TOKENEX
NO DATA. NO THEFT.

Control Number	Control Title	Description	Sophistication Level	Security Measures	Control Mapping
SO 01	Information Security Policy	The DSP establishes and maintains an information security policy. The document details information on main assets and processes, strategic security objectives.	3	The Information Security and Privacy Policy addresses the security and continuity of our platform. Supporting policies are place to document specific requirements for assets and processes. Policies are reviewed at least annually and after significant changes to the environment. Policies are updated to reflect internal or external change, security incidents and industry best practices. Employees acknowledge policies upon hire and annually. These policies define security requirements that employees must adhere to.	PCI DSS: 12.1, 12.1.1 CSA CCM: GRM-01, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09
SO 02	Risk Management	The DSP establishes and maintains an appropriate governance and risk management framework, to identify and address risks for the security of the offered services. Risks management procedures can include (but are not limited to), maintaining a list of risks and assets, using Governance Risk management and Compliance (GRC) tools and Risk Assessment (RA) tools etc.	3	TokenEx has implemented a risk management program based on industry best practice to assess risks to our platform and the support networks and assets. The risk management methodology is reviewed annually, taking into account changes and past incidents. Risk assessments are conducted at least annually and in the event of significant changes. Risks are identified, scored, and remediated. Risk assessment results. are distributed to applicable stakeholders.	PCI DSS: 12.2 CSA CCM: GRM-02, GRM-04, GRM-08, GRM-10, GRM-11, STA-01, STA-04, STA-04, STA-05, STA-06
SO 03	Security Roles	The DSP assigns appropriate security roles and security responsibilities to designated personnel. (i.e. CSO, CISO, CTO etc.	3	TokenEx has assigned security roles and responsibilities to designated personnel. A Governance, Risk, and Compliance Committee and subcommittees for security, privacy, vendor management, and compliance are in place. Teams have been established for incident response and business continuity/disaster recovery. TokenEx regularly reviews the structure of security roles and responsibilities and adjusts to reflect changes in the environment. TokenEx has 24x7x365 support available to respond to security incidents. Employees are trained annually on how to identify and report incidents.	PCI DSS: 12.4 CSA CCM: BCR-10, CCC-01, DSI-06, GRM-06, HRS-03, HRS-07, IAM-02, IAM-05, IAM-09, IAM-10, SEF-01, SEF02, SEF-03
SO 04	Third Party Management	The DSP establishes and maintains a policy with security requirements for contracts with suppliers and customers. SLAs, security requirements in contracts, outsourcing agreements etc., are established to ensure that the dependencies on suppliers and residual risks do not negatively affect security of the offered services.	3	Third party management policies and procedures are in place and are reviewed at least annually to reflect any changes and to continually improve our processes. All procurement of third party services or products follows our vendor management processes. This process includes a risk assessment and review of the third party's security posture. Security requirements are included in contracts with third-parties. Vendors are reviewed at least annually and following any changes or incidents. Any third party security incidents would be tracked.	PCI DSS: 12.8.3 CSA CCM: CCC-02, STA-01, STA-02, STA-03, STA-04, STA-05, STA-05, STA-06, STA-07, STA-08, STA-0
SO 05	Background Checks	The DSP performs appropriate background checks on personnel (employees, contractors and third party users) before hiring, if required, for their duties and responsibilities provided that this is allowed by the local regulatory framework. Background checks may include checking past jobs, checking professional references, etc.	3	Policy and procedures for background checks and reference checks are in place and reviewed at regular intervals, taking into account changes and past incidents. TokenEx performs background checks on all employees, including, at a minimum: SSN verification, academic credentials, employment history, Domestic Terror Watchlist and criminal history.	PCI DSS: 12.7 CSA CCM: HRS-020
SO 06	Security Knowledge & Training	The DSP verifies and ensures that personnel have sufficient security knowledge and that they are provided with regular security training. This is achieved through for example, security awareness raising, security education, security training etc.	3	TokenEx administers security and privacy awareness training upon hire and monthly for all employees. Training includes a validation of employee knowledge. The training program is continually reviewed and content is delivered based on TokenEx policies and procedures, industry trends, changes to the environment, and security incidents and events.	PCI DSS: 6.5, 9.9, 9.93, 12.6.1, 12.10.4 CSA CCM: HRS-08, HRS-09
SO 07	Personnel Changes	The DSP establishes and maintains an appropriate process for managing changes in personnel or changes in their roles and responsibilities.	3	All new hires are required to complete security training and to review TokenEx policies. TokenEx reviews access for personnel following changes in job function and revokes access rights, badges, and equipment, if no longer necessary or permitted. TokenEx has implemented policies and procedures for changes to personnel which include timely revocation of access rights, badges, and equipment for terminated employees. Policies and procedures are periodically evaluated for effectiveness and are updated as required to reflect any changes or past incidents.	CSA CCM: HRS-04
