SECURE PROCUREMENT POLICY

Document Owner: Jamil Alio

Effective Date: August 2024

Version: 1.0

Document Approver: Rikan Patel

Table of Contents

OVERVIEW AND SCOPE

Overview

This document sets forth Business 2 Business's key policy procedures related to the secure onboarding of new IT vendors and installing new software on Company endpoints. This policy ensures the procurement process must be fully managed to ensure that any new security risks must be addressed, as well as compatibility with current systems must be always maintained.

Purpose

This policy and its supporting procedures are designed to provide Business 2 Business with a documented and formalised set of standards, procedures and restrictions for the secure onboarding of new IT vendors and the installation of new software on Company endpoints.

Scope

This Policy and supporting procedures cover all system components within the sensitive data environment that are owned, operated, maintained, and controlled by Business 2 Business and all other system components, both internally and externally, that interact with these systems, and all other relevant systems.

- Internal system components are those owned, operated, maintained, and controlled by Business 2 Business and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system components deemed in scope.

- External system components are those owned, operated, maintained, and controlled by any entity other than Business 2 Business, but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the sensitive data environment and any other environments deemed applicable.

Please note that when referencing the term "system component(s)" or “system resource(s)” it implies the following: Any network component, server, or application included in or connected to the sensitive data environment, or any other relevant environment deemed in-scope for purposes of information security.

ROLES AND RESPONSIBILITIES

The following roles and responsibilities regarding secure procurement management practices are to be developed and subsequently assigned to authorised personnel within Business 2 Business:

- **Risk Committee**: Responsibilities include approving and monitoring adherence to this policy. Additionally, the Risk Committee reviews the results from the annual reviews of critical vendors, used software and approves the termination of critical software components.

- **Chief Executive Officer (CEO):** Responsibilities include managing critical vendors throughout the life cycle of their relationship with Business 2 Business, which includes:
    - Reviewing and approving the selection of critical vendors and their contracts before execution.
    - Reviewing and approving requests to initiate searches for new vendors.
    - Conducting risk assessments and initial due diligence of potential new vendors.
    - Reporting the results of periodic monitoring of suppliers to the Risk Committee

.

    - Completing the new vendor off-boarding checklist after termination.
    - Maintaining the master supplier list.

- **Business Owner:** Responsibilities include identifying the need for a vendor, creating and proposing the business case to the CEO for approval, assisting the CEO in conducting risk assessments and initial due diligence of potential suppliers and managing supplier(s) on a day-to-date basis. As appropriate, the Business Owner will escalate performance-related issues of suppliers.

- **Vendors, Contractors, Other Third-Party Entities:** Responsibilities for such individuals and organisations are much like those stated for end-users: adhering to the organisation's policies, procedures, practices, and not undertaking any measure to alter such standards that protect client data. Additionally, vendors, contractors, and other third-party entities are expected to complete due diligence and ongoing monitoring assessments per the requirements set forth in the Policy. Vendors, contractors, and other third-party entities are required to immediately notify Business 2 Business of any policy violations involving client data.

SUPPLIER RISK MANAGEMENT POLICY

Supplier Risk Management Lifecycle

Effective risk management of suppliers' entails oversight and monitoring throughout the lifecycle of the company's relationships with them. In general, the supplier risk management lifecycle is comprised of:

- Identifying a business need for a service.
- Conducting a risk assessment of the proposed supplier relationship.
- Performing initial due diligence of suppliers.
- Negotiating and entering into contracts with suppliers.
- Monitoring suppliers on an ongoing basis.
- Managing to remediate issues related to suppliers.
- Terminating relationships with suppliers, as appropriate.

Company-wide adherence to a defined framework of risk mitigating controls enables us to assess, manage, and mitigate the risks a supplier presents from initial assessment through termination. The following sections outline the specific controls in each element of the supplier risk management lifecycle. The supplier's risk rating determines our execution, including intensity and frequency, of these controls.

