



Traceability and Verification System

INFORMATION SECURITY PROCEDURE

Version: 02.00 (22 October 2025)

Document control

Version	Date	Description	Author
0.1	9 Jun 2022	Initial draft covering technical controls	Andy Peacock
0.2	15 Jun 2022	Updated format and content relating to internal processes and policies	Matt Rymell
0.3	20 Jun 2022	Updates following internal review and clarifications	Matt Rymell
0.4	22 May 2023	Transition to TRVST document. Minor edits and updates throughout	Alexander Blecken
00.10	27 July 2023	Document shared with Data Sharing Task Team, VTI Steering Committee and other stakeholders	Alexander Blecken
00.19	18 October 2023	Updated version including all comments and feedback received from Data Sharing Task Team, VTI Steering Committee and other stakeholders	Alexander Blecken
00.20	22 November 2023	Revised version shared with Data Sharing Task Team, VTI Steering Committee and other stakeholders	Alexander Blecken
00.10	13 March 2024	Final Version	Alexander Blecken
02.00	22 October 2025	Revised version after review by Enterprise Agreement Signatories	Richard Wilder

Table of Contents

Document control	2
Table of Contents	3
1 Introduction	5
2 Scope	5
3 Internal Security Measures	6
3.1 Policies and Processes	6
3.2 Information Security Asset Lists and Risk Assessment	6
3.2.1 Assets Inventory, Risk Assessment and Treatment	6
3.3 Information and Document Classification	7
4 TRVST System Security and Continuity Measures	7
4.1 Architectural Specification	7
4.2 Firewalls	7
4.2.1 Denial of Service Protection	7
4.3 Access Management	8
4.3.1 Secure Data Access	8
4.3.2 Secure and Authorised Access to Data	8
4.3.3 Placing Inactive Accounts On Hold	8
4.4 User Interface Authentication	8
4.4.1 Password Policies	8
4.4.2 Password Resets	9
4.4.3 Multi-factor Authentication	9
4.4.4 CAPTCHA Verification	9
4.5 System Account Authentication	9
4.6 Data Encryption	9
4.6.1 Data Encryption in Transit	9
4.6.2 Data Encryption at Rest	9
4.7 Malware Protection	9
4.8 Mobile App	10
4.9 Data Integrity and Non-Repudiation	10
4.10 System Redundancy, Resilience and Availability	10
4.10.1 Backup	10
4.11 Monitoring and Auditing	10
4.11.1 Security Monitoring	10
4.11.2 Auditing	11
4.12 Changes to Production Environments	11
4.13 Patching	11
4.13.1 TRVST System	11
4.13.2 Operating System	11

4.14	System Security Testing	11
4.15	Service Continuity Planning	12
4.15.1	TRVST Continuity Plan	12
4.15.2	TRVST System Provider / UNICEF Business Continuity Plan.....	12
4.16	Security and Data Breach Incident Management	12

1 Introduction

The Traceability and Verification System (TRVST) is a digital platform developed through collaboration by a multi-stakeholder group called the Verification and Traceability Initiative (VTI). This platform enables countries to verify the authenticity of health products and improve end-to-end traceability across supply chains. TRVST is a powerful tool that significantly reduces the risks of falsified and diverted health products and supports the move toward national traceability of vaccines, medicines, and other health items.

TRVST is not intended to replace national traceability systems; instead, it functions as a global interoperability hub, connecting manufacturers, regulatory agencies, and national systems. The platform allows product verification where national systems are not yet established and supports traceability throughout the upstream supply chain before reaching the country level.

By design, TRVST facilitates compliance with regulations governing work of National Drug Regulatory Authorities (NDRAs) pertaining to product verification and by providing transparency into product logistics. Additionally, it grants access to patient information leaflets (PILs) via barcode scanning. This feature supplies healthcare providers with accurate, up-to-date product information, facilitating informed decisions regarding patient care. Patients can also use this feature to authenticate their medications and access essential information about the proper administration of their health products.

