Trust Your Supplier

Information Security Management Program

V 2.0

Disclaimer

The information contained in this document is confidential, privileged and only for the information of the intended recipient, and may not be used, published, or redistributed without the prior written consent of Chainyard Supplier Management (CSM).

The information presented in this document is made in good faith and while every care has been taken in preparing these documents, CSM makes no representations and gives no warranties of whatever nature in respect to this document, including but not limited to the accuracy or completeness of any information, facts and/or opinions contained therein.

Information presented in this document is subject to change based on governance board inputs, member comments, and future design and implementation decisions.

Table of Contents

VERSION LOG

Date	Document Version	Changes	Author
9/11/2020	1.0	First publication	Melissa Bracken
11/11/2020	1.0	Review First publication	Ravi Sabhikhi
09/97/2022	2.0	AWS support	Ravi Sabhikhi
10/13/23	2.0	Reviewed no changes	Ravi Sabhikhi

Confidentiality

The contents of this document are considered CSM and IT People Confidential and are provided to TYS stakeholders upon request.

1. Purpose of Document

This document provides a high-level view of the Information Security Management program followed by Chainyard Supplier Management (CSM) in hosting the 'Trust Your Supplier' application, and addresses a variety of audiences, including security auditors, operations teams, TYS network participants, legal teams, and chief information security officers. It provides an overview of the comprehensive set of information security policies and protections CSM has in place. These policies apply to various aspects of the TYS application and network, covering the principles of the CIA triad: confidentiality, integrity, and availability. These practices were created by CSM to protect sensitive information, prevent unauthorized access, and reduce security risks and incidents.

Information presented in this document is subject to revisions.

1.1 GLOSSARY

Terms and Acronyms	Description	Definition
Chainyard	Brand used by IT People Corp. for providing various blockchain services to enterprise clients.	The company whose solutions practice developed TYS.
CIA	Confidentiality, Integrity, and Availability	Also referred to as the 'CIA Triad'; a well-known model for the development of security policies
COBIT	Control Objectives for Information and Related Technologies	A framework for IT management and governance, created by the Information Systems Audit and Control Association (ISACA)
CSM	Chainyard Supply Management	The entity related to Chainyard that owns TYS
ISMS	Information Security Management System	A documented system that includes a set of security controls, implemented by a company to protect their assets from threats.
PII	Personally Identifiable Information	Includes any data that could identify a specific person
TYS	Trust Your Supplier	The supplier onboarding application consisting of a network of buyers and suppliers and the subject of this document.

2. Background

2.1 COMPANY OVERVIEW

IT People Corporation, established in 1999 and based in Morrisville NC, provides information technology services to enterprise clients. The company offers blockchain consulting services, advisory services, and solutions under the brand 'Chainyard'.

Chainyard's solutions practice develops and commercializes blockchain solutions from concept to production. Their first solution consists of a business network for supplier and buyer collaboration, leveraging blockchain and other technologies. This application is known as 'Trust Your Supplier' (TYS) and is owned by a separate entity known as 'Chainyard Supplier Management' (CSM). The operations and support for this network is provided by Chainyard on behalf of CSM.

2.2 TYS OVERVIEW

Trust Your Supplier is a cross-industry permissioned blockchain-based business network deployed as a SaaS solution. It simplifies and accelerates the onboarding and lifecycle management process of suppliers, also providing them with a 'digital passport' that includes their identity and credentials, bringing more transparency and trust to the supply chain environment. Its business network is used by buyers, suppliers, verifiers, banks, and other third parties. Buyers may invite suppliers to join the network and provide relevant supplier profile information, ask verifiers to validate that information, and onboard the suppliers to conduct business with them.

TYS utilizes the IBM Blockchain Platform built on Hyperledger Fabric, an open source modular blockchain framework, and is currently deployed on the IBM and AWS clouds... Hyperledger Fabric is an enterprise-grade, distributed ledger platform that offers modularity and versatility for a broad set of enterprise use cases through plug and play components, such as consensus, privacy, and membership services. The IBM and AWS Clouds offer storage options with inherent scalability and flexibility and is designed to support traditional and cloud-native workloads.

The flexibility of Hyperledger and secure storage options of IBM allow the application to be easily adaptable while safely storing and backing up customer data in a cloud environment.