Need Identification

Business needs for suppliers must be legitimate, within budget, and in the company's best interests. The Business Owner is an employee who has identified this need and would manage the day-to-day relationship with the supplier. The Business Owner proposes the business case to the CEO (or someone to whom he/she has delegated this authority) who will decide whether to authorise engaging potential suppliers.

Risk Assessment

After we identify a need, risk assessments provide insight into our decision to establish a supplier relationship. The CEO ensures that assessments are thorough, accurate, and fair.

Using a defined methodology, the CEO, with input from the Business Owner, assesses a potential supplier to evaluate its criticality and riskiness. Relevant assessment criteria may include but need not be limited to the supplier's expertise, experience, and reputation, the nature, and necessity of the service, whether a supplier needs access to Sensitive or Confidential data, the supplier's security infrastructure, and the supplier's level of contact with customers.

The risk assessment results in a risk rating - critical, high, or low - for the supplier. (See Appendix A for rating definitions). A supplier's risk rating determines the level and intensity of initial due diligence and ongoing monitoring of a supplier. It also facilitates management's ability to appropriately manage process dependencies on suppliers and quickly identify which suppliers have access to sensitive or confidential data.

Initial Due Diligence

Before entering into a contract with a potential supplier, the CEO, with input from the Business Owner, conducts due diligence reviews to verify the ability of the supplier to meet Business 2 Business's needs in a safe and compliant manner. A supplier's risk rating determines the scope and depth of supplier due diligence. As a general matter, our evaluation focuses on a potential supplier's technical and industry expertise, control environment, and operational and logistical matters (e.g., location).

Due diligence results inform our decision to contract a potential supplier. They detail the qualitative and quantitative aspects of potential suppliers to determine if a relationship would help achieve our identified need without introducing incremental risks. The CEO reviews and approves all high and critical suppliers.

Contracting

In addition to the management approvals, entering into a business relationship with a supplier requires a written contract recording the agreement. Contractual provisions depend on the type of service and the supplier's risk rating. Contracts should include clear and concise language regarding the arrangement between Business 2 Business and the supplier, covering such topics as:

- Scope of services and duration;
- Performance standards and reporting against these standards;
- Cost, compensation, or fee structure;
- Rights, responsibilities, and remedies of each party;
- Non-disclosure agreements;
- Protection of intellectual property;
- Security and confidentiality, including the requirement to comply with our Information Security Policy (as appropriate) when accessing our local or remote network and handling and storing any Company or customer data;
- Obligations and timeframes for reporting cybersecurity incidents;
- Business continuity and disaster recovery planning;
- Other internal controls (e.g., records retention, insurance); and
- Terms for recourse should a supplier not meet contractual terms.

Before execution and at renewal, the CEO reviews all contracts with all critical and high-risk suppliers and ensures that they include the required contractual terms. (See Contract Provisions and Considerations Document). Corporate officers have the sole authority to enter into contracts on behalf of the company. Any requested changes to a supplier's contract, whether regarding availability, the scope of services, etc., must take into account the criticality of the supplier's services to Business 2 Business's operations and go through the Change Control Process.

Ongoing Monitoring

We are responsible for maintaining the adequacy and quality of the services our suppliers provide on our behalf, and for managing the risks of such services. In order to meet this responsibility, we continue to monitor our contractors after contract execution. Monitoring can include many activities, ranging from service level performance checks to information security assessments, resiliency reviews, and control documentation requests. Additionally, the Business Owner may identify matters relating to the supplier's performance or risk levels through regular interactions with a supplier and should escalate critical or important matters to the appropriate parties.

The frequency and scope of ongoing monitoring are risk-based and commensurate with the nature of the services the supplier provides:

- **Critical suppliers:** At least annually, we review critical suppliers and our contracts with them. Additionally, we review vendor questionnaires or compliance reports, as applicable, to assess potential impacts to our business and document the results. If a critical supplier stores or accesses sensitive or confidential data, our assessment must cover the supplier's adherence to our Information Security Policy at a minimum.

