



Scouts BSA

Troop 924 Data Governance Policy

Evanston, Illinois

Effective Date: 01 April 2019

Revision Date: N/A

DRAFT

DOCUMENT CONTROL

Document Title	Scouts BSA Troop 924 Data Governance Policy		
Summary:	This document defines the policies of Evanston Boy Scout Troop 924 regarding data governance.		
Date of Issue:	01 February 2019		
Version:	Version 1.0		
Contact Officer:	Troop Committee Member /Webmaster and Scoutmaster		
Relevant References:	BSA Internal References: <ul style="list-style-type: none"> • Boy Scouts of America Rules and Regulations, 2016 Update • Boy Scouts of America Protection of Personal Information • Boy Scouts of America Social Media Guidelines, 2017 Update • Boy Scouts of America Brand Identity Guide 310-0231, 2012 Printing • DAMA International Guide to Data Management Body of Knowledge (DAMA DMBOK ®) 		
Change History	Version	Who	What
	1.0	Brown, Kary	TBD: Policy approved by Troop Committee

CONTENTS

INTRODUCTION.....	4
Background.....	4
Objectives.....	4
Scope.....	4
Who Should Read This Policy.....	5
POLICY.....	5
Data Access.....	5
Data Usage.....	5
Data Integration.....	6
Data Integrity.....	7
RESPONSIBILITIES.....	7
Data Governance Structure.....	7
<i>Webmasters</i>	8
<i>Data Reporters</i>	8
<i>Troop Committee</i>	8
PROCESS.....	9
Data Governance Standards.....	9
Communicating Data Governance Standards.....	9
OVERSIGHT.....	10
RESOURCES.....	10
CONTACTS.....	10
DEFINITIONS.....	10

INTRODUCTION

Background

Troop data are assets maintained to support Troop 924's mission. To support effective and innovative management, troop data must be accessible, must correctly represent the information intended, and must be easily integrated across Troop 924's information systems to support the organization's strategic plans.

The Troop 924 Troop Committee and Adult Leaders recognize the value-added benefits of being able to aggregate information across multiple systems and business processes that enable Troop 924 to be a well governed and sustainable Scouts BSA Troop. The Troop Data Governance team is responsible for establishing data governance policies, procedures, standards, and guidelines for ensuring maximum value and appropriate custodianship of the Troop's data.

Objectives

The Data Governance Policy addresses data governance structure and includes sections on data access, data usage and data integrity and integration. Adherence to the data governance policy and procedures shall;

- Establish appropriate responsibility for the management of troop data as a troop asset.
- Improve ease of access and ensure that once data are located, users have enough information about the data to interpret and care for them correctly and consistently.
- Improve the security of the data, including the protection of youth, confidentiality and protection from loss.
- Improve the integrity of the data, resulting in greater accuracy, timeliness and quality of information for decision-making.
- Establish standard definitions for key troop data to promote data integrity and consistency.

The purpose of data governance is to develop troop-wide policies and procedures that ensure that our data meet these objectives within and across our data systems.

Scope

For the purpose of this policy, the terms "Scouts BSA Troop 924" or "Troop 924" includes the following areas:

- Administration
- Advancement
- Outdoor Programs, including High Adventure and Ma-Ka-Ja-Wan Scout Reservation (MSR)
- Development & Alumni Relations, including local Order of the Arrow activities
- Equipment
- Fundraising
- Health/Medical Affairs

- Information Technology
- Investments
- Training
- Treasury
- Youth Protection

“Troop Data” refers to data elements that are aggregated into metrics relevant to operations, planning, or management of any unit at Troop 924 required for use by more than one organizational unit, or included in official administrative reporting.

Policy applies to anyone engaged with Troop 924 voluntarily, by employment, or contract who creates, manages or reports these data referenced in scope above on behalf of Troop 924, or relies on these data for decision making and planning.

Who Should Read This Policy

All Troop 924 personnel who use data, regardless of the form of storage or presentation. All Troop Committee members have the responsibility to understand and implement this policy, including, as necessary, the adoption of specific procedures for their respective areas in furtherance of and in accordance to this policy.

POLICY

Data Access

One purpose of the data governance policy is to ensure that appropriate **trained** adult leaders have access to troop data and information as necessary. While recognizing the troop’s responsibility for the security of data, the procedures established to protect that data must not interfere unduly with the efficient conduct of the troop. The policy applies to all uses of Troop 924 data covered by the scope of this policy regardless of the offices or format in which the data reside.

The value of data as a troop resource is increased through its widespread and appropriate use; its value is diminished through misuses, misinterpretation, inaccuracies, and unnecessary restrictions to its access.

The institution will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the Webmaster to have an appropriate access level. The Troop Committee will provide the technology framework for data access to be provisioned. The Webmaster is responsible for ensuring the access levels are appropriate. Read-only access to administrative information may be provided to Troop Committee members for the support of troop business without unnecessary difficulties/restrictions.

