



Traceability and Verification System

Information Security Incident Response Procedure

Version: 02.00 (14 January 2026)

Document control

| Version | Date | Author | Changes |
|---------|------------------|-------------------|---|
| 00.01 | 15 May 2023 | Alexander Blecken | Document initiation |
| 00.10 | 27 July 2023 | Alexander Blecken | Document shared with Data Sharing Task Team, VTI Steering Committee and other stakeholders |
| 00.19 | 18 October 2023 | Alexander Blecken | Updated version including all comments and feedback received from Data Sharing Task Team, VTI Steering Committee and other stakeholders |
| 00.90 | 22 November 2023 | Alexander Blecken | Revised version shared with Data Sharing Task Team, VTI Steering Committee and other stakeholders |
| 01.00 | 13 March 2024 | Alexander Blecken | Final version |
| 02.00 | 14 January 2026 | Richard Wilder | Amended version based on comments received |

Table of Contents

| | |
|--------------------------------------|----------|
| Document control | 2 |
| Table of Contents | 3 |
| 1 Introduction | 4 |
| 2 Definitions | 5 |
| 3 Scope | 5 |
| 4 Standards | 6 |
| 5 Process | 7 |
| 5.1 Overview | 7 |
| 5.2 Identification | 7 |
| 5.3 Reporting..... | 8 |
| 5.4 Preliminary Measures | 8 |
| 5.5 Incident Response Team | 9 |
| 5.6 Containment and Eradication..... | 9 |
| 5.7 Communication | 9 |

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 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 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.

SolidSoft Reply serves as the TRVST System Provider, 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](#).

This document defines the process to be followed for reporting and management of Security Incidents, of which data protection incidents and Personal Data breaches are subsets. It aims to ensure a quick, effective, and orderly response to information Security Incidents. It also covers reporting and management of information security Vulnerabilities and Security Events.

The type of data stored in the TRVST system are described in the Data Access Rules. It is important to note that many of the data are high-risk and thus access to these and other data are strictly controlled. Any Information Security Incident must be immediately reported such that the effects can be mitigated.

2 Definitions

The terms and abbreviations used in this document are defined in the Enterprise Agreement. For ease of reference, the terms which are most relevant to understanding this document include:

| | |
|-----------------------------|---|
| Data Breach | A Security Incident leading to the accidental, unlawful, illegitimate, or unauthorized destruction, loss, alteration, access, use or disclosure of Data transferred, stored or otherwise processed through the TRVST System, including Personal Data and Confidential Information. |
| Information Security | Preservation of the confidentiality, integrity and availability of data and other information (in this case, the assets within the scope of this document). |
| Security Event | An occurrence or change in circumstances which indicates that there is an ongoing or imminent Threat to Information Security. An event doesn't necessarily lead to an incident and may be prevented by in-place controls. Examples are a virus captured by antimalware, an unauthorized person inspecting secure buildings, theft of a locked and encrypted laptop, or a Distributed Denial of Service (DDoS) attack thwarted by prevention tools. |
| Security Incident | One or more Security Events which indicate that there has been – or is expected to be – negative impact to Information Security (the confidentiality, integrity or availability of assets and data within the scope of this Procedure). Examples include a virus not being captured by anti-malware, an unauthorized person gaining access to a secure building, theft of an unlocked or unencrypted laptop or a system outage caused by a DDoS attack. |
| Threat | A (potential) cause of a Security Event or Security Incident. Examples include viruses, malicious actors (amateur hackers, cybercriminals, state-sponsored hackers etc.), opportunistic thieves. |
| Vulnerability | A weakness in Information Security that could be exploited by a Threat. Examples are anti-malware not being in place, unlocked doors in buildings, unencrypted hard drives on laptops, DDoS protection not being in place |

3 Scope

This Procedure applies to all staff, personnel and consultants of the TRVST Org (UNICEF), TRVST System Provider (SolidSoft Reply) and TRVST Project Management Unit. It also applies to all TRVST users as defined in the TRVST Data Access Rules. This Procedure covers Security Incidents involving the TRVST system which may include Personal Data or otherwise high-risk information. It covers all information security Vulnerabilities, Threats, Security Events and Security Incidents relating to the TRVST data or assets. These data and assets include but are not necessarily limited to:

- TRVST Org, TRVST System Provider and TRVST PMU premises (whether owned or rented)
- Physical assets of TRVST Org, TRVST System Provider and TRVST PMU, including staff laptops and other devices which contain TRVST information or connect to TRVST resources.
- All TRVST-related electronic data, assets and resources managed by TRVST Org, TRVST Solution Provider and TRVST PMU, including email and messaging accounts; cloud-based tools, storage and repositories; customer systems, data and storage; data stored on staff laptops and devices.

