GuardWare
INSIGHT

GuardWare INSIGHT helps organisations conform to ACSC ISM and DISP

1. HELPS TO ENSURE PROPER HANDLING OF DEFENCE LABELLED INFORMATION

Information marked Official, Official: Sensitive and Protected has strong security considerations. GuardWare INSIGHT helps to enforce these security requirements and ensure sensitive data is not mishandled.

2. HELPS TO ESTABLISH TRUSTED INSIDER PROGRAM INLINE WITH ACSC INFORMATION SECURITY MANUAL (ISM) AND DISP

Risk from users (trusted insiders) either due to human error or malicious insider activity, is a growing concern in defence. Programs like DISP (Defence Industry Security Program) now require defence suppliers to have a mandatory Trusted Insider management program, which requires companies to monitor user access (and their actions) when dealing with sensitive data. The type of security controls that organisations should adopt have been listed by Australian Cyber Security Centre (ACSC) in their latest iteration of the ISM (Information Security Manual) when mitigating risk from trusted insiders. The following extract from the ISM showcases the requirements of a Trusted Insider Program.

Trusted insider program

As a trusted insider's system access and knowledge of business processes often makes them harder to detect, establishing a trusted insider program can assist organisations to detect and respond to trusted insider threats before they occur, or limit damage if they do occur. In doing so, organisations will likely obtain the most benefit by logging and analysing the following user activities:

- rapid and numerous file copying or changes
- unauthorised or excessive use of removable media
- connecting devices capable of data storage (e.g. mobile devices and digital cameras) to systems
- unusual system usage outside of business hours
- data access or printing which is excessive compared to the normal baseline for a user or their peers
- data transfers to unauthorised cloud computing services or webmail
- use of unauthorised Virtual Private Networks, file transfer applications or anonymity networks.

Security Control: 1625; Revision: 0; Updated: Nov-20; Applicability: O, P, S, TS
A trusted insider program is developed and implemented.

Security Control: 1626; Revision: 0; Updated: Nov-20; Applicability: O, P, S, TS
Legal advice is sought regarding the development and implementation of a trusted insider program.

GuardWare INSIGHT software offers a one-stop solution to the data security, trusted insider, and compliance requirements of defence suppliers. It is regarded as a people centric security solution that can help companies establish a trusted insider program and implement the above suggested controls. It does this through a simple, 3 step approach:

Step 1. **Classify sensitive data.** Discovers and classifies files containing ITAR, CUI, defence classified data, tender information and intellectual property.

Step 2. **Monitor its usage**. Monitors all movements and user interactions with sensitive data, using specified rules and artificial intelligence.

Step 3. **Alerts when at risk.** Provides clear reports on data risks, identifying who accessed it, the actions performed on it, how it was shared, and alerts in case of breaches.