A-LIGN

TokenEx, Inc.

Type 2 SOC 3

2022

TOKENEX®

A-LIGN.COM

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 1, 2021 to March 31, 2022

Table of Contents

SECTION 1

ASSERTION OF TOKENEX, INC. MANAGEMENT

ASSERTION OF TOKENEX, INC. MANAGEMENT

April 30, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within TokenEx, Inc.'s ('TokenEx' or 'the Company') Tokenization Platform System throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that TokenEx's service commitments and system requirements relevant to Security, Availability, and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "TokenEx, Inc.'s Description of Its Tokenization Platform System throughout the period April 1, 2021 to March 31, 2022" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that TokenEx's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). TokenEx's objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "TokenEx, Inc.'s Description of Its Tokenization Platform System throughout the period April 1, 2021 to March 31, 2022".

TokenEx uses Microsoft Azure ('Azure' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TokenEx, to achieve TokenEx's service commitments and system requirements based on the applicable trust services criteria. The description presents TokenEx's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TokenEx's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve TokenEx's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of TokenEx's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2021 to March 31, 2022 to provide reasonable assurance that TokenEx's service commitments and system requirements were achieved based on the applicable trust services criteria.

Jeffrey Rudd
CFO
TokenEx, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: TokenEx, Inc.

Scope

We have examined TokenEx, Inc.'s ('TokenEx' or 'the Company') accompanying description of Tokenization Platform System titled "TokenEx, Inc.'s Description of Its Tokenization Platform System throughout the period April 1, 2021 to March 31, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that TokenEx's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

TokenEx uses Azure to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TokenEx, to achieve TokenEx's service commitments and system requirements based on the applicable trust services criteria. The description presents TokenEx's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TokenEx's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TokenEx, to achieve TokenEx's service commitments and system requirements based on the applicable trust services criteria. The description presents TokenEx's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TokenEx's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

TokenEx is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that TokenEx's service commitments and system requirements were achieved. TokenEx has provided the accompanying assertion titled "Assertion of TokenEx, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. TokenEx is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within TokenEx's Tokenization Platform System were suitably designed and operating effectively throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that TokenEx's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on TokenEx's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of TokenEx, user entities of TokenEx's Tokenization Platform during some or all of the period April 1, 2021 to March 31, 2022, business partners of TokenEx subject to risks arising from interactions with the Tokenization Platform, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
April 30, 2022

SECTION 3

TOKENEX, INC.'S DESCRIPTION OF ITS TOKENIZATION PLATFORM SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2021 TO MARCH 31, 2022

OVERVIEW OF OPERATIONS

Company Background

TokenEx was founded in 2010 with the objective of helping clients secure their most sensitive data through the tokenization platform. Tokenization is the replacement of sensitive data with nonsensitive tokens. TokenEx is a privately-held company headquartered out of Edmond, Oklahoma with offices in Tulsa, Oklahoma.

The TokenEx system is an open integration cloud-security platform that gives customers the freedom and flexibility to secure datasets while maintaining integrations with service providers, partners, and vendors. TokenEx serves industries that handle Payment Card Industry (PCI) data, personally identifiable information (PII), Automated Clearing House (ACH) payments, protected health information (PHI), nonpublic information (NPI), and structured, unstructured, or other data sets. The platform ensures data is available when customers need it. TokenEx continually strives to enhance redundancy, availability, and scalability to meet customers' needs.

Top Industries served by TokenEx include: Payments, Retail, Travel and Insurance.

Description of Services Provided

Because TokenEx has a diverse customer base, solutions support a variety of data acceptance channels and data storage methods to ensure sensitive data entering and leaving the customer environment can be secured. The TokenEx platform is omnichannel and interface agnostic.

Application Program Interface (API)

With the TokenEx API, a customer's webpage or application sends a call to the TokenEx application server using industry standard encryption. This method allows customers to tokenize, detokenize, delete, or validate a token. For PCI data, TokenEx also supports multiple methods for customers to send a payment transaction to a payment processor. This allows customers to avoid storing or interacting with sensitive data in their environments. Sensitive data stored in the TokenEx environment is encrypted at rest. Tokenized data cannot be detokenized without a valid key for detokenization and a specific TokenEx ID. The ability to detokenize can be allowed or disallowed based upon the customer's request. The ability to modify, allow, or disallow API key assignment is limited to authorized TokenEx support staff. Transmissions are supported using secure protocols.

Managed File Transfer

TokenEx supports secure batch file transmissions for customers who have large volumes of data to be processed, batch transactions in place with processors, or share files with third-party partners. The customer (or another third-party) sends batch files containing sensitive data or tokens via Secure File Transfer Protocol (SFTP). Data transmitted to TokenEx is transmitted through secure protocols and whitelisted Internet protocol (IP) addresses. Batch files are processed in memory to be tokenized or detokenized.