Manufacturers upload product master data, batch and lot numbers, expiry dates, and serial information into TRVST. These data are used to authenticate products when authorized users scan barcodes. Verification can be done directly through mobile or web interfaces or via data exchange between national systems and the TRVST Repository. The TRVST Repository acts as a central database that stores all product information and enables verification. This data exchange is managed through the TRVST Application Programming Interface (API), which facilitates secure communication and data sharing among systems.

Data sharing and security are core to TRVST's design. The platform complies with strict data governance and information security standards to protect the confidentiality, integrity, and availability of all exchanged data. These measures promote trusted collaboration among stakeholders while ensuring adherence to relevant data protection and privacy laws.

TRVST plays a crucial role in safeguarding the integrity of health supply chains, strengthening regulatory oversight, and enhancing patient safety.

The TRVST System Provider is responsible for the system's technical development and maintenance. UNICEF functions as the TRVST Organization and legal entity overseeing the management, governance, and stewardship of the data. This includes supervising system use, ensuring compliance with regulations, and managing the data shared on the platform.

More general information on TRVST is available in the [TRVST document repository](#).

2 Scope

This document summarizes the information security procedures related to:

- The TRVST system as deployed in Production Environments
- Development and testing of the TRVST system
- Operation and maintenance services that support the TRVST system
- TRVST System Provider's staff are involved in designing, developing, testing, building, deploying, operating, monitoring, maintaining, supporting and documenting the TRVST system.

In the event of any conflict or inconsistency between the provisions of a Data Governance Document and the TRVST System Provider Information Management System (IMS) -or Subresource Integrity (SRI)-denominated documents referenced in this Information Security Procedure, the following order of precedence shall apply, with a document identified on the list below taking precedence over those listed subsequently:

- Sections 1-18 of the Enterprise Agreement
- Any Data Governance Document other than that giving rise to the inconsistency
- Any document referenced within the Information Security Procedure other than that giving rise to the inconsistency.

3 Internal Security Measures

3.1 Policies and Processes

The TRVST Service Provider shall be ISO 27001:2013 certified as reviewed and confirmed by TRVST. InThe TRVST System Provider's staff receive annual training in Information Security and Data Protection and specialist training is given to those individuals who are directly involved in activities relating to Information Security.

TRVST System Provider shall (a) maintain its ISO 27001:2013 and UK Government Cyber Essentials accreditation and certification (or higher) throughout the term of the Agreement, and (b) update its Security Policies and Procedures (as necessary) from time-to-time to comply with best IT security practices, and all applicable laws and regulations. TRVST System Provider shall not downgrade its security standards or the security configuration of any system that processes, provides access to, or otherwise interacts with Data without the prior written consent of all TRVST User Organizations.

At least as required in Section 4.14, the TRVST System Provider shall periodically (at least once every twelve (12) months) perform formal security reviews to ensure the confidentiality, availability, and integrity of Data that comes into the possession or control of TRVST System Provider through the TRVST System. TRVST System Provider shall report the outcome of such security reviews to TRVST Org, who in turn, shall promptly (within five (5) working days) report any negative findings to the TRVST User Organizations.

3.2 Information Security Asset Lists and Risk Assessment

3.2.1 Assets Inventory, Risk Assessment and Treatment

The TRVST System Provider shall establish an Information Security Risk Register , assigned owners and risk assessed in terms of the threats and vulnerabilities. Appropriate treatments (controls) are being assigned to mitigate the risks. In most cases these treatments already exist and are shown in this document.

This document defines the initial set of controls for the TRVST system, but the Information Security Risk Register and risk assessment/treatment will be updated should any assets change, be added or removed. An end-to-end review of the Information Security Risk Register is carried out at least once annually.

The TRVST system includes a large number of assets. Assets in the Information Security Risk Register are typically shown at a generic level, rather than listing each individual asset. A full list of assets shall be maintained in a live inventory via the Microsoft Azure Portal.

3.3 Information and Document Classification

Information within the TRVST system, including system data, data in supporting tools and systems in any issued documents, shall be classified and handled in accordance with the Data Classification or Information Classification Policy of the TRVST System Provider.

