USER GUIDE | DATA INTEGRITY

FRONTLINESMS

Acknowledgments

This document has been published with generous support from Internews. This User Guide would not have been possible without the time and attention of the mobile for development community and, most importantly, our users. Technical writing was primarily contributed by Kristina Lugo and Carol Waters, with minor contributions from several other authors. Graphic design by Jessica Lo. FrontlineSMS is grateful for the oversight and advice of an advisory group that included staff, community members, partner organizations, and experts in this field.

Table of Contents

GLOSSARY

Address Book
refers to a person's contact list, stored on a mobile phone. Address books usually contain information like the name, phone number, physical address, e-mail address, and/or organizational affiliation for each contact.

Communication/SMS Hub
is the combination of a computer, a mobile device (either a modem or a phone), and software that enables a user to manage either a high volume of text messages and/or complex interactions.

FrontlineSMS
is a piece of open source software that provides an interface for complex and high volume communications, primarily focused on SMS. FrontlineSMS is a software used to create SMS hubs. FrontlineSMS also offers limited MMS capabilities, forwarding to e-mail, and http triggers for users with Internet access.

Geolocation Data
is information that identifies the location of a mobile device, typically at the time that a message is sent. This information is typically expressed in latitude and longitude coordinates, although any location- identifying information (such as address or proximity to landmarks) can be considered geolocation data.

Hardware
is the physical parts or components of an electronic device. Here, this is most commonly used to refer to either a computer or a mobile phone.

Mobile Network
refers to the physical infrastructure used to transmit voice, text, and internet data. This commonly refers to towers, tranceivers (or cells), and a source of electricity, although the details of each vary by mobile network operator.

Mobile Network Operator
is a company that offers mobile services and administers a mobile network.

Modem
refers to a device that converts and transmits information into a digital format that can be sent using a telephone network. Here, the term modem refers specifically to devices that enable a user to send digital information over a mobile phone network.

Global System for Mobile (GSM)
is a set of mobile network standards that determine how mobile networks manage information to provide services. GSM standards are adopted, in varying degrees, by mobile network operators to provide uniform services and interact across networks more easily.

Global System for Mobile Association (GSMA)
is an association of mobile network operators and related stakeholders. The GSMA is largely recognized to be the organization that sets, updates, and promotes the adoption of GSM standards.

Multi-Media Message Service (MMS)
refers to a way to send messages that include one or more mediums, typically audio recordings, video recordings, or photographs. A mobile phone must be MMS enabled and have access to some form of Internet infrastructure in order to send and receive MMS messages.

Operating System (OS)

is the software that controls how an electronic device processes information and applications. Operating systems are the most important, and determinative, piece of software on any device.

Personal Identification Number (PIN)

is a password or personally kept number that is used to lock a piece of hardware or software. Typically, computers, mobile phones, and certain types of software enable a user to set a PIN to limit access to information or an application.

Secure Digital (SD) Card

is a memory card that can be used with a mobile phone, in order to store information. SD cards are removable and are typically used to increase the amount of information that a user can access on their mobile device.

Server

is a piece of hardware or software that provides services to more than one user. Here, the term server is used to refer to hardware that stores information or applications within a mobile network. Software- refers to the programs, applications, and/or data that an electronic device uses to process information.

Subscriber Identification Module (SIM) Card

is the chip used to connect a mobile phone to a mobile network. SIM Cards contain several unique pieces of information, including a serial number, user/account identifying information, some security protocols, and/or passwords.

Short Message Service (SMS)

commonly known as 'text messages', SMS is a way to send short messages using an alphabet, numbers, and symbols. SMS messages are digital information that can be transmitted over mobile networks, without Internet signal.

Universal Serial Bus (USB)

is a type of connection, or port, on an electronic device. This standard is used to make it easier to connect devices, cords, and accessories (i.e.- keyboards, cameras, and printers).

1 EXECUTIVE SUMMARY

1.1 Background Information

FrontlineSMS is a software platform that enables structured communication via text messaging, using only a computer and a mobile phone or GSM (Global System for Mobile) modem. The platform enables two-way messaging between users and groups of people via mobile networks without the need for an Internet connection.

- Create and manage SMS-related contact groups
- Send and receive messages via special on-screen consoles
- Provide incoming and outgoing message history for each contact
- Engage with contact groups (e.g. surveys, contests)
- Manage a text-based information service with automated responses
- Export information in .csv (comma separated values) format for analysis

1.2 Purpose

The purpose of this guide is to provide FrontlineSMS users designing, implementing, and monitoring programs with data integrity concerns in mind with a data integrity framework. The guide is intended to help users to understand, analyze, and address the vulnerabilities, risks and threats that can affect the integrity of the information communicated through the FrontlineSMS platform.

Users and potential users have different needs for protecting sensitive information. The goal of this guide is to outline the actions that can be taken to mitigate the risks posed by information being lost, changed or read by unauthorized third parties. However, it is important to recognize that FrontlineSMS may not be an appropriate tool to use in some environments where data integrity needs go beyond the capabilities of the platform and SMS itself, and that incautious use may put the organization, program and users at risk.

FrontlineSMS does not define the exact details of how users should deploy the software or address issues of data integrity. Users should evaluate their individual program goals, standards, and operating context to decide on the steps that should be taken to protect the integrity of their information.

1.3 Approach

This guide addresses 'data integrity', as opposed to mobile security, in an effort to draw the discussion into ways to ensure the confidentiality, authenticity, availability, and usability of information regardless of context. Though there are many overlaps, mobile security is highly contextual and is therefore an analysis best left to users. Still, many of the suggestions in this guide are designed to help users protect themselves and their stakeholders. Data integrity, however, also includes an array of considerations and design elements focused on improving the quality of information exchange, regardless of security context. This guide approaches risk, not just from the perspective of the user, but with a focus on the risks to the quality and usability of the information exchanged through a FrontlineSMS hub.

1.4 FrontlineSMS Requirements

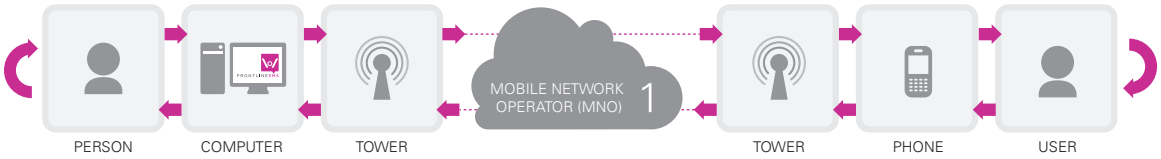
The following are the required system components to deploy FrontlineSMS:

SERVER	Infrastructure	A working power source and access to a GSM network.
	Hub	A computer, laptop, or netbook with a USB serial port to install software and connect peripheral devices. The type of port needed depends on the type of mobile peripheral device.
	Mobile Phone or GSM Modem	A supported GSM modem or phone (please see list of currently supported devices- due to technical differences between makes and models, not all GSM modems or phones will work with FrontlineSMS). A GSM modem is recommended over a phone because it can typically send and receive text messages faster than phones, especially when sent at high volume.
	SIM Card	A SIM card with either a service plan or credits that allow it to send and receive SMS. The SIM card should be inserted in the mobile device that will be connected to the FrontlineSMS computer.
CLIENT	One mobile phone per user or field agent	Access to at least a second mobile phone that is not connected to the computer FrontlineSMS is installed on. This mobile should also be able to send and receive SMS messages to test the installation and configuration of FrontlineSMS. Ideally, this mobile should use the same mobile network provider as the server because, in some places, using different mobile networks may cause large delays between the sending and receipt of SMS. This is not true for all mobile markets and is not a requirement of the FrontlineSMS system.

For information on how to set up the platform, see the FrontlineSMS website: http://www.frontlinesms.com.

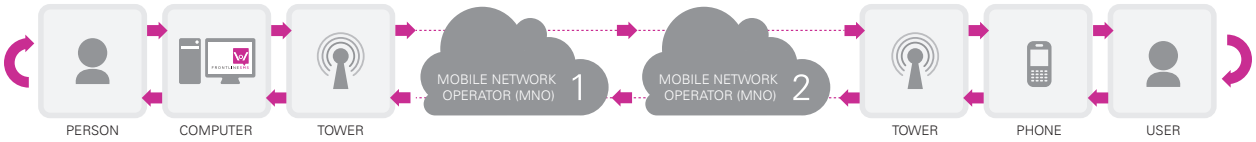
1.5 Overview of Vulnerabilities, Risks, Threats and Risk Reduction

Each element of a FrontlineSMS deployment (the GSM standard, mobile network operator(s), mobile phones, computer hardware, computer software and the human operators) is vulnerable to information being lost, stolen, corrupted or deleted.



Single Mobile Network Operator

This diagram depicts the path of an SMS interaction between a FrontlineSMS user and a mobile phone, or end user, who both subscribe to the same mobile network operator. In this diagram, a FrontlineSMS user enters the message into the communications hub and clicks "send." The message travels through the mobile device to the nearest tower via radio waves. The tower then sends this message back to the mobile network operator's short message service center, which logs the message and user information. Once the mobile network operator determines the end user's availability, it routes the message to the tower base station closest to the intended recipient. The tower communicates that message to the end user's phone via radio waves. The phone receives the data, processes it, and then displays it to the end user. Once the end user reads the message, they type in a response, which follows the same path in reverse, back to the communication hub running FrontlineSMS, which receives and processes the response into usable data.



Multiple Mobile Network Operators

This diagram illustrates the way that data travels during an SMS interaction between a FrontlineSMS user who subscribes to one mobile network operator's services and an end user who subscribes to another mobile network operator's services. The message follows the same path as in the above, except that once the message has been received by the mobile network operator's short message service center, it usually gets sent through a network of cables, signals, and switches that route the message to the short message service center of the end user's mobile network operator. This varies, according to the way that the mobile networks interoperate. In some instances, the FrontlineSMS user's mobile network operator will be able to route the message directly to the end-user's handset.

1.5.1 Global System for Mobile (GSM)

The GSM standard has processes in place to secure information (e.g. voice calls and user information). However, these processes can be broken by an unauthorized user or third party. The broken processes can allow unauthorized users to copy and see all the information stored on the SIM card (e.g. SMS messages, address book) and also use the credits on the SIM card to send and receive voice calls and SMS. An unauthorized user or third party can also perform a man-in-the-middle attack to read SMS messages or listen to voice calls.

To reduce risks, users should minimize the amount of sensitive information communicated and stored on the SIM card or use code words for names of people and places.

1.5.2 Mobile Network Operator (MNO)

No MNO offers end-to-end encryption of SMS messages, leaving SMS vulnerable to being read by unauthorized users. MNOs store all subscriber information, including SMS message content, billing information, geolocation data, usage patterns, and call traffic. This information can be requested by the government or accessed by the employees of the MNO. The government, man made incident or unplanned events such as natural disasters can disrupt mobile service. All of these standards and issues vary from one operator to another.

Users should minimize the amount of sensitive information communicated using mobile services and use code words for names of people and places. If possible, users should not provide identification when buying a SIM card and always have a backup plan for communications if mobile services are stopped.

1.5.3 Mobile Phone

Mobile phones are the key component of FrontlineSMS programs because they are used to send communications and collect information from end users. Vulnerabilities can be found in the hardware and software of the mobile phone.

Mobile phones can be stolen or damaged if they are physically accessed. Malware can be loaded onto a phone by inserting removable storage from an unknown or untrusted person, downloading and uploading files from the Internet or using email services. Malware can load programs on the mobile to allow an unauthorized user to monitor communications or take control of the handset.

Users should lock their mobiles using a strong 8-digit PIN and store their mobiles in a case and bag to reduce the risk of damage or theft. Users should minimize the amount of sensitive information stored on the SIM, handset and removable media. Users should not access the Internet using their mobile and should not insert removable media from an unknown or untrusted person.

1.5.4 Computer Hardware

Computer hardware includes the computer which runs FrontlineSMS and the surrounding environment. Computer hardware can be destroyed by unauthorized users or by its environment, meaning that the information stored on the computer can be lost temporarily or indefinitely. If an unauthorized user gains access to the computer, the sensitive information can be accessed and program resources, such as mobile credits, can be used.

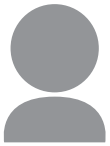
Users should regularly back up and encrypt all the important information to external storage, and keep the external storage in a locked cabinet. Users should keep the computer away from dust, liquids and food. The computer hardware should be locked to a table and laptops should be kept in a locked cabinet. All computer hardware should be stored in a locked room.