SO 08	Physical Security	The DSP establishes and maintains policies and measures for physical and environmental security of datacenters such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc.	3	TokenEx reviews our IaaS provider's security and compliance reports to ensure secure requirements are being met. Our IaaS provider is responsible for the physical security controls to protect TokenEx systems and data, including: Prevent unauthorized physical access to facilities and infrastructure and set up environmental controls, to protect against unauthorized access, burglary, fire, flooding, etc.; A list of personnel with authorized access to facilities containing information systems and appropriate authorization credentials (e.g., badges, identification cards) is maintained by the organization; Visitors are authenticated before authorizing access to the facility; Data center environmental conditions (e.g., water, power, temperature and humidity controls) shall be secured, monitored, maintained, and tested to ensure protection from unauthorized interception or damage; Implement a policy for physical security measures and environmental controls; Document procedure for emergency cases; A designated official within the organization to review and approve the list of personnel with authorized access has been identified; Visitors are escorted as required according to security policies and procedures; Visitor's access records to the facility are maintained by the organization; The Physical access to the premises is monitored by the organization; Industry standard implementation of physical and environmental controls; Evaluate the effectiveness of physical and environmental controls periodically; Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents; Physical access records are kept and stored in case of an audit or investigation; Physical access records are retained as dictated by applicable regulations or based on an organization-	PCI DSS: 8.6, Requirement 9 CSA CCM: DCS-01, DCS-02, DCS-03, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, DCS10, DCS-1

SO 09	Security of Supporting Utilities	The DSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc.	**3**	TokenEx uses an IaaS provider for secure hosting of customer data. TokenEx reviews our IaaS provider's security and compliance reports to ensure secure requirements are being met. Our IaaS provider is responsible for the physical security and environment controls to protect TokenEx systems and data, including: Ensuring security of supplies, such as electric power, fuel or HVC; Implementing a policy for security of critical supplies, such as electrical power, fuel, etc.; Implementing industry standard security measures to protect supplies and supporting facilities; Advanced security measures to protect supplies; Reviewing and updating policy and procedures to secure supplies regularly, taking into account changes and past incidents.	
SO 10	Access Control to Network and Information Systems	The DSP established and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management, authentication of users, access control systems, firewall and network security etc.	**3**	All users are assigned unique IDs and are authenticated before accessing the Customer Portal or TokenEx systems or networks. TokenEx complies with PCI requirements for password security. Only authorized users are allowed to access the Secure Data Environment and permissions are assigned on the basis of least privileged access. Administrators who support the platform must access the secure environment through VPN using multifactor authentication. Access attempts are logged and monitored. Access is periodically reviewed. TokenEx's Access Control policy defines requirements for protecting access to network and information systems and addresses roles, rights, responsibilities and procedures for assigning and revoking access rights. TokenEx continuously reviews policies and access control mechanisms for improvement opportunities.	PCI DSS: Requirement 1, Requirement 2 CSA CCM: EKM-01, EKM-02, EKM-03, EKM-04
SO 11	Integrity of Network Components and Information Systems	The DSP establishes, protects, and maintains the integrity of its own network, platforms and services by taking steps to prevent successful security incidents. The goal is the protection from viruses, code injections and other malware that can alter the functionality of the systems or integrity or accessibility of information	**3**	Anti-malware software is installed on all servers and laptops and is centrally managed. Users are technically prevented from disabling or circumventing anti-virus. Intrusion detection, file integrity monitoring, IP reputation management, and system and networking monitoring are in place to maintain the integrity of TokenEx networks and systems. Passwords are never stored or transmitted in clear-text. The effectiveness of measures to protect integrity of systems are continuously evaluated and reviewed.	PCI DSS: Requirement 4
SO 12	Operating Procedure	The DSP establishes and maintains procedures for the operation of key network and information systems by personnel. (i.e. operating procedures, user manual, administration procedures for critical systems etc.)	**3**	Responsibilities for the operation of our platform has been assigned to qualified systems administrators. Operational procedures are documented and processes are monitored for compliance. Policies and procedures are continuously reviewed, taking into account incidents or changes.	