Any Troop Committee member denied access may appeal the denial to the Troop Committee. Escalation to the Troop Committee Chair and Scoutmaster should only be pursued if the Troop Committee decision needs to be appealed.

Data Usage

Another purpose of data governance policy is to ensure that troop data are not misused, and are used ethically, according to any applicable law, and with due consideration for individual privacy. Use of data depends on the security levels assigned by the Webmaster.

In order to protect the identities of the Troop's youth members, considerations must be made with respect to data flowing through assets not owned by the troop. Official Troop use of Third-Party applications, websites, social media, and other data interfaces shall be restricted unless prior written consent has been provided by the Troop Committee Chair upon recommendation by the Troop's Key Three. No personally identifiable data and/or information should be shared with third-party outlets without prior consent. Consent shall be granted via a signed release that has been filed with Troop 924. Youth imagery may only be posted to the web, social media, etc. via Troop-approved media channels. Note-adults may post images of their child(ren) in third-party sites via their *personal accounts*, however, it is required that adults receive permission from the appropriate parent(s) or guardian(s) prior to posting any images that contain the identifiable likeness of a child other than their own.

The Troop 924 Troop Committee must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to Troop policy consistent with the security levels assigned to the data. Data usage falls into the categories of *update* and *dissemination*.

Update

Authority to update data that is reported as key troop data shall be granted by the Webmaster only to Troop Committee members whose job duties specify and require responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with Troop 924's desire to provide excellent service to the troop, as well as to adhere to the most current BSA's Youth Protection guidelines. The Webmaster shall ensure that adequate internal controls and/or change management procedures are in place to manage 'updates' to key troop data, their definitions and processes.

Dissemination

Dissemination of data must be controlled in accordance with the security practices set forth by the Webmaster. Appropriate use must be considered before sensitive data are distributed. Unauthorized dissemination of data to either internal/external Troop Committee is a violation of this policy.

Data Integration

Data integration refers to the ability of data to be assimilated across information systems. It is contingent upon the integrity of the data and the development of a data model, corresponding data structures, and domains. Data model designs should focus on utilizing Master Data Management (MDM) methodologies in order to streamline how data is integrated when applicable.

System-to-system interfaces are a standard practice to move data from one system to another in order to streamline processes that extend across systems and contribute to using data efficiently and effectively.

Operational processes often require systems to exchange information. System interfaces are often developed between systems to facilitate the exchange of such information. The systems that exchange information fall into two broad categories:

- Internal—Systems that are implemented within the Troop 924 network. They can either be procured, procured but modified, or custom developed products.
- External—Systems that do not reside within Troop 924. These systems are hosted by vendors and/or through sub-contracts managed by vendors.

Downloading of individually identifiable data from central systems to electronic files for the purpose of uploading or connecting the data to non-central systems (e.g., shadow systems, external vendors) without the knowledge of the Webmaster is not permitted. This practice introduces risks associated with data integrity, security, and long-term sustainability of information systems that may not be mitigated due to the nature of the practice. Departments and/or Troop Committee responsible for these practices that are found to be in violation of this policy, may result in disciplinary actions up to and including dismissal from employment consistent with Troop Committee Guidelines.

Approval by the Webmaster is specific to each request. Data granted for one purpose is not universally granted for all purposes. Each new use case must be approved by the Webmaster in a new request or an amendment to the original request, even if you already have the data.

Documented agreements regarding data use, retention, and responsibility should exist with the Webmasters (and vendors in the case of data integration with external entities) of the systems providing and utilizing data. Data extraction practices that are already in use should be registered and documented agreement developed with the appropriate Webmaster member.

Data Integrity

Data systems and/or processes that create and/or help to create troop reports should incorporate data integrity and validation rules to ensure the highest

levels of data integrity are achieved. Validation rules within data systems may need to include reconciliation routines (checksums, hash totals, record counts) to ensure that software performance meets expected outcomes. Data verification programs such as consistency and reasonableness checks shall be implemented to identify data tampering, errors, and omissions.

RESPONSIBILITIES

Data Governance Structure

The function of applying policies, standards, guidelines, and tools to manage the institution's information resources is termed data governance. Responsibility for the activities of data governance is shared among the roles listed below. Descriptions of roles and responsibilities below provide the framework of how data governance will be implemented and maintained.

Current membership of each Troop Committee role can be found at: www.troop924.org

Webmaster

Webmaster is appointed by the Troop Committee to develop data centric policies and carry out the overall administrative data security policies. Webmasters are responsible for making known the rules and procedures to safeguard the data from unauthorized access and abuse. They authorize the use of data within their functional area, and monitor to verify appropriate data access. They assist troop data users by providing appropriate documentation and training to support troop data needs. Webmasters coordinate and manage the data in the business process that results in the data adhering to Evanston Boy Scout Troop 924 standards. Once data have entered the system, there is a process by which they are validated, transmitted, stored, and archived. The capture and checking are typically based on a functional process or business process. This data manager role oversees adherence to the business process and in some cases develops the process. While there may be several data managers, the Webmasters will appoint one as primary for each application.