TRVST project documentation will be marked as Confidential, with access restricted to TRVST System Provider staff and contractors and UNICEF TRVST Project staff. This will be achieved through use of access controlled internal project repositories (SharePoint based) and a repository provided by the TRVST Org for file sharing and review. Sharing of files via email is not prohibited under the “Confidential” categorisation but is discouraged and staff will be encouraged to use shared links to repositories. TRVST Org and TRVST System Provider shall employ best reasonable efforts to avoid the inclusion of TRVST User Organizations’ Confidential Information or Data in such project documentation. In circumstances where the inclusion of TRVST User Organization’s Confidential Information or Data is strictly necessary, TRVST Org shall promptly notify TRVST User Organization and work with them in good faith to minimize, redact or otherwise remove such information as reasonably required by TRVST User Organization, prior to uploading the relevant project documentation to any project repository.

4 TRVST System Security and Continuity Measures

4.1 Architectural Specification

TRVST system architecture and non-functional security requirements will be captured in appropriate specifications (e.g. Solution Architecture and Design Specification, Non-functional Specification). The specifications capture any relevant controls detailed in this document.

4.2 Firewalls

The TRVST System is protected by a Web Application Firewall (“WAF”) to reject unauthorised traffic and requests.

Firewalls provide a mechanism of filtering the data requests attempting to connect to the System. The Firewall is responsible for scanning packets of data to identify whether the contents contain patterns or structures which are consistent with previously identified malicious forms. Any threats which are identified can then be intercepted before they are able to reach the applications.

The TRVST system uses a WAF developed by Barracuda Networks Inc. The Barracuda WAF protects systems against a variety of attacks including the OWASP Top 10 and application-layer Denial of Service attacks. The WAF is the only part of the system exposed to the internet where multifactor authentication is not required (for example, the multifactor authentication required on the public facing OBP API), applying security policies to all external traffic before routing it to the relevant API endpoint or application.

4.2.1 Denial of Service Protection

The WAF is able to utilise its capabilities in restricting and controlling the network to identify and protect against Denial-of-Service attacks (DoS).

4.3 Access Management

4.3.1 Secure Data Access

Access to TRVST data is provided in a secure and controlled fashion to ensure that the system supports many viewpoints without compromising the regulatory interest of different countries or the commercial interests of manufacturers.

- Data access is segregated according to roles, countries and manufacturer/products.
- Data access is anonymised through summaries and roll-ups of detailed events.
- TRVST maintains an audit trail of all reported events and changes to data for individual items. The data provides current and historic visibility for reporting, analysis and data visualisation purposes.
- All TRVST users (human and system) are authenticated and authorised using modern and secure standards.
 - Dashboard users are required to utilise secure username and password authentication.
 - System connectivity is permitted with the use of secure API connectivity standards.

4.3.2 Secure and Authorised Access to Data

TRVST only allows authorised users to access data related to their role. All integrated systems are fully validated to ensure security. TRVST is able to support additional authentication through the use of one-time passcode distribution.

TRVST includes role-based access control, restricting access to pre-defined reports and the data they can contain according to role. For example, a government official may only be able to access and view data relevant to their country.

The TRVST Administrator if provided unrestricted access to all master data, batch serialization data, verification data and user profiles for duly authorised TRVST Users (e.g. users representing managing entities), as required. This data can be downloaded directly by users via the reporting capability.

4.3.3 Placing Inactive Accounts On Hold

The TRVST System Provider has an operational process for monitoring user access to accounts – including dashboard accounts - and, if required, locking these if they have not been used for a defined period (e.g. three (3) months). The same process can be used to close the account after a further period (e.g. after 6 months). Personal data is deleted from such accounts on closure.