SO 13	Change Management	The DSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc.	**3**	TokenEx's change management process includes testing, approval, and documenting all changes to the secure data environment. Impact and backout plans are documented. Customers are notified of significant changes which affect the offered services. Change management procedures and reviewed and updated regularly, taking into account changes and past incidents.	PCI DSS: 6.4.6, 12.1.1.1 CSA CCM: CCC-01, CCC-02, CC03, CC04, CC05, CC06
SO 14	Asset Management	The DSP establishes and maintains asset management procedures and configuration controls for key network and information systems.	**3**	Secure baseline configurations are developed based on industry standards, documented, implemented and maintained. Assets are monitored to ensure compliance with baseline configurations. Policies and procedures for asset management and configuration controls are in place and reviewed and updated at least annually or upon changes or incidents. Assets are documented in an inventory list, and the asset list is reviewed and updated annually and upon changes. TokenEx maintains separate environments for development, test, and production.	PCI DSS: 12.1, 12.2 CSA CCM: DSI-01, HRS-01
SO 15	Security Incident Detection & Response	The DSP establishes and maintains procedures for detecting and responding to security incidents appropriately. These should consider detection, response, mitigation, recovery and remediation from a security incident. Lessons learned should also be adopted by the service provider.	**3**	TokenEx has a documented Incident Response Plan for identifying, responding to, and remediating security incidents. At least annually, we exercise our plan, documenting test results and noting improvement opportunities. Our plan is updated to reflect any changes to the environment or security incidents/events. IT Operations staff are available 24x7x365 to respond to incidents. Monitoring and automated alerts are in place to notify staff of incidents or events. All employees are trained how identifying and reporting incidents. TokenEx's incident response process includes an investigation of incidents and documentation of actions taken. Lessons learned are documented and remediation is performed to reduce the risk of future incidents.	PCI DSS: 12.10, 12.10.1, 12.10.2 CSA CCM: SEF-03, SEF-04, SEF-05
SO 16	Security Incident Reporting	The DSP establishes and maintains appropriate procedures for reporting and communicating about security incidents.	**3**	As part of our Incident Response Plan, reporting processes are established in the event that incidents need to be communicated to third parties, customers, or government authorities. Procedures also include internal requirements for incident response communication. We review and update our Incident Response Plan, including reporting and communication procedures, at least annually or in the event of any incidents or significant changes.	PCI DSS: 12.10.2, 12.10.4, 12.10.5, 12.10.6 CSA CCM: SEF-01, SEF-02, SEF-04
SO 17	Business Continuity	The DSP establishes and maintains contingency plans and a continuity strategy for ensuring continuity of the services offered.	**3**	TokenEx employs redundancy at every layer possible in our infrastructure, and our platform is designed to accommodate operating failures to ensure availability. TokenEx replicates data offsite to geographically diverse locations. Monitoring is in place to detect issues with the replication process. Failover testing is conducted regularly and is used to validate our RTO/RPO requirements. TokenEx has a documented business-continuity and disaster-recovery plan, which is reviewed, updated, and tested at least annually. Plans are updated based on any changes, past incidents, and lessons learned from exercises. Personnel involved in the continuity operations plan are trained in their roles and responsibilities.	PCI DSS: 12.10.1 CSA CCM: BCR-01, BCR-02, BCR-03, BCR-04-BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11
SO 18	Disaster Recovery Capabilities	The DSP establishes and maintains an appropriate disaster recovery capability for restoring the offered services in case of natural and/or major disasters.	**3**	TokenEx employs redundancy at every layer possible in our infrastructure, and our platform is designed to accommodate operating failures to ensure availability. TokenEx replicates data offsite to geographically diverse locations. Monitoring is in place to detect issues with the replication process. Failover testing is conducted regularly and is used to validate our RTO/RPO requirements. TokenEx has a documented business-continuity and disaster-recovery plan, which is reviewed, updated, and tested at least annually. Plans are updated based on any changes, past incidents, and lessons learned from exercises. Personnel involved in the continuity operations plan are trained in their roles and responsibilities.	PCI DSS: 12.10.1 CSA CCM: BCR-09, BCR-11

SO 19	Monitoring & Logging	The DSP establishes and maintains procedures and systems for monitoring and logging of the offered services (logs of user actions, system transactions/performance monitors, automated monitoring tools etc.)	**3**	Extensive logging and monitoring are in place throughout our secure data environment in accordance with industry best practices and PCI requirements. TokenEx utilizes a variety of toolsets for automated collection and analysis of monitoring data and logs. Alerts are generated to notify operations staff of critical security events. Logging and monitoring policy and procedures are implemented and reviewed and updated at least annually, taking into account changes and past incidents.	CSA CCM: IVS-01
SO 20	System Tests	The DSP establishes and maintains appropriate procedures for testing key network and information systems underpinning the offered services.	**3**	Formal patching processes are conducted on a regularly scheduled basis. Patches are tested and validated in test prior to deploying in production. Networks and systems are tested through regular vulnerability scans and pen tests. Significant system or network changes are validated through additional security testing. Code changes are tested prior to deployment through manual and automated review. Policies and procedures have been implemented and are reviewed and updated, taking into account changes and past incidents.	
