Data Privacy and Network Security User Manual

This Data Privacy and Network Security User Manual provides operational and technical guidance to OneImpact implementers to ensure data privacy and network security during OneImpact CLM projects. The User Manual consists of the following parts:

1. Require Personnel to Sign OneImpact Confidentiality Agreements
2. Prepare a OneImpact Incident Response Plan
3. Conduct Periodic OneImpact Data Audits
4. Require Use of Passwords and Multi-Factor Authentication (MFA) to Access the OneImpact Network
5. Implement Data and Network Access Controls
    a. Role-Based Access Control
    b. Public Wi-Fi and Virtual Private Networks (VPNs) Policy
    c. Antivirus Software
    d. Auto-Lock
6. Ensure OneImpact Data Provided to Third Parties is De-Identified and Anonymized
7. Segment the OneImpact Network
8. Implement a OneImpact Data Deletion and Destruction Policy
9. Conduct Regular Maintenance and Upkeep of the OneImpact Network

Require Personnel to Sign OneImpact Confidentiality Agreements

OneImpact implementers should require all personnel involved in OneImpact CLM to sign a OneImpact Confidentiality Agreement. The agreement should prohibit all personnel from disclosing, releasing or using in any other unauthorized way information collected by OneImpact on penalty of disciplinary or legal action, depending on the severity of the transgression. All personnel should be required to sign the confidentiality agreement before they are permitted to work on any OneImpact-related project. For example, personnel should be required to sign the agreement prior to receiving passwords, keys or any other kind of access to data collected by OneImpact. Personnel required to sign the OneImpact Confidentiality Agreement should include all people involved in OneImpact-related project working at the implementing organization and all other people with access to the data or network, such as government authorities, health care officials, any other partner organizations that collect, store or use OneImpact data.

Prepare a OneImpact Incident Response Plan

OneImpact implementers should prepare an incident response plan to identify and respond to data breaches, data misuse, data theft, administrator errors and other data privacy or network security incidents. An incident response plan consists of several seps and sets forth actions, escalations, mitigation, resolution, and notification of any potential incidents

impacting the confidentiality, integrity, or availability of OneImpact user data. The steps and activities include:

⇒ ***Preparation***: Create, document and approve the plan, ensure detection technologies and tools are available and in place, and organize and train an incident response team who will conduct the incident response;
⇒ ***Coordination***: Convene the incident response team and coordinate with all necessary stakeholders, such as Dure Technologies, and OneImpact implementers;
⇒ ***Identification***: Identify the privacy or security incident of concern using relevant technology and tools, and learn where and how the incident occurred, what and who is affected, and what the scope of the impact is;
⇒ ***Containment***: Contain the threat and mitigate the damage from the privacy or security incident;
⇒ ***Investigation***: Conduct an investigation and gather as much information as possible about the incident to fully understand why and how it occurred;
⇒ ***Eradication***: Eliminate the root cause of the privacy or security threat, such as removing malware, rearranging access controls, reprogramming problematic functions, etc.;
⇒ ***Recovery***: Restore affected systems, and consider changing passwords, applying patches, reconfiguring firewalls, etc.;
⇒ ***Remediation***: Provide remedy and redress to people affected by the privacy or security incident, such as users of an app, website or other electronic service; and
⇒ ***Lessons Learned*****:** Review and analyze the results of the investigation and the effectiveness of the incident response plan, more broadly, to understand what happened during the incident to identify and implement lessons learned, including updating and improving training for the incident response team to protect against future incidents.

In the event of a OneImpact data privacy or network security incident, to fullest extent possible, OneImpact implementers should work closely with the Stop TB Partnership and Dure Technologies to implement these stages and activities of the OneImpact Incident Response Plan.

Conduct Periodic Data Audits

OneImpact implementers should conduct periodic data audits of OneImpact CLM. A data audit is an analysis of the quality and utility of data collected by a particular process, technological device or organization. The goals include to improve the efficiency of processes, ensure compliance with laws and other norms, and to generally examine and better understand data collection, storage and use policies, processes, practices and

purposes. In practice, a data audit comprises a series of steps to ask, answer and analyze the results of questions about data content, processes, practices and purpose. These may be represented by the following questions:

⇒ *What kinds of data are we collecting?*
⇒ *Is there consensus around a clear, justifiable purpose for each kind of data we collect?*
⇒ *What is the integrity of the data—i.e., is it accurate, truthful, etc.?*
⇒ *Who is collecting, storing and using the data?*
⇒ *How and where are we storing the data?*
⇒ *How long do we keep the data?*
⇒ *How do we protect the data?*
⇒ *What is our process for honoring a request from a data subject to delete or modify their data?*
⇒ *Are our data policies, processes and practices in compliance with all applicable law and regulation, as well as human rights norms?*

The results of the data audit should be considered in light of the OneImpact Legal Landscape Assessment and the OneImpact Conceptual Framework, to ensure OneImpact implementers are in compliance with applicable law and working in accordance with the conceptual framework.