4.4 Authentication Interface for TRVST Users

4.4.1 Password Policies

TRVST supports the enforcement of policies for password complexity and expiry. TRVST's external interfaces (TRVST Dashboard) are configured to meet the following requirements:

- Password expiry, as agreed by stakeholders (90 days by default)
- Password length as agreed with stakeholders (at least 12 characters by default)
- Password reuse as agreed with stakeholders (cannot reuse last 10 passwords by default)
- Passwords to use at least 3 different character types (Uppercases, Lowercase, Numeric, Special Character)
- Accounts to be locked out after a configurable number of invalid attempts (locked out for half an hour after 3 attempts by default).

4.4.2 Password Resets

TRVST users can reset their passwords at any time through a self-service user interface. Password resets can be enforced at regular intervals or by administrators.

4.4.3 Multi-factor Authentication

Two factor authentication to the dashboard is supported. This uses one-time passcodes communicated over a separate channel (email, SMS) to end-users.

4.4.4 CAPTCHA Verification

TRVST supports the use of CAPTCHA technology to provide assurance of human user access.

4.5 System Account Authentication

TRVST supports the use of system accounts for client systems that integrate with it using its verification API. Verification applications are issued with a set of credentials which uniquely identify it to TRVST.

The Connected Partner API is secured using X509 certificates issued to manufacturers together with a 36-character password. System users requesting data from the systems require a randomly generated ID and password that are 36 characters long. X509 certificates are changed every 12 months and system user passwords change daily.

4.6 Data Encryption

The TRVST System employs encryption of data at rest and in transit. TRVST System Provider shall ensure that all Data is handled, processed, and stored, at all times, in such a manner as consistent with the data security classification applicable to such Data, as outlined in the Data Access Rules. TRVST System Provider shall protect all Data from corruption and from unauthorized access and interference both while such Data is within the possession and/or control of TRVST System Provider and while (if transmission is strictly required for the purpose of managing, maintaining, or supporting the TRVST System) it is in transit across a network (whether public or private). Data encryption is used to ensure that, if an unauthorised individual gains access to a system, they are unable to read the data within it. Data encryption can be employed utilising numerous mechanisms both on stored data (data at rest) and data being communicated in messages (data in transit).

4.6.1 Data Encryption in Transit

The TRVST interfaces and dashboards support data transmission security industry standards including HTTPS and end-point encryption. TRVST system data is encrypted using at least TLS 1.2 when in transit.

4.6.2 Data Encryption at Rest

TRVST data is encrypted at rest using Microsoft Azure Storage Services. Updates to security protocols will be made as part of the ongoing maintenance of the TRVST System, and as and when Microsoft Azure makes updates.

4.7 Malware Protection

Operating systems within the TRVST Azure subscription shall be protected using Microsoft Defender.

4.8 Mobile App

Mobile app users are only able to use this to look up information and cannot use it to upload or modify data. Such look up information is restricted to pack verification details and EPIL data. The TRVST system APIs block the app server from any further access utilising the Azure Identity API.

From Release 2.0 onwards access to the app can be restricted to authorised users if required by stakeholders.

4.9 Data Integrity and Non-Repudiation

All data upload transactions are immutably stamped with details including the date/time and user/organisation performing the upload. These details are captured in the TRVST system transaction audit trail and non-repudiation database for future reference in case of data integrity or repudiation queries.

4.10 System Redundancy, Resilience and Availability

System capacity, redundancy and availability have been designed into the system to meet the TRVST contractual Service Levels.

The TRVST system is based on Microsoft's Service Fabric Architecture which allows the system to be scaled in response to demand. The TRVST System Provider's Operations Team monitors system capacity and demand to allow such response. Service Fabric also provides a level of load balancing and "self-healing" in the event that individual parts of the system are experiencing capacity or other performance issues.

4.10.1 Backup

The TRVST system utilises Microsoft's backup technologies. Backups of business data are taken every four hours, with the last two backups being retained. Recovery requires Microsoft to supply the backups and for this data to be restored into the system. Such recovery may take up to 24 hours.

The TRVST software code is stored under source control in the cloud-based Azure DevOps system. Azure DevOps data is backed up and replicated (mirrored) to a secondary Microsoft data centre (in a separate region) to provide resilience and ability for data recovery.

