# VPDSS 2.0 CONFORMANCE USING GUARDWARE INSIGHT

Organisations in Victoria that perform the functions of a public entity are required to comply with the Part 4 of the Privacy and Data Protection Act, 2014 (PDP Act). In relation to this OVIC has published the Victorian Protective Data Security Framework and issued the Victorian Protective Data Security Standards (VPDSS) to assist Victorian public-sector organisations meet their obligations for the protection of public sector information.

VPDSS is targeted to provide a set of criteria for the consistent application of risk-managed security practices across Victorian government information. It is a comprehensive data security standard covering all aspects from process, people to the required controls for the various aspects of digital and physical security. Following are the listed objectives of this standard:

- manage information throughout its lifecycle (creation to disposal)
- manage information across all the security domains (information, personnel, ICT, physical)
- manage security risks to information (CIA)
- manage external parties with access to information
- share information with other agencies with confidence
- minimise security incidents.

While managing security of information assets on corporate devices and application gets handled by traditional security like firewalls, email security and access control some of the listed objectives are much harder to achieve. Noteworthy exception being risk associated with:

1) Discovery, classification and control of PII and critical information asset (CIA)
2) Ensuring data governance by having actionable visibility on all aspects of data lifecycle and ensuring data is not being stored, moved and accessed in a secure manner by authorised users
3) Preventing data leaks due to human error or due to malicious intent by in insider
4) Sharing and controlling information using non-council risky means like Dropbox, Gmail, and storage media
5) Ensuring data governance by giving visibility and control to data owners
6) Measuring the effectiveness of user awareness sessions
7) Measuring risk through on going risk assessments
8) Controlling information when accessed by remote, BYOD and work from home scenarios

# GuardWare INSIGHT helps to conform with Victorian Protective Data Security Standards

GuardWare INSIGHT is specifically designed to fill these gaps and help organizations achieve compliance. Its application has merit across majority of the standards as listed under VPDSS. The below chart highlights how GuardWare INSIGHT helps in conformance with VPDSS.

| Standard # | Standard | Statement of Objective | How GuardWare INSIGHT assists in meeting the 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. | To clearly establish, articulate, support and promote the security governance arrangements across the organisation and manage security risks to public sector information. | GuardWare INSIGHT helps with the implementation of the security management framework. It helps to locate PII data, monitor its usage and movement and highlights areas of potential risks on an ongoing basis in line with privacy principals.<br><br>By doing this it helps to align organizations security management processes with risk management framework.<br><br>GuardWare INSIGHT helps to implement information security management workflow by defining roles and responsibilities of different information owner within the organization. This helps to streamline monitoring of sensitive PII information and ensure it is managed securely.<br><br>GuardWare INSIGHT helps to automate information security performance indicators and monitors information security obligations against these.<br><br>Helps in conformance with VPDSS elements E1.010, E1.030, E1.040 and E1.070 |

| Standard # | Standard | Statement of Objective | How GuardWare INSIGHT assists in meeting the standard |
|---|---|---|---|
| **2 Information Security Value** | An organisation identifies and assesses the security value of public sector information. | To ensure an organisation uses consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity and availability. | GuardWare INSIGHT helps in the development of information asset register (IAR) through data identification and discovery scans. The scans help to locate where sensitive information is stored to be mapped into the IAR.<br><br>The scans help to check whether the correct security markings are applied on sensitive information.<br><br>The scans help to locate externally generated information and ensure it is being used in accordance with originators instructions.<br><br>The scans help to ensure data is properly disposed off. Scans ensure there is no remanent data left in the network.<br><br>Helps in conformance with VPDSS elements E2.020, E2.040, E2.050, E2.080 and E2.090 |
| **3 Information Security Risk Management** | An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks. | To ensure an organisation manages information security risks through informed business decisions while applying controls to protect public sector information. | GuardWare INSIGHT helps to automate the risk assessment by continually monitoring the environment for security threats and vulnerabilities and produce a risk score.<br><br>GuardWare INSIGHT Risk management - feeds into the organizational overall risk profile. The system provides a high-level risk and compliance score for the areas covered under GuardWare. The system produces reports highlighting key risks |

| Standard # | Standard | Statement of Objective | How GuardWare INSIGHT assists in meeting the standard |
|---|---|---|---|
| | | | which feed into the risk management processes.<br><br>GuardWare INSIGHT forms a major part of the controls required to protect sensitive data. The system monitors sensitive data when being accesses, saved and moved and protects it from being breached due to risky user actions or malicious intent.<br><br>Helps in conformance with VPDSS elements E3.010, E3.020, and E3.050 |
| **4 Information Access** | An organisation establishes, implements and maintains an access management process for controlling access to public sector information. | To formally authorise and manage the physical and logical access to public sector information. | GuardWare INSIGHT helps to audit access of sensitive files and alerts in case of non-authorized access.<br><br>GuardWare INSIGHT also helps to implement access control on documents through encryption which is synced with Active directory roles. This way information remains secure from unauthorized access, loss or a breach.<br><br>Helps in conformance with VPDSS elements E4.010, E4.040, E4.050, E4.060 and E4.070. |
| **5 Information Security Obligations** | An organisation ensures all persons understand their responsibilities to | To create and maintain a strong security culture by ensuring that all persons understand the importance | GuardWare INSIGHT helps to implement a strong security culture by monitoring user actions against defined policies and highlights risky actions. These risky actions are fed back to the users through user centric reports. This helps in improving their |