1.5.5 Computer Software

Computer software includes the Operating System (OS) and all applications installed on the computer that is running FrontlineSMS. If user accounts are shared or the passwords on the OS and applications are weak, unauthorized users can log in and see sensitive information. If removable media is inserted to the computer or if the email services are accessed, malware and viruses can be loaded onto the computer, and used to read information stored on the computer or to take control of the machine.

All users should have a separate account with a strong password to the OS and applications that contain sensitive information (e.g. the FrontlineSMS platform). Users should not insert removable media into the computer if it is from an unknown or untrusted person, and should limit the use of the Internet to prevent malware and viruses from being loaded. If possible, and if data security is a high priority, the computer running FrontlineSMS should not be used to access the internet.

1.5.6 Human Participation



Sensitive information is at risk of being changed or deleted by insiders that have access to the information. Information can be protected from being changed or deleted by creating separate roles and user accounts with different access rights for each person that can access the computer with the FrontlineSMS platform. Public-facing programs that ask end users to provide information are at risk of receiving information that is wrong or exaggerated.

FrontlineSMS programs relying on the accuracy of information provided by end users should create robust processes for checking its accuracy. Questions or observations received by end users should be validated by a trusted source or by deploying a team member.

2 INTRODUCTION

2.1 Background Information

FrontlineSMS is a software platform that enables structured communication via text messaging, using only a computer and a mobile phone or GSM (Global System for Mobile) modem. The platform enables two-way messaging between users and groups of people via mobile networks without the need for an Internet connection.

FrontlineSMS can be used to:

- Create and manage SMS-related contact groups
- Send and receive messages via special on-screen consoles
- Provide incoming and outgoing message history for each contact
- Engage with contact groups (e.g. surveys, contests)
- Manage a text-based information service with automated responses
- Export information to Excel and .csv for analysis

2.2 Purpose

The purpose of this guide is to provide users with a framework to understand, analyze, and address the vulnerabilities, risks and threats that can affect the integrity of the information communicated through the FrontlineSMS platform. That said, mobile networks are inherently insecure and end users are only able to mitigate, as opposed to prevent, a significant number of the possible threats to data integrity. While there are a large number of ways that user information can be lost, altered, stolen, changed, or read by third parties, this guide focuses on the ways that users experience information corruption and steps that they can take to mitigate individual threats. This guide is intended to be a useful resource and framework, but is not intended to be comprehensive or prescriptive.

Users and potential users have different needs for protecting sensitive information. The goal of this guide is to outline the actions that can be taken to mitigate the risks posed by information being lost, changed or read by unauthorized third parties. However, it is important to recognize that FrontlineSMS may not be an appropriate tool to use in some environments where data integrity needs go beyond the capabilities of the platform and SMS itself, and that incautious use may put the program and/or users at risk.

FrontlineSMS does not define the exact details of how users should deploy the software or address issues of data integrity. Users, evaluating their individual program goals, standards, and operating context, should design the program and determine the necessary steps to protect the integrity of their information. Security analysis also involves determinations about the likelihood of a threat manifesting and the impact that such a compromise could have on their program, themselves, and their stakeholders. These are two indispensable parts of determining appropriate measures accomplish the user's goals. These determinations are strongly informed by local context.

Although this guide goes into more depth, security analysis boils down to three over-arching questions:

1. Do you trust the mobile network operator to protect your data?
2. What protections do the government, regulatory, and legal infrastructure provide for data?
3. Are there third parties who may be interested in the information that travels through your system?

The impact and likelihood of a risk occurring can be reduced if specific countermeasures are taken to protect the information. These actions may be behavioral or technological. For example, deleting an SMS message which contains sensitive information immediately after it is sent is a behavioral action that reduces the risk of an unauthorized user reading messages if the mobile is lost or stolen. Password protecting or encrypting information is a technological action that can be taken to reduce risk.

Likelihood refers to a user's assessment of the probability that a vulnerability will be exploited by threats. For example, a user in a hostile natural environment such as very dry or very wet conditions would anticipate the potential danger of weather conditions to be high, compared to someone who lived in a more moderate climate. Similarly, if a user is running a program that transfers sensitive information from which a third party may gain something, such as leverage over another person, the likelihood of a vulnerability being exploited is higher than if the information being communicated is openly available.

The term impact refers to the user's assessment of the seriousness of the potential for harm or damage, should a threat become real. For example, in many places, the impact of a community becoming aware of a Tuberculosis diagnosis may be very different than if a community discovers a patient's HIV status. Impact varies substantially based on local and cultural contexts.

FrontlineSMS has been deployed in many countries to great effect in internal information management processes that call for the transmission of sensitive data, such as health records. At times, this guide recommends against the transmission of sensitive data via SMS, on the grounds that it is impossible to guard against interception and alteration of the data. This may be more pressing for users working in activist or politically sensitive implementations. All users should carefully think through the framework we propose below (see section 2.6) to determine the level of risk inherent in their activity and, from that, the level of countermeasures they feel they should take.

2.3 Audience

This guide is designed for FrontlineSMS users designing, implementing, and monitoring their programs with data integrity concerns in mind.

2.4 Scope

This guide analyzes five major components of a FrontlineSMS deployment: GSM

1. Mobile network operator
2. Mobile phone
3. Computer hardware
4. Computer software
5. Human participation

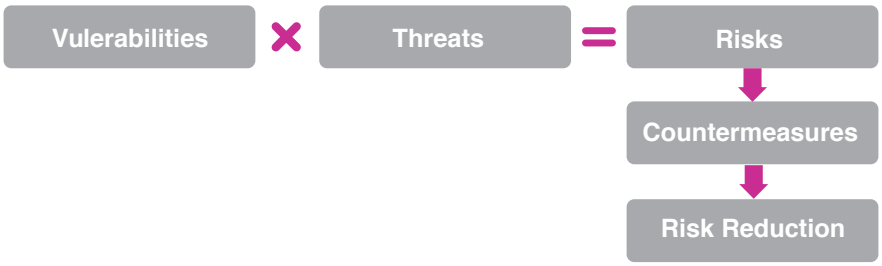
For each of the components, this guide outlines a list of risks and actions that can be taken to reduce the number and impact of the risks that can occur when deploying FrontlineSMS. These lists are intended to be instructive but not exhaustive.

2.5 Approach

This guide addresses 'data integrity', as opposed to mobile security, in an effort to draw the discussion into ways to ensure the confidentiality, authenticity, availability, and usability of information regardless of context. Though there are many overlaps, mobile security is highly contextual and is therefore an analysis best left to users. Still, many of the suggestions in this guide are designed to help users protect themselves and their stakeholders. Data integrity, however, also includes an array of considerations and design elements focused on improving the quality of information exchange, regardless of security context. This guide approaches risk, not just from the perspective of the user, but with a focus on the risks to the quality and usability of the information exchanged through a FrontlineSMS hub.

2.6 Framework

This guide provides a framework to understand the level of risk inherent in any SMS-based activity, given the vulnerabilities and threats that may arise when using FrontlineSMS. This user guide sets out the weaknesses inherent in the platform and its operating context (vulnerability), and how the weakness could allow an unauthorized user to see, change, corrupt or remove sensitive information (threat). These two factors, taken together, lead to risks. The user must then analyze their operating context to think through the likelihood of the threat being exploited, and the potential impact of sensitive information being viewed, changed or deleted. The outcome of these deliberations should help users to determine how they act to mitigate that risk (counter-measures).



For each of the five major components listed in Section 2.4, the guide considers the following:

Vulnerabilities

Vulnerabilities are weaknesses or points of access that can be taken advantage of by unauthorized users. For example, physical access is a vulnerability for mobile phones because it can lead to the phone being stolen or damaged accidentally with water.

Threats

Threats are actions or events that may cause negative data integrity consequences. Threats can be planned or unplanned events. An example of a planned threat is an outsider who steals a phone with sensitive information on it. An example of an unplanned threat is a phone that is accidentally dropped into a puddle.

Risks

Risks are the negative impact on the program or end users that can happen if a threat takes action on vulnerability. Examples of risks include sensitive information being read, lost, stolen, changed, corrupted or deleted.

Risk Reduction

By understanding the vulnerabilities of the system being employed, and the environment in which they are operating, users have the option to consider and deploy appropriate countermeasures to reduce the risks to their program, staff and users. Risks can rarely be entirely neutralized, but users can reduce and mitigate risks by taking a responsible and informed approach program design and management.

2.7 FrontlineSMS Requirements

This section outlines the hardware and software needed to deploy FrontlineSMS.

SERVER	Infrastructure	A working power source and access to a GSM network.
	Hub	A computer, laptop, or netbook with a USB serial port to transfer files and connect peripheral devices. The type of port needed depends on the type of mobile peripheral device.
	Mobile Phone or GSM Modem	A supported GSM modem or phone (users should check the list of currently supported devices: http://devices.frontlinesms.com/pub - due to variations in software and hardware between makes and models, not all GSM modems or phones will work with FrontlineSMS). A GSM modem is recommended over a phone because they can typically send and receive text messages faster than phones. In this guide, 'mobile' is used throughout to designate this element of the FrontlineSMS installation.
	SIM Card	A SIM card with either a service plan or credits that allow it to send and receive SMS. The SIM card should be inserted in the mobile device that will be connected to the FrontlineSMS computer.
CLIENT	One mobile phone per user or field agent	Access to at least a second mobile phone that is not connected to the computer above. This mobile should also be able to send and receive SMS messages to test the installation and configuration of FrontlineSMS. This mobile should use the same mobile network provider as the server because in some countries large delays may occur when SMS messages are sent from one mobile network to another.

For information on how to set up the platform, see the FrontlineSMS website: http://www.frontlinesms.com.

3 GLOBAL SYSTEM FOR MOBILE (GSM)

Section Overview

The GSMA has processes in place to protect sensitive information but it is possible for sensitive information to be read and changed by unauthorized users. Therefore, the amount of sensitive information communicated through GSM networks should be minimized and communicated carefully. Sensitive information should not be stored on SIM cards.

Vulnerabilities	Weak authentication	One-way authentication
Threats	Man-in-the-middle attack	SIM card is copied
Risks	Sensitive information is read and modified by unauthorized users	Communications sent using a subscriber's SIM card
	Financial loss	Mobile services are not accessed
Risk Reduction	Do not communicate sensitive information in SMS or voice calls	Minimize the storage of sensitive information
	Use code words and names to communicate sensitive information	Backup and remove sensitive information regularly
		Own and use multiple SIM cards

The Global System for Mobile is a set of standards for operating mobile phone infrastructure used by more than 800 mobile operators globally, affecting more than 5 billion subscribers, making it the most widespread system for mobile phone service in the world. These standards are defined and publicized through an organization called the Global System for Mobile Association, who represents the interests of its 800 member organizations. The FrontlineSMS platform is designed to operate on mobile networks that use GSM standards.

MNOs use GSM networks to structure the way that mobile phones connect to nearby cell towers, forming the underlying infrastructure for cellular networks. MNOs use these networks to offer mobile services such as SMS, voice, and Internet access. MNOs adapt GSM standards in differing degrees, however, resulting in large variations in data integrity provisions and security contexts. This section provides an overview of the ways that mobile phones connect to GSM networks, including the ways and types of information that move through MNO infrastructure. Given the variation in network operation, this information is intended to be informative, as opposed to comprehensive. .

When a mobile device is powered on, it communicates with the network, which tracks the following information:

- International Mobile Equipment Identity (IMEI) number – this number uniquely identifies the hardware of the mobile device.
- International Mobile Subscriber Identity (IMSI) number – this number uniquely identifies the SIM card. The IMSI links a user's account and phone number.
- Temporary IMSI (TIMSI) number – a temporary number which is updated with the user's location to help manage roaming and other services.
- Location - the user's estimated location, determined based on the amount of time it takes to send a signal to three or more nearby cell towers. The accuracy of the location depends on the number of cell towers nearby.

The GSMA has outlined several principles and processes that can be employed by MNOs to maintain data integrity for the communication, information, and billing needs mentioned above. These processes include:

- User Confidentiality – use of the unique TIMSI to prevent a user's identity and location information from being seen and read by an unauthorized user. Access to the IMSI could allow an unauthorized user to identify a user. A TIMSI is created and sent so that the IMSI is not sent over the network. User Authentication – use of an identity test and authentication key to determine whether a user is allowed to connect to the network. This process prevents an unauthorized user from connecting to the network. If the authentication key is discovered, an unauthorized user can duplicate a SIM card and connect to the network.
- Privacy – use of encryption and authentication algorithms to protect private user information and communications such as voice calls and SMS. These algorithms may or may not be used by a mobile network operator. If an unauthorized user gains access to the encryption and authentication keys, voice calls can be heard and SMS messages can be read.

