samegoal

Technical and Compliance Handbook

Last revised 4/21/22

This handbook is intended to help technical and compliance-focused education professionals understand SameGoal's policies in this area. It is meant as a companion document to SameGoal Terms & Privacy. Purposes include:

- **Crosswalk:** Provide a crosswalk from common areas of interest to relevant areas of Terms & Privacy.
- **Elaborate:** Further elaborate on areas addressed in Terms & Privacy based on frequently asked questions.
- **Address:** Provide information on areas not covered in Terms & Privacy but commonly of interest.

We expect this handbook to change from time to time as we work to clarify our policies. In the event this handbook conflicts in any way with SameGoal Terms & Privacy, our Terms & Privacy prevail.

SAMEGOAL TECHNICAL AND COMPLIANCE HANDBOOK

Table of Contents

Preface

SameGoal takes data security, privacy and compliance very seriously. At a glance:

- SameGoal has had no known data breaches since 2008 (founded).
- SameGoal has received 1EdTech TrustedEd Apps Certification.
- SameGoal has never been found in violation of FERPA by the Family Policy Compliance Office.
- No LEA to date has terminated its use of SameGoal due to company failure to fulfill its security obligations.

Our strong commitment to data security, privacy and compliance contribute to SameGoal's 99%+ annual customer retention rate.

1. Definitions

The following terms are used throughout this handbook.

1.1 SameGoal Services

"SameGoal Services" includes all services provided by SameGoal in the course of fulfilling a contractual license term.

1.2 Client

"Client" means any entity or individual who purchases SameGoal Services. The most common SameGoal Clients are local education agencies (LEAs) and state agencies.

1.3 User

"User" means individuals authorized by the Client to access and use SameGoal Services.

1.4 Client Data

"Client Data" refers to any data entered or exchanged through use of SameGoal Services.

1.5 Record

"Record" means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, microfiche and email.

1.6 Education Records

"Education Records" are Records that are directly related to a student and that are maintained by an educational agency or institution, or a party acting for or on behalf of

the agency or institution. Learn more

1.7 Personally Identifiable Information

"Personally Identifiable Information" or "PII" means information and metadata that, alone or in combination, is linked or linkable to a specific student so as to allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Personally identifiable information includes but is not limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address or phone number of the student or student's family; (d) personal identifiers such as the student's state-assigned student identifier, social security number, student number or biometric record; (e) indirect identifiers such as the student's date of birth, place of birth or mother's maiden name; and (f) demographic attributes, such as race, socioeconomic information, and gender.

1.8 Student Profile

"Student Profile" means a collection of PII data elements relating to a student of the Client.

1.9 Incident

"Incident" means a suspected, attempted, or imminent threat of a security event that compromises, or has the potential to compromise, the integrity, confidentiality, or availability of Client Data.

1.10 Data Breach

"Data Breach" is an incident that results in the confirmed disclosure of Client Data to an unauthorized party.

1.11 Mine Client Data

"Mine Client Data" means the act of searching through, analyzing, accessing, or extracting Client Data, metadata, or information not necessary to provide SameGoal

Services.

1.12 Securely Destroy

"Securely Destroy" means to remove Client Data from SameGoal systems, paper files, records, databases, and any other media regardless of format so that Client Data is permanently irretrievable by SameGoal and any subcontractors through the normal course of business.

2. System Architecture, Updates and Maintenance

2.1 System Architecture

SameGoal provides a fully hosted, standards-based web application.

SameGoal is architected as a distributed system, meaning all servers can easily be run from any machine in SameGoal's production infrastructure. The number of servers running for any portion of the system can easily be scaled up or down.

Each Client has its own, separate database on SameGoal servers.

2.2 Hosting

All Client Data is hosted on dedicated, SameGoal owned and operated servers colocated at SOC 2 Type II Audit Certified data centers. Production servers are physically located in Elk Grove Village, IL. Backup servers are physically located in Madison, WI.

SameGoal uses no third-party hosting providers.

2.3 System Requirements

SameGoal provides a web-based application that supports the current and previous version at any given time of all major web browsers, including Chrome, Firefox, Microsoft Edge and Safari.

SameGoal supports any platform these browsers run on, including desktop computers, Chromebooks, laptops, tablets and mobile devices.

A PDF plugin must be installed in order to print documents from SameGoal, and JavaScript must be enabled in the browser. However, there are no other technologies, licenses or dependencies required to use SameGoal. Learn more

2.4 Network Requirements

Users accessing SameGoal must be connected to the internet. The internet may be accessed over Wi-Fi, wired connection, or a User's device data plan. SameGoal does not require out of the ordinary bandwidth requirements.

If a Client's Users access SameGoal from behind a firewall, access to **samegoal.com** must be permitted.

If a Client chooses to use LDAP/Active Directory to authenticate its Users with SameGoal, a network connection is required; the SameGoal IP Range must be permitted.

