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.

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

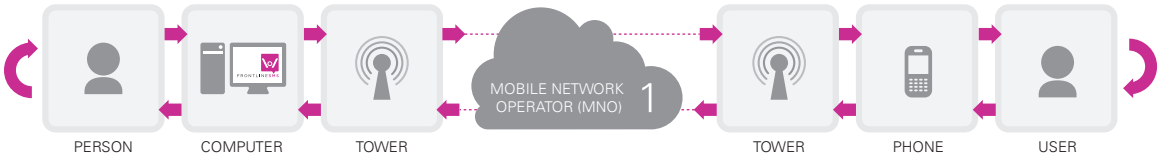
The following are the required system components to deploy FrontlineSMS:

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.

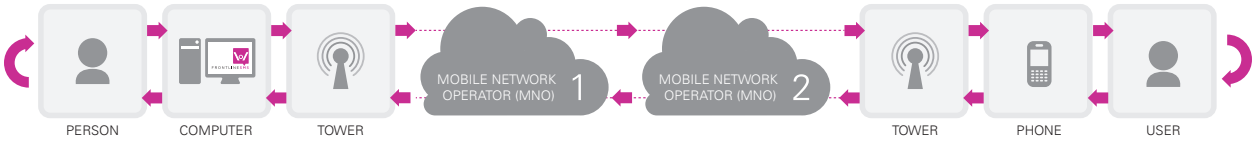
1.5 Overview of Vulnerabilities, Risks, Threats and Risk Reduction

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.

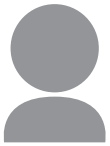
Users should regularly back up and encrypt all the important information to external storage, and keep the external storage in a locked cabinet. Users should keep the computer away from dust, liquids and food. The computer hardware should be locked to a table and laptops should be kept in a locked cabinet.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