TRVST System Provider shall ensure that any Data is appropriately backed-up and shall have in place and maintain up-to-date service and business continuity procedures (as referenced in Section 4.15) to ensure that in the event of a failure of or disruption to, the TRVST System Provider's infrastructure the TRVST System Provider is able to continue providing all TRVST-related services to normal performance levels within the shortest practicable time. If TRVST System Provider is affected by any event that requires it to invoke its service or business continuity procedures it will notify TRVST Org, who in turn, will promptly (within five (5) working days of such event occurring) notify all TRVST User Organizations.

4.11 Monitoring and Auditing

4.11.1 Security Monitoring

The TRVST System Provider shall use Microsoft tools to monitor its Azure-based systems for any activity which might suggest a Security Breach. Outputs from these tools can be used to audit for unusual activity or to provide diagnostic information during Security Incidents.

4.11.2 Auditing

Each authentication and authorisation action within TRVST is recorded in an audit trail which can be reviewed in case of any suspicious activity.

4.12 Changes to Production Environments

The TRVST System Provider's Change Management procedures shall not allow changes to Production Environments that have not been authorised by its Change Advisory Board (CAB) and, wherever possible, the System Owner (which is the TRVST Org in the case of the TRVST system):

- Low risk changes may be pre-authorised ("Standard Changes") by both parties to allow for routine maintenance to be carried out without requiring approvals in each instance.
- "Emergency Changes" may be made to restore the TRVST service in case of severe performance issues or to respond to security or continuity incidents. In case of such changes, the System Owner will be contacted for approval where possible but the TRVST System Provider reserves the right to perform these changes without System Owner approval if strictly necessary, to maintain the system integrity.
- Other types of change are termed "Non-standard changes" and will require both CAB and System Owner approval. Such changes include functional changes and defect fixes associated with scheduled TRVST releases.

4.13 Patching

4.13.1 TRVST System

Patching of the TRVST system will follow the TRVST System Provider's Change Management Procedures. These allow for Emergency Changes to be applied for high criticality patches (including those for high-risk vulnerabilities). The Change Management process is covered in Section 4.12.

4.13.2 Operating System

TRVST System Provider's Patch Management Policy shall require that routine Operating System patches are applied within 120 days and that high criticality Operating System patches are applied within 14 days of issuance. Such patching will be registered as a Standard Change for the TRVST system to allow these to be pre-authorised. All patches are risk assessed and smoke tested in a non-Production or staging environment prior to deployment.

The TRVST System Provider shall routinely receive and monitor notifications from Microsoft and other vendors relating to Operating System patches.

4.14 System Security Testing

The following security testing will be carried out on the TRVST system:

- Static security testing will be performed on TRVST source code using a specialist application security (vulnerability) testing tool. This tool identifies any common security vulnerabilities that may be present in the source code so that these can be addressed appropriately prior to application build. This testing is carried out automatically as part of the development activities.
- Annual penetration testing and infrastructure vulnerability scanning will be carried out on the TRVST system. This are arranged by the TRVST System Provider to be carried out by an

independent third-party specialist organisation. Reports from these tests will be produced together with recommendations for any remediation activities.

4.15 Service Continuity Planning

4.15.1 TRVST Continuity Plan

The TRVST System Provider uses a standard template for its system Service Continuity Plans which includes the following sections:

- Purpose, objectives and scope
- Plan administration, including ownership, distribution, storage, training, testing and review requirements
- Continuity incident management process
- Impact assessment of availability loss of incidental system components
- Risk assessment of the range of continuity incidents and events.
- Continuity scenario response plans.

The response plans are tested annually (where practical; certain catastrophic scenarios cannot be practically tested).

4.15.2 TRVST System Provider Business Continuity Plan

TRVST System Provider maintains a Business Continuity Plan for its internal activities. This is reviewed and tested annually.

4.16 Security and Data Breach Incident Management

Management of Security Incidents or Data Breaches follow the TRVST Information Security Incident Response Procedure..