Require Use of Passwords and Multi-Factor Authentication (MFA) to Access the OneImpact Network

OneImpact implementers should implement strong password policies throughout OneImpact networks, requiring all personnel with access to the networks to use long passwords with different characters and periodic password changes. Ideally, implementers should provide password managers to all OneImpact network users.[1] Each user could then use a password manager to generate unique, strong passwords and securely store them.

OneImpact implementers should require Multi-Factor Authentication (MFA) on all computers and devices used in OneImpact networks.[2] MFAs are an authentication method that require a network user to present two or more pieces of evidence—i.e., factors or

[1] For resources on password managers, *see, e.g.*, https://www.consumerreports.org/digital-security/everything-you-need-to-know-about-password-managers/; https://www.cnet.com/news/password-managers-a-little-pain-for-a-lot-better-security-world-password-day/; https://en.wikipedia.org/wiki/Password_manager; https://www.cnet.com/how-to/best-password-manager-to-use-for-2020-1password-last-password-more-compared/.
[2] For resources on MFAs, *see, e.g.*, https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication; https://en.wikipedia.org/wiki/Multi-factor_authentication; https://www.onelogin.com/learn/what-is-mfa.

credentials—to log into and access a network. These factors include unique knowledge (something the user and only the user knows, like a password), possessions (something the user and only the user has, like a smart card), and inherence (something the user and only the user is, like a fingerprint). MFAs increase network security by making it more difficult for unauthorized users to successfully provide these unique credentials to access the network.

Implement Data and Network Access Controls

OneImpact implementers should implement data and network access controls for the OneImpact network. Data access controls comprise practices, protocols and technologies that limit access to certain kinds of data only to designated, authorized personnel. Network access controls are practices, protocols and technologies that control how and whether computers and devices access a computer network.

Role-Based Access Control

OneImpact implementers should use role-based access control (RBAC) for OneImpact networks and data. RBAC restricts access to a network or certain data in a network based on a person's role in an organization. It is one of the primary methods for advanced access control to data and networks. OneImpact implementers should designate specific roles with designated duties within an established hierarchy to which corresponding authorizations are granted to access the OneImpact network and data. The underlying principle should be to restrict personnel's' access to the network and data, unless access is required for a specific role to effectively perform its duties.

Public Wi-fi and Virtual Private Networks (VPNs) Policy

OneImpact implementers should enforce a policy to prohibit the use of public wi-fi in OneImpact networks and require all computers and devices to use Virtual Private Networks (VPNs) when remotely accessing OneImpact networks. Public wi-fi networks are inherently less secure than personal, private networks. Though they are generally safer than in the past, hacking incidents on public wi-fi are still common. VPNs extends private networks across public networks so that users may send and receive data within a public network as if their computer or device was connected to a private network.[3] VPNs accomplish this by disguising a user's internet protocol (IP) address and establishing secure and encrypted connections with servers. VPNs can be used on any device that connects to the internet. In

[3] For resources for VPNs, *see, e.g.*, https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html; https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html; https://www.merriam-webster.com/dictionary/VPN.

essence, VPNs provide user's strong protections for privacy and security when they connect to the internet using a public network.

Antivirus Software

OneImpact implementers should require antivirus (also called anti-malware) software be used on all computers and devices accessing OneImpact networks. Antivirus software are computer programs that prevent, detect and remove malware.[4] Malware is software intentionally designed to cause damage to a computer or device, a server, or an entire network. Among other things, malware could be used to access and/or steal OneImpact data or harm the operation of OneImpact networks. Requiring all computers and devices operating within a OneImpact network to protect against malware will provide an added layer of privacy and security for OneImpact data.

Auto-Lock

OneImpact implementers should require auto-lock be set on all computers and devices used in OneImpact networks, especially, but not only, those used to remotely access the network. Auto-lock is a feature that locks a user's computer or device after a preset time, requiring them to reenter their password and other credentials (if using MFA) to reenter the network. Auto-lock is a common security feature on smart phones, for example. It increases network security by limiting the amount of time during which an unauthorized network user can gain access to the network after a user has logged in and left their device unattended.

