FORTRA

DATASHEET (PSPF COMPLIANCE)

Fortra for Protective Security Policy Framework (PSPF) Compliance

Fortra's suite of defensive security solutions gives Australian Government entities the operational capability to enforce PSPF controls consistently, demonstrate compliance, and close the gap between policy and real-world practice.

Data Security Solutions for PSPF Compliance

As Australia continues to experience an increasing number of disruptive cyberattacks—including ones targeting government entities—it's now more important than it's ever been for those entities to protect their people, information and resources, both domestically and internationally. According to the Protective Security Policy Framework (PSPF), this demands an active, continuously managed security program.

Most government entities' Accountable Authorities, CSOs, and CISOs understand what's expected of them and the entities they oversee. The greater challenge, however, lies in how to effectively meet those requirements, and it's compounded by several common obstacles:

Fragmented visibility – Sensitive data is often scattered across cloud platforms, SaaS applications, email, and on-premises systems, most entities lack a complete picture of where sensitive information lives, who has access to it, and how it's being handled.

Inconsistent classification and marking – The PSPF requires specific classifications with both visual and metadata markings applied consistently. Without the right tools, this process is error-prone, inconsistently applied, and difficult to audit.

SOLUTION SUMMARY

HIGHLIGHTS

Fortra's PSPF compliance solutions make it easy to:

- Discover and classify sensitive data at scale
- Apply PSPF protective markings consistently
- Enforce need-to-know access controls
- Detect threats before they become incidents
- Satisfy Essential Eight reporting requirements
- Demonstrate compliance for annual PSPF reporting
- & more

Disconnected security controls – Many entities rely on a mix of siloed solutions that don't communicate with one another or otherwise integrate well, allowing incident-prone gaps to emerge that must be addressed.

Reporting and accountability burdens – The PSPF requires entities to produce documented evidence of their security posture, including annual protective security reports and Technology Security Risk Management Plans (TSRMPs), which can be tedious and taxing without automated monitoring and reporting capabilities.

The PSPF sets out Australian Government policy across six security domains that connect with and impact one another: **Governance, Risk, Information, Technology, Personnel, and Physical.** Through an integrated approach, Fortra's data security tools directly address many of the requirements prescribed across these domains by the PSPF:

Governance

PSPF SECTION	REGULATORY REQUIREMENT	FORTRA CAPABILITY	EVIDENCE / OUTPUT
Section 3.5	Provide security awareness training to all personnel, including contractors, at engagement and annually thereafter.	Role-based phishing simulation and security awareness training.	Post-training, personnel are knowledgeable about various cyber risks that can lead to data leaks, fraud, and (more importantly) business, financial, and reputational damage.
Section 3.5	Provide targeted security training to personnel in specialist or high-risk positions.	Targeted training campaigns, assignable by role, department, or risk profile.	As opposed to a 'one size fits all' approach to training, the highest-risk personnel are identified, ensuring that the users who handle PSPF-regulated data are taught the gravity of compliance errors and cyber threats.
Section 3.6	Report significant or externally reportable security incidents to the relevant authority within the applicable timeframe.	Real-time alerting and incident logging with user, file, and timestamp context.	Real-time alerting and incident logging ensure *immediate* action in the wake of an incident, limiting or even avoiding accidental/ malicious data loss in the process.

Risk

PSPF SECTION	REGULATORY REQUIREMENT	FORTRA CAPABILITY	EVIDENCE / OUTPUT
Section 5.1	Determine and document the entity's tolerance for security risks.	Continuous risk visibility across cloud environments, including misconfigurations and access anomalies.	Continuous monitoring also means continuous posture evaluation, meaning it takes less time to identify flux in overall risk tolerance and apply more precise remediation.
Section 6.1	Manage security risks arising from procurement and outsourced services.	Identification of sensitive data accessible by third-party integrations and cloud services.	A generated audit trail with complete visibility over all data assets and access privileges, along with prevention mechanisms to proactively prevent inadvertent or wrongful data sharing.
Section 6.1	Use secure and verifiable third-party vendors; manage and approve residual risks with the CISO.	Monitoring of third-party cloud application usage and flagging of unauthorized or unverified applications.	Ensures only company-vetted and approved applications are used; i.e., constant enforcement of sensitive data flow.
Section 7.3	Implement an insider threat program for entities managing security clearance subjects.	Endpoint-level monitoring for anomalous data movement and exfiltration behavior.	A real-time audit of data transactions and movements, with stopgaps and actions to restrict leaks of sensitive information.