This Procedure does not apply to any non-TRVST system that is not integrated with or related to the TRVST data or assets, provided that such non-TRVST system is not capable of posing a security risk to TRVST data and assets. Such incidents are handled through established Policies and Procedures of the TRVST Org and/or TRVST System Provider.

In the event of any conflict or inconsistency between the provisions of a Data Governance Document and the UNICEF or TRVST System Provider IMS-or SRI-denominated documents referenced in this Data Breach 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 Data Breach Procedure other than that giving rise to the inconsistency.

4 Standards

Effective Information / Cyber Security Incident Management involves both proactive and reactive measures such that Security Events and Security Incidents are captured, reported, mitigation actions executed and communications to appropriate management levels are informed as quickly as possible.

The TRVST System is governed by the TRVST Information and Security Procedures, which set the Information Security and Continuity policies and controls that are being applied during development and operation of the TRVST System, and how these will be documented. These policies and controls take into account the risks relating to the confidentiality, integrity, privacy, and availability of TRVST information and continuity of the operational TRVST system.

All TRVST User Organizations will be made aware of their responsibility to report Security Incidents as quickly as possible.

This Data Breach Procedures is based on applicable policies and standards of the TRVST Org (UNICEF) and the TRVST System Provider (SolidSoft Reply). These include, amongst others:

- a) UNICEF Policy on Information Security (CF/ITSS/POLICY/2014-001)
- b) UNICEF Standard on Information Security Incident Management (ICTD/STANDARD/2018/005),
- c) [UNICEF Policy on Personal Data Protection](#) (POLICY/DFAM/2020/001)
- d) SolidSoft Reply Information Security and Data Protection Policies (IMS0079)

The TRVST System Provider (SolidSoft Reply) handles reported data breaches according to its Standard Operation Procedure for Management of Information Security Incidents (IMS0089). The TRVST Org (UNICEF) handles Personal Data breach according to the UNICEF Procedure for Personal Data Breach (PROCEDURE/DFAM/2020/009).

This Information Security Incident Response Procedure focuses on the actions in response to Security Events and Security Incidents involving and specific to the TRVST System. It is complementary to the applicable policies but does not amend or replace them. Standards and Procedures of the TRVST Org and the TRVST System Provider need to be read in conjunction with them.

5 Process

5.1 Overview

The response to an information Security Incident generally includes:

1. Identifying a Security Incident
2. Reporting of the Security Incident
3. Taking preliminary measures
4. Forming an Incident Response Team
5. Responding to an incident, which includes containing the incident, eradicating the information security weakness(es) found to cause or contribute to the incident. and collecting evidence as soon as possible after the occurrence
6. Communicating in the appropriate manner to the relevant stakeholders the existence of the Security Incident or any relevant details thereof to other internal and external people or organizations with a need-to-know

5.2 Identification

For the purposes of this document, examples of Security Incidents include

- a) Access by an unauthorized third party of TRVST data that is unencrypted or can be decrypted without unreasonable effort
- b) Lost or stolen computing devices containing a copy of TRVST data that is unencrypted or can be decrypted without unreasonable effort
- c) Unauthorized or accidental alteration of TRVST data
- d) Unauthorized or accidental deletion of TRVST data
- e) Unplanned loss of availability of TRVST data for a significant period (the significance being determined by the sensitivity of the data)

There are a number of indications that an Security Incident may have occurred. These should be treated as warning signals necessitating further investigation. These include, for instance,

- Network and or system monitoring alarms
- Antivirus software alerts
- Web server crashes/defacement/redirects.
- System administrator sees a filename with unusual characters.
- Host records an auditing configuration change in its log like for example disabling of security auditing on windows servers.
- Application logs multiple failed login attempts.
- E-mail administrator sees a large number of bounced e-mails with suspicious content.
- Network administrator notices an unusual deviation from typical network traffic flows.
- Access violations
- Undocumented/unapproved changes.
- Human errors.
- Denial of service attacks like ransomware etc.

5.3 Reporting

All TRVST User Organizations and the TRVST System Provider have the obligation to report Security Incidents in accordance with this section.

At the TRVST Org, the UNICEF Global Shared Services Centre (GSSC) handles Security Events, Vulnerabilities and Security Incidents, perform initial assessment, open a ticket if appropriate, and escalate to the appropriate person/team for necessary action, follow-up the progress, inform the reporting person about the progress, and close the ticket once the issue is fully addressed.

GSSC Customer Care has established an escalation for high-risk and confidential cases, to ensure privacy is maintained and information only accessed by those with the appropriate clearance and roles to handle such cases. The Customer Care Team is available 24 hours a day, 7 days a week.