Data Reporters

Data Reporters are individuals within the institution who have an intricate understanding of the data in their area. They establish reporting procedures for troop data, which may include recommending changes to data entry practices. They are responsible for implementing the decisions of the Webmasters in functional areas, assuring that census, backup, and retention plans are implemented according to defined needs. Because data reporters have a hands-on role with data, they monitor or oversee monitoring of data quality.

Troop Committee

The Troop Committee is responsible for allowing access within the rules and standards set by the Webmaster for their area. The Troop Committee should work with the Webmaster for each area to document the agreed upon procedures that will be followed to administer security access.

It is the responsibility of the Troop Committee to routinely monitor access and ensure that access levels are up to date.

PROCESS

Data Governance Standards

The purpose of establishing standards is to ensure that troop data have a high degree of integrity and that key data elements can be integrated across functional units and electronic systems so that faculty, staff, and management may rely on data for information and decision support.

Troop data will be consistently interpreted and clearly documented, according to the best practices agreed upon by the Troop Committee, and it will have documented values in all Evanston Scout Troop 924 systems. It is the responsibility of the Webmaster to ensure the correctness of the data values for the elements within their charge.

Troop data are defined as data that are maintained in support of a functional unit's operation and meet one or more of the following criteria:

1. the data elements are key fields, that is, integration of information requires the data element;
2. the institution must ensure the integrity of the data to comply with internal and external administrative reporting requirements, including troop planning efforts;
3. the data are reported on or used in official administrative reports;
4. a broad cross section of users requiring data.

It is the responsibility of the Webmaster, in conjunction with the Troop Committee, to determine which core data elements are part of our troop data.

Documentation (metadata) on troop data will be maintained within a troop repository according to specifications provided by the Troop Committee. These specifications will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is derived and used. The interpretation will include acceptable values for each element, and any special considerations, such as timing within an academic or fiscal calendar.

All adult leaders are expected to bring data problems and suggestions for improvements to the attention of the Webmaster or any member of the Troop Committee.

Communicating Data Governance Standards

The Webmaster is responsible for establishing data standardization and standard reporting practices. The Webmaster will obtain approval from the Troop Committee when standards are developed and/or modified. A central repository will be maintained and should be referenced for specific guidelines and decision outcomes related to data governance as set forth within this policy. The repository of reporting standards, documented troop data, and key decisions can be found at:

- TBD

OVERSIGHT

Penalties for deliberate violations of this policy will be adjudicated in accordance with applicable disciplinary policies and procedures of the Troop Committee and the Northeast Illinois Council, and/or the Scouts, BSA.

RESOURCES and POLICIES IN EFFECT

- Boy Scouts of America Policies
 - Boy Scouts of America Rules and Regulations, 2016 Update
 - Boys Scouts of America Protection of Personal Information
 - Boy Scouts of America Social Media Guidelines, 2017 Update
 - Boy Scouts of America Brand Identity Guide 310-0231, 2012 Printing
 - Any other current and adopted Boy Scouts of America National Policy
 - Any other current and adopted North East Illinois Council (NEIC) Policy
- Related Federal Regulations
 - Family Educational Rights and Privacy Act (FERPA)
 - <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
 - Health Insurance Portability and Accountability Act (HIPAA)
 - <http://www.hhs.gov/ocr/privacy/>

CONTACTS

Scoutmaster: scoutmaster@troop924.org

Troop Committee Person/Webmaster: kary.brown@gmail.com

DEFINITIONS

Data Element

A single data item. For example, last name is a data element.

Data Dictionary

A reference tool which provides a description of all the core troop data elements.

Data Dissemination

The distribution of data to either internal or external stakeholders. Included in dissemination is the sending of data to external entities including vendors that provide services for Evanston Boy Scout Troop 924.

Data Integrity

The qualities of reliability and accuracy of data values that permit the institution to have dependable data on which to make plans, projections and decisions. Data integrity contributes to the efficient operation of the institution by supporting quality customer service to students, faculty and employees, and helping the institution remain competitive.

Data Integration

The ability of data to be assimilated across information systems, is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

Data Model

A diagrammatic representation of the objects and their properties that are needed within an organization to accomplish its mission. Sometimes represented as an ER (entity-relationship) diagram or a data flow diagram.

Data Value

The set of values that each data element can have. For example, Eagle, Life, Star, First Class, and Second Class are a selection of values of the data element named "Rank".

Troop Data

The data elements that are aggregated into metrics relevant to operations, planning, or management of any unit at Evanston Scout Troop 924, that are reported to Troop 924's Troop Committee, parent organizations, sponsors, federal and state organizations, generally referenced or required for use by more than one organizational unit, or included in official administrative reporting.

Metadata Repository

Information about the data in an organization's electronic systems. It is used to catalog the data elements and to enable software development tools and operational systems to assess the data. Webmasters add interpretive information to the repository so that the meaning of each element is clear, and can be use consistently across all systems. Data dictionaries are built from the repository.