Big Brothers Big Sisters of the Capital Region (BBBSCR) Data Security and Privacy Plan

Last Updated: August 7, 2023

1. Introduction

At Big Brothers Big Sisters of the Capital Region (BBBSCR), we are committed to safeguarding the confidentiality, integrity, and availability of all data and information entrusted to us. This Data Security and Privacy Plan outlines our organization's approach to protecting sensitive data and ensuring compliance with data protection regulations. The plan is designed to address potential risks and establish measures to maintain the highest level of data security and privacy for the size and budget of this organization.

2. Scope
This plan covers all data collected, processed, and stored by BBBSCR, regardless of the format (physical or digital) or the location where it is stored. It applies to data related to our program participants, employees, volunteers, donors, partners, and any other individuals or entities associated with BBBSCR.

3. Data Classification
We categorize data into different levels based on its sensitivity and potential impact on individuals and the organization. The data classification levels are as follows:

a) Confidential Data: Personally identifiable information (PII), financial data, health information, and any other sensitive data requiring strict protection.
b) Internal Use Data: Non-public information used for internal purposes, not publicly disclosed but not classified as highly sensitive.
c) Public Data: Information that can be freely shared with the public without any risk to individuals or the organization.

4. Data Collection and Usage

4.1 Purpose Limitation: We collect and process data only for specific and legitimate purposes, clearly communicated to the individuals involved.

4.2 Data Minimization: We collect and retain only the minimum amount of data necessary to fulfill the intended purpose.

4.3 Consent: We obtain explicit consent from individuals before collecting or processing their personal data, and we provide them with information about the purposes and handling of their data.

4.4 Data Access and Usage: Access to sensitive data is restricted to authorized personnel with a legitimate need for access. Data shall be used only for its intended purpose and not be shared or disclosed outside the organization without proper authorization.

5. Data Security Measures

5.1 Physical Security: Physical access to data storage areas is restricted and monitored. Confidential documents and physical media are securely stored.

5.2 Information Security Policy: BBBSCR maintains an Information Security Policy that outlines security best practices, acceptable use, and access control measures.

5.3 Data Encryption: Confidential data is encrypted both in transit and at rest to protect against unauthorized access.

5.4 Access Controls: Access to data systems and databases is granted based on the principle of least privilege, and multi-factor authentication is enforced for privileged accounts.

5.5 Audits and Assessments: Security audits and assessments will be conducted at the earliest possible time the organization can incur the cost to hire a third-party contractor to perform these audits and assessments. The purpose of which is to identify vulnerabilities and provide an outside perspective to ensuring compliance with security standards.

6. Data Breach Response

6.1 Incident Response Plan: BBBSCR has an Incident Response Plan in place to handle data breaches promptly and effectively. The plan includes identification, containment, eradication, recovery, and lessons learned phases.

6.2 Notification: In the event of a data breach that poses a risk to individuals' rights and freedoms, affected individuals and relevant authorities will be notified as required by applicable laws and regulations.

7. Data Retention
Data will be retained only for as long as necessary to fulfill the purpose for which it was collected or as required by law. Once data is no longer required, it will be securely and permanently disposed of.

8. Training and Awareness
All employees and volunteers handling data at BBBSCR will receive regular training on data security, privacy best practices, and their responsibilities in safeguarding data.

9. Compliance and Monitoring

BBBSCR is committed to complying with all applicable data protection laws and regulations. The Data Security and Privacy Plan will be reviewed periodically, and updates will be made as necessary to address emerging risks and changing regulations.

10. Reporting Incidents or Concerns
Any data security incidents or privacy concerns should be promptly reported to the designated data protection officer or the appropriate authority within BBBSCR.

11. Conclusion
This Data Security and Privacy Plan reflects BBBSCR's commitment to upholding the highest standards of data security and privacy. By implementing these measures and fostering a culture of security and privacy awareness, we ensure the protection of our stakeholders' data and maintain their trust in our organization.