Should an information Security Incident transpire, TRVST User Organizations or the TRVST System Provider (as applicable) must inform [GSSC Customer Care](#) as quickly as possible. UNICEF staff and consultants with access to UNICEF's intranet can reach GSSC Customer Care by submitting a [GSSC General Enquiry](#) in Service Gateway; or voice calling "Customer Care" in Microsoft Teams or chatting with an agent in Service Gateway. TRVST User Organizations and the TRVST System Provider can contact GSSC Customer Care by dialing +361 790 9300 from any telephone or sending an email to customercare@unicef.org.

TRVST User Organizations or the TRVST System Provider must report Security Incidents as soon as possible (ideally within 24 hours). Any Security Incident that directly or indirectly impacts, affects or otherwise concerns a TRVST User Organization's Data must be reported to TRVST Org as soon as possible (no later than within 24 hours) after the TRVST System Provider or TRVST User Organization becomes aware of the Security Incident. The report should include

- How the TRVST User Organization or TRVST System Provider became aware of the Security Incident
- How the Security Incident occurred
- Time of breach (e.g., date, time and time zone)
- Confirmation of type of data (e.g. high-risk or Personal Data) was affected
- What Personal Data was affected (if applicable)
- Number of people whose data was affected (if applicable);
- Who gained access to the data (if known);
- Actions already taken to correct the Security Incident, if any.

The TRVST User Organization / TRVST System Provider (as applicable) informs the TRVST Project Manager, Max Kabalisa (mkabalisa@unicef.org) of the Security Incident.

Upon receipt of the notice from the TRVST System Provider or TRVST User Organization, the TRVST Org informs any of the affected TRVST User Organizations immediately.

Security Events and Vulnerabilities shall be documented and reported to TRVST Org by the TRVST System Provider as part of its formal security review process (described in Section 3.2 of the Information Security Procedures).

5.4 Preliminary Measures

When a Security Incident is reported by a TRVST User Organization, GSSC Customer Care promptly notifies the Security Operation Center, Budapest (+361-790-9300) and the TRVST System Provider Helpdesk, which will raise a ticket. The TRVST System Provider's Quality Team will be copied on that email and will lead the response from the TRVST System Provider. The TRVST System Provider will then

respond to the Security Incident by following in accordance with the Standard Operation Procedure for Management of Information Security Incidents (IMS0089).

In all cases, the UNICEF Security Operations Center in consultation with the TRVST Project Manager and the TRVST System Provider Helpdesk will take immediate technical and operational measures in line with UNICEF ICTD operating procedures to document the Security Incident and prevent it from worsening pending the preliminary review.

If the Security Incident involves Personal Data, it must be handled in accordance with the UNICEF Procedure for Personal Data Breach (PROCEDURE/DFAM/2020/009). The Procedure prescribes accelerated timelines, e.g. the conclusion of an initial review of the Security Incident, including any related Data Breach within 24 hours.

5.5 Incident Response Team

An Incident Response Team will be formed consisting of the TRVST Project Manager, a representative from the TRVST System Provider, any representative from UNICEF ICTD as nominated by the Security Operation Center, and any other stakeholder as nominated by the TRVST Project Manager.

In case Personal Data was part of the Security Incident, the UNICEF Data Protection and Privacy Specialist is also a member of the Incident Response Team.

As a default and unless otherwise determined by the TRVST Project Manager, the representative from the TRVST System Provider will lead the Incident Response Team.

5.6 Containment and Eradication

As soon as a Security Incident has been identified, steps must be taken to contain it and, where necessary, prevent it from spreading. Rapid response may be needed, and such decisions should not be delayed unnecessarily.

The Incident Response Team should discuss and consider whether it needs to contain the threat by:

- Removing or blocking unauthorized access
- Blocking dangerous IP or email addresses
- Restricting or monitoring physical access (in case of physical breach)
- Other actions

The Incident Response Team should also consider and act on the steps to eliminate the cause, such as:

- Deleting malware
- Changing targeted IP addresses
- Disabling breached user accounts (or resetting passwords)
- Hardening any vulnerabilities which were exploited

5.7 Communication

In all communications, consideration shall be given to minimizing the information to be communicated and the stakeholders to whom this shall be communicated (including internal staff). This is in order to prevent the potential of further exploitation of vulnerabilities, disclosure of high-risk information or distraction of managing a broader audience than needed.

Where determination has been made that there was a Personal Data breach with a risk to the rights of an individual, or allegations of such breach have been communicated to UNICEF, communications may be required to the affected persons (data subjects), UNICEF associates, governing body (or bodies) of the TRVST System, the media or others. Communication with data subjects follows the UNICEF Procedure on Personal Data Breach, Paras 23-25. All reasonable efforts shall be made to notify data subjects within 72 hours of receipt of UNICEF becoming reasonably certain that a data breach has occurred that has resulted in a high risk to the individuals affected.

Subject to the last paragraph of Section 5.3, whereby reporting to the affected TRVST User Organization(s) is always required, the Incident Response Team determines whether other communications are appropriate.