- **High-risk suppliers:** We review high-risk suppliers at least once every two years or as needed after a material event, such as restructuring of the supplier or a change in the activities handled by the supplier.

- **Low-rated suppliers:** We review low-risk suppliers as needed after a material event.

The CEO, or a delegate, reports results of reviews of critical suppliers to the Risk Committee and all suppliers to the CEO, including risks and performance issues identified, remedial steps, and materials changes to supplier risk ratings, contracts, and scope of services.

Issue Management

If an employee, customer, or other third party identifies an issue related to or about our supplier's conduct or the services it provides on our behalf, we assess the issue, prioritise the issue based on impact and urgency, develop an action plan, and assign an owner, and track resolution of plans. As appropriate, we escalate supplier-related issues to customers according to a timeline commensurate with the issue, severity, or service-level standards delineated in contracts with customers.

Termination

When terminating a contract with a supplier, we look to minimise operational impact, protect customer and corporate assets and data, and communicate service changes appropriately to relevant internal and external parties. The CEO completes a supplier off-boarding checklist that covers, as appropriate, destruction or return of internal and customer data, removal of system access rights, and transition plans. We require additional actions for terminating critical or high-risk suppliers.

Master Supplier List

The CEO is responsible for maintaining a master list of all company suppliers in a secure location on our shared folder. The master list is a centralised repository that assists with assessing our overall supplier risk level, ensuring we perform periodic assessments on schedule in accordance with this Policy, and streamlining our operational processes. For each supplier, the master list should include, as applicable: contact name, service provided, risk rating, the level of information classification to which the vendor has access, the date of last periodic review, and any relevant contract details (e.g., start and end dates, attachment to executed contract).

POLICY ADMINISTRATION

Ownership and Review

The Policy Owner owns this Policy and is responsible for reviewing the Policy for updates annually or following any major changes to Business 2 Business's sensitive data environment. The Policy Approver retains approving authority over this Policy.

Monitoring and Enforcement

Business 2 Business periodically monitors adherence to this Policy to help ensure compliance with applicable laws, requirements, and contractual agreements that apply to Client & Consumer Data. Business 2 Business may also establish enforcement mechanisms, including disciplinary actions, to help ensure compliance with this Policy.

Related Documents

- Information Security Policy.

APPENDIX A – CRITERIA FOR SUPPLIER RISK RATINGS

Business 2 Business suppliers have risk rating criteria that consist of the following:

Rating	Criteria
Critical	· Daily operations significantly depend on the service. Failure or significant impairments would halt or seriously disrupt business processes. · Supplier provides a service critical to develop, support, and secure our services. · Supplier accesses, handles, and stores sensitive or confidential data (internal and customer). · Replacing the supplier would be extremely difficult and costly.
High	· Daily operations regularly incorporate but do not depend on the service. Failure or significant impairments to this service would impair, but not prevent or seriously disrupt, business processes. · Supplier provides a service to develop, support, and secure our services, although the service is not a critical function. · Supplier accesses, handles, and stores sensitive or confidential data (internal and customer). · Replacing the supplier would be moderately difficult and costly.
Medium	· Operations use the service regularly but unevenly (e.g., not every day or not every user). Failure or significant impairments to this service would present challenges to, but not disrupt, business processes. · Supplier provides a service to partially develop, support, and secure our services, although the service is not a critical function.

	· Supplier partially accesses, handles, and stores sensitive or confidential data (internal and customer). · Replacing the supplier would take effort and some money.
Low	· Operations use the service regularly but unevenly (e.g., not every day or not every user). Failure or significant impairments to this service would present challenges to, but not disrupt, business processes. · Supplier knows about our pipeline of customers but has no access to sensitive or confidential data. · Replacing the supplier would take effort and some money.