Encrypted Devices

For TokenEx customers that use payment card pin pads as a data acceptance channel, TokenEx accepts and decrypts data from these devices. The encrypted data is sent to TokenEx, decrypted by a Security Module, and sent through the standard processes for tokenization.

iFrame

To further reduce compliance scope and risk, TokenEx offers hosted tokenization through a customizable iFrame. This solution allows for end users to enter sensitive data through a TokenEx hosted iFrame included as part of the customer's website and is designed to be customizable to ensure the added security is transparent to the end user.

Customer Portal

The TokenEx portal provides customer visibility into details about their transaction usage, total token counts, and outage details, as well as links to development documentation and the TokenEx support tickets. Communication through the portal is secure and encrypted. Users with administrative credentials can also view and manage credentials and whitelisted IPs. Access to the portal requires multi-factor authentication (MFA).

Principal Service Commitments and System Requirements

TokenEx designs its processes and procedures related to the system to meet its objectives for its tokenization services. These objectives are based on the service commitments TokenEx makes to its user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that TokenEx has established in relation to tokenization services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the Privacy Policy and terms of service available on the TokenEx website.

TokenEx establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in TokenEx's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, hoe the system is operated, how the internal business systems and networks are manages, and ow employees are hired and trained. In addition to these policies, standard operating procedures document how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System

Infrastructure

Primary infrastructure used to provide TokenEx's Tokenization Platform system is Azure virtual machines (VMs).

Software

Primary software used to provide TokenEx's Tokenization Platform system includes Windows, Linux as the host Operating System, CrowdStrike for Endpoint detection and response and Qualys for Vulnerability Scanning.

People

TokenEx's organizational structure provides the overall framework for planning, directing, developing, and controlling operations. Personnel and business functions are separated as needed, and access and roles are clearly defined. This structure is defined to provide for clear communication and effective segregation of duties.

Regular staff meetings are held throughout the Company to discuss current projects, customers, and industry activity. Cross departmental executive leadership meetings are held at least monthly to ensure open communication and strategic planning across the Company.

New-hire checklists are utilized to track the onboarding process, which includes reference verification and extensive background checks prior to employment. Screenings for new employees who will have access to customer data include searches for social security number validation, national/federal criminal database, traffic violations, sex offender registry, domestic terror watchlist, county criminal court, as well as education and employment verifications.

TokenEx ensures new hires complete security awareness training, and review and acknowledge the TokenEx Acceptable Use Policy (AUP) and Company Handbook, which includes the Ethical Business Policy. New employees are also required to sign Nondisclosure Agreements (NDA) upon hire. Other applicable company policies are made available to personnel and are formally acknowledged on an annual basis. System description materials are defined and available to users who interact with the system and how-to guides are defined for employees who support the operation of the system. New employees are trained on the operation of the system to ensure they are qualified to perform their job responsibilities.

Data

TokenEx classifies data into three levels:

- High Risk: Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure
- Confidential: Data that would not expose TokenEx to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure
- Public: Information that may be freely disseminated

TokenEx treats customer data, as well as payroll, personnel, and financial information, as high risk. Because this data represents the main business of TokenEx services, customer data is subject to TokenEx policies - specifically those that address security and confidentiality. TokenEx also has procedures for the destruction of confidential information and disposes of confidential information in accordance with the terms listed in its agreements with its customers.

The Data Retention and Classification Policy establishes standards for the classification, retention, and disposal of data and is reviewed annually. The Media Storage and Distribution Policy establishes procedures for the storage and destruction of confidential data and is reviewed annually.

TokenEx information technology (IT) and support groups are responsible for the overall availability of data, including system backups, system monitoring, data processing, as well as identifying and resolving issues. Confidential information transmitted beyond the boundaries of the system via API request is specifically approved by the customer. As data flows from customers to TokenEx, and in some cases on to trusted third parties, data is encrypted while in transit, as well as when at rest. TokenEx does not transfer production data to test or development environments. TokenEx utilizes industry standard best practices to obtain test data. Service agreements specify that customers are not permitted to use production data in the test environment.

Processes, Policies and Procedures

The processes and procedures that make up the TokenEx system are an integral part of how the Company operates and provides services. Employees are encouraged to remain vigilant and raise security issues or suspicious activities as they arise.

TokenEx security policies are updated, reviewed, and approved annually. Most TokenEx policies cover some aspect of data security, while maintaining continuous availability of the platform. The Information Privacy and Security Program and supporting policies define the information security requirements for the Company. The Access Control Policy establishes access requirements for the TokenEx environment including password parameters and user account provisioning processes. The Key Management Policy defines how security keys are generated, handled, managed, and stored. Additional control procedures at TokenEx related to the administration and operation of its applications are defined and periodically reviewed in policies that cover the following categories:

- Logical Security
- Physical and Environmental Safeguards
- Network Maintenance
- Application Change Management
- Bring Your Own Device (BYOD)
- Backup and Availability
- Customer Ticketing and Incident Management
- Customer Implementation
- Confidentiality

Physical Security

Physical access to the production environment is limited and controlled by TokenEx's cloud provider. The cloud provider maintains policies and procedures to govern the issuance and maintenance of physical access privileges. Please see the “Subservice Organizations” section below for a detailed listing of controls owned by Azure.