Even these measures, however, may not ultimately protect users from governments or third parties accessing the types of information listed above, which can be used to track location, identity, and activity.

3.1 Questions to consider

- What sensitive information is sent over mobile networks?
- Is there an actor or group of actors with an interest in intercepting or sabotaging data sent via SMS?
- What negative impacts would there be if SMS messages were read by an unauthorized user?
- What controls or practices are used when sending sensitive information using SMS?
- Is more than one SIM card available or used?
- How often is the call history, SMS history and contact information on SIM cards backed up and/or removed?

3.2 Data Integrity Analysis

The following section outlines the vulnerabilities related to the GSM as well as the associated threats, risks and actions to reduce risk.

3.2.1 Weak authentication

The authentication algorithm is used to prove the identity of a user to the network. The most common way to exploit this is to copy a SIM card, which requires the IMSI number and the authentication key. The IMSI number is usually written on the SIM card and a weak authentication algorithm may allow unauthorized users to discover the authentication key and duplicate the SIM card using SIM cloners. When a SIM card is cloned, all voice and SMS messages will go to both cards but the network will not allow both SIM cards to make voice calls at the same time. If the user experiences dropped calls for unknown reasons or receives calls and messages from unknown numbers, there is a possibility, but not a guarantee, that the SIM card has been cloned.

Before a SIM card is verified to be real and connected to the network, a random number is sent to the SIM card that can be changed by an unauthorized user. If the user cannot connect to the network but others nearby can, there is a possibility, but not a guarantee, that the random number may have been changed.

THREATS		
	SIM card copied	Unauthorized users can copy SIM cards using SIM card copying technology, such as an 8-in-1 or 16-in-1 card reader, which can be bought on the Internet. The user's SIM and an extra SIM are both placed into the SIM copier and then the SIM copier is connected to the USB port of a computer to copy the information from the stolen SIM card to the new SIM card. An unauthorized user can insert the copied SIM card into a different mobile handset and use the copied SIM card to access the user's account. When a SIM card is copied, all information stored on the original SIM card (e.g. SMS messages, contact information, mobile credits) can also be copied. For example, if the SIM card of the local village health worker is copied, any patient health information and SMS communications on the SIM can be copied. In some cities, there are known locations or people that copy SIM cards in exchange for money. There are also devices that third parties can purchase which enable them to clone SIM cards.

SIM card is not verified	If the random number used to authenticate a user to the network is changed many times, a denial of service attack can occur which prevents the SIM card from working because it cannot be authenticated to the network. For example, if a patient wants to send an SMS to confirm a meeting time with a doctor but cannot authenticate to the network, the patient will not be able to send the SMS.

RISKS

Communications sent using a subscriber's SIM card	If a SIM card is copied, a fake user can pretend to be the owner of the SIM card and send and receive messages without the permission and knowledge of the real user. For example, an unauthorized user who copied a SIM card can send false survey responses to a FrontlineSMS platform on behalf of the owner of the SIM card.
Financial loss	If a SIM card is copied, an unauthorized user can use the credits remaining on the copied SIM card that were paid for by the owner of the account for voice calls, SMS messages and data services.
Sensitive information read by unauthorized users	If a SIM card is copied, all sensitive information stored on the SIM card, such as SMS messages, call history, contact information, browsing history, pictures and videos, can be read by an unauthorized user. The unauthorized user can read all the messages sent using the SIM and find the contact information stored in the address book. For example, the government can copy the SIM of a protester and discover SMS communications with political parties and photos of protesters.
Mobile services not accessed	If a SIM card is not verified because of a denial of service attack, the user will not be able to access mobile services, such as voice or SMS. For example, a user will not be able to receive a loan from a microfinance institute if their SIM card is not verified.

Minimize storage of sensitive information	To reduce the risk of sensitive information on a SIM card being read by unauthorized users, minimize the amount of storage of SMS messages, call history, SMS history, contact information, photos or videos on the SIM card. Do not store unnecessary SMS messages (especially outgoing), call history details and contact information. As much as possible, do not save and store the real names of contacts in the handset's address book, to protect the identity and contact information of the senders and recipients of SMS messages. If a SIM card is stolen, all stored information can be viewed by the unauthorized user. Storing information on the SIM card is more technologically secure than storing information on a handset or removable media, but SIM cards are at greater risk of being stolen because they usually contain valuable information and SMS credits. If this information must be saved, delete it as soon as possible from the SIM card and save it to the handset, an SD card or removable storage so that this information cannot be seen if the SIM card is copied.
Backup and remove sensitive information regularly	To reduce the risk of sensitive information on a SIM card being read by unauthorized users, back up and remove sensitive SMS or MMS communications stored on a mobile phone (if the make and model of the phone has this capability). Information may be backed up by choosing to save it to the mobile phone instead of the SIM card, using a SIM card reader that plugs into the USB port of a computer or, depending on the mobile phone, connecting the mobile directly to a computer and copying the information. Information backed up to a computer or another storage device can be loaded onto a different SIM card. Encrypt or password-protect information that is backed up to protect sensitive information from unauthorized users. Deleting sensitive information cannot completely stop unauthorized users from finding out what information was stored on the SIM card. If an unauthorized user gets a mobile, SIM card, or Micro-SD card from which information was deleted, they may be able to discover the deleted information using forensic techniques and tools.
Communicate less sensitive information	To reduce the impact of unauthorized users reading sensitive information, minimize the amount of sensitive information sent via SMS. Use other ways to communicate the information indirectly, in-person or using code words. If this communication is necessary, include as little sensitive information in SMS communications as necessary and carefully review all messages before they are sent.

Use pre-determined code words	To reduce the impact of unauthorized users reading sensitive information, use pre-determined numbers or alternate words to represent information such as locations (e.g. 14984 for the local polling station) or the identity of end users (e.g. Mr. X for the full name of client or patient).
Own and use multiple SIM cards	To reduce the impact of mobile services not being accessible, own and use more than one pre-paid SIM card from multiple operators in case a SIM card is not working or is suspected to have been cloned. For example, have one backup SIM for the primary MNO, a backup roaming SIM for the primary carrier and another SIM for a different carrier.

3.2.2 One-way authentication

One-way authentication means that a network is able to determine whether a user has a registered account, but a user is unable to determine whether the network is authentic. An authentic network is a registered MNO in the country and an authentic user is a subscriber who has purchased a SIM card and services from an MNO. Unauthorized users can pretend to be the authentic network using a man-in-the-middle attack to monitor the SMS and voice communications of an authentic user without that user's permission or knowledge.

THREAT	
Man-in-the-middle attack	In a man-in-the-middle attack a device, such as an IMSI-catcher or virtual base transceiver, is used to trick the user into thinking that the device is a valid base station (see Section 4.2 for more details) for the network operator. Mobile phones automatically try to authenticate to the base station with the strongest signal and because the device is pretending to be a base station, all of the mobile phones that are nearby will provide their authentication information to the device. Using the authentication key from an authorized user, the device will pretend to be a mobile device and connect to the network. Each base station chooses its own method of encryption, so the unauthorized user can choose no encryption method and will then be able to see all traffic passing to and from the mobile. For example, an unauthorized user could pretend to be a base station and read SMS communications sent to- and- from a lawyer and their client. In this case, an unauthorized user could change the information sent by the lawyer to the client and provide the wrong information. A man-in-the middle attack does not give an unauthorized user access to a subscriber's logged information and records that are centrally stored at the operator level. Due to the effort and technical knowledge needed to successfully perform this attack, the chance of this threat happening is low, but it is a threat that can affect any user of GSM networks.

RISK	Sensitive information changed by unauthorized users	If sensitive information is caught in a man-in-the-middle attack, it can be changed before being sent to a recipient. For example, an SMS message sending the location of a meeting or healthcare appointment could be changed to communicate the wrong address.
	Sensitive information is read by unauthorized users	If a man-in-the middle attack occurs, sensitive information can be read by unauthorized users. See section 4.2.2 for more details.
RISK REDUCTION	Communicate less sensitive information	To reduce the risks of sensitive information being read or changed by unauthorized users, communicate less sensitive information. See section 3.2.1 for more details.
	Use code words	To reduce the risks of sensitive information being read or changed by unauthorized users, use code words. See Section 3.2.1.

4 MOBILE NETWORK OPERATOR

Section Overview

The billing information stored by an MNO is typically accessible to many of their employees and contains sensitive information about the subscriber. Users should assume that their communications and information can be seen by unauthorized users; minimize the amount of sensitive information they send using SMS; and use code words to communicate sensitive information.

Vulnerabilities	SMS is not encrypted by MNOs in transit Infrastructure is damaged	Sensitive information is stored by MNOs
Threats	SMS messages are caught by unauthorized users Mobile services are stopped by environmental damage or third parties Unlocking code for the mobile is shared	Reports of subscriber information provided to a third party Subscriber information accessed by employees of MNO Log files are lost or stolen SIM card is locked to the MNO
Risks	SMS messages are read by unauthorized users User is physically tracked Voice calls and SMS messages are not sent	Subscriber information shared and sold to a third party Employees of MNOs read and share subscriber information Financial loss
Risk Reduction	Minimize the amount of sensitive information sent using mobile services Use code words in mobile communications Power off the mobile phone when not in use	Do not provide identification when purchasing a SIM card Create a plan for communications when mobile services are stopped Use dual or triple SIM phones

Section 1.5 outlines the GSM standard and discusses common characteristics of Mobile Network Operators (MNOs), but it is important to note that MNOs operate in different ways depending on the legal frameworks and standards of their country of operation, the size and scope of the network, the age of the network, and the features they are licensed to provide (i.e. 2G, 3G, or 4G). There are FrontlineSMS users in countries all over the world and therefore, many different MNOs are used by the FrontlineSMS users and their end users. MNOs in every country are required by regulatory oversight to cooperate with law enforcement and the penalty for non-compliance can be a large fine or loss of their operating license. In many contexts, the relationship between the government and the MNO may present additional threats and risks, such as political access to mobile communications and SMS.

Practices and processes that can differ for MNOs include:

1. the level of information shared with partners or contractors
2. the level of encryption used between the mobile station and base station
3. the types of information stored
4. sharing of communications with the government
5. the ability of employees to access subscriber information
6. the ability to lock phones
7. the ability to buy a SIM card without providing identification
8. the method for connecting parts of the network together

MNOs can store and send information differently. A majority of MNOs use the 'store and forward' method of sending SMS where SMS messages are stored in unencrypted format in the central SMS center and are only sent when recipient is available and has a signal. Some MNOs use the 'forward and forget' method which tries to send the SMS message once and if the recipient is not available, the message will not be stored or sent.

MNOs can also store different types and amounts of sensitive information, which can include:

- User identity information – name, address, age, date of birth and additional contact information.
- Billing information - location, senders and recipients of communications and timing of communications. Most billing information is shared with a user to verify that the phone bill is correct.
- Location information – approximate location and information detailing when the user is or is not accessing or using mobile services. Current location and past locations are tracked by the MNO when the mobile phone is powered on and connected to the network by monitoring the closest cell towers to the user.
- SMS details - sender, recipient, location, date, and timestamp are attached to individual SMS as they are sent and centrally logged even after the SMS is successfully delivered.
- PIN Unlock Code (PUC) –code needed to unlock a SIM card if the wrong PIN was entered more than three times. MNOs assign a PUC to each SIM card and usually provide users with the PUC upon request if the PIN is forgotten or the wrong PIN is entered more than three times.
- Equipment information - list of mobile phones which are banned from the network because they are lost or stolen. This information may or may not be stored and used depending on the country.
- As the practices, standards and legal requirements for operators vary worldwide, this section is written to apply to most operators, but may vary. The relationship between an MNO and the

government may also have large consequences for whether a user is able to make legal complaints or seek recourse if their system is compromised.

4.1 Questions to consider

- Is identification required when purchasing a SIM card?
- What backup plan is in place in case mobile services are stopped?
- What is the negative impact if SMS messages are read by an unauthorized user?
- Is the mobile powered off when it is not in use?
- Is the mobile phone locked to the MNO?

4.2 Data Integrity Analysis

Differences in MNO practices and processes for data retention and protection can give rise to different levels of risk. Some MNOs encrypt the SMS messages between the mobile phone and the base station (see 3.2 for more details). All MNOs log and store billing information, including a large amount of sensitive information such as location, senders and recipients of communications, and call log. Therefore, all subscribers are at risk of the billing information being viewed by a third party.

