SMP 365 Security & Data Handling Statement

Effective Date: 9 May 2026

This Security & Data Handling Statement applies to SMP 365 software products, services, applications, APIs, and Microsoft Marketplace offerings provided by SMP 365 SAAS Pty Ltd.

This statement applies to all supported SMP 365 systems including Permit to Work, LMS, ICAM + AI Assisted Investigations, Contractor Management, Risk Management, Incident Management, EMS, Psychosocial Risk Management, Hazardous Goods Management, Travel Management, Action Management, Dashboards & Analytics, and Safety Mobile Applications.

1. Microsoft-Native Security Architecture

SMP 365 systems are designed as Microsoft-integrated business applications operating primarily within customer-controlled Microsoft environments including Microsoft 365, SharePoint Online, Microsoft Azure, Microsoft Entra ID, and Microsoft Graph.

This approach allows customers to leverage existing Microsoft enterprise security investments, governance models, and compliance controls.

2. Customer-Controlled Tenancy

SMP 365 systems are designed to operate primarily within the customer's own Microsoft tenant environment.

Customers retain control over user permissions, authentication policies, retention settings, audit logging, Microsoft Purview policies, and tenant governance controls.

3. SharePoint-Native Architecture

SMP 365 solutions are built using Microsoft SharePoint and Microsoft 365 technologies.

This architecture enables customers to inherit Microsoft platform capabilities including role-based permissions, audit history, Microsoft identity integration, enterprise authentication controls, and Microsoft compliance tooling.

4. Customer Ownership of Data

Customers retain ownership of investigation records, permits, risk assessments, contractor records, training records, environmental records, uploaded evidence, and operational business information.

SMP 365 does not claim ownership over customer operational data stored within customer-controlled Microsoft environments.

5. Configurable AI Services

Certain SMP 365 systems may optionally utilise Azure OpenAI, Azure AI Speech Services, Azure Document Intelligence, and Azure Cognitive Services.

AI-assisted functionality may support investigation assistance, evidence analysis, transcription, summarisation, workflow recommendations, and operational insights.

Customers control whether AI-assisted functionality is enabled within their environment.

6. AI-Assisted Output Disclaimer

AI-generated outputs are assistive only, may contain inaccuracies, require human review and verification, and do not constitute legal advice or compliance certification.

Operational decisions, investigation outcomes, and regulatory compliance responsibilities remain solely with the customer.

7. Microsoft Security Inheritance

Customers may leverage Microsoft enterprise capabilities including Microsoft Entra ID, MFA, Conditional Access, Microsoft Defender, Microsoft Purview, Microsoft Sentinel, Microsoft Compliance Manager, audit logging, and Microsoft data retention policies.

8. Security Controls

SMP 365 utilises commercially reasonable security practices including encrypted HTTPS communications, role-based access controls, API authentication controls, licensing validation systems, audit logging, and secure Azure infrastructure.

No software platform can guarantee absolute security.

Customers remain responsible for tenant administration, endpoint security, operational governance, and internal compliance obligations.

9. Data Processing & Hosting

Depending on customer configuration, data may be processed within customer Microsoft 365 environments, customer-selected Microsoft Azure regions, authorised SMP 365 infrastructure, and Microsoft cloud services.

10. Third-Party Services

SMP 365 systems may integrate with Microsoft 365, SharePoint Online, Microsoft Azure, Microsoft Graph, Azure AI Services, Microsoft Marketplace, and Microsoft Power Platform.

11. Security Incident Reporting

Customers should promptly report suspected unauthorised access, suspected data breaches, suspicious licensing activity, operational security concerns, or platform misuse.

Email: support@smp365.com
Website: https://www.smp365.com

12. International & Regulatory Considerations

SMP 365 systems are designed to support organisations operating within recognised international and ISO-aligned operational management frameworks.

Customers remain responsible for ensuring their own compliance with workplace legislation, privacy laws, operational regulations, and data residency obligations.

13. Changes to This Statement

SMP 365 may update this Security & Data Handling Statement periodically to reflect platform changes, Microsoft ecosystem changes, operational improvements, and security enhancements.

14. Contact Information

SMP 365 SAAS Pty Ltd
Global Microsoft-Integrated Safety & Risk Software Provider

Level 2, 1 Prowse Street
West Perth WA 6005

Australia

Email: support@smp365.com
Website: https://www.smp365.com