SMART
OUTSOURCE

Security Standards

SMART
OUTSOURCE

Table of Content

SMART OUTSOURCE

Your Data, Our Priority

At Smart Outsource, we understand that security is a top concern for businesses handling sensitive information. Here, we prioritize security at every level, implementing a holistic security approach that ensures end-to-end protection of your data and systems. Our 360° security framework integrates stringent controls across physical, network, application, and personnel security. With internationally recognized standards, cutting-edge technology, and industry best practices, we ensure maximum security and compliance for your business.

International Cybersecurity Standards & Frameworks We Follow

ISO/IEC 27001 Security Practices – Ensuring compliance with international information security standards.

National Institute of Standards and Technology (NIST) Cybersecurity Framework – A gold-standard approach to preventing, detecting, and responding to cyber incidents.

Essential Eight Maturity Model – A cybersecurity framework by the Australian Signals Directorate (ASD) designed to protect against cyber threats.

Compliance with the Privacy Act 1988 – Ensuring proper handling of personal data and compliance with Australian legal requirements.

Center for Internet Security (CIS) Critical Security Controls – Implementing best practices to defend against known security risks.

Our Multi-Layered Security Approach

We take a proactive approach to security, incorporating multiple layers of defense to keep your data safe.

EMPLOYEE SCREENING & BACKGROUND CHECKS

Comprehensive Background Checks – Identity, criminal, employment, and educational verification for every employee.

NDA & Confidentiality Agreements – Mandatory for all employees, ensuring legal accountability for data protection.

Role-Based Access Controls (RBAC) – Employees receive only the level of access needed for their roles.

Continuous Employee Risk Assessment – Periodic re-evaluation of employee access rights and security compliance.

Insider Threat Monitoring – Proactive tracking of behavioral anomalies to detect potential risks.

Biometric Authentication for Critical Systems – Ensuring that only authorized personnel access highly sensitive systems.

SECURITY AWARENESS & TRAINING

A well-trained workforce is the first line of defense against cyber threats. Our security training includes:

Mandatory Cybersecurity Training – Covering phishing, malware, data privacy, and compliance standards.

Simulated Phishing & Social Engineering Tests – Regular testing of employee awareness to strengthen resilience.

Incident Response Training – Educating employees on quick and effective response to security breaches.

Security Best Practices for Remote Workers – Guidelines for employees accessing systems from outside the office.

Secure Development Training for IT Teams – Teaching secure coding principles to mitigate application vulnerabilities.

PHYSICAL SECURITY

Access Control & 24/7 Surveillance – Biometric authentication, security guards, and AI-powered CCTV monitoring.

Asset Management & Clean Desk Policy – Preventing unauthorized access to confidential materials.

Data Center Security – Restricted access, temperature monitoring, and fire suppression for hardware safety.

Secure Disposal of Deprecated Storage Devices – Safe decommissioning of old hard drives and storage media.

Visitor Management System – Mandatory ID verification, tracking logs, and escorts for all visitors.

Security Alarm & Incident Response – Automatic alarms triggered in case of unauthorised access attempts.

NETWORK SECURITY

Enterprise-Grade Firewalls & Next-Gen IDS/IPS – Multi-layered defense against cyber threats.

End-to-End Encryption (AES-256, SSL/TLS) – Encrypting all data in transit and at rest for maximum security.

Zero Trust Network Architecture (ZTNA) – Continuous authentication for every user, device, and request.

Regular Penetration Testing & Vulnerability Assessments – Identifying and eliminating security weaknesses.

Advanced Threat Intelligence & AI-Based Monitoring – Using AI-driven analytics to detect and mitigate threats proactively.

Geo-Fencing & IP Whitelisting – Restricting access based on geographical locations to prevent unauthorized logins.

APPLICATION & SYSTEM SECURITY

Application Whitelisting – Only approved software is allowed to run, blocking unauthorised programs.

Office Macro & Script Execution Blocking – Preventing execution of malicious macros and scripts.

Automated Patch Management – Deploying security patches within 24 hours of vulnerability disclosure.

Endpoint Detection & Response (EDR) Solutions – AI-driven security measures monitor, detect, and remediate endpoint threats.

System Hardening – A collection of tools, techniques, and best practices to reduce vulnerability and minimize attack surfaces in the system.