Ensure OneImpact Data Provided to Third Parties is De-Identified and Anonymized

OneImpact implementers, with assistance from the Stop TB Partnership and Dure Technologies, should ensure all OneImpact data that is provided to the Stop TB Partnership, all government authorities, and all other third parties is de-identified and anonymized. This includes all data that is aggregated together to create larger datasets. De-identification is the process of removing personally identifiable information (PII) from data so that the identity of the person who provided the data cannot be ascertained. De-identification is not a single technique but rather a collection of methods, algorithms and tools that can be applied to different kinds of data resulting in different levels of protection. Data anonymization is a form of de-identification that involves removing PII from data sets, so that the people who provided the data remain anonymous. Anonymization aims to

[4] For resources on antivirus software, *see e.g.*, https://www.antivirussoftwareguide.com/free-antivirus-software; https://us.norton.com/internetsecurity-malware-what-is-antivirus.html; https://en.wikipedia.org/wiki/Antivirus_software.

irreversibly removal the link between the data subject their health data, so that it would be virtually impossible to reidentify the person.

Segment the OneImpact Network

OneImpact Implementers should ensure all OneImpact networks are segmented to protect the personally identifiable information (PII) of community users. Network segmentation divides computer networks into smaller parts in order to protect sensitive data. This is done by segmenting the data in a protected part of the network and controlling the flow of traffic to and from this part. Network segmentation can be accomplished using internal firewalls,[5] Access Control Lists (ACL),[6] Virtual Local Area Networks (VLAN)[7] or software-defined access technologies.[8] OneImpact network segmentation should be applied in coordination with a OneImpact role-based access control policy, discussed above, so that only select personnel are provided access to the protected segment of the network.

Implement a OneImpact Data Deletion and Destruction Policy

OneImpact implementers, with assistance from the Stop TB Partnership and Dure Technologies, should implement a OneImpact Data Deletion and Destruction Policy with clear protocols. The principle underlying data deletion and destruction policies is that data should be deleted from all computers, devices and drives as soon as it is no longer required for the purposes for which it was collected. Data deletion and destruction policies enhance data privacy and security by ensuring data is stored for the shortest length of time possible. That is, the shorter the duration of storage, the less chances for privacy or security incidents. Data deletion and destruction policies also require all data be removed form computers, devices and drives used to store data which are no longer required for a particular project. Or, if computers, devices or drives used in the network are to be discarded, they must be overwritten or destroyed so their data may not be accessed after they are discarded.

In order to develop an effective data deletion and destruction policy, OneImpact implementers should work with the Stop TB Partnership and Dure Technologies to establish

---

[5] *See* https://www.vmware.com/topics/glossary/content/internal-firewall and https://docstore.mik.ua/orelly/networking/firewall/ch04_04.htm.
[6] *See* https://www.imperva.com/learn/data-security/access-control-list-acl/ and https://en.wikipedia.org/wiki/Access-control_list.
[7] *See* https://www.dummies.com/programming/networking/cisco/virtual-local-area-network-vlan-basics/ and https://en.wikipedia.org/wiki/Virtual_LAN.
[8] *See* https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/what-is-software-defined-access.html and https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/solution-overview-c22-739012.html.

protocols for when data collected by OneImpact is no longer required for TB community-led monitoring and must therefore be deleted. The policy should apply to all entities that store OneImpact data, including the Stop TB Partnership, Dure Technologies, OneImpact implementers, government authorities and all other partners. The data deletion and destruction policy should also establish protocols for the deletion and destruction of data upon the completion of OneImpact projects and when computers, devices or drives used in these projects are discarded.

Conduct Regular Maintenance and Upkeep of the OneImpact Network

OneImpact implementers, with assistance from the Stop TB Partnership and Dure Technologies, should establish standards and protocols for the maintenance and upkeep of OneImpact networks to ensure they are operating effectively and securely based on the most up-to-date privacy and security software, protocols and technologies. Among other things, this entails:

- ⇒ Ensuring regular software updates;
- ⇒ Monitoring network activity for security concerns or incidents based on the OneImpact Incident Response Plan; and
- ⇒ Network testing for common vulnerabilities, such as network device hardware malfunctions, firewall issues, presence of unauthorized network devices, or unauthorized user network access.

Developing a OneImpact Network Maintenance Checklist may be helpful to create easy-to-follow, routine instructions to ensure OneImpact networks are monitored, maintained and kept up to date at regular intervals, such as during bi-weekly or monthly maintenance checks.