2.5 Product Updates

SameGoal maintains a cross-functional team that reviews customer feedback and enhancement requests on a quarterly basis. Feature and functionality enhancements that SameGoal, in its own discretion, determines are most likely to deliver a high degree of benefit to a large number of Clients are prioritized for placement on the product development roadmap. Product updates are free of charge throughout a license term, but each update may apply to all, or only some, license editions.

SameGoal is also updated frequently in response to state and federal legislative changes. These compliance-related updates bypass quarterly review, and instead are handled as quickly as possible by our state customization team. These compliance-related changes are deployed to all SameGoal license editions.

2.6 Software Updates

Software updates are released often. They vary in scope (e.g. very minor bug fixes or state changes) to general functionality enhancements. When a software update is deemed significant in nature, Clients are provided notice and documentation in advance.

Software updates are applied globally across all Clients. Assistance from Client's technical staff is not required. Individual Clients cannot opt out of updates.

2.7 Software Maintenance

SameGoal performs all upgrades, patches and updates related to SameGoal Services. From the Client's perspective, there are no standard maintenance windows for SameGoal.

2.8 Services Availability

SameGoal agrees to maintain 99% uptime during regular business hours. See Service Level Agreement, 4. Minimum Applicable Service Levels

2.9 Backups

Each Client's data is housed in a separate PostgreSQL database. Under normal operations, all databases are backed up at least once per day. These backups are automated and actively monitored.

Database backups are regularly placed on each Client's SameGoal SFTP account, where they may be securely downloaded by the Client.

Both SameGoal and the Client can use the standard PostgreSQL database retoration utility pg_restore to restore a Client database. PostgreSQL is free and open source.

2.10 Disaster Recovery

SameGoal takes steps to prepare for and prevent against deleterious effects of unexpected events and catastrophic emergencies. Some examples include:

- **Power or network failure:** All Client Data is served from SameGoal servers colocated within SOC 2 Type II Audit Certified data centers. These data centers provide redundant power and internet.

- **Drive failure:** All Client Data is stored in triplicate. SameGoal Services may continue to read/write from remaining drives while a failed drive is replaced.
- **Server failure:** SameGoal production serving infrastructure includes additional machines for server failover. Because SameGoal is a distributed system, application severs may be moved to another server when necessary.
- **Other hardware failure:** SameGoal production serving infrasture includes redundant hardware (e.g. switches, cables, ports, etc) that can be put in service when needed.
- **Natural disaster:** SameGoal maintains geographically dispersed hosting infrastructure. Hosting may be moved to another geographic location in the event of a natural disaster or other catastrophic event.

In the event all three copies of Client Data became unusable or unavailable, SameGoal is able to restore to the Client's last backup. In most cases of catastrophic failure, SameGoal anticipates service restoration in less than one day. In extreme cases, restoration time could increase.

2.11 Programming Technologies

SameGoal uses Go, C++ and PostgreSQL server-side. SameGoal uses the Closure Library JavaScript framework on the front-end browser application. All technologies used by SameGoal are either open source or proprietary to SameGoal. See [open-source libraries used by SameGoal]()

2.12 Integration

SameGoal provides many methods of Client Data integration.

Data integration may include the transfer of information stored in another application to SameGoal Services, from SameGoal Services to another application, or both. Integration may occur on a one-time basis, automatic basis, or both with respect to the extent of integration(s) involved. See Data and Privacy Agreement, 4. Integration

2.13 Accessibility

SameGoal strives to address the accessibility needs of its diverse Users, many of whom use assistive technologies with the program. As accessibility issues are reported, they are triaged and resolved.

SameGoal has not completed a formal review process to ensure compliance with Section 508 and does not publish a Voluntary Product Accessibility Template (VPAT). These are areas of future consideration.

3. Data Ownership

The Client owns Client Data entered or exchanged through use of SameGoal services. See Data and Privacy Agreement, 6. Data Ownership

- **Backups:** The Client may download full backups of its data.
- **Integration:** The Client is entitled to integrate Client Data entered or exchanged through use of SameGoal Services with any other application, including those not operated by SameGoal.

4. Data Privacy

4.1 Information Collected

SameGoal collects information related to user accounts, students, special program documentation and system access. See Data and Privacy Agreement, 1f. Information Collected. Data is collected via:

- Bulk imports, typically during implementation
- Users entering data while using the application
- Integration with third party systems

Client Data is collected for Special Programs documentation and includes PII. PII data elements SameGoal Services collects includes, but is not limited to:

- Student's name
- The name of the student's parent and/or other family members
- The address of the student and/or student's family
- A personal identifier, typically the student's "Student ID"
- Other indirect identifiers, including the student's date of birth

4.2 Use of Client Data

SameGoal uses Client Data for the following purposes:

- Providing SameGoal Services;

- Auditing, research and analysis in order to maintain, protect and improve SameGoal Services;
- Ensuring the technical functioning of the network;
- Protecting the rights or property of SameGoal or its Users; and
- Developing new services.

