Security Risk Assessment Checklist

DATA SECURITY

- □ Does the vendor implement strong encryption for data at rest and in transit (e.g., AES-256, TLS 1.2+)?
- □ Are encryption keys securely stored and managed?
- □ Does the vendor conduct regular penetration testing to identify potential vulnerabilities?
- □ Are data backup and recovery mechanisms in place and tested regularly?

ACCESS CONTROL AND AUTHENTICATION

- □ Does the vendor use multi-factor authentication (MFA) for all systems with access to sensitive data?
- □ Are the principles of least privilege and role-based access control (RBAC) enforced?
- □ Are user access reviews conducted at least on a quarterly basis?
- □ Are there controls for revoking access promptly upon termination of staff or contract?
- □ Are access policies and roles reviewed and updated at least on a quarterly basis?
- □ Does the vendor support single sign-on (SSO) or federated identity management?
- □ Does the vendor maintain logs and audits of access to sensitive systems and data?

INCIDENT RESPONSE CAPABILITIES

- □ Does the vendor have an established incident response plan?
- □ Is the incident response plan regularly tested and updated?
- □ Has the organization established processes and formal agreements for third-party service providers to provide immediate notification in the event of a disruption that impacts the delivery of the products and/or services they provide?
- □ Are there clear escalation processes and communication protocols during incidents
- □ Are backups of scoped systems and data performed? If yes, are they stored offsite
- □ Are backup and replication issues regularly reviewed and addressed as necessary
- □ Are lessons learned from incidents integrated into risk management processes?

COMPLIANCE WITH REGULATIONS

□ Does the vendor comply with relevant regulations (e.g., GDPR, HIPAA, PCI-DSS, CCPA, NIST)?

□ Are there certifications or third-party assessments (e.g., SOC 2, ISO 27001) to verify compliance?

□ Is there a dedicated internal audit, risk management, or compliance department, or a similar oversight unit responsible for evaluating, identifying, and monitoring the resolution of regulatory issues?

□ Does the vendor provide audit-able proof of compliance and regulatory adherence?

RISK MANAGEMENT

□ Does the vendor have a risk management plan that includes the identification and mitigation of security risks?

□ Is there a defined process for evaluating and agreeing on acceptable risk levels?

□ Are risk assessments performed regularly to keep up with evolving threats and business needs?

□ Are key risk indicators (KRIs) tracked to measure the effectiveness of controls?

VENDOR TRANSPARENCY AND ACCOUNTABILITY

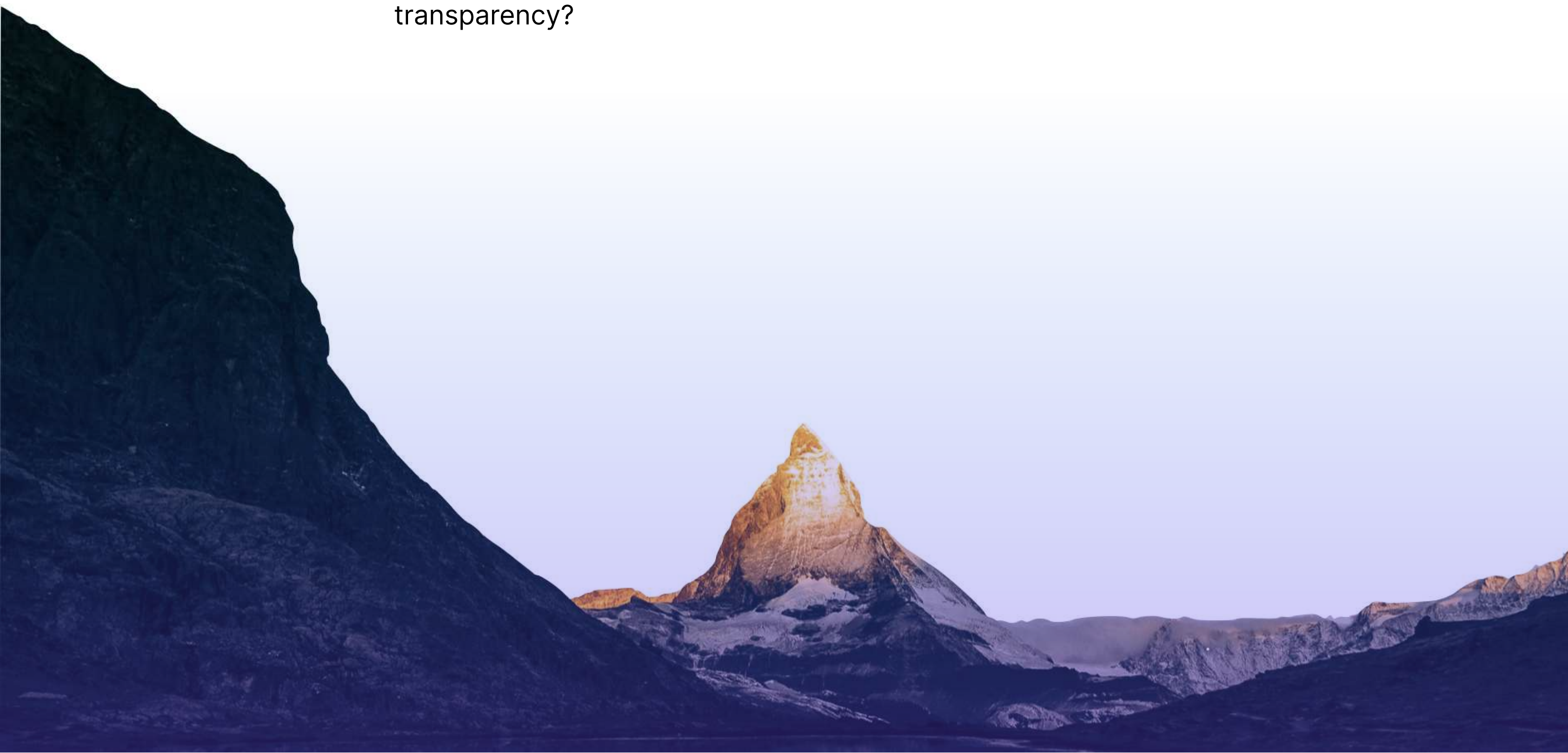
□ Does the vendor provide full visibility into their security measures, including sub-vendors?