The vulnerabilities of MNOs can cause sensitive information to be read and used by unauthorized users or third party, financial loss or mobile services to be stopped. Users can also be physically tracked. The amount of sensitive information communicated and stored should be minimized and users should have an extra SIM card available for use.

The following section outlines the vulnerabilities related to MNOs as well as the associated threats, risks and actions to reduce risk.

4.2.1 No encryption for SMS

MNOs may use a weak (or no) encryption algorithm when SMS messages are transmitted from the mobile to the base station. This means that SMS messages are not encrypted from the base station to the mobile phone of the recipient. As mentioned in Section 3, when encryption algorithms are weak, it enables an unauthorized user with the proper equipment to catch and read the sensitive information in the message.

It is very difficult to know if sensitive information sent via SMS has been caught or read by an unauthorized user, therefore, users should avoid transmitting sensitive information and use code words in the SMS messages.

THREATS	Sensitive information caught by unauthorized users	If SMS messages are not encrypted, an unauthorized user with access to the MNO network can monitor a cell tower using basic mobile phones and open source software to read the information contained in the SMS messages sent and received from a mobile number. For example, an unauthorized user could see an SMS message from a child that is a victim of violence who is asking for help.
RISK	SMS messages read by unauthorized users	If sensitive information is caught by unauthorized users, SMS messages can be read by unauthorized users. In addition to the sensitive information sent in the message, the unauthorized user will also be able to see the sender and recipient information gathered by the mobile network operator for each message. For example, an unauthorized user can read the SMS message of a child who is a victim of violence to discover the exact location, name of the child and the recipient of the message.
RISK REDUCTION	Communicate less sensitive information	To reduce the risk of sensitive information being read by unauthorized users, communicate less sensitive information. See Section 3.2.1.
	Use code words	To reduce the risk of sensitive information use pre-determined code words. See Section 3.2.1.

4.2.2 Unauthorized Third-Party access to subscriber information

MNOs track and store a large amount of sensitive information in unencrypted format that can be accessed by employees or other unauthorized users with access rights to the databases or applications where the information is stored. Sensitive information that can be accessed by employees is outlined in Section 6.

It is very difficult to know if sensitive information is being collected or accessed by unauthorized users. All MNOs store sensitive information in databases and use this information for billing, therefore, users should assume that their sensitive information can be read.

THREATS	Sensitive information read by MNO employee	MNO employees (e.g. network administrator or engineer) may access and keep subscriber information and/or share the information for money or personal gain. For example, an employee can see the details of SMS messages from a subscriber organizing a protest. The illegal theft of information by an operator has happened in countries with high levels of corruption, and should be considered a threat for all users of the GSM network.

	Log files stolen or lost	Operator logs and records, which can include billing information or SMS messages, may be lost or stolen due to flaws in information management or security by the mobile network operator. Some MNOs outsource the management of their subscriber information, allowing information to be transmitted and viewed by third parties. For example, an African MNO may outsource their operations to an organization in China whose employees will also have access to subscriber information.
	PUC shared	A third party with physical access to a phone can pay an employee of the MNO to provide the PUC in order to unlock the phone. For example, if a mobile phone is stolen from a protester, a third party can pay the employee of the MNO to retrieve and share the PUC to be able to unlock the phone and view all the information stored on the SIM card.
RISK	Sensitive information shared or sold to a third party	A third party (e.g. government or political party) can convince an employee of an MNO to access user records, monitor communications, and/or collect information from the operator without the users knowing. This information will allow the third party to view the contents of SMS messages, details of billing information, and location information, and to monitor all voice, SMS and data communications sent and received by the user. For example, the local government can monitor the content of SMS messages for communications about a protest and track down the users organizing or participating in the protest. The level of risk of this occurring depends on the legal standards and political environment, the history of legal requests by operators for subscriber information, and whether or not a subscriber's activities are considered criminal in nature, politically sensitive, or high-profile.
	User physically tracked	If the location information of a user is accessed by an employee of the MNO and sold to a third party, the user can be physically tracked down and then be subject to further monitoring, violence or prosecution. For example, the location of a citizen organizing a protest against the government may be monitored, and the user caught and imprisoned.
	Sensitive information read by unauthorized users	If the PUC of a SIM is shared and unlocked, sensitive information can be read by unauthorized users. See section 5.2 for more details.
	Financial loss	If the PUC of a SIM is shared and unlocked, credits on the SIM can be used. See Section 4 for more details.

Research operator	To reduce the risk of sensitive information being read, shared or sold to a third party, perform research regarding the operator(s) used, the local authorities and political climate, and any known incidents of monitoring or stopping mobile services in the past, in order to understand what information, if any, is likely to be monitored.
Escalation	To reduce the impact of sensitive information being read, shared or sold to a third party, users should change operators and/or take legal action (where available and appropriate) if they learn that someone has granted unauthorized access and/or alteration of their information when it passes through the mobile network.
Do not provide identification when purchasing a SIM	To reduce the risk of physical tracking and user identity information being stored and shared with a third party, do not give identifying information such as full name or address when buying a SIM card if possible. An increasing number of MNOs require this information when purchasing a SIM card, however, some MNOs allow customers to purchase a pre-paid SIM card without identification.
Power off phone when not in use	To reduce the risk of physical tracking, mobile phones should be powered off and the battery should be removed when it is not in use, or not needed (e.g. in the evenings or if the user is traveling between cities or regions). Removing the battery prevents the MNO or a government from knowing the location of a mobile phone, whereas a phone with the battery can still be activated or interacted with by specific parties. For example, if a user organizing events in different cities, it is best to power off the mobile phone when traveling in between events so that the user's location or destination is not known.

4.2.3 Service Interruption

In recent events, services on mobile phones have been stopped because of political instability or natural disaster. For example, in the immediate aftermath of the recent earthquake, Japan's three largest MNOs reported little to no wireless service throughout the entire country because thousands of base stations were put out of service by the natural disaster.

If mobile services are stopped, the user may not be able to communicate with others using the mobile phone for several days.

THREATS	Mobile services stopped	Mobile services can be stopped for cities, regions or countries due to unplanned events such as natural disasters, or deliberately by the MNOs controlling the users, towers and regions. When services are stopped, voice calls, SMS and data services over the GSM network cannot be used. For example, several MNOs have recently stopped mobile services during times of unrest.
	Automatic lock out	If the FrontlineSMS platform sends a large number of SMS messages in a short time period, this may be viewed as an SMS spam operation and the account may be automatically locked by the MNO. Some MNOs will automatically prevent a large number of SMS messages being sent using third party platforms such as FrontlineSMS. For example, an agricultural information announcement may be viewed as spam by the MNO and not be sent to the recipients.
	SIM locking	In certain countries, MNOs have the ability to lock a mobile phone to the network. This means that when a user buys a cell phone from an MNO, the device may be locked to only work properly when using a SIM card from that MNO.
RISK	Communications are not sent	If mobile services are stopped, the MNO locks the mobile services of a SIM, or a mobile device is used which is locked to a different network, communications will not be sent. Important and/or sensitive information cannot be communicated. For example, a community health worker may not be able to send an urgent alert to a clinic or hospital about an incoming patient.
	Financial loss	If a large amount of SMS messages are sent and the MNO considers the SMS messages spam, the MNO may choose not to send the text message and still charge the user, resulting in the loss of the credits. The higher the rate and volume of SMS message sending, the more likely an MNO is to consider that activity spam, and the more money a user may lose.

Create a service interruption plan	To reduce the risks that can arise from service interruption, create a back-up communications plan in case mobile services are stopped. These plans often include meeting at agreed upon locations or using alternative communications platforms that do not use GSM networks. Users should research the SMS restrictions (e.g. terms of frequency of use) for their MNO before sending a large number of SMS messages.
Use dual (or triple) SIM phones or SIM adapter	To reduce the risks that can arise from service interruption, use a dual (or triple) SIM phone or SIM adapter. Dual or triple SIM phones and SIM adapters allow you to use more than one SIM card with a mobile phone. Dual SIM phones should be used with different MNOs so that if services are stopped on one MNO, the other SIM card may be used. SMS messages from a SIM card should be used to send SMS messages to recipients using the same MNO. Doing this will usually saves the user money and the communication can be sent faster and more securely. See also 3.2.1 for more details when using more than one SIM card.

5 MOBILE PHONE

Section Overview

Mobile phone hardware is vulnerable to being lost, stolen or damaged. Mobile phone software is vulnerable to malware that can be acquired from removable media or using the Internet. Users should limit physical access to the mobile and use an 8-digit PIN to protect saved information. Sensitive information stored on the phone should be limited and removed on a regular basis.

Vulnerabilities	Removable storage	Internet Access
	Physical Damage	Bluetooth
	Weak PIN	
Threats	Phone is stolen	PIN is discovered
	Mobile hardware destroyed	Viruses downloaded or uploaded
Risks	Financial loss	Sensitive information accessed by unauthorized users
	Information is lost	Communications are not sent
	Unauthorized control of the mobile	
Risk Reduction	Store the mobile in a secure location	Do not use insecure connections
	Minimize use of removable storage	Limit downloading
	Use strong PIN	Backup and remove sensitive information regularly
		Turn off Bluetooth

The use of a mobile phone can be customized to the needs of the program and end users. Mobile phones are a key component of FrontlineSMS programs. Mobile phones and modems are used to connect a FrontlineSMS hub to the GSM network. FrontlineSMS programs are built on the ability of mobile phones to send and receive SMS messages. The risks of using mobile phones are more controllable by end users than those encountered by using the GSM and MNOs.

The components of a mobile phone include:

Hardware

- Mobile handset – the make and model of the phone (e.g. Nokia 1100). The physical design of the handset is different depending on the company that created the handset and the model of the handset
- Removable storage – cards that are inserted to the mobile phone to upload and store information. The main types of removable storage used with a mobile phone include the:
    - SIM card – contains information that allows the user to connect to the network and send and receive communications. The SIM may also be used by the phone to store information such as SMS messages and contact information found in the address book
    - Memory card – There are at least three main types of memory cards used: SD, MicroSD, and MMC. They are used to provide more memory and storage of information such as pictures, music, and videos. Some handsets allow users to save SMS messages onto the SD card or allow users the option to not store SMS messages on the SIM.

Software

- Operating System (OS) – every mobile phone is pre-loaded with an OS that influences the user experience and functionality of the mobile phone, including local connectivity and input methods. The OS of a mobile phone depends on the make and model and has built-in security functionalities.
- Applications – applications are programs on the mobile phone that help a user perform tasks. Applications can be pre-installed or can be downloaded by some phones. Examples of applications include a calculator or games.

Mobile phones are used for everyday communications as well as personal tasks (e.g. banking, health).

Mobile phones store and send the following types of sensitive information:

- Sent and received SMS messages stored on the phone
- Address book and contact information (full names, phone numbers, addresses and other personal information)
- Call history
- Pictures and videos

5.1 Questions to consider

- What sensitive information is stored on the SIM? SD card? Handset?
- Is sensitive information backed up, cleaned and removed from the mobile phone?
- What, if any, applications are available and used on the mobile phone?
- Is additional security software needed or available?
- Is the Internet access necessary and supported by the mobile phone?
- Can the Internet be accessed via Wi-Fi or only via cellular data network?
- Is the Bluetooth function enabled on the mobile phone?

5.2 Data integrity Analysis

The following section outlines the vulnerabilities related to mobile phones as well as the associated threats, risks and risk reduction actions.

5.2.1 Physical access

Physical access to mobile phones occurs when an unauthorized user steals, takes, or borrows the phone. Mobile phones are vulnerable to being lost or confiscated by authorities including commercial entities, law enforcement agencies, security agencies, and intelligence agencies.

THREATS	Phone is stolen or lost	An unauthorized user can steal a mobile phone in a public area or plan to steal the phone by following the user and waiting until the mobile is unattended. A mobile can also be accidentally lost by the user.
	Phone is borrowed	An unknown person can access the mobile phone by asking the user to borrow the mobile phone. For example, an unknown person can ask the user to borrow their mobile to make a voice call because their phone is out of battery.
RISK	Sensitive information is lost	If the phone is lost, stolen or borrowed, sensitive information stored on the mobile phone can be lost when the mobile itself is lost, stolen or compromised. See Section 3.2.1 for more details.
	Sensitive information read by unauthorized user	If the phone is lost, stolen or borrowed, the sensitive information on the phone can be accessed. If there is no PIN for the SIM or if the unauthorized user discovers the PIN, all the sensitive information stored on the mobile can be read. See Section 6.2.1 for more details.
	Financial loss	If the phone is lost, stolen or borrowed, the unauthorized user can use the SMS credits on the SIM card that were paid for by the owner of the account. See Section 6.2.1 for more details.