Computing infrastructure is stored in cages. Access to the cage/cabinet is controlled by the cloud provider and consists of biometric authentication plus proximity key. The cloud provider manages and monitors access to the cages and cabinets using cameras and periodically reviews a log of users accessing the cage. Visitors are not allowed access into the data center cages.

Logical Access

Separate environments are maintained for development, test, and production servers. Production systems are continually monitored, and access is restricted to authorized TokenEx employees or contractors. A privileged access management (PAM) solution is in place to manage role-based access to the systems and to provide additional monitoring capabilities. Users accessing the system are authenticated by strong, complex passwords. New access to the production environment requires approval and is provisioned and tracked with a ticket. Remote access to the system is limited to authorized personnel through a virtual private network (VPN), which requires MFA. Procedures are in place to monitor unauthorized access attempts to the production environment and timeouts are enabled to restrict the length of active sessions.

User access rights are reviewed after a change in job responsibilities. System, application, and database access rights are removed upon employee termination and reviewed annually. When a contractor leaves a TokenEx project, their access and accounts are removed immediately.

TokenEx services are monitored in real time and access activity is logged. Log information is accessible for real-time operational metrics. The data can be retrieved and reviewed as needed to maintain and troubleshoot the system.

Application-level access is granted to customers after they have tested their connectivity in the TokenEx test environment. New customers are approved and set up in the Customer Portal during the onboarding process. Subsequent customer requests for access modifications are managed by authorized customer representatives. Access to data is restricted to a pre-set, matching, and valid TokenEx ID and API key, as well as a customer-defined IP whitelist to successfully complete an API request. Native SFTP authentication to customer data is restricted by username, password, and IP whitelist. The system is configured to restrict customers from seeing other customers' data.

Computer Operations - Backups

Transactional replication as well as incremental and full backups are in place. TokenEx's performs system level backups including nightly volume-based snapshots for critical systems. Log data, databases, source code, and other high-priority data types are backed up, encrypted and securely stored. The automated backup system is configured to send e-mail alert notifications to IT personnel regarding the failure of backup jobs.

Computer Operations - Availability

Incident response procedures are approved by the governance, risk management and compliance (GRC) Committee and an annual tabletop exercise to test the Incident Response Plan. In the event of a security incident involving customer data, TokenEx commits to timely customer notification. Employees are instructed how to report failures, incidents, and concerns through acknowledgement of the Employee Handbook and AUP as well as periodic security awareness training.

The availability principle refers to the assurance that information and systems are available for operation and use to meet the Company's objectives. In relation to the TokenEx system, availability is dependent mainly on capacity monitoring and maintenance, data backup processes, and recovery infrastructure including test procedures. TokenEx has designed its control environment to address both internal and external availability risks specifically related to protection from environmental hazards, as well as the proper monitoring, maintenance, and utilization of backups and recovery activities. In evaluating the suitability of the design of availability controls, TokenEx considers availability commitments and requirements, as well as the likely causes of system down time and equipment damage.

Change Control

TokenEx maintains and follows a documented change management process. Changes and updates are made as necessary to the system and are documented and tracked in a ticketing system. Production releases are tested and approved by the Chief Technology Officer (CTO) prior to release to production. Changes are made available for customer testing prior to release to the production environment. For significant product changes, TokenEx has a third-party perform a security assessment prior to migration to production.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by TokenEx The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with TokenEx's policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by TokenEx These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based MFA system.

Boundaries of the System

The scope of this report includes the TokenEx system performed in the Tulsa, Oklahoma facility.

This scope of this report does not include the cloud hosting services performed by Azure at the various facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common Criteria / Security, Availability, and Confidentiality criterion was applicable to the TokenEx Tokenization Platform system.

Subservice Organizations

This report does not include the cloud hosting services provided by Azure at the various facilities.

Subservice Description of Services

TokenEx relies on Azure as a subservice organization to provide the third-party services listed below. These services are not included within the scope of this report. TokenEx relies on this subservice organization to design, implement, and operate suitable controls that, along with the TokenEx controls, achieve TokenEx's service commitments and system requirements based on the Security, Availability, and Confidentiality criteria.

Complementary Subservice Organization Controls

TokenEx's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to TokenEx's services to be solely achieved by TokenEx control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of TokenEx.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

TokenEx management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as service level agreements. In addition, TokenEx performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization
- Testing controls performed by vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

TokenEx's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to TokenEx's services to be solely achieved by TokenEx's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of TokenEx's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to TokenEx.
2. User entities are responsible for notifying TokenEx of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of TokenEx's services by their personnel.

5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize TokenEx services.
6. User entities are responsible for providing TokenEx with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying TokenEx of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

Privacy practices are maintained to ensure the collection, handling, processing, storage, validation, disclosure, retention, and disposal of PII is consensual and in accordance with specified purpose and applicable laws. C1.1, C1.2 13.d, 13.e, 13.f, 13.g, 13.h, 13.i, 13.j, 13.k, 13.l, 13.m, 13.n Data input to, processed in, and output from the system is validated for correctness and appropriateness.