SandBox Union

Third Party Assurance

Table of Contents

1. Introduction
2. Purpose
3. Scope
4. Policy Sections
   - 4.1 Identification of Risks Related to External Parties
   - 4.2 Addressing Security When Dealing with Customers
   - 4.3 Addressing Security in Third Party Agreements
   - 4.4 Service Delivery
   - 4.5 Monitoring and Review of Third-Party Services
   - 4.6 Outsourced Software Development
5. Related Policies
6. Related Procedures
7. Revision History

1. Introduction

SandBox Union has multiple third-party service providers and vendors including both upstream third parties and downstream third parties. Additional security and due diligence is needed for upstream and downstream third parties because they have the potential to access SandBox Union systems and data.

2. Purpose

The purpose of this Third Party Assurance policy is to protect SandBox Union systems and data when interacting and connecting with third party service providers. SandBox Union performs due diligence and signs contracts/BAAs/SLAs prior to establishing any relationship with third parties.

3. Scope

This Third Party Assurance policy and related policies, standards, and procedures will apply to all SandBox Union full-time, part-time; temporary and intern employees, contractors, sub-contractors, consultants, affiliates, and any individuals or companies utilizing SandBox Union provided IT equipment, computers, and/or networks or have access to the data environment, including any third-party contracted by SandBox Union to handle, process, transmit, store, or dispose of SandBox Union's data. This includes external partners or suppliers who have access to, or are responsible for, SandBox Union's information regardless of its form or medium.

4. Policy Sections

4.1 Identification of Risks Related to External Parties

Due diligence, including an evaluation of the information security risks posed by external parties, shall be carried out to identify any requirements for specific controls where access to sensitive information (e.g., covered information, cardholder data) by external parties is required prior to establishing a formal relationship with the service provider. Access by external parties to the organization's information will not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. All security requirements resulting from work with external parties or internal controls shall be reflected by the agreement with the external party. It shall be ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets.

All remote access connections between the organization and all external parties shall be secured via encrypted channels (e.g., VPN). Any covered information shared with an external party will be encrypted prior to transmission.

External parties shall be granted minimum necessary access to the organization's information assets to minimize risks to security. All access granted to external parties will be limited in duration and revoked when no longer needed.

The identification of risks related to external party access shall take into account the following issues:

(i) the information asset(s) an external party is required to access;
(ii) the type of access the external party will have to the information and information asset(s), such as:
(a) physical access (e.g. to offices, computer rooms, filing cabinets),
(b) logical access (e.g. to an organization's databases, information systems),
(c) network connectivity between the organization's and the external party's network(s) (e.g. permanent connection, remote access), and
(d) whether the access is taking place on-site or off-site;
(iii) the value and sensitivity of the information involved, and its criticality for business operations;
(iv) the controls necessary to protect information that is not intended to be accessible by external parties;
(v) the external party personnel involved in handling the organization's information;
(vi) how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed;
(vii) the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information;
(viii) the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information;
(ix) practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident;
(x) legal and regulatory requirements and other contractual obligations relevant to the external party are considered; and
(xi) how the interests of any other stakeholders may be affected by the arrangements.

4.2 Addressing Security When Dealing with Customers

The following security terms shall be addressed prior to giving customers access to any of the organization's assets:

(i) description of the product or service to be provided;
(ii) the right to monitor, and revoke, any activity related to the organization's assets; and,
(iii) the respective liabilities of the organization and the customer.

It shall be ensured that the customer is aware of their obligations, and accepts the responsibilities and liabilities prior to accessing, processing, communicating, or managing the organization's information and information assets.

4.3 Addressing Security in Third Party Agreements

The following terms shall be implemented for inclusion in the agreement in order to satisfy the identified security requirements:

(i) the information security policy;
(ii) controls to ensure asset protection;
(iii) user and administrator training in methods, procedures, and security;

(iv) ensuring user awareness for information security responsibilities and issues;
(v) provision for the transfer of personnel, where appropriate;
(vi) responsibilities regarding hardware and software installation and maintenance;
(vii) a clear reporting structure and agreed reporting formats;
(viii) a clear and specified process of change management;
(ix) access-control policy(ies);
(x) arrangements for reporting, notification (e.g., how when and to whom), and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement;
(xi) a description of the product or service to be provided, and a description of the information to be made available along with its security classification;
(xii) the target level of service and unacceptable levels of service;
(xiii) the definition of verifiable performance criteria, their monitoring and reporting;
(xiv) the right to monitor, and revoke, any activity related to the organization's assets;
(xv) the right to audit responsibilities, defined in the agreement, to have those audits carried out by a third-party, and to enumerate the statutory rights of auditors;
(xvi) the penalties exacted in the event of any failure in respect of the above;
(xvii) the establishment of an escalation process for problem resolution;
(xviii) service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities;
(xix) the respective liabilities of the parties to the agreement;
(xx) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g. data protection legislation) especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries;
(xxi) intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work; and
(xxii) conditions for renegotiation/termination of agreements.

SandBox Union shall identify and mandate information security controls to specifically address supplier access to the organizations information and information assets.

Agreements shall include requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain. SandBox Union shall maintain written agreements (contracts) that include an acknowledgement that the third party (e.g., service provider) is responsible for the security of the data the third party possesses or otherwise stores, processes or transmits on behalf of the organization, or to the extent that they could impact the security of the organizations information environment.

Agreements shall ensure that there is no misunderstanding between the organization and the third party. SandBox Union shall satisfy themselves as to the indemnity of the third party.

SandBox Union shall establish personnel security requirements including security roles and responsibilities for third-party providers that are coordinated and aligned with internal security roles and responsibilities.

SandBox Union shall ensure a screening process is carried out for contractors and third-party users. Where contractors are provided through an organization, (i) the contract with the organization shall clearly specifies the organizations responsibilities for screening and the notification procedures they need to follow if screening has not been completed, or if the results give cause for doubt or concern, and (ii) in the same way, the agreement with the third-party clearly specifies all responsibilities and notification procedures for screening.

4.4 Service Delivery

Service level agreements (SLAs) or contracts with an agreed service arrangement shall address liability, service definitions (e.g., reliability, availability and response times for the provision of services), security controls, and other aspects of services management (e.g., monitoring, auditing, impacts to the organization's resilience, and change management).

4.5 Monitoring and Review of Third-Party Services

A periodic review of service-level agreements (SLAs) shall be conducted at least annually and compared against the monitoring records.

4.6 Outsourced Software Development

Outsourced software development contracts shall address licensing arrangements, code ownership, intellectual property rights, certification and rights of access for the audit of the quality and accuracy of work, escrow arrangements, quality and security functionality requirements for the developed code, and security testing and evaluation prior to installation.

5. Related Policies

- [Insert related policies]

6. Related Procedures

- [Insert related procedures]

7. Revision History

Version	Date	Approved By	Change Description
1.0	01/22/2021	Joseph Organisciak	