Information

PSPF SECTION	REGULATORY REQUIREMENT	FORTRA CAPABILITY	EVIDENCE / OUTPUT
Section 9.1	Assess the sensitivity of official information based on the potential damage if its confidentiality was compromised.	Impact-based classification guidance at the point of content creation.	Downstream data management systems will act upon both content- and context-driven classification, ensuring comprehensive protection against inadvertent data leaks.
Section 9.2	Set security classifications at the lowest reasonable level.	Policy tips and suggested classification prompts to prevent over-classification.	Any artifact, newly created or pre-existing, will have a minimum level of classification to prevent data leakage.

Section 9.2.3	Clearly mark security classified information with the applicable classification using text-based markings.	Automatic application of visible text-based markings to headers, footers, and email subject lines.	Applied markings are clear, concise, and automated, preventing human error and any resulting data leakage.
Section 9.2	Set security classifications at the lowest reasonable level.	Policy tips and suggested classification prompts to prevent over-classification.	Any artifact, newly created or pre-existing, will have a minimum level of classification to prevent data leakage.
Section 9.6	Apply the Australian Government Email Protective Marking Standard to OFFICIAL and classified email.	PSPF-compliant email markings in Outlook; classification-aware routing and handling.	Clear visual markings ensure users and recipients are aware of email origin, sensitivity, and appropriate actions.
Section 9.7	Apply the Recordkeeping Metadata Standard's Security Classification property to information on systems that store, process, or communicate classified information.	Persistent metadata injection using the Security Classification sub-property.	Classifications are ported with the artifact even when processed by third-party systems like email, file transfer, or DLP solutions.
Section 10.1	Implement operational controls for information holdings proportional to their value, importance, and sensitivity.	Automated discovery, inventory, and classification of sensitive data holdings across cloud environments.	Comprehensive, organization-wide discovery and classification capabilities enable comprehensive visibility and more precise, consistent downstream policy enforcement across all data artifacts.
Section 10.2	Maintain an auditable register for TOP SECRET information and accountable material.	Continuously updated inventory of sensitive data locations, classification levels, and access permissions.	All sensitive information is discovered and classified based on its content, context, and user attributes, meaning all of an organization's assets and their metadata are gathered in an auditable inventory.
Section 12.1	Provide access to classified information outside the entity only to those with a need-to-know, in accordance with Minimum Protections and Handling Requirements.	Enforcement of need-to-know sharing policies, blocking classified file transmission to unauthorized external recipients.	Policies implemented via DLP, email, and file transfer mechanisms ensure constant third-party access monitoring (and when needed, revocation) capabilities based on applied classifications, meaning only the intended parties are granted access.

Technology

PSPF SECTION	REGULATORY REQUIREMENT	FORTRA CAPABILITY	EVIDENCE / OUTPUT
Section 13.1	Apply ISM cyber security principles across all stages of each technology system's lifecycle, on a risk-based approach.	Continuous vulnerability discovery, prioritization, and remediation tracking.	Based on discovered vulnerabilities and misconfigurations, an organization's system is given a risk score with prioritized, actionable remediation tactics—ensuring timely, risk-based threat mitigation.
Section 14.1.1	Develop and maintain a cyber security strategy in accordance with the ISM and Guiding Principles to Embed a Zero Trust Culture.	Identity-verified, least-privilege access enforcement.	Access to data assets is only granted on a verifiable, need-to-know basis as opposed to trusting a user or device by default.
Section 15.1	Use a Protective DNS service or equivalent mechanism to prevent connections to known malicious endpoints.	Web traffic inspection and filtering of connections to known malicious domains.	Enforcement of security policies is extended to the web, meaning users will be blocked from connecting to malicious domains and prompted to reinforce security awareness.
Section 15.2	Protect digital infrastructure processing classified information with a Gateway or Security Service Edge.	Gateway-level traffic inspection; zero-trust network access controls.	Fortra's CASB, ZTNA, and SWG solutions work together to protect all Saas based applications, private applications and data, and websites against unauthorized access.

Personnel

PSPF SECTION	REGULATORY REQUIREMENT	FORTRA CAPABILITY	EVIDENCE / OUTPUT
Section 17.2	Provide access to classified information only to personnel with a need-to-know.	Classification label-based access controls.	Robust, granular classification of all artifacts at rest or in motion ensure downstream systems grant access based on strict classification-based policy conditions.
Section 21.3	Actively assess, monitor, and manage the ongoing suitability of personnel.	Behavioral risk metrics from phishing simulations and training engagement.	Risk metrics based on engagement with trainings and social engineering simulations quantify user competency, meaning those with the highest risk profiles can be identified and trained accordingly.

Fortra Closes the Gap Between PSPF Requirements and Real-World Practice

Whether you're conducting a gap assessment, preparing for annual PSPF reporting, or building a zero-trust architecture from the ground up, Fortra's experts and integrated solutions are here to help. Talk to a Fortra expert today.

CONTACT US

FORTRA®

Fortra.com