SIEM-Based Log Analysis – Continuous logging and monitoring of all system activities.

ACCESS CONTROL & AUTHENTICATION

Multi-Factor Authentication (MFA) – Requiring two or more authentication factors for all critical systems.

Session Timeout & Auto-Logout – Reducing risk from abandoned active sessions.

Privileged Access Management (PAM) – Restricting admin privileges to authorized personnel only.

Just-in-Time (JIT) Access Control – Granting temporary admin access only when required, reducing long-term exposure.

Azure Active Directory & Conditional Access – Enforcing adaptive authentication policies.

USB Port & External Drive Blocking – Preventing unauthorized data transfers.

DATA PROTECTION & BACKUP

Daily Encrypted Backups – Storing backups in secure offsite & cloud environments.

Data Loss Prevention (DLP) Solutions – Blocking unauthorized sharing of confidential data via emails, USBs, and screenshots.

Watermarking on Screens & Documents – Preventing unauthorised copying and information leakage.

Strict Data Retention & Secure Deletion Policies – Ensuring that old data is securely erased after the retention period.

Tamper-Proof Audit Logs – Ensuring all actions are logged and protected from unauthorized changes.

CYBER THREAT MONITORING & INCIDENT RESPONSE

Real-Time System Monitoring – AI-driven tools for constant threat detection and anomaly detection.

Automated Threat Detection & Response – SIEM-based cyber threat intelligence platform.

24/7 Security Operations Center (SOC) – Always-on security monitoring and response team.

Compliance with Notifiable Data Breaches (NDB) Scheme – Ensuring legal compliance under Privacy Act 1988.

Email Recipient Monitoring & Filtering – Blocking emails with sensitive data from being sent to unauthorized recipients.

Our Control Mechanism

We implement seven layers of security controls to provide holistic protection against cyber threats.

Directive Controls (Security Policies & Governance)

- Security awareness training
- Incident response plans
- ISO 27001 and NIST-based security policies

Deterrent Controls (Discouraging Malicious Activity)

- Employee monitoring & behavioral analytics
- Legal action for policy violations
- Visible security measures (CCTV, warnings, monitoring alerts)

Preventive Controls (Blocking Threats Before They Occur)

- MFA, PAM, and Zero Trust security model
- Next-generation firewalls and IDS/IPS
- USB & external drive blocking
- Application whitelisting and system hardening

Compensating Controls (Alternative Safeguards)

- Watermarking on sensitive documents
- Download & access tracking logs
- Secure data handling policies

Detective Controls (Identifying Incidents & Breaches)

- SIEM event logging & AI-driven anomaly detection
- Penetration testing & vulnerability assessments
- Network & endpoint behavior monitoring

Corrective Controls (Responding to Incidents)

- Automated threat remediation & rollback
- Incident response team (24/7 SOC)
- Immediate account suspension for security policy violations

Recovery Controls (Restoring Systems After an Attack)

- Daily encrypted backups & offsite storage
- Disaster recovery plan & business continuity procedures
- Secure rollback for compromised systems

How We Ensure Compliance & Security Resilience

Regular Security Audits – Internal and third-party assessments to proactively identify and mitigate risks.

Penetration Testing & Vulnerability Scans – Simulating real-world cyberattacks to test and strengthen system defenses.

Legal & Regulatory Compliance – Adhering to ISO 27001, NIST Cybersecurity Framework, CIS Controls, the Australian Privacy Act 1988, and the Essential Eight Maturity Model by the Australian Signals Directorate (ASD) to meet the highest security standards

Automated Compliance Monitoring – Utilizing security tools to track compliance adherence and detect deviations in real-time.

Third-Party Risk Assessments – Evaluating vendors and service providers to ensure compliance with our security policies.

Data Sovereignty & Residency Compliance – Ensuring sensitive data is stored and processed within approved jurisdictions.

Business Continuity & Incident Response – Proactive disaster recovery planning to minimize downtime and ensure rapid recovery.

Policy-Driven Data Governance – Enforcing strict data retention, classification, and encryption policies to prevent unauthorized access.

Lost Devices Security – Devices automatically erase all data after 10 failed login attempts, followed by a forced password reset to prevent unauthorised access.