| Standard # | Standard | Statement of Objective | How GuardWare INSIGHT assists in meeting the standard |
|---|---|---|---|
| | protect public sector information. | of information security across all the security areas and their obligations for protecting public sector information. | behaviours in future.<br><br>The detected risky actions also help focus and improve user education sessions as they can now be focused on real issues being faced by the organisation.<br><br>Helps in conformance with VPDSS elements E5.010, E5.020, E5.030 and E5.040. |
| **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. | To ensure a consistent approach for managing information security incidents, in order to minimise harm/damage to government operations, organisations or individuals. | GuardWare INSIGHT facilitates the standardization of incident management process through the generation of various reports. The reports help to<br><br>• Detect and report<br>• Assess and decide<br>• Respond (contain, eradicate, recover, notify)<br><br>GuardWare INSIGHT helps to implement incident management workflow by sending specific reports to information owners. This ensures people who understand the value of the information are the ones who are reviewing them. This process also helps to detect and identify the type of the incident. For example is the detected incident a criminal action or a policy violation.<br><br>Helps in conformance with VPDSS elements E6.030 and E6.050 |

| Standard # | Standard | Statement of Objective | How GuardWare INSIGHT assists in meeting the 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. | 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. | BC/DR events often result in users changing their behaviours in handling data which can result in data leakage.<br><br>The system helps to ensure there is no leakage or mishandling of data in the event of a BC/DR event.<br><br>Helps in conformance with VPDSS elements E7.030. |
| **8 Third Party Arrangements** | An organisation ensures that third parties securely collect, hold, manage, use, disclose or transfer public sector information. | To confirm that the organisation's public sector information is protected when the organisation interacts with a third party. | Not applicable. |
| **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 | To promote the organisation's security capability and ensure adequate tracking of its exposure to information security risks. | GuardWare INSIGHT plays a critical role in the implementation of VPDSS. The system monitors usage, movement and storage of sensitive info and reports in the event of a breach. The system can monitor sensitive info at content level this ensures clear audit trail is available of what data is lost, who did it and how it was lost. The reports are a key part of this reporting and compliance to VPDSS.<br><br>Helps in conformance with VPDSS element E9.010 |

| Standard # | Standard | Statement of Objective | How GuardWare INSIGHT assists in meeting the standard |
|---|---|---|---|
| | (OVIC). | | |
| **10 Personnel Security** | An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access public sector information. | To mitigate an organisation's personnel security risks and provide a consistent approach for managing all persons with access to public sector information. | GuardWare INSIGHT actively monitors and access of sensitive information by users and helps to check for unauthorised access. This ensures organisation's personal security policies are implemented properly and are being adhered to on an ongoing basis.<br><br>Helps in conformance with VPDSS elements E10.010 and E10.080 |
| **11 ICT Security** | An organisation establishes, implements and maintains Information Communications Technology (ICT) security controls. | To maintain a secure environment by protecting the organisation's public sector information through ICT security controls. | GuardWare INSIGHT is a data centric security system that helps to monitor and protect sensitive data when in use, when moved and when stored.<br><br>GuardWare INSIGHT helps to locate sensitive data through scans and helps to destroy data that is no longer required.<br><br>GuardWare INSIGHT helps to prevent breaches caused by users due to human error or malicious behaviours.<br><br>GuardWare INSIGHT secures key information using encryption. This ensure data remains secure when in use, when moved and when stored.<br><br>GuardWare INSIGHT provides media management capabilities. |

| Standard # | Standard | Statement of Objective | How GuardWare INSIGHT assists in meeting the standard |
|---|---|---|---|
| | | | GuardWare can help to block or alert on the usage of unauthorised communication channels and networks.<br><br>GuardWare INSIGHT audits the installed and used software through Software Audits and identifies changes to the baseline.<br><br>GuardWare monitors and movement of sensitive information on all encrypted and non-encrypted communication channels these include emails, chat, websites, cloud apps and external storage media.<br><br>Complete logs of each activity is maintained and highlights potential security issues.<br><br>Helps in conformance with VPDSS elements E11.040, E11.050, E11.060, E11.080, E11.100 and E11.110 |
| **12 Physical Security** | An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services. | To maintain a secure environment by protecting the organisation's public sector information through physical security controls. | Not Applicable |