SO 21	Security Assessments	The DSP establishes and maintains appropriate procedures for performing security assessments of critical assets	**3**	Vulnerability scans and penetration tests are regularly conducted, particularly when new systems are introduced and following changes. Vulnerabilities are identified, remediated, and retested. Business owners and communication channels have been established for all third parties to identify security related issues. Policies and procedures for security assessments and security testing have been established and are periodically evaluated for effectiveness.	PCI DSS: 6.6 CSA CCM: AAC-02
SO 22	Compliance	The DSP establishes and maintains a policy for checking and enforcing the compliance of internal policies against the national and EU legal requirements and industry best practices and standards. These policies are reviewed on a regular basis.	**3**	TokenEx has a formal compliance program in place to monitor compliance against standards, regulations, and legal requirements. Policy and procedures have been established for compliance, auditing, and monitoring. TokenEx uses a GRC tool to manage compliance obligations and periodic tasks. TokenEx ensures asset compliance through continuous monitoring, vulnerability scans and penetration testing. Significant gaps are investigated and remediated. Compliance, auditing, and monitoring policy and procedures are reviewed at least annually, taking into account changes and past incidents.	CSA CCM: AAC-01, AAC-02, AAC-03
SO 23	Security of Data at Rest	The DSP establishes and maintains appropriate mechanisms for the protection of the data at rest	**3**	TokenEx classifies all data according to a classification scheme which takes into account data's value, legal requirements, sensitivity, and criticality to TokenEx. Customer data is considered high risk. Customers have complete control over their data, including deletion. TokenEx will only delete customer data outside of these instructions after the termination of the agreement in accordance with our standard terms. TokenEx has processes in place to securely delete data and can provide a certificate of deletion. Data is encrypted at rest using AES-256. Key management policies and procedures have been established in accordance with industry best practices. Data is never stored outside of the secure environment. Removable media is not used to store data. Policies and procedures around confidentiality and integrity of data at rest have been established and all relevant personnel are made aware of what it implies for their work. Policies are reviewed at least annually. All TokenEx assets are classified according to the classification scheme. Information is labelled and handled in accordance with the classification scheme	PCI DSS: 12.6 CSA CCM: DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07
SO 24	Interface Security	The DSP should establish and maintain an appropriate policy for keeping secure the interfaces of services which use personal data	**3**	Security policies are in place for keeping interfaces secure and employees are made aware of their responsibilities under our security policies. Data is encrypted in transit using SFTP or HTTPS/TLS 1.2+. Access to the Secure Data Environment or Customer Portal requires 2FA. Accounts must be unique. Policies are reviewed at least annually and are updated to reflect any past incidents or exceptions, tests, or incidents affecting other providers.	PCI DSS: 2.3 CSA CCM: AIS-01, AIS-02, AIS-03, AIS -04
SO 25	Software Security	The DSP establishes and maintains a policy which ensures that the software is developed in a manner which respects security	**3**	TokenEx has established a secure software development lifecycle. Physically separate networks are maintained for development, test, and production. Production data is never used for test or development. Code changes are tested throughout the SDLC prior utilizing peer reviews and automated testing. Results of code assessments are used to regularly enhance developer training and the SDLC process.	PCI DSS: 2.4 CSA CCM: AIS-04
SO 26	Interoperability & Portability	Online marketplace and cloud providers use standards which allow customers to interface with other digital services and/or if needed to migrate to other providers offering similar services.	**3**	To assure interoperability and portability, TokenEx uses API and batch to allow customers to interface with other digital services and/or if needed to migrate to other providers offering similar services. TokenEx uses these methods to return customer data upon request from an approved user. The effectiveness of interoperability & portability measures are periodically evaluated and reviewed.	CSA CCM: IPY-01, IPY-02, IPY-03, IPY-04, IPY-05
SO 27	Customer Monitoring & Log Access	The cloud provider grants customers access to relevant transaction and performance logs so customers can investigate issues or security incidents when needed.	**3**	As part of our service, customers get access to our Customer Portal which grants them to ability to view log data and reports on tokenization usage. This data is specific to each customer and customers can only view data about their vaults/tokens. Extensive logging and monitoring are in place throughout our secure data environment in accordance with industry best practices and PCI requirements. TokenEx utilizes a variety of toolsets for automated collection and analysis of monitoring data and logs. Alerts are generated to notify operations staff of critical security events. Logging and monitoring policy and procedures are implemented and reviewed and updated at least annually, taking into account changes and past incidents.	CSA CCM: IVS-01