Frequently Asked Questions

Security & Data Protection

1. What happens if any account is hacked or a device is lost?
We implement multi-layered security measures. In case of a lost device, all data is automatically erased after multiple failed login attempts. Accounts have MFA, endpoint security, and restricted access to prevent unauthorised breaches.

2. How is my sensitive information protected?
We use end-to-end encryption, zero trust architecture, role-based access control (RBAC), and 24/7 monitoring to safeguard your data.

3. Can employees access my confidential data?
No, only authorised personnel with a valid business need can access data under strict role-based access control (RBAC).

4. Do you monitor employee activities?
Yes, our SIEM system & employee monitoring tool logs and monitors all activities in real time to prevent data leaks and insider threats.

5. Where is my data stored?
We comply with data sovereignty laws and store data in approved, secure locations.

6. What measures prevent unauthorized downloads or data transfer?
USB ports are blocked, file downloads are monitored, watermarking is used, and email filtering is in place to prevent data leaks.

7. Do you conduct background checks on employees?
Yes, all employees undergo comprehensive background checks, including identity, criminal, and employment history verification.

8.How often do you update security policies?
Our policies are continuously reviewed and updated to align with the latest cybersecurity frameworks.

9. Can employees access the platform from any network or device?
No, access is restricted through Point-to-Point VPN Tunneling, meaning only pre-approved devices and networks can connect. Even if an attacker obtains login credentials, they cannot access the system without connecting through the secure VPN tunnel.

10.What happens if an employee loses their device?
If a device is lost or stolen, our security mechanisms will:

✓ Automatically erase all data from the device after 10 failed login attempts.
✓ Block VPN access from that device immediately.
✓ Force a password reset to prevent unauthorised access.

Compliance & Legal Assurance

11. Are you compliant with international security standards?
Yes, we follow ISO 27001, NIST, CIS Controls, and the Privacy Act 1988 (Cth).

12. Do you sign NDAs with clients?
Yes, every project is covered by a strict NDA and confidentiality agreement.

13. What happens in case of a security breach?
We follow a rapid response protocol with forensic investigation, system isolation, impact assessment, and client notification as per compliance laws.

14. Can I conduct a security audit on your company?
Yes, clients can request a security audit as part of our transparency and compliance framework.

Service Reliability & Infrastructure

15.How do you ensure business continuity?
We have a robust disaster recovery plan, redundant data centers, and daily backups.

16. What happens if there’s a natural disaster or power failure?
Our offices have uninterruptible power supplies (UPS), cloud backups, and remote failover solutions.

17. How do you prevent downtime?
We have a high-availability infrastructure, proactive maintenance, and real-time system monitoring.

18. What level of support do you offer?
We provide 24/7 dedicated support with real-time incident response teams.

Team & Operations Security

19. Where are your employees located?
Our workforce is global but operates under centralized security controls.

20. How do you train employees on cybersecurity?
Employees undergo mandatory cybersecurity training, simulated phishing tests, and role-specific security workshops.

21.Can I choose specific team members for my project?
Yes, we allow clients to handpick vetted professionals based on their needs.

22. How do you manage insider threats?
We enforce strict access controls, behavioral monitoring, and AI-driven anomaly detection.

Technology & IT Management

23. What tools and software do you use?
We use Microsoft Entra ID, enterprise-grade firewalls, endpoint security, cloud security platforms, and encrypted communication tools.

24. Do you support cloud-based collaboration?
Yes, we integrate with Microsoft Azure, AWS, and other secure cloud solutions.

25. Can I integrate my own security tools with your infrastructure?
Yes, we offer customizable security integrations with client-preferred tools.

26. What cybersecurity framework do you follow?
We align with NIST, Essential Eight, and Zero Trust Architecture principles.