RISK REDUCTION	Store the mobile in a secure location	To reduce the risks that can occur from physical access, mobile phones should be stored in a case or bag at all times to prevent accidental damage and make theft more difficult. Users should take normal precautions to avoid theft and accidental loss, such as avoiding placing the phone on a table in a crowded place and/or carrying it somewhere secure.
	Use a strong password and PIN	To reduce the risk of sensitive information being read, create a strong PIN and do not share the PIN with anyone else. Use the following rules to create a strong PIN: • Use a PIN with 8 digits • Do not use 3 or more consecutive numbers (e.g. 1234, 456) • Do not repeat 2 or more side-by-side(e.g. 11, 22) • Using a PIN on a SIM card will also prevent the SIM from being used on another handset if the correct PIN is not entered.
	Avoid sharing with unknown people	To reduce the risk of sensitive information being read, never let an unknown or untrusted person use a mobile with sensitive information on it.

5.2.2 Physical damage

Mobile phones are vulnerable to physical damage such as water, dust and fire, for example, by being placed on a table with liquids nearby, or by knocks and impacts, accidental dropping. There is very little to do if a phone is destroyed- most of the mitigating measures available are preventative.

Users will know if a mobile phone has been damaged because it does not work properly when it is turned on, off, or if the screen is broken.

THREATS	Mobile hardware destroyed	Physical damage or damage from water, dust, static electricity, power spikes, and fire can cause mobile devices to stop working.

RISK	Sensitive information is lost	All the sensitive information stored on a mobile phone can be lost if the mobile phone is damaged by water, dust, fire or from other accidents such as dropping the phone. See Section 6.2.1 for more details.
	Communications are not sent	The user cannot send any communications if the mobile phone is damaged. See 6.2.1 for more details.

RISK REDUCTION	Avoid physical damage	To reduce the risks that occur if a mobile is damaged, keep mobile phones in a waterproof hard case, plastic bag or shock case to provide protection against water, dust and fire and other accidents.
	Routine backup	To reduce the risk of sensitive information being lost, regularly back up information on the mobile. See Section 3.2.1 for more details.

5.2.3 Weak PIN

Most mobile phones can be locked or unlocked using a PIN. Once a PIN or pass code is set on a mobile phone, the correct PIN must be known and entered on the mobile before it can be used. PIN numbers on GSM networks are usually between 4-8 digits.

If a mobile is lost or stolen, it is difficult to know whether the PIN has been discovered.

THREATS	PIN discovered	If a weak PIN is used, an unauthorized user may access the information stored on a mobile by trying different combinations. PINs that are 4 digits are easier to discover than 8 digit PINs. PINs such 1234, 1111, the user's birth date or year, and the current year are easily guessable.
RISK	Sensitive information read by unauthorized	If a PIN is discovered and the phone is unlocked, sensitive information can be read by unauthorized users. See Section 3.2.1 for more details.
	Financial loss	If the PIN is discovered and the phone is unlocked, mobile credits on the SIM card can be used. See 5.2.1 for more details.
RISK REDUCTION	Use a strong PIN	To reduce the risks of financial loss and sensitive information being read, use a strong PIN. See 5.2.1 for more details.

5.2.4 Removable storage

Removable storage devices such as SIM cards and SD cards represent a vulnerability for mobile phones because they can be used to load applications onto mobile phones, including viruses and malware. The term malware refers to any software, program, or code designed to cause harm or access a mobile or computer without the owner's permission or knowledge. Backup programs may also function as malware or can be reconfigured to function as malware. Although malware can be designed to accomplish a wide range of things, it is typically designed to accomplish one or more of the following: track user location; destroy or corrupt information; take control of a piece of hardware (mobile phone or computer); and/or monitor user communication. Due to the large amount of variation, this guide discusses the most

common types of malware, however, users should evaluate their context to identify the most likely or dangerous types of compromise to their program.

Users may notice changes in the speed or behavior of a phone if malware has been loaded onto it. If the phone becomes slower unexpectedly, this is a possible sign that malware may be present. Another key indicator is a phone's rate of battery depletion. If the battery suddenly starts depleting at a noticeably faster rate, malware may have been loaded on the phone or the phone may be under the control of a remote user. It is very difficult to know if sensitive information is being read by an unauthorized user as a result of suspected malware being present.

THREATS	Malware or viruses	Most mobile phone malware is designed to give an unauthorized person access to the phone in order to monitor calls and/or SMS usage. It may also be used destroy information or to prevent use of certain features of the phone. Examples of malware include: • Spyware – gives an unauthorized user the the ability to collect and monitor information on the mobile • Viruses – has the ability to copy themselves and infect other devices When a SIM card or SD card is inserted into a mobile phone, the mobile reads and shows the information stored on the card. SD cards may contain applications with malware on purpose or accidentally. Malware, such as a virus, can be loaded onto a mobile phone and allow unauthorized users to collect, store, corrupt or delete all the information and communication stored on the mobile device. Depending on the type of malware, the program may also allow third parties to take full or partial control of the information on the mobile phone.
RISK	Sensitive information read and used by unauthorized user	Unauthorized users may monitor voice and SMS communication or read and review sensitive information stored on the mobile device, SIM card, or SD card including photos, videos or notes. Third parties may also use identifying information, such as location data or call history, to track the user of the mobile phone. See Section 3.2.1 for more details on the types of sensitive information that can be read from a SIM card.

Unauthorized control of mobile	Malware can load a program onto the mobile that allows an unauthorized user to have partial or full control of the information and applications on the mobile phone. The unauthorized user can then stop the mobile from functioning properly and remove or change user information. Some malware initiates calls or data charges to the user's account that can lead to large bills or the depletion of a pre-paid SIM.

RISK REDUCTION

Minimize use of removable storage	To reduce the risks that occur due to malware, do not use an SD card if it is not needed and never insert an unfamiliar or distrusted SD card into a mobile phone. For example, an unknown person may approach you and ask you to insert their SD card into your mobile because their mobile phone is out of battery and they need to access information stored on their SIM card. Do not insert their SD card into your mobile because you do not know what type of information is contained on the SD card. The SD card may contain malware that is known or unknown by the unknown person.
Routine backup and removal	To reduce the risks that occur due to malware, regularly back up and remove sensitive information stored on the mobile. See Section 6.2.1 for more details.

5.2.5 Internet access

Increasingly, mobile phones have the ability to access the Internet using Wi-Fi or data plans. This is not a requirement when using FrontlineSMS and doesn't necessarily have any direct effects on the design or implementation of SMS integration. The use of Internet-enabled phones may, however, subject a user to additional security threats.

Mobile phones with data plans access the Internet when cellular data services are available. This may be via a web-browser application or other dedicated applications. Internet-enabled phones can also connect to a network without a data plan by accessing the wireless network settings on their mobile phone and connecting to a nearby Wi-Fi network. Some Wi-Fi networks require users to enter a password before connecting to the Internet.

Internet access allows a mobile phone to connect with many other users, websites and applications. It is difficult to know which of these are secure and which are not. Insecure users, websites and applications can be connected to on purpose or by accident.

Users may know if malware has been loaded onto the mobile if the services become slower or if there are unknown applications on the mobile. Some malware does not show up in the user interface for the phone, especially spyware. It can be very difficult to know if sensitive information is being read by unauthorized users.

THREATS	Phone is stolen or lost	An unauthorized user can steal a mobile phone in a public area or plan to steal the phone by following the user and waiting until the mobile is unattended. A mobile can also be accidentally lost by the user.
	Phone is borrowed	An unknown person can access the mobile phone by asking the user to borrow the mobile phone. For example, an unknown person can ask the user to borrow their mobile to make a voice call because their phone is out of battery.
RISK	Sensitive information is lost	If the phone is lost, stolen or borrowed, sensitive information stored on the mobile phone can be lost when the mobile itself is lost, stolen or compromised. See Section 3.2.1 for more details.
	Sensitive information read by unauthorized user	If the phone is lost, stolen or borrowed, the sensitive information on the phone can be accessed. If there is no PIN for the SIM or if the unauthorized user discovers the PIN, all the sensitive information stored on the mobile can be read. See Section 6.2.1 for more details.
	Financial loss	If the phone is lost, stolen or borrowed, the unauthorized user can use the SMS credits on the SIM card that were paid for by the owner of the account. See Section 6.2.1 for more details.
RISK REDUCTION	Store the mobile in a secure location	To reduce the risks that can occur from physical access, mobile phones should be stored in a case or bag at all times to prevent accidental damage and make theft more difficult. Users should take normal precautions to avoid theft and accidental loss, such as avoiding placing the phone on a table in a crowded place and/or carrying it somewhere secure.
	Use a strong password and PIN	To reduce the risk of sensitive information being read, create a strong PIN and do not share the PIN with anyone else. Use the following rules to create a strong PIN: • Use a PIN with 8 digits • Do not use 3 or more consecutive numbers (e.g. 1234, 456) • Do not repeat 2 or more side-by-side(e.g. 11, 22) • Using a PIN on a SIM card will also prevent the SIM from being used on another handset if the correct PIN is not entered.
	Avoid sharing with unknown people	To reduce the risk of sensitive information being read, never let an unknown or untrusted person use a mobile with sensitive information on it.

5.2.6 Bluetooth

Many mobile phones also enable communication via Bluetooth, which is a short-range communications tool that can be used to wirelessly connect devices at distances up to 750 meters. Bluetooth can also be used to connect mobile phones, or other devices, to computers. Although largely regarded as a comparatively secure platform, there are a number of ways in which it can be used to corrupt or access devices without the owners' knowledge. As such, Bluetooth is a known entry point for viruses and malware. It is very difficult to know if sensitive information is being read or monitored by unauthorized users.

Typically, mobile phones include Bluetooth in their settings menus. In these menus, users can either 'enable' or 'disable' Bluetooth. When Bluetooth is 'enabled', other devices with Bluetooth may discover and/or connect to the mobile phone or computer, enabling a wide range of interactions. These communications may include access to software or information contained on the mobile phone. When 'disabled', others are unable to access a mobile phone via Bluetooth.

THREATS	Phone is stolen or lost	An unauthorized user can steal a mobile phone in a public area or plan to steal the phone by following the user and waiting until the mobile is unattended. A mobile can also be accidentally lost by the user.
	Phone is borrowed	An unknown person can access the mobile phone by asking the user to borrow the mobile phone. For example, an unknown person can ask the user to borrow their mobile to make a voice call because their phone is out of battery.
RISK	Sensitive information is lost	If the phone is lost, stolen or borrowed, sensitive information stored on the mobile phone can be lost when the mobile itself is lost, stolen or compromised. See Section 3.2.1 for more details.
	Sensitive information read by unauthorized user	If the phone is lost, stolen or borrowed, the sensitive information on the phone can be accessed. If there is no PIN for the SIM or if the unauthorized user discovers the PIN, all the sensitive information stored on the mobile can be read. See Section 6.2.1 for more details.
	Financial loss	If the phone is lost, stolen or borrowed, the unauthorized user can use the SMS credits on the SIM card that were paid for by the owner of the account. See Section 6.2.1 for more details.

RISK REDUCTION

Store the mobile in a secure location	To reduce the risks that can occur from physical access, mobile phones should be stored in a case or bag at all times to prevent accidental damage and make theft more difficult. Users should take normal precautions to avoid theft and accidental loss, such as avoiding placing the phone on a table in a crowded place and/or carrying it somewhere secure.
Use a strong password and PIN	To reduce the risk of sensitive information being read, create a strong PIN and do not share the PIN with anyone else. Use the following rules to create a strong PIN: • Use a PIN with 8 digits • Do not use 3 or more consecutive numbers (e.g. 1234, 456) • Do not repeat 2 or more side-by-side(e.g. 11, 22) Using a PIN on a SIM card will also prevent the SIM from being used on another handset if the correct PIN is not entered.
Avoid sharing with unknown people	To reduce the risk of sensitive information being read, never let an unknown or untrusted person use a mobile with sensitive information on it.

6 COMPUTER HARDWARE

Section Overview

Program information can be lost if computer hardware is damaged. Computer hardware should be kept safe from environmental damage such as water and dust, from the public, and from unauthorized users.