Since the data TYS gathers and processes may be sensitive, confidential, and/or PII (Personally Identifiable Information), it is critical that Chainyard have a thorough, well-built Information Security Management System (ISMS) to ensure appropriate measures are put in place to secure and protect that data.

2.3 TERMS USED IN THIS DOCUMENT

'TYS' and 'Chainyard' are terms used throughout this document. 'TYS' refers to the Trust Your Supplier application, which resides on the IBM Cloud. 'TYS team' or 'TYS personnel' refers to the Chainyard employees who work on TYS. While Chainyard Supplier Management owns the application, this document will refer to it as 'Chainyard'. All 'Chainyard' actions and employees are referring to those from Chainyard assigned to the TYS application, as all CSM employees are also Chainyard employees.

3. ISMS Overview

An Information Security Management System (ISMS) defines the policies, procedures, guidelines, and methods to systematically manage and protect data that is sensitive, confidential, private, or contains PII, as well as assets surrounding the sensitive data, such as physical resources and software. An ISMS applies to both the organizations and the solutions that process such data. Chainyard has designed a comprehensive ISMS to ensure the confidentiality, integrity, and availability of customer data, using a risk-based approach that continuously re-evaluates potential risks and their mitigation strategies. This includes the effective ability to detect and prevent unauthorized or inappropriate access to data.

The scope of the TYS ISMS includes governing documentation (information security policies), a security technology infrastructure, and administrative actions to ensure policies are enforced, monitored, and periodically audited for risks.

3.1 INFORMATION SECURITY POLICIES

The TYS ISM addresses the below information security elements. These guide Chainyard personnel actions and dictate how TYS and its infrastructure must be set up, covering the entire data management cycle from data capture to storage to disposal.

- Personnel Security
- Operations Management
- Physical and Environmental Security
- Network Security
- Identity Management and Access controls
- Data Management
- Compliance and Regulations
- Cybersecurity, Privacy and Data Retention
- Business Continuity and Disaster Recovery
- Risk Management
- Incident Management

3.2 INFORMATION SECURITY INFRASTRUCTURE

The Information security infrastructure is the framework of technical controls used by TYS. These include:

- Data Security/Privacy
- Data Encryption
- Data Retention
- Logical Access Controls
- Network Security

3.3 INFORMATION SECURITY ADMINISTRATION

Administrative information security actions TYS undertakes include:

- TYS employee training

- Audits and pen tests (internal and external)
- Security Incident Response Plans

4. Security Standards & Certifications

The TYS ISMS is guided by recognized international security standards and its security policies reference best practices to the largest extent possible. The TYS ISM borrows best practices from COBIT (Control Objectives for Information and Related Technologies) and these ISO standards:

- ISO 27001 – international standard for information security
- ISO 27005 – information security risk management
- ISO 27014 - governance of information security
- ISO 27701 – privacy information management systems / GDPR

The TYS ISM attempts to comply with prevailing security standards and practices to minimize data security and privacy risks. Additionally, TYS has completed and is in the middle of several security certifications, as listed below.

4.1 TYS SOC 1 TYPE 2

Work on a SOC 1 Type 2 certification for *IT General Controls* is currently in progress.

4.2 TYS SOC 2 TYPE 1 CERTIFICATION

TYS received **SOC 2 Type 1** certification in July 2020. SOC 2 is performed as an external audit and confirms that a SaaS provider manages client data securely and protects the interests and privacy of clients. It is based on meeting a broad set of security measures that the SaaS company may customize to meet their needs.

SOC 2 Type 1 results in a report that describes the system a company uses for processing data and ensuring the security and privacy of that data, and evaluates the suitability of the design.

4.3 TYS SOC 2 TYPE 2

SOC 2 Type 2 includes everything from Type 1 plus an evaluation of the *effectiveness* of the security controls the organization put in place, after monitoring them for a set period. This assures customers that their data is safe within TYS, and that the application is fully compliant with privacy laws. Work on this certification is currently in progress.

4.4 PCI COMPLIANCE

Work on this certification is currently in progress.