Client Control & Customisation

27. Can I restrict access to specific team members?
Yes, you can enforce custom RBAC policies.

28. Do you support multi-factor authentication (MFA)?
Yes, MFA is mandatory for all accounts and logins.

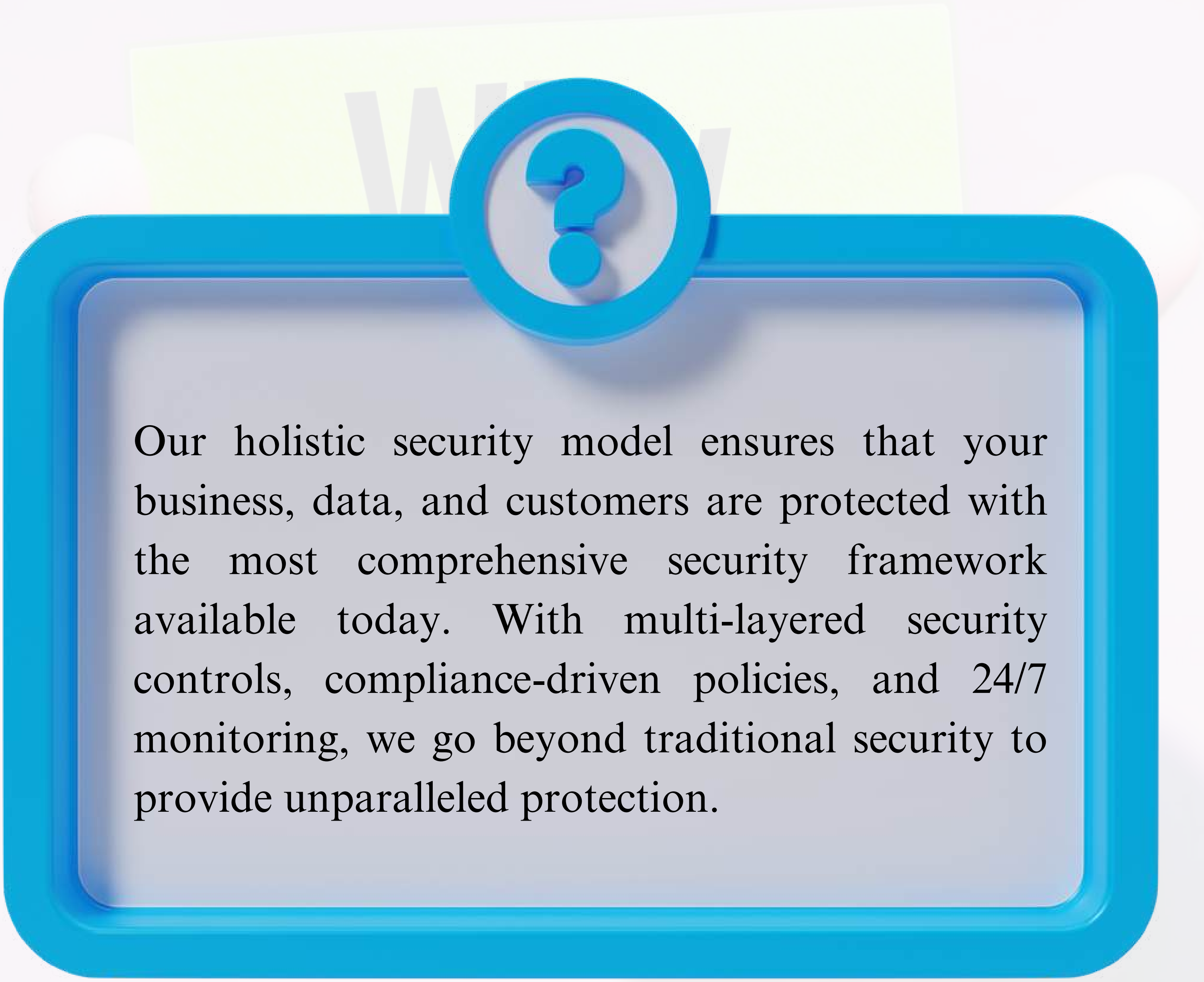
29. Can I request a dedicated IT security manager for my project?
Yes, we provide dedicated security professionals for high-priority projects.

30. How do you manage client credentials and sensitive access?
All credentials and sensitive access are managed through Microsoft Entra ID and its Single sign-on (SSO) to prevent the exposure of credentials.

31.Do you provide real-time security dashboards?
Yes, clients can access a customised security dashboard for monitoring and reporting.

32. How do you handle employee offboarding?
Departing employees' access is immediately revoked, and their devices undergo data wiping.

Why Choose Smart Outsource?



Our holistic security model ensures that your business, data, and customers are protected with the most comprehensive security framework available today. With multi-layered security controls, compliance-driven policies, and 24/7 monitoring, we go beyond traditional security to provide unparalleled protection.