Vulnerabilities	Destruction	Unauthorized access
Threats	Planned events	Team members
	Unplanned events	Third party
Risks	Program information is lost	Program resources, such as SMS credits, are used
	Sensitive information accessed by unauthorized users	Program is stopped
Risk Reduction	Perform regular backups of all information on the computer	Teach all team members physical controls to protect the hardware
	Use a surge protector in case of power outages	Password protect program resources

Computer hardware is the physical equipment on which the FrontlineSMS platform is running. This likely includes some combination of the following:

- Desktop computer – the part of the computer that stores all the information in the hard drive and usually contains the ports that are used to connect to the Internet or to connect removable media. The hard drive is the most important part of the computer.
- Monitor – the part of the computer that displays the screen. The monitor is connected to the desktop computer and displays the information on the screen.
- Laptop – a computer that was designed to have the same functionalities of a desktop but can be easily carried around.
- GSM modem or tethered GSM phone – connects the computer to the GSM network and allows SMS messages to be sent and received.

The computer is important because it runs the FrontlineSMS platform and stores all of the associated information. Because FrontlineSMS is a piece of software that operates without access to the Internet, all of the information associated with the use of the program resides on a computer's hard drive. This may include sensitive information, such as phone numbers, records of incoming and outgoing messages, and personal details, are stored on the computer. A GSM modem is required to be able to connect to the mobile network.

6.1 Questions to consider

- Where in the office is the computer located on which the FrontlineSMS platform is deployed?
- Is a laptop or desktop used to run the FrontlineSMS platform?
- Can the computer running FrontlineSMS be easily accessed by others?
- Is the computer stored in a place where it can be damaged by dust, heat or moisture?
- What physical controls are in place to protect the computer(s) from unauthorized access and damage when the office is closed on the evenings and/or weekends?
- How many personnel have access to the room in which the computer is stored?
- Is the information on the computer running FrontlineSMS backed up regularly? If yes, how is the backup performed?

6.2 Data Integrity Analysis

The following section outlines the vulnerabilities related to the hardware used for the FrontlineSMS platform as well as the associated threats, risks and actions to reduce risk.

6.2.1 Destruction

All hardware is vulnerable to physical destruction. It is nearly impossible to predict, let alone plan for, the full range of circumstances that may damage essential hardware. Yet, the way in which damage to hardware differs the most, both in terms of potential risks and mitigation steps is by the intent or cause of the damage. We separate the threats to computers into planned and unplanned events, as they imply different types of risk reduction steps. A planned event is when someone intentionally acts to harm the equipment and/or data used to implement a FrontlineSMS program. Planned events include a range of actions, including theft, sabotage and damaging a computer. An unplanned event refers to accidental or environmental damage. This may include the damage caused by spilling water or excessive flooding in the place where the hardware is stored.

Users can tell if computer hardware has been damaged if it does not work properly when turned on, makes abnormal sounds, or if there is a visible change in the appearance of the device. A screen may be broken or not turn on at all. Hardware can be damaged temporarily and fixed, or may be irreparably damaged.

THREATS	Planned events	Planned events any party damaging the hardware on purpose by dropping it or using force, or other incidents such as spilling water. For planning purposes, the major distinction is how authorized and unauthorized access is managed, both for employees and the public. For example, a visitor may plan to spill water on the computer in order to damage it.
	Unplanned events	Unplanned events include environmental damage such as humidity, sand, dust, water or accidental events such as someone spilling water on the computer or knocking the device off a surface. Power fluctuation and other infrastructural irregularities are also unplanned events that happen in some areas.
RISK	Information is lost	Planned or unplanned events that destroy computer hardware can cause information contained on the computer to be lost temporarily or indefinitely. If a backup was made of the information, the data will be lost temporarily but can be recovered by reloading the backup to a fixed or alternate computer. For example, if water is spilled on the computer, it may stop working, but if turned off immediately and left for 24 hours, it may dry out and function again, as long as no components were damaged or shorted out. Depending on the amount of damage done to the hardware, the information may be able to be recovered by a computer hardware expert. If a backup was not made and the information cannot be recovered by an expert, then the information is lost indefinitely. This includes all sensitive information contained for the program such as end user information, surveys and budgets.
	Program is stopped	Planned or unplanned events that destroy computer hardware will cause the FrontlineSMS program to stop functioning until reloaded on a working computer. If FrontlineSMS is being used to communicate urgent or time-sensitive information, hardware damage may result in the loss of key information or the inability to provide assistance that others rely upon. The impact of this risk is very high if the hardware is destroyed at a critical time. For example, if the hardware of an election monitoring program is irreplaceably destroyed on election day, it will be impossible to use FrontlineSMS for monitoring without another computer.

Backup information regularly	To reduce the risks of information being lost and the program being stopped, back up all information to external storage (i.e. external hard drive, USB keys, CDs or DVDs) on a regular basis and store the backup data in a secure location. Create extra copies of the information on the computer and secure those files using encryption or passwords. Store digital copies in a folder that cannot easily be accessed or seen by unauthorized users of the computer or the program.
Use ruggedized hardware	To reduce the risks of information being lost due to environmental factors, use ruggedized hardware. Ruggedized hardware is hardware that is designed for rough environments and does a better job of operating in difficult conditions (e.g. water, dust, humidity) than regular hardware.
Physical controls	To reduce the risks of hardware being damaged, train users on how to protect and behave around computer hardware. All users should be made aware of the following ways to prevent physical damage to the hardware: • Do not allow liquids close by to the hardware used for the FrontlineSMS software, especially the computer. • To the extent possible, minimize exposure to the environmental elements and keep the computer in a well-ventilated area. • Keep the hardware free from dust, food and/or other contaminants. Wipe the computer and keyboard with a clean cloth on a regular basis. • Keep the computer on a stable surface that is not likely to break. Also, keep the computer away from the edge of the surface and in a place where it cannot easily fall or be seen by unauthorized users (i.e.-facing windows). • Try to only use the computer indoors. If reception is an issue, it may be worth investing in an external range-extending antenna. These antennas allow the use of a GSM modem up to 20 km from the nearest cell tower and may complicate geo-location by MNOs. • If possible, lock the computer that runs FrontlineSMS to a desk so that it cannot be easily removed from the room.
Use a surge protector	Fluctuations in electricity can overload, and thus damage, computer hardware. It is a good idea to unplug computers when they are not in use. Also, it is advisable to use a surge protector to guard against power fluctuations, even in locations where variations in electricity are not common.

6.2.2 Unauthorized User Access

In addition to damage, there is a risk that people who are not meant to access a computer will do so. Unauthorized users may include intruders in the room that contains the computer hardware used for the FrontlineSMS program; friends or guests of an authorized user accessing the hub without permission; or an otherwise authorized user of the computer accessing information that he or she is not authorized to view. For example, a lawyer who is managing their clients on an instance of FrontlineSMS would not be authorized to review the cases of other lawyers using the same instance.

It is very difficult to track whether sensitive information has been accessed by unauthorized users unless that information was changed or removed. It is possible to use a secure operating system with auditing functionality, or install additional auditing software which can be used to record computer activity. Users can also track whether program resources were used by looking at the balance of credits and seeing when they were used and for what purposes (SMS or voice).

THREATS	Team members	Team members may access certain types or categories of information gathered through an instance of FrontlineSMS that is not relevant to their role and may compromise the privacy or security of a stakeholder. Additionally, employees may have an independent incentive to alter or destroy information in a FrontlineSMS system.
	Third party	An outsider or unauthorized user who plans on accessing, altering or destroying hardware or information stored on the computer. For example, a third party can access the computer hardware if the office is not locked in the evening.
RISK	Information is lost	If the computer hardware is accessed by an unauthorized user, information can be lost. See 7.2.1 for more details.
	Sensitive information is accessed by unauthorized user	If the computer hardware is accessed by an unauthorized user, sensitive program information may be read, copied, or exported. This can happen in a range of ways, including an unauthorized user accessing an unlocked system, peering over the shoulder of an authorized user, or stealing the computer. For example, an unauthorized user could take these opportunities to access all the contacts in the FrontlineSMS platform. Unauthorized access to information can result in the compromise of the privacy, dignity, and security of system users.

Sensitive information is copied or printed by unauthorized user	If the computer hardware is accessed by an unauthorized user, sensitive program information may be copied. An unauthorized user can copy information by accessing the computer hardware and inserting removable media to copy information. Similarly, unauthorized users could take pictures of FrontlineSMS screens, write down, or use the system to communicate key pieces of information. For example, phone numbers of end users stored in a database can be copied to a USB key. Information downloaded from FrontlineSMS is not tracked by the platform, and can easily be imported into Excel and printed. It is difficult to track what was printed, who printed it and how many copies were made.
Program resources used	If the computer hardware is accessed by an unauthorized user, program resources may be used. An unauthorized user can use related hardware, such as the printer, or program resources such as SMS credits. For example, an unauthorized user can access the FrontlineSMS platform and use the SMS credits for personal use.

RISK REDUCTION

Use strong physical security controls	Users should consider the following actions to secure the physical access to the hardware: • Do not allow visitors to enter the room containing the computer hardware if a team member is not in the room. Team members should be responsible for their visitor. • Lock the room containing the computer hardware at all times, especially evenings and weekends. • Only provide keys to trusted team members who need access to the system. • Keep the computer facing away from windows. • Lock the computer to the desk and lock all laptops in cabinets when not in use. • Copies of sensitive information should not be left unattended on desks and should be locked in a cabinet when the office is closed. • Do not share passwords or leave passwords written on notepads around the computer.
Password protect program resources	To reduce the risk of sensitive information being copied or printed, require users to enter a password before information resources can be printed. By doing this, an unauthorized user who copies a file with sensitive information will not be able to access the printer to make copies.
Backup information regularly	To reduce the risk of sensitive information being lost, back up information regularly. See Section 6.2.1.

7 COMPUTER SOFTWARE

Section Overview

If a computer's software is not secure, unauthorized users are able to access sensitive program information more easily. Each user accessing the computer that contains the FrontlineSMS hub should use a password and should not share their password. To the extent possible, users should consider limiting the use of Internet, uploading/downloading and email services on this computer.

Vulnerabilities	Software flaws Insecure access to the software Use of the internet	Software flaws Insecure access to the software Use of the internet
Threats	Malware uploaded or downloaded Emails monitored Man-in-the-middle attack	Information is not available or incorrect
Risks	Sensitive program information is accessed, changed or removed Unauthorized control of computer	Incorrect information used and sent Program information is lost
Risk Reduction	Secure sensitive information using encryption or password Perform regular backups Create separate user accounts to the computer and the FrontlineSMS platform Limit user access	Use anti-virus at all times Use email services only if the URL starts with HTTPS Keep the software license valid Train users to secure access to computer software

Computer software includes the Operating System (OS) and applications installed on the computer running the FrontlineSMS platform. Operating systems manage computer hardware and control how applications are used on the computer. Usually, a computer's OS and some initial applications are pre-loaded before the hardware is purchased. Applications are programs that help users perform tasks. For example, FrontlineSMS helps users to send and receive SMS messages, Microsoft Excel helps users to organize their information and Firefox helps users to browse the Internet. Each OS has built-in security features that protect some of the sensitive information stored on the computer. Computer users can

choose to download additional applications from the Internet, peripheral devices, or wireless networks. Users may also delete applications, although replacing a computer's OS is a more involved process. Frontline SMS runs on Windows, Mac OS and Linux Operating Systems (OS), but works most smoothly with Windows. Linux is the most secure OS, but additional technical skills or support may be needed to use FrontlineSMS with this and Mac OS. FrontlineSMS does not require Internet access. While there are many applications that can help FrontlineSMS perform tasks, there are also applications that can cause data integrity risks to the users.

It is important to maintain a high level of data integrity in computer software to prevent information from being lost, damaged, changed or stolen.

7.1 Questions to consider

- Who currently has login access to the computer and FrontlineSMS platform?
- What does the organization, staff, and/or volunteers use as "safe computing practices"?
- Are the operating system and software licensed and up-to-date?
- Is the organization using an anti-virus program? Is it up to date and used on a regular basis?

7.2 Data Integrity Analysis

The following section outlines the vulnerabilities related to the computer software as well as the associated threats, risks and actions that can reduce risk.

7.2.1 Software flaws

Software flaws arise when either software has an embedded mistake or someone figures out how to exploit an aspect of software for unintended uses. Software flaws may cause an application to function improperly or produce the wrong information. For example, a recent flaw in Microsoft PowerPoint allowed unauthorized users to stop the computer from working or load malware onto the computer. FrontlineSMS users may also use a variety of software that has software flaws.

