisation.

The VPDSF also includes a 5-step action plan for implementation that requires the following:

- Identification of your information assets.
- Determination on the 'value' of this information.
- Identification of any risks to the information.
- Application of security measures to protect the information.
- Management of risks across the information lifecycle.

In addition to the 5-steps, there are activities that must be conducted throughout the process to ensure that the steps are completed thoroughly and rigorously.

These steps include:

- The completion of a detailed Security Risk Profile Assessment (SRPA).
- The completion of a VPDSF self-assessment.
- The development of a Protective Data Security Plan (PDSP).
- A mandatory review of the PDSP every 2 years, or sooner if there is a significant change to the organisation.

OVIC oversees the compliance and monitoring activities related to the VPDSS, which may include audits.

What are the Victorian Protective Data Security Standards (VPDSS)?

The Victorian Protective Data Security Standards, or VPDSS, were created as a tool that would outline the path to a consistent application of security measures across the information network for the Victorian public sector. The VPDSS consists of 18 high-level mandatory standards, each with 4 protocols that work to protect data across 4 domains – information, personnel, ICT and physical security.

Security Governance	(12 standards) Executive sponsorship of and investment in security management, utilising a risk based approach
Information Security	(Three standards) Protection of information, regardless of media or format (hard and soft copy material), across the information lifecycle from when it is created to when it is diposed.
Personnel Security	(One standard) Engagement and employment of eligible and suitable people to access information
ICT Security	(One standard) Secure communications and technology systems processing or storing information
Physical Security	(One standard) Secure physical environment (eg. facilities, equipment and services) and the application of physical security measures to protect information

The Assurance Model

In the efforts to monitor and measure the efficacy of the protective security measures found in the VPDSF, OVIC has designed with Assurance Model to outline the activities that their agency will engage in while overseeing the data practices across the public sector. The Assurance Model is comprised of four parts:

1. **Security Planning** that addresses the activities that assess risk and the development of an action plan.
2. An **Organisational Compliance** approach that supports the continuous improvement mandate of the BPDSS.
3. The **Risk-Based Assurance** approach used by OVIC to assess the effectiveness of the VPDSF across the public sector.
4. The **Assurance Reporting** obligations for OVIC.

The 6-Point Approach to Comprehensive Cyber Security

Navigating the requirements of the VPDSF is no easy task. However, Int Tec Solutions embraces a security strategy that permeates the entire cyber landscape of an organisation and actively involves personnel in establishing and maintaining the highest level of security possible. While these activities can benefit organisations in any sector, they can be especially valuable for those in the public sector as they provide the assurances necessary in meeting the requirements of the VPDSF.

Int Tec Solutions 6 Points of Comprehensive Cyber Security

Identification	Vulnerability	Disruption	Mitigation	Response	Stabilisation
Audit network environment	Identify risk factors	Install and update all anti-virus, anti-spyware and anti-malware programs	Create situation-based response plans that can be enacted quickly	Maintain an active role in network assessments	Develop security policies
Prioritise threats as they are detected	Create comprehensive security road map	Develop and implement a real-time monitoring plan	Assist with backing up all necessary data to migrate a massive data loss	Work with in-house IT team to identify the best solutions to meet the intended business function	Train staff on best practices
Educated on new threats and vulnerabilities	Train employees on threat response	Identify and implement appropriate response	Communicate with team members to get systems restored quickly	Conduct thorough research on new network elements to identify any potential weaknesses	Advise on IT strategies that will facilitate the long-term business goals
Security awareness	Ensure all network components are up-to-date and appropriate patches are installed	Coordinate with other agencies if necessary	Communication with business leadership to ensure compliance to public reporting requirements		Choosing an SEO expert (identifying key indicators of knowledge, experience and depth)
Security training	Test security routinely to identify weaknesses	Cooperate with law enforcement when criminal activity is detected	Analyse past data breaches and successful attacks to identify areas for improvement		Continue assessing and re-assessing to ensure that the best solutions are in place
	Review access to ensure data is accessed by only those who need it	Facilitate communication between response team members to ensure a rapid and effective response			Develop long-term preventative maintenance plan/schedule

1. Risk identification

As experts with decades of experience, the professionals at Int Tec Solutions stay up to date on established threats that continue to evolve as well as new, emerging cyber threats. The breadth of knowledge allows them to rapidly and effectively identify and prioritize cyber threats so that prevention and response measures can be executed quickly.

2. Vulnerability reduction

Vulnerability reduction – By employing all available security measures and empowering employees within the organisation with the knowledge necessary to reduce cyber threats, clients can be assured that their level of vulnerability is greatly reduced.

3. Disruption and prevention of attacks

Disruption and prevention of attacks – With their extensive level of threat intelligence, the professionals at Int Tec Solutions can quickly detect data corruption and configuration anomalies that are red flags of a cyber-attack. This ability to quickly recognize an attack is the biggest factor in preventing data breaches.

4. Mitigation of incidents

Despite providing the best security measures available, no organisation is 100% immune from a cyber-attack, which is why Int Tec Solutions also works with their clients to develop mitigation plans so that data losses and downtime are reduced or eliminated.

5. Respond to changes in the network

With the rapid progress of digital technology, the only constant has been persistent change. As new applications and infrastructure solutions are developed, the older ones are replaced. The rise in cloud computing and the rapid proliferation of the Internet of Things (IoT) is also contributing to the fluidity and mutable nature of network environments. Int Tec Solutions is committed to providing the highest level of security for the unique network needs of their clients, no matter how much those needs may change.

6. Work to stabilise the entire cyber landscape

As the cyber security plan begins to take shape, the key to ensuring long-term security is empowering organisations in their ability to create policies and education on the importance of maintaining security. In this role, clients can depend on Int Tec Solutions to serve as a trusted and knowledgeable advisor that will help to develop successful strategies that support long-term cyber security.

Int Tec Solutions

Beyond the VPDSF

Achieving the goals laid forth by the VPDSF can be intimidating for any sized organisation, which is why the professionals at Int Tec Solutions can assist with every component to ensure full compliance is achieved. This service can begin during the planning process with the Risk Profile Assessment and carry through the entire process, during which only reporting and mandatory reviews are required. Despite the low level of requirements that are formally dictated by the VPDSF once the Protective Data Security Plan has been adopted, Int Tec Solutions will continue to be a proactive party that seeks out new vulnerabilities in a rapidly changing data landscape and working to ensure that these threats are properly accounted for.

In addition to ensuring that VPDSF requirements are met, Int Tec Solutions approaches data management in a more holistic manner and is able to offer their clients a wide range of consultational and supportive services to meet the spectrum of their IT needs.

39 Ninth Street, Mildura VIC 3500
Tel 1300 885 847 | (03) 5022 0000
Email support@inttec.com.au
Web inttec.com.au

Int Tec Solutions