Vendor Management Policy

Doorway

SOC 2 Criteria: CC2.3, CC3.2, CC3.3, CC3.4, CC4.1, CC4.2, CC6.4, CC9.2, P6.2, P6.4
ISO 27001 Annex A: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2

Keywords: Vendors, SOC report review, 3rd party applications, Vendor contracts

---

Purpose

The purpose of this policy is to establish requirements for ensuring third-party service providers/vendors meet Doorway requirements for preserving and protecting Doorway information.

Scope

The policy applies to all IT vendors, partners and human resource platform integrations who have the ability to impact the confidentiality, integrity, and availability of Doorway's technology and sensitive information, or who are within the scope of Doorway's information security program. This policy also applies to all employees and contractors that are responsible for the management and oversight of IT vendors, partners and human resources platform integrations of Doorway.

Background

This policy prescribes the minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

Roles and Responsibilities

The Security Officer is responsible for updating, reviewing, and maintaining this policy.

Policy

Doorway makes every effort to assure all 3rd party organisations are compliant and do not compromise the integrity, security, and privacy of Doorway or its customer data. 3rd parties include customers, partners, human resources platform integrations, subcontractors, and contracted developers.

- IT vendors are prohibited from accessing Doorway's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.
- All IT vendors must comply with the security policies defined and derived from Doorway's Information Security Program to include the *Acceptable Use Policy*.
- IT vendors, partners and human resources platform integrations must ensure that organisational records are protected, safeguarded, and disposed of securely. Doorway strictly adheres to all applicable legal, regulatory and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally-Identifiable Information (PII).
- Doorway may choose to audit IT vendors, partners and human resources platform integrations to ensure compliance with applicable security policies, as well as legal, regulatory and contractual obligations.

Vendor Inventory

An inventory of third party service providers shall be maintained, and the inventory will include:

- Vendor risk level
- Types of data shared with the third party
- Brief description of services
- Main point of contact at the third party
- How access is granted to the third party vendor
- Significant controls in place
- Security report and/or questionnaire

Vendor risk level assessment will be based on the following considerations:

- **High**: the vendor stores or has access to sensitive data and a failure of this vendor would have critical impact on your business
- **Moderate:** the vendor does not store or have access to sensitive data and a failure of this vendor would not have critical impact on your business
- **Low:** the vendor doesn't store or have access to any data and a failure of this vendor would have very little to no impact on your business

Vendor Contracts

Formal contracts that address relevant security and privacy requirements must be in place for all third parties that process, store, or transmit confidential data or provide critical services. The following must be included in all such contracts:

- Contracts will acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits;.
- Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party.

- Contracts identify information security policies relevant to the agreement.
- Contracts establish training and awareness requirements for specific procedures and information security requirements.
- Contracts identify relevant regulations for sub-contracting.
- Contracts implement a monitoring process and acceptable methods for validating the adherence to security requirements of delivered information and communication technology products and services.
- Contracts implement specific processes for managing information and communication technology component lifecycle and availability and associated security risks.
- Contracts identify and outline use of key controls to ensure the protection of organisational assets – e.g. physical controls, controls for protection against malicious code, physical protection controls, controls to protect integrity, availability and confidentiality of information, controls to ensure the return or destruction of information assets after their use, controls to prevent copying and distributing information.
- Contracts define information security requirements and identify the owner of information and how intellectual property rights are regulated.
- Contracts identify the recourse available to Doorway should the third party fail to meet defined security requirements~~;~~.
- Contracts establish responsibilities for responding to direct and indirect security incidents including timing as defined by service-level agreements (SLAs~~);~~).
- Contracts specify the security requirements for the return or destruction of data upon contract termination~~;~~.
- Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract.
- Contracts stipulate geographic limits on where data can be stored or transmitted.
- Contracts stipulate that data imported from human resources platform integrations adheres by Doorway's *Code of Conduct policy*.

Vendor Services Change Management

Changes to the provision of services by vendors, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of business information criticality, systems and processes involved and re-assessment of risks. The following aspects will be considered:

- Changes to supplier agreements;
- Changes made by the organisation to implement:
    - Enhancements to the current services offered;
    - Development of any new applications and systems;
    - Modifications or updates of the organisation’s policies and procedures;
    - New/changed controls to resolve security incidents and improve security.
- Changes in supplier services to implement:
    - Changes and enhancement to networks;
    - Use of new technologies;
    - Adoption of new products or newer versions/releases;
    - New development tools and environments;
    - Changes to physical location of service facilities;
    - Change of suppliers;
    - Subcontracting to another supplier.

Revision History

Version	Date	Editor	Description of Changes
1.0	17.03.2022	Henry Sinclair	Initial Creation
2.0	13.10.2022	Hugh Fraser	Inclusion of HR platform integration specifications