It can be very difficult for users to identify small amounts of data loss or alteration. Some indications that it is possible but not guaranteed that information was lost or changed include, but are not limited to, information not appearing where it was saved, or being in a different place within the system. Unexpected pop-ups suddenly appearing on the computer or applications becoming inaccessible are also indications that the system has been corrupted with malware. Users can check the processes running in the task manager to see if there are unknown programs running and, if so, stop them.

THREATS	Data is not available or incorrect	Software flaws can cause the information used by the software to be incorrect or missing. The type of data lost depends on the software being used. For example, a software flaw could include false information in a report or could cause information to be missing from a report.
	Applications not working properly	Software flaws can cause applications to not function properly. For example, a flaw in the software could prevent SMS messages from being sent or received.
	Unauthorized loading of malware	If unauthorized users know about flaws in the software, they can use these flaws to connect and load malware or viruses onto the computer. See Section 5.2.4 for a detailed definition of malware and viruses.
RISK	Information is lost	If the application is not working properly, this can cause users to lose information for a period of time by not performing the function correctly. See section 8.2.1 for more details.
	Incorrect information used	If data is incorrect or not available, the contact or program may make decisions based on faulty information. This can cause a range of negative outcomes, from losing credibility to endangering program participants. It can be very difficult to know if small amounts of information have been changed or removed and the effects can be very serious.
	Sensitive data read, changed, corrupted or removed by unauthorized users	If malware or viruses are loaded onto the computer, unauthorized users can monitor all the information sent and received on the computer as well as allow unauthorized users to read, change or remove the information stored on the computer. See 5.2.4 for more details on malware.
	Unauthorized control of computer	If malware or viruses are loaded onto the computer, an unauthorized user control of the computer to shut down all or some of the applications of the computer. Malware can stop a user from accessing information or from performing actions such as sending or receiving SMS. For example, an unauthorized user with control of the computer can find and read all of the results of a program survey.

RISK REDUCTION	License check and updates	To reduce the risks that arise from software flaws, use a licensed operating system and software and perform any upgrades to the software as soon as they are available. A valid license allows the user to contact the OS vendor and receive support when needed.
	Use anti-virus	Anti-virus programs monitor and identify malware on a computer. Regular use of an anti-virus program may help identify and eliminate malware before it's able to cause damage. Most operating system providers (e.g. Microsoft for Windows) give anti-virus support to users with a license. There are also a number of anti-virus software programs which can be downloaded.
	Perform regular backups	To reduce the risk of information being lost, perform regular backups. See 6.2.1 for more details.

7.2.2 Removable media and peripherals

Removable media includes discs (DVDs, CDs), removable storage devices (USB flash drives, external hard drives), memory cards (Compact Flash and SD cards) and phones or GSM modems. Peripherals include keyboards, printers, Bluetooth and any devices that are used by connecting to the computer's physical ports. The primary difference is that removable media can be used to save or transfer information and peripherals can be used to perform activities more efficiently. Removable media and peripherals, when used with multiple computers, can become carriers for malware and viruses. Due to this, many operating systems automatically run virus scans on removable media and peripherals. When this doesn't take place, users may consider scanning new peripherals for viruses.

As described in other sections, computers may show signs of malware by functioning improperly or not functioning at all. Users can check the processes running in the task manager to identify and stop unrecognized programs. Users can also check the properties of a file to see the last date and time it was accessed. If the file was accessed on at a time when the computer is unaccounted for, sensitive information may have been accessed, damaged, or copied.

THREATS	Malware loaded	When removable media or a peripheral is inserted into a port, the computer reads and displays the information stored on the removable media and may automatically load the drivers or programs necessary to use the removable media or peripheral. Removable media or peripherals may intentionally or unintentionally contain applications with malware. See Section 5.2.1 for a detailed definition of malware and viruses.
	Sensitive information is printed	When a printer is connected to the computer, copies of sensitive information can be printed.

RISK	Sensitive information read, changed or removed by unauthorized users	If malware is loaded or sensitive information is printed, sensitive information can be read, changed or removed by unauthorized users. Unauthorized users may be able to read and review all the information stored on the computer, including program information such as SMS sent and received, budget, contact information, location, and more. See 8.2.1 for more details.
	Copies of sensitive information made	If malware is loaded, copies of sensitive information can be made. Removable media may run programs to copy information without the user knowing. For example, a CD inserted into the computer can run a program in the background and copy incoming and outgoing SMS messages. See Section 8.2.2 for more details.
	Unauthorized control of computer	If malware is loaded, this can allow an unauthorized user to control the computer. See 8.2.1 for more details.
RISK REDUCTION	Minimize use of removable media	To reduce the risks that can occur from removable media being inserted into the computer, avoid removable media if it is not necessary and don't insert removable media into a distrusted or unfamiliar computer.
	Secure sensitive information	To reduce the risk of sensitive information being read, changed, corrupted or deleted, secure sensitive information stored on the computer using password protection or, if available, encryption. Some software, such as Microsoft Word, comes with a feature that allows you to password protect documents.
	Limit user access	To reduce the risks that can occur from unauthorized physical access to the software, limit the number of people who have the administrative rights to print sensitive information, access the computer, or upload and download files. Only enable users who need the computer or software and for users who can be trusted. Create a Guest account that does not allow access rights to see any sensitive information for visitors or other personnel.

7.2.3 Internet use

Browsing the Internet can expose users to a range of threats from unsecure websites, including malware, uploading and downloading files, and supporting unprotected communication. FrontlineSMS users can manage these by avoiding, to the extent possible, accessing the Internet on computers that contain sensitive information. For example, e-mail services that use the HTTP protocol are not encrypted when they are sent and may allow third parties to intercept or read the information contained in online communications.

Users can detect malware through irregular behavior, such as unexpected pop-ups or inaccessible applications. Users can check the processes running in the task manager to see if there are unknown programs running, and stop them.

THREATS	Malware loaded	Malware can be downloaded unintentionally from the Internet or uploaded intentionally by an unauthorized user. See Section 8.2.2 and 5.2.4 for more details..
	Email monitoring	Emails sent using HTTP can be easily monitored by a third party and the information included in the email can be read by the third party. For example, an email containing contact information of end users can be monitored if HTTP is used.
	Man-in-the-middle attack	Emails sent using HTTP can be easily changed by a third party using a man-in-the-middle attack. This can be done when a third party controls the information sent to and from two different users. For example, if a citizen is organizing an event and emails the location of a protest to five contacts, the third party can use a man-in-the-middle attack to see this email and change the location.
RISK	Sensitive information read, changed or removed by unauthorized users	If malware is loaded, email is monitored or if a man-in-the-middle attack occurs, sensitive information can be read, changed or deleted by unauthorized users. See Section 8.2.1 for more details.
	Unauthorized control of computer	If malware is loaded, an unauthorized user can take control of the computer. See Section 8.2.1 for more details.

RISK REDUCTION

Limit internet use on the computer	Ideally, minimize the amount that the computer which runs FrontlineSMS is used to access the Internet. Internet access is not required to use the FrontlineSMS platform.
Limit user access	To reduce the use of the Internet on the FrontlineSMS computer, limit user access to the computer. See 8.2.2 for more details.
Use anti-virus software	To reduce the threats of malware and viruses, use an anti-virus to protect from malware detected in program files that are downloaded. See Section 7.2.1 for details.
Secure sensitive information	To reduce the impact of an unauthorized user gaining control of the computer, secure sensitive information using a password lock or encryption. See Section 7.2.1 for details.
Use secure web services	To reduce the threats of emails being monitored, use secure web services. Only send emails if the URL address begins with HTTPS. For example, Gmail is known to be secure. If you're using an email system where the URL address does not begin with HTTPS, consider switching accounts. Successful HTTPS connections are shown in many browsers using a padlock icon in the address bar or in the bottom right-hand corner. In order to make sure these protections are being used, make sure the padlock icon appears locked.

7.2.4 Insecure access

A computer's OS applications may be accessed by unauthorized users in-person or using remote access. The term remote access refers to the process of accessing a computer using another computer in a different location via the Internet. This is an increasingly common feature found in malware. Remote access does not require the user to physically access a computer. As long as the computer is connected to the Internet, it can be accessed from anywhere in the world. An unauthorized user can also gain remote access to a computer through social engineering.

If users share accounts, it may be very difficult to know if sensitive information has been accessed by an unauthorized user unless information was changed or removed. Some applications store log files to show the dates and times a certain user logged in and even the activities that the user performed on the application. A FrontlineSMS user can investigate whether sensitive information has been accessed by an unauthorized third party by looking for unusual activity in the log files, although some malware erases or masks this data.

THREATS	User accounts are shared	When user accounts are shared, one or more people use the same user names and password to log onto a computer or application. This happens if users intentionally share their user names and passwords or if user names or passwords have not been created for each person that can access the computer. The username and password to log onto the computer and the applications of the computer may be shared within a group of people, even those not working on the program. For example, a team member in charge of communications and a team member in charge of monitoring survey activity who share the same account can see and edit the same information.
	Unlocked workstations	If a workstation is left unattended and the computer is not locked with a password, the OS and all applications that the user is logged into can be seen and used. Information contained on the computer and applications can be read by unauthorized users. For example, a user can go for a lunch break and leave the FrontlineSMS application open.
RISK	Sensitive information accessed by unauthorized users	If user accounts are shared or a workstation is unlocked, all users will be allowed to see, use and change all information on the computer, even if it is not necessary for the user to see, use or change the information. For example, if a user goes for a break and does not log out of the FrontlineSMS platform, the platform may be accessed an unauthorized user.
	Unauthorized control of the computer	If remote access is granted to a third party or unauthorized user, this may lead to unauthorized control of the computer or the information stored on it. See Section 8.2.1 for more details.

Limit user access	To reduce the risk of sensitive information being accessed by unauthorized users, limit user access. See Section 8.2.2 for more details.
Train users to secure access to the OS and applications	To reduce the risk of sensitive information being accessed by unauthorized users, train users on how to secure the computer software. Users should take the following actions to prevent unauthorized access to the OS and applications: • Lock their workstations when leaving the computer unattended to go for a break or to the washroom. Workstations can be locked by hitting the ctrl+key+delete keys of the keyboard • Create and use strong passwords. The password should be at least 8 characters long and include at least 1 number, 1 uppercase letter, 1 lowercase letter, and 1 symbol • Do not share passwords or write passwords down and keep the written password by the computer • Create a Guest account for the OS that cannot access sensitive information or the FrontlineSMS platform and only allow visitors to use this account • Do not enable remote access to the computer.

8 HUMAN PARTICIPATION

Section Overview

Sensitive information is at risk of being changed or deleted by insiders or being incorrect when provided by end users. Specific actions should be taken to make sure that information sent by end users is real before it is used or responses are sent. Users of the FrontlineSMS platform should have separate accounts.

Vulnerabilities	User roles not properly defined	Data collection structure
Threats	User access rights are overlapping	Fake information used
	SMS spoofing	Mobile services stopped
	Fake information provided	Program stopped
Risks	Program resources used	Fake information used
	Financial loss	Mobile services stopped
	Information changed, corrupted or deleted	Program stopped
Risk Reduction	Separate user roles and duties	Create a plan for checking information from end users
	Keep track of all actions on the computer	

As with any system based on communicating with people, technology is only a small part of the process of gathering and processing information. As this Guide has described, there are a number of technical risks to data integrity that come from the mechanisms of communication, including the mobile network, the MNO, mobile phones, computer hardware and computer software.

Perhaps the most common threat to high-quality data, however, is the way that programs are designed to collect and analyze information- especially as it relates to how people interact with FrontlineSMS. Program design refers to how an individual or an organization engages with a network of people; considerations here include outreach, incentives for participation, the substance of interactions, sustainability, and monitoring and evaluation, among others. Program design also refers to how the information is handled from the time it is created to the time that it is destroyed. This means how users input, store, analyze, repackage, redistribute, and/or delete information in the system.

Human participation is the process of end users sending and receiving confidential information. As with

more security-driven concerns, human participation in any system must be locally appropriate. This means considering the context of the people you're engaging. Here, we're using context to refer to technological factors- such as literacy, technological literacy, device availability, and infrastructure- as well as non-technological factors- such as culture, cost, and relationship between you and the people in question. In addition, users of FrontlineSMS should consider how both internal staff and trusted agents use the system, as well as the network of end users.