4.5 OTHER CERTIFICATIONS

TYS is planning to meet additional information security standards that include:

- Undergoing ISO 27001 and other security certifications as appropriate
- Regular security testing of the solution through penetration testing to check standards are being met

5. TYS Information Security Management System

The following sections describe the topics that the TYS ISMS covers through its policies, information security infrastructure, and administrative actions. Combined, these topics form a comprehensive plan that makes sure TYS fully protects sensitive data from potential risks and meets international regulations such as GDPR.

5.1 DATA SECURITY GOVERNANCE

Data security governance is defined as protecting data and meeting relevant regulatory requirements by defining a framework of effective and efficient policies and processes that apply to all data in every stage of software development. Chainyard has undertaken this and shall routinely update TYS policies after periodic reviews of pertinent laws and regulations, security risks, and the effectiveness of the security measures managing those risks.

Chainyard conducts regular reviews to check that policies and processes continue to support data security goals and adapts them to changing risks and threats. To monitor the effectiveness of its controls, TYS goes through:

- Penetration and vulnerability tests
- Audits conducted by internal teams across the ISMS
- Contingency and response plan exercises

5.2 SECURITY RISK MANAGEMENT

The TYS ISMS utilizes a risk-based approach where risks are continuously reevaluated. TYS risk management security measures focus on managing risks by minimizing dangers and avoiding potential crises in and around the network and application. Operational and application risks are addressed, such as identifying data breaches, malicious actors, and application weaknesses that could be exploited.

TYS personnel, or independent third parties, regularly run the system through an information security risk assessment process to identify, analyze, evaluate, and treat identified risks. This process takes place at least once a year, is guided by the international ISO 27005 standard, and has allowed TYS to adopt a risk assessment methodology that includes scoping, business impact assessment, threat profiling, vulnerability assessment, risk evaluation, and risk treatment. If new risks are identified, TYS updates the relevant ISMS policies to address them.

5.3 DATA SECURITY

5.3.1 OVERVIEW

Chainyard puts comprehensive data security policies and procedures in place for TYS, so that data owners can be confident their data is meeting the well-known CIA Triad model of data confidentiality, integrity, and high availability.

TYS safeguards customer data from loss and unauthorized access using reasonable methods to keep risks at an acceptable level. Data from different customers is segregated using logical access controls. TYS may use additional measures to those described below.

It is the responsibility of member organizations to ensure proper security measures are in place for their users, networks, and facilities that connect with TYS.

5.3.2 DATA PROCESSING AND STORAGE

TYS classifies data so that it is appropriately stored either on or off the blockchain, based on the security level the data requires and whether it may need to be deleted from TYS in the future.

Backup and recovery of the ledger is native to the blockchain since a copy of the ledger is held on multiple nodes. Blockchain data is also immutable, so on-chain data processed by TYS is never lost.

Off-chain data, which includes PII data, is replicated in multiple instances of each off-chain database. Off-chain data is backed up by IBM every 24 hours and the backups retained for 30 days. TYS personnel test all backup mechanisms once annually.

5.3.3 DATA ENCRYPTION

TYS preserves data confidentiality by encrypting data whenever possible. Data is encrypted at rest and in motion to ensure the network and databases are sufficiently hardened. Member organizations own keys that enable them to encrypt blockchain data and any PII data they commit off-chain. These cryptographic keys are securely managed and only the organization that owns the keys can access them.

Additional encryption measures include:

- A FIPS-140-2 compliant Key Management Service provided by TYS
- Login passwords protected using PBKDF2 encryption and a random 16 byte salt value for each user, with a SHA-512 cryptographic hash function and hashes stored off-chain
- Data in transit encrypted using HTTPS or TLS

5.3.4 APPLICATION ACCESS

Only Chainyard personnel who need to have access to the application and customer data to perform their job functions are authorized access and given the appropriate role-based privileges. TYS subcontractors do not have access. Chainyard shall identify in writing all employees granted access to a customer's data upon that customer's written request.

Chainyard employee access rights are reviewed at least every six months and access to the application and data is rescinded for those whose role no longer requires it. Personnel that separate from the company have their access rescinded as a part of the separation process. It is expected that member organizations regularly review and adjust access lists under their control and inform Chainyard of users whose access and credentials should be rescinded.

Data owners have control over which organizations and users may access their data stored in TYS, accomplished through role-based access privileges and user credentials they create within the application. As an example, buyers only have access to data from suppliers who have given their organization permission to view it.

