Vendor Security Guidelines

1. Introduction

This document sets forth the Vendor Security Guidelines that all third parties, contractors, suppliers, and service providers (“Vendors”) must follow when handling our organization’s data, systems, or services. The purpose of these guidelines is to ensure that every vendor relationship upholds the same level of security, confidentiality, and integrity that our customers and regulators expect from us.

---

2. Vendor Onboarding and Due Diligence

Before entering into a contract, every vendor must undergo a security risk assessment. This process includes evaluating the vendor’s information security program, reviewing certifications such as ISO 27001 or SOC 2 where applicable, and determining whether they can meet the minimum requirements of our own controls.

For example, if a vendor is providing cloud storage services, they must demonstrate that their platform enforces encryption at rest and in transit, maintains strict access controls, and conducts regular penetration testing. If they cannot meet these standards, remediation measures must be agreed upon before any data sharing begins.

---

3. Data Handling and Protection

Vendors are required to collect, process, and store data only for the purposes explicitly stated in the contract. All personal or sensitive information must be encrypted during transmission and storage. If a vendor is providing payroll services, the employee records they receive must not be used for any purpose other than salary disbursement and reporting.

A practical scenario could involve a payroll vendor who wants to use anonymized data for statistical analysis. In this case, the vendor must first seek written approval, demonstrate that the anonymization process is irreversible, and confirm that the analysis does not expose any personal identifiers.

---

4. Access Control and Authentication

Access to our systems or shared platforms must follow the principle of least privilege. Vendors must assign accounts only to personnel who require access to perform contracted duties, and such access must be removed immediately once the individual no longer requires it.

For instance, if a software vendor is contracted to perform a one-time system upgrade, temporary accounts must be created with time-bound access. Once the work is completed, those accounts must be revoked without delay. Shared accounts are not permitted, and multi-factor authentication must be enforced for any remote access.

---

5. Network and System Security

Vendors who provide technology solutions must ensure their infrastructure is adequately protected against malware, ransomware, and other cyber threats. Firewalls, intrusion detection systems, and endpoint protection must be active and regularly updated.

Consider a vendor hosting a customer support platform. If a zero-day vulnerability is identified in their system, they must immediately apply emergency patches, monitor for indicators of compromise, and communicate the incident and remediation steps to us. This allows our teams to assess the downstream risks and implement protective measures internally.

---

6. Incident Reporting and Breach Notification

In the event of a security incident or data breach, vendors must notify us without undue delay, but no later than seventy-two (72) hours after discovery. The notification must include the nature of the incident, categories of data affected, and remediation steps taken.

For example, if a vendor providing document management services discovers unauthorized access to stored contracts, they must immediately alert us with details of how the breach occurred, what data was accessed, and the measures being implemented to prevent recurrence. Failure to notify within the agreed timeline will be considered a material breach of contract.

---

7. Subcontracting and Third-Party Dependencies

If a vendor intends to engage subcontractors to perform part of the contracted services, they must disclose this arrangement in advance. Subcontractors are required to comply with the same security obligations outlined in these guidelines.

Suppose a logistics vendor contracts a smaller delivery company to handle shipments. That subcontractor must follow the same requirements for secure data handling and physical asset

protection as the primary vendor. Responsibility for compliance remains with the original vendor, regardless of delegation.

---

8. Compliance with Legal and Regulatory Standards

All vendors must comply with applicable data protection and security laws, including but not limited to GDPR, CCPA, HIPAA, and the Privacy Act (NZ), depending on the jurisdiction of operation. Vendors must also adhere to industry-specific regulations relevant to the services provided.

As an example, a healthcare technology vendor managing patient data must comply with HIPAA in the United States and equivalent local privacy legislation in other regions. Failure to meet these obligations could lead to regulatory penalties, for which the vendor will be held accountable.

---

9. Termination and Data Return or Destruction

Upon termination of the contract, vendors must securely return or destroy all data provided during the engagement. The method of destruction must be verifiable and irreversible, and a certificate of data destruction must be provided where appropriate.

For instance, if an IT vendor maintained backup services, at the end of the engagement they must delete all stored backups and confirm through an attestation letter that no residual data remains on their systems. Retention beyond the contract period is not permitted unless mandated by law, and in such cases, vendors must continue to protect the data under these guidelines.

---

10. Continuous Monitoring and Audits

Vendors must accept that we reserve the right to conduct security audits or request independent audit reports to verify compliance. These may include on-site assessments or reviews of SOC 2 Type II reports.

A realistic scenario could involve a vendor providing software-as-a-service (SaaS) tools. During an audit, they may be asked to share penetration test results, access logs, and evidence of patch management. Vendors unable or unwilling to provide this evidence will be considered non-compliant and subject to corrective actions, which may include suspension of the partnership.

---

11. Enforcement and Accountability

Failure to adhere to these guidelines may result in corrective measures, including contract suspension or termination. Vendors are contractually liable for damages or losses caused by their failure to protect data or maintain adequate security measures.

For example, if a vendor fails to patch a known vulnerability that results in the theft of customer information, they may be held responsible for covering the cost of remediation, regulatory fines, and reputational damages incurred by our organization.