End users are people who engage with the FrontlineSMS systems using their phones and may never see the communication hub. Typically, the FrontlineSMS platform is used to communicate with end users in several different ways:

- Public-facing – when a FrontlineSMS system is designed to engage with anyone who would like to contribute information to the system for purposes such as services, surveys, and/or reporting. Typical examples are opinion polls for radio stations and reporting on incidents such as election violence.
- Bounded network– when a FrontlineSMS system is designed to work with a defined group of end users, usually staff or people who have been trained by the user. A popular example of this is managing community health workers that work in rural areas.
- Hybrid model- when a FrontlineSMS system is designed to accept public-facing input, which is then used to inform the response of a bounded network, such as verification by staff or emergency response. Similarly, systems that are designed for repeated interaction with an end user can develop a 'trusted user' group from people who consistently produce high-quality input. Typical examples of this include journalism organizations and domestic or domestic abuse hotlines.

There are important differences and data integrity considerations between each type of end user engagement. Each of these structures also affects the program design and human participation considerations listed above. For example, if you have a public-facing program, managing outreach so that the public knows what number to text message may be more difficult than for a program who is working through agents that the user also has personal access to. The structure of engagement with end users is one of the most determinative factors in designing of a FrontlineSMS system.
Another the major design element is how a user collects information. While there are a number of different types of information, information collected through FrontlineSMS can be categorized into two different types:

- Structured data – information that is received in a predetermined format and is easily organized in a structure such as a database. For example, a survey question that expects only Yes/No or numerical answers, which are then stored in a database.
- Unstructured data – information that can be sent in any format and is not easily organized in a database. For example, a health question from an expecting mother is unstructured data because it can be any length, can include numbers, letters and symbols.

Each type of information has different benefits and disadvantages, which vary according to context. Structured data, for example, is easier to process once it's received, but requires the user to know how data should be input into the system. This may limit the complexity of the structure of that data, which may affect the amount or specificity of data that can be collected. Structured data is often used

for surveys or monitoring and evaluation because it can be easily organized in databases as records. Unstructured data, on the other hand, enables end users to input whatever type of information, both questions and answers, they like. For this reason, the information collected can be more specific and detailed. Unstructured data, however, is harder to automatically process or analyze, which means that it usually requires a person to respond to or process the text message. This can be more time consuming and expensive. Whether input is structured or unstructured does not inherently affect whether that data is high quality. It does, however, have an affect on how that information should be processed.

A critical consideration in gathering information which is intended to be authoritative in some degree – so, which is intended to be acted on, to form part of research data or to be published as fact – is the level of trust you have in the source and the veracity of the data. Unstructured data such as event reports contributed by the public can be verified by confirming whether they are true through follow-up visits or investigation, or to a lesser extent by giving greater weight to clusters of similar reports from a number of different individuals (heatmapping is an example of this kind of approach). Within bounded networks, reporters can often be assumed to be more trustworthy because they are, in effect, themselves agents of the program and have incentives to report accurately, such as continued employment or tangible community benefits. Where reports come from a wider range of sources, such as in public-facing projects, it may still be possible to build up a picture of the reliability of certain sources so that their reports can be given greater weight.

Where misinformation has the potential to bring benefits to reporters, for example, by manipulating market price information, extra care should be taken to independently verify information where possible or indicate clear caveats about the quality of the data.

It is important to maintain a high level of data integrity in program design and human participation to prevent from information from being used or from information being changed.

8.1 Questions to Consider

- Does each user have a separate user account?
- Is the program public-facing, bounded or a combination?
- What is the incentive for people to contribute to your system?
- What type of information is gathered from end users: structured or unstructured?
- What organizational processes are in place to ensure that received data is valid and accurate?

8.2 Data Integrity Analysis

The following section outlines the vulnerabilities related to the program design and human participation as well as the associated threats, risks and risk reduction actions.

8.2.1 Data collection structure

FrontlineSMS programs are either public-facing, bounded, or both, and may collect structured data, unstructured data or both. Public-facing and public-facing but bounded programs can allow end users to provide information to the FrontlineSMS platform. These face additional threats and vulnerabilities because they allow incoming information from end users.

If the SMS platform receives an overwhelming number of SMS messages in a short time period, it is possible but not guaranteed that mobile services might be stopped.

It is very difficult to know when SMS spoofing has occurred or when a message received is fake. Users should deploy a team member or have a trusted source verify urgent information that is received by an end user.

THREATS	Incorrect information sent	End users or outsiders may send fake or exaggerated information accidentally, to gain attention or to protest. End users can easily provide fake information to public-facing programs. For example, an end user can send a fake message reporting a protest that is occurring.
	SMS spoofing	SMS spoofing happens when a third party uses basic technology to set the caller ID that a user sees when the message is received. For example, a third party can pretend to be a recipient of a microloan and send a message to the FrontlineSMS platform requesting the loan be sent to a different mobile number.
	Large number of SMS messages sent	The FrontlineSMS platform may stop working if a third party sends an overwhelming amount of SMS messages because the platform will be overloaded by receiving many more messages than it can handle. This is called a distributed denial of service (DDoS) attack and can happen using an SMS gateway or services provided by the MNO for an SMS system connected to a computer. For example, if a FrontlineSMS program is asking for responses to a survey, a third party can send thousands of SMS messages to the platform in a short time period causing the platform to stop working.
RISK	Incorrect information used	If incorrect information is sent, fake messages provided by end users may be used in a survey or a program team member may take action on the message. For example, these messages can be responses to elections and surveys or they can be emergency messages asking for help.
	Services stopped	If a large number of SMS messages are sent, and services are stopped or the platform becomes overloaded, mobile services can be stopped for the SIM card. This includes voice calls, SMS and data services. The SIM will not be able to send or receive any communications.

Program stopped	If a large number of SMS messages are sent, and services are stopped or the platform becomes overloaded, the user will not be able to use the SIM card for the program. If there are no extra SIM cards, the FrontlineSMS program may be stopped completely. The impact of this risk can very high when the program has strict timelines. For example, if a program is focused on providing election monitoring and a DDoS attack happens the night before the election, the program may not be available on the day of the election.
Financial loss	If a large number of SMS messages is sent and an MNO charges users for receiving SMS messages and a DDoS attack happens, the user will lose money. The more SMS messages sent in a DDoS attack and the higher the rates of an MNO, the more money is lost by the owner of the account that's being imitated, or 'spoofed'.

RISK REDUCTION

Create a plan for checking end user information	To reduce the risk of incorrect information being used, create a plan to understand the different types of information that will be received by the program and response actions to high-priority information (e.g. messages asking for help). Include details and actions for how to check if the message is real and for understanding messages in different languages. The following checks should be performed for structured data: • Length – the expected number of characters or digits (e.g. if a survey requires a Y/N answer, the length should be 1) • Characters – the types of characters allowed (e.g. only numbers are allowed for a phone number) • Range – the range of numbers that can be accepted (e.g. digits 2-9 are acceptable for the first digit of a mobile number) • Format – the expected character and type (e.g. DDD-DDD-DDDD is the format for a telephone number) Checking the validity of unstructured data is much more complex. Verify incoming information by using a trusted source or deploy a team member to verify the information received. For example, an SMS is received that policemen are attacking citizens in a nearby city. Deploy a team member to verify this fact or contact a trusted source that is close by to that city.
Own and use multiple SIM cards	To reduce the risks of financial loss or the program being stopped, own and use multiple SIM cards. See 3.2.1 for more details.

8.2.2 Users roles not clearly defined

User roles are not clearly defined if users share accounts to log onto the computer or only one role (administrator) is used for the computer or the FrontlineSMS platform. When only one role is defined for the computer or for the FrontlineSMS application, each user can see, change and delete the same information. Some users do not need all of these access rights. User roles are not properly defined if users have more access privileges than required.

Users can know if program information was changed or deleted if information that was previously stored no longer appears and if the information shown is not was is expected. It is very difficult to know if small changes were made to program information. Users can know if program resources were used if authorized users did not send or receive communications and the balance is lower than expected.

THREATS	Overlapping access rights	Overlapping rights enables users to have more privileges than is appropriate for their role in the program. When program teams are small, it is possible to have all members working on all aspects of the program and for access rights to naturally overlap. For example, if a user is in charge of buying SMS credits and also in charge of approving expenses for the program, the user may be able to buy extra SMS credits for personal use and use the program's finances to pay for the SMS credits.
	Extra access rights	Extra access rights enable a user to be able to see more information than is appropriate for their role in the program. For example, a user whose role is to analyze survey responses received through FrontlineSMS has extra access rights if they are able to see the full contact information of the respondents to the survey in the FrontlineSMS platform itself.
RISK	Program resources used	If a user has overlapping access rights, program resources can be used. For example, if a user has access rights send and receive SMS communications and also is responsible for monitoring spend on SMS, they may be able to use program resources to send and receive for personal communications.
	Information changed or deleted	If a user has extra access rights, information can be changed or deleted. For example, if a user should only have access rights to read processed election or survey information outside FrontlineSMS but has access rights to the platform on the computer, they could change and delete information, affecting the election or survey results.

RISK REDUCTION

Separate user roles and accounts	To reduce the risk of program resources being used and information being changed of deleted, create a separate user account for people allowed to access to the FrontlineSMS system. The system administrator should be in charge of assigning roles and access rights and give each user the minimum amount of access needed to perform their tasks. For example, users that approve program expenses should not be able to claim program expenses without being audited by an independent supervisor.
Keep track of all actions on the computer and application	To reduce the impact of program resources being used and information being changed or deleted, use a logging application to keep track of all actions of all users. By keeping track of actions, it may be possible to discover which user is responsible when program information is changed or deleted, or when program resources are used.

9 CONCLUSION

This User Guide is a framework for analysis and a reflection of the experiences of FrontlineSMS users, not as a definitive or comprehensive explanation of mobile security. By focusing on simple instructions, program design elements and data quality, this framework and these recommendations are intended as locally available and accessible tools for a wide range of audiences.

Our hope is that it serves as a foundation for thoughtful discussion and analysis of mobile network environments and program design. We're happy to host that discussion on our forums at http://community.frontlinesms.com and will do our best to build additional user input into the resources we make available.

APPENDIX A: DATA INTEGRITY QUESTIONNAIRE

This checklist will provide users with an idea of how well their sensitive information is being protected and the actions that need to be taken to better protect their sensitive information.

COMPONENT	QUESTION	YES	NO
GSM Network	Do you send sensitive information over mobile networks?		
	Is there a negative impact if an unauthorized user reads the SMS messages sent and received?		
	Are the call history, SMS history and contact information on SIM cards stored for long periods of time on the mobile phone?		
	Do you only have one SIM card available for use?		
Mobile Network Operator	Did you provide your real and full name when buying your SIM card(s)?		
	Has your program been negatively affected by the government disrupting mobile services in the past?		
Mobile phones	Have you inserted an SD card from an unknown or untrusted person into the handset?		
	Have you lost information stored on your SIM card?		
	Has your mobile been damaged by water, dust or fire?		
	Is your handset not locked with a strong 8-digit PIN or password?		
	Do you access the Internet with your mobile phone?		
Computer Hardware	Is the room where the FrontlineSMS hardware located open at all times?		
	If the FrontlineSMS computer is damaged, will you lose all the program information?		
	Could food, water and dust damage the computer?		
	Are paper copies of sensitive information easily accessible?		
Computer Software	Is the operating system and software not licensed or up to date?		
	Do you not currently run anti-virus software on the computer?		
	Do users share accounts to access the FrontlineSMS computer and application?		
	If backups are performed, are the backup files stored in a folder that every user can access?		
	Does your email service use HTTP?		
Human Participation	Does each user have the same access rights when the log onto the computer?		
	Are all messages received by end users entered into the system without any checks if information is real or not?		
	Are users able to send SMS messages using the FrontlineSMS platform without being tracked?		

APPENDIX B: RESOURCE GUIDE

The following table shows where users can find more information and resources to understand the tools and actions needed to secure sensitive information.

TOPIC	SOURCE
Mobiles in-a-Box	Tactical Tech http://www.tacticaltech.org
Protection Manual for Human Rights Defenders	Frontline Defenders http://www.frontlinedefenders.org
Digital Security and Privacy for Human Rights Defenders	
Mobile Security Risks	MobileActive http://www.mobileactive.org
A Guide to Mobile Phones	Free B.E.A.G.L.E.S http://www.freebeagles.org
Mobile Malware Evolution	Securelist http://www.securelist.com
Mobile Security Threats	F-Secure http://www.f-secure.com/en_US/security/security-center/mobilie
Movements.org	Movements.org http://www.movements.org