5.3.5 NETWORK HARDENING

Overall network hardening and security is divided between Chainyard (responsible for the TYS application) and IBM and AWS Clouds (responsible for the platform). TYS measures include ensuring network elements accessible to the internet are protected through a primary web-app firewall placed in front of the node application HTTPS ports. IBM Cloud has an internal firewall, which uses three interfaces to protect TYS components in the cloud at all times.

All TYS connections with external authorized third parties are run across an API and mutually authenticated using cryptographic techniques. Any information flow coming from a third party is filtered to check for malware, viruses, and data integrity issues. Third party web applications connecting to TYS require an SSL certificate.

All servers are in IBM Data Centers and are managed and operated by IBM. As such, they adhere to IBM physical policy guidelines and are protected against attacks, accidents, and natural disasters.

- IBM security measures follow the NIST 800-53 PE security and privacy control framework as well as ISO 27001 A11 requirements.
- AWS security measures, Please refer to document provided by AWS CHINA- AWS-China-Security-Complaince.doc

Only authorized TYS personnel who have IBM and AWS Cloud TYS Network Admin accounts review, support, or update network configurations.

5.3.6 PRODUCT DEVELOPMENT

Chainyard has well-defined source code security policies that assist with intrusion prevention. Chainyard's TYS developers construct source code in a way that removes as many security risks as possible while allowing the code to operate effectively. They utilize tools that allow them to find problems and make code corrections during the development process, including code reviews, vulnerability scans, and penetration tests. External agency code reviews take place once annually.

5.3.7 ANTI-MALWARE

Chainyard developer laptops are equipped with malware protection software and developers conduct thorough code reviews and use npm scan tools to prevent malicious JavaScript packages from being injected into the application's code. The TYS engineering team is installing an overall antivirus solution for the application, and an antivirus engine is present to scan documents prior to upload.

Organizations who access TYS must ensure machines on their side are also secure.

5.3.8 PERSONNEL

New Chainyard employees who need access to TYS must complete a defined set of security checks and sign a confidentiality agreement prior to being onboarded to Chainyard and given access to TYS. All TYS employees receive annual security training emphasizing the importance of customer data security, confidentiality, privacy, and potential risks. Employees have security responsibilities laid out in their job definitions. Upon separation, employees shall return all company assets and have their TYS access revoked within a prompt predefined timeframe.

5.3.9 PHYSICAL SECURITY

Physical security is applicable to members of the network, the Chainyard premises where TYS development takes place, and the data centers where TYS is hosted. It is the responsibility of members to conform to TYS security policies that apply to their assets. Chainyard restricts access to TYS premises to the appropriate personnel through badge access devices, and physically secures all IT equipment and devices within those

facilities. Employees adhere to a set of security procedures and policies that ensure all employee equipment is properly secured within each suite.

IBM and AWS data centers hosting the TYS infrastructure on the IBM and AWS Clouds follow IBM and AWS physical policy guidelines and are protected against attacks, accidents, and natural disasters.

- IBM security measures follow the NIST 800-53 PE security and privacy control framework as well as ISO 27001 A11 requirements.
- **AWS Physical security policy,** Please refer to document provided by AWS CHINA- AWS-China-Security-Complaince.doc

5.4 USER ACCOUNTS AND LOGINS

TYS users can access the application via a desktop browser over an HTTPS user interface. Each member organization's Org Admin invites their users and assigns roles to each using the lowest privileges necessary; the TYS application shall not create default user accounts.

The TYS team deletes the login credentials of Chainyard users who no longer need access to the application due to company separation or a change in duties. It is the responsibility of member organizations to promptly delete users who no longer need access, accomplished by the Org Admin managing permissions within the application.

All TYS users are responsible for choosing and properly securing their login password, which must follow the rules laid out in the TYS Password Policy. Limits are placed on user sessions so they are not open-ended, and users may only run one session at a time.

User access logs are maintained by TYS that include details such as date and time of access and user ID. These can be provided to a customer upon request.

5.5 DATA PRIVACY

TYS established a data privacy policy guided by ISO 27701 (implementation of Privacy Information Management Systems) that ensures data entering the application is properly classified and handled. TYS keeps abreast of worldwide country-specific privacy laws and regulations and performs privacy risk assessments on the application at least annually, updating the privacy policy based on gaps found. TYS also provides annual privacy education to its personnel.

