Statistics without Borders Confidentiality, Data Security and Data Privacy Policies

This policy outlines behaviors expected of all Statistics without Borders (SWB) volunteers who handle data and will provide guidelines for proper storage and transfer of data.

Purpose

The primary objectives of this data security policy are to:

- Protect the privacy of individuals
- Protect the integrity and confidentiality of the data
- Prevent inappropriate disclosure of the data

Data confidentiality, privacy and security are priorities for SWB to ensure the protection of its customers. The protection of data is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not to be expected that this policy can effectively deal with the malicious theft scenario or that it will reliably protect all data. Its primary objective is user awareness and to avoid accidental loss or disclosure scenarios.

Data Definition and Use

The data received by SWB will be used solely for the purpose of fulfilling the requirements of the intended project and will not be used for other purposes, without prior permission from the client organization.

Data, for the purpose of this policy, include *all* information that is communicated between the client and SWB project participants. This includes documents, written and verbal communications and other types of information that are shared or created during the course of the project. This includes documents, written and verbal communications and other types of information that are shared or created during the course of the project.

Data received by SWB in any form as part of client communication or during the project will be used solely for the purpose of fulfilling the requirements of the intended project and will not be used for other purposes, without prior permission from the client organization.

While this policy covers all types of data, of particular concern for the purpose of confidentiality, security and privacy are sensitive information pertaining to both physical persons and organizations, which includes invention description(s), technical and business information relating to proprietary ideas and inventions, ideas, patentable ideas, trade secrets, drawings and/or illustrations, patent searches, existing and/or contemplated products and services, research and development, production, costs, profit and margin information, finances and financial projections, customers, clients, marketing, and current or future business plans and models, regardless of whether such information is designated as sensitive at the time of its disclosure.

Data Classification

All information covered by this policy is to be classified among one of three categories, according to the level of security required. In descending order of sensitivity, these categories are *"Confidential", "Internal Use Only,"* and *"Public."*

- *Confidential*: includes sensitive personal information (SPI) or personally identifiable information (PII) and must be given the highest level of protection against unauthorized access, modification or destruction. SPI/PII is information that can be used to identify or locate a specific individual. Examples of confidential information include, but are not limited to, information protected under privacy laws, names, date or place of birth, address, national ID, medical/health information, account number of any type, IDs, handles, and URLs, among others as well as any content that can be used to determine the identity of the individuals through triangulation and deduction.
- *Internal Use Only:* is less sensitive than confidential information, but if exposed to unauthorized parties could contribute to identify theft, financial fraud and/or violate State and/or Federal laws, or is restricted by the client.
- *Public:* is generally available to the public, or if it were to become available to the public, would have no material adverse effect on individual members of SWB, the client organization and/or any related parties.

It is the responsibility of the SWB Business Consultant and the client to identify which data that will be used during the project belong to which of these categories, and to agree on protocols to protect the confidential and internal use categories.

Data Access

It is the responsibility of SWB volunteers working with client data to ensure that data identified as confidential or internal use only not be made available outside the project team. Access to the confidential and internal use only data, whether raw or in a format specific to an application or software tool (i.e., application-native),normally be limited to the SWB volunteers processing and/or analyzing the data. processing and/or analyzing the data.

Storage and Retention

Copies/duplication of data will be kept to the minimum necessary to complete the project.

All confidential data or data for internal use only will be removed from equipment/environment within 120 days of sign-off for project completion or sooner if requested by the client. All data not publicly available will be encrypted according to industry best practices and destroyed at the end of the maximum retention period.

Data Transfer

Any transfer of data (email attachments, email body, FTP, removable media, etc.) with confidential or for internal use only information will be encrypted, transmitted using secure file transfer protocols, and/or transferred via a secure file sharing service.

Encrypted data file and password/key for unencrypting it will not be transmitted via the same channel.

Other

- Minimum encryption level for data with sensitive information is PGP, AES-128, or equivalent or stronger. The encrypted data file may be keyed or self-extracting (password).
- All back-ups and other copies due to current operational process must adhere to the same standards above.
- Any unauthorized use or disclosure of sensitive data will be reported to the organization within 72 hours of discovery by SWB.