□ Does the vendor maintain clear communication about any sub-vendor relationships

□ Are third-party and sub-vendor relationships clearly defined, and are they held to the same security standards?

□ Does the vendor have a process for reviewing and updating security practices regularly?

□ Are there any legal or operational limitations that may restrict the vendor’s transparency?



MONITORING AND AUDITING

- □ Is continuous monitoring of the vendor’s security posture in place to detect new vulnerabilities?
- □ Are automated vulnerability scanning tools used to detect issues in real-time?
- □ Does the vendor provide reports on security performance and remediation efforts
- □ Does the vendor use sub-vendors or third parties for critical services?
- □ Are the security practices of sub-vendors regularly reviewed and aligned with the primary vendor’s standards?
- □ Do you require third parties to follow data privacy and security practices that meet or exceed your policy and comply with your requirements?

APPLICATION SECURITY

- □ Is there an anti-malware policy or program that has been approved by management, communicated to appropriate constituents, and has an owner assigned to maintain and review it, including defined operating systems that require antivirus and a mandate for deploying new anti-malware signature updates within 24 hours?
- □ Is there a Vulnerability Management Policy or Program that has been approved by management, communicated to appropriate constituents, and has an owner assigned to maintain and review it?
- □ Are network vulnerability scans performed against internal and external networks and systems?
- □ Are server security configuration standards documented and based on external industry or vendor guidance, including the removal or disabling of vendor default passwords and unnecessary services before placing any device or system into production?
- □ Are all systems and applications patched regularly?

BUSINESS CONTINUITY AND DISASTER RECOVERY

- □ Does the vendor have a documented business continuity plan in place?
- □ Are disaster recovery plans tested at least annually?
- □ Does the vendor maintain backups of critical data, and are these backups stored securely?
- □ Is there a formal, documented program for conducting disaster recovery exercises and tests for information technology systems?
- □ Are local governing authorities involved in the disaster recovery testing process?
- □ Are recovery time objectives (RTO) and recovery point objectives (RPO) clearly defined?

PHYSICAL SECURITY

- □ Is there a physical security program for all secured facilities (such as data centers and office buildings) that has received management approval, been communicated to relevant stakeholders, and has a designated owner responsible for maintenance and review, including documented access controls?
- □ Do the physical security measures incorporate an electronic access control system (such as key cards, tokens, fobs, or biometric readers)?
- □ Do the physical security measures include alarmed entry and exit doors (for forced entry or propped open scenarios) and/or monitoring by security personnel, along with environmental controls to protect computers and other physical assets (e.g., fire detection and suppression systems)?
- □ Do the physical access controls involve the collection of access equipment (like badges, keys, or PIN changes) when an employee is terminated or has a change in status?
- □ Do the physical access controls mandate reporting of any lost or stolen access cards or keys?
- □ Are visitors allowed access to the facility?Are the scoped systems and data stored in a data center?

ADAPTING TO THE EVOLVING THREAT LANDSCAPE

- □ Are employees regularly trained on recognizing and responding to emerging cyber threats?
- □ Does the vendor use AI or machine learning tools for proactive threat detection
- □ Does the company conduct regular threat intelligence briefings or updates for key stakeholders?
- □ Are the company's cybersecurity measures regularly tested against the latest known threat vectors?
- □ Are evolving security frameworks and regulations regularly integrated into the vendor's security practices?

SecurityPal
Salesforce Tower
415 Mission St Floor 37
San Francisco, CA 94105