Data is managed by its owner organization, which is the only entity that can securely share their data with other TYS business participants.

All PII and Sensitive Personal Information (SPI) do not require immutability or historical tracking and are stored off-chain, so as to be compliant with GDPR regulations such as 'Right to Forget'. The PII data owner decides how long to retain PII data, when to delete it, and manages any objections to it.

Network Administrators of the TYS Consortium are responsible for protecting the privacy rights of individuals' data when maintaining and updating the network configurations.

5.6 SECURITY INCIDENT MANAGEMENT

A Security Incident Management Plan is in place and shall undergo revisions as future requirements are defined. It references ISO/IEC Standard 27035 security incident guidance, which includes a five-step process of preparing

for incidents, monitoring and reporting incidents, assessing and working out how to mitigate incidents, responding by resolving incidents, and documenting lessons learned.

The plan guides the Chainyard TYS Security Incident Response Team on how to react in the event of a security breach. If there is a high-level security incident, the incident response team notifies member organizations immediately and attempts to resolve it within 24 hours. Critical data or security breaches require the team to engage with the appropriate state and federal law enforcement agencies.

IBM Cloud Services has a global IBM Product Security Incident Response Team who detects and prevents cloud intrusions. The team identifies risks in the IBM Cloud, Blockchain and Containers products TYS uses, and defines solutions to resolve them.

Event Logging

Event logging is crucial to tracing and investigating security incidents. TYS retains logs for 30 days using appropriate security methods, after which it archives and stores them. These include security logs, audit logs, authentication logs, application logs, server logs, and database logs. These are available to member organizations upon request.

5.7 BUSINESS CONTINUITY PLANNING (BCP)

TYS Business Continuity Planning results in the formal definition of a process that allows the TYS application to quickly recover from threats (such as malware attacks) and disasters (such as power outages), enabling member organizations to continue doing business during that time. Chainyard has documented the overall TYS BCP process and trained TYS support and operations personnel on it.

Chainyard conducts annual BCP drills, including DAST and SAST application security testing, and remediates any vulnerabilities found. External agencies periodically conduct penetration tests and code reviews as a part of the BCP process. Chainyard updates the BCP process document annually with lessons learned from drills and tests.

5.8 THREAT MANAGEMENT

TYS follows defined threat and intrusion detection policies that are refined in the Business Continuity Plan. The TYS team monitors network traffic, logs, and security events using integrated SIEM tools, to find intrusions at an early stage and minimize the impact of a possible attack.

TYS has undergone internal and third party security audits and penetration tests and shall continue to periodically have such audits and penetration tests to address the security status of the application and minimize any vulnerabilities. Member organizations may audit the TYS service upon approval of the Governance Board.

5.9 CHANGE MANAGEMENT

TYS has a structured system development methodology in place that follows the documented Chainyard Software Development Life Cycle (SDLC) approach to delivering blockchain-based solutions. This defined change control process ensures proper documentation and approval of any TYS-related changes, reducing the possibility of errors or unauthorized changes. The TYS development team uses an agile delivery management process and utilizes development tracking and version control tools.

Application security patches that update TYS production code follow secure deployment procedures.

5.10 TRANSITION OF SERVICES

Chainyard shall, pursuant to a mutually agreed upon contract with the customer, assist in the orderly transition of a customer's data to another provider or to an internal customer system, should the customer choose to end their affiliation with the TYS network. Chainyard shall delete all TYS off-chain customer data within 60 days of a customer's separation date.

5.11 DATA RETENTION

TYS data is split between the blockchain ledger, off-chain data, and application data. To comply with privacy regulations, TYS does not store PII information on the blockchain. TYS data stored in the blockchain is immutable and a data owner can permanently block access to it by destroying the keys used to encrypt it. A data owner can directly delete their data stored off-chain, application-specific data, and data backups stored on the cloud.

TYS personnel shall promptly remove the PII data of Chainyard employees who have separated from the company. It is the responsibility of individual organizations to delete PII data associated with an employee if that employee leaves the organization.

TYS personnel shall delete an organization's off-chain data from TYS databases and replicas within 60 days of an organization's termination of TYS membership.

TYS personnel shall delete an organization's off-chain data if they are not active in TYS for a period of two years (no user logins and no data updates).