SameGoal does not:

- Mine, sell or rent Client Data
- Use Client Data for its own commercial benefit
- Use Client Data to create a Student Profile other than as required to perform SameGoal Services
- Store Client Data outside the continental United States
- Share Client Data with any third party without an explicit request from the Client, except when required by law

See Data and Privacy Agreement, 1.d User communications

4.3 Advertisements

SameGoal does not display advertisements or share information with advertisers. Users are not tracked or targeted for advertisement using any first or third party technology. See Data and Privacy Agreement, 1e. Advertisements

4.4 Qualified FERPA Exception

SameGoal has access to Client's Education Records. Pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA"), a Client using SameGoal Services designates SameGoal as a "school official" with "legitimate educational interests" in Client's Education Records and PII disclosed pursuant to Client's use of SameGoal Services.

- SameGoal abides by the FERPA limitations and requirements imposed on school officials.
- SameGoal uses Education Records soley for the purposes described in 3.2 Use of Client Data
- SameGoal has never been found to be in violation of FERPA by the Family Policy Compliance Office.

4.5 Subcontractors

SameGoal does not use subcontractors in conjunction with delivering SameGoal Services, except for:

- Server colocation services at SOC 2 Type II Audit Certified data centers
- Local support partners in some states

4.6 Policy Changes

SameGoal may make changes to its "Terms of Service", "Service Level Agreement" and "Data and Privacy Agreement" from time to time. When these changes are made, SameGoal will provide 30 days advance notice and make an updated copy available to you from within, or through, the affected SameGoal Services. See Terms of Service, 12. Changes to the Terms

5. Data Security

5.1 Security Safeguards

SameGoal stores and processes Client Data in accordance with commercial best practices, including implementing appropriate administrative, physical and technical safeguards to secure Client Data from unauthorized access, disclosure, alteration and use.

5.1.1 Administrative Safeguards

SameGoal restricts access to Client Data, internal systems and internal infrastructure to exclusively SameGoal employees, contractors and agents who need access in order to operate, develop, support or improve SameGoal Services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

5.1.2 Physical Safeguards

Client Data is hosted at SOC 2 Type II Audit Certified data centers. These data centers provide superior physical safeguards, including:

- 24/7 armed guards
- Biometric access requirements
- Limited authorized personnel

Physical access to locked server cabinets at these data centers is restricted to a small number of individuals whose identity is verified at point of entry. All data is encrypted both in transmission and at rest.

Similarly, remote access to both production and backup servers is restricted to a small number of individuals. Remote server access requires authentication via public key only (no passwords), SSH protocol version 2 connections only, and provides no shell access.

5.1.3 Technical Safeguards

SameGoal uses many technical safeguards to protect against unauthorized access, alteration, disclosure or destruction of Client Data. Technical safeguards include, but are not limited to:

- Maintaining a secure server configuration, including:
  - Strict firewall
  - Minimum number of ports open
  - Hardened services on open ports
  - Automatic application of security updates
- SFTP security measures, including:
  - Authentication via public key only (no passwords)
  - No shell access for Users
  - SSH protocol version 2 connections only
- Mandatory encryption of all data both in transmission and at rest
- Defensive domain registration
- Enforcement of strong passwords
- Web application tracking of document edit version history
- Regular security audits of SameGoal code base and serving infrastructure
- Storage of all Client Data in triplicate
- Automatic backups to geographically-dispersed remote locations
- Intrusion detection system (IDS)

A common attack vector for web applications is a compromised User account. To that effect, SameGoal employs complete segmentation of Client Data; each Client has its own, separate database.

5.2 Verification of Security Safeguards

SameGoal regularly verifies expected security safeguards are in place. Some methods include:

- Regular security audits using third-party auditing tools. These tools may also be used by a Client at any time to independently verify security safeguards for **samegoal.com**. A few examples:
    - Qualys SSL Labs Server Test - **A+ Rating** on 4/20/22
    - Security Headers Test - **A Rating** on 4/20/222
- Regular first party vulnerability scanning
- Regular first party penetration testing
- Periodic risk assessments and timely resolution of security vulnerabilities

A "SOC 2 Type 2 Independent Service Auditor's Report" can be provided by SameGoal's colocation hosting service provider upon Client request.

SameGoal does not provide results or confirmation of commissioned third-party security audit results, or commission third-party security audits at Client request.

If a Client independently uses or subscribes to a third-party security monitoring software, Client may use this to analyze SameGoal and provide SameGoal with results. However, these programs often lack nuance and understanding of the systems they scan, and frequently return false positives. For this reason, SameGoal may decide whether or not to review, respond and/or take action on any Client-provided third-party audit report at its own discretion.

6. Incidents and Data Breach

6.1 Incident Evaluation

Immediately upon becoming aware of a security Incident, or upon receiving a complaint of an Incident, SameGoal will fully investigate the Incident following industry best practices. SameGoal will also take steps to prevent developments that may result in the Incident becoming a Data Breach and resolve the Incident.

6.2 Data Breach

If investigation of an Incident confirms Client Data was disclosed to an unauthorized party, SameGoal will provide written notice to the Client. SameGoal will not provide notice directly to individuals whose PII was involved, to regulatory agencies, or other entities without first providing written notice to the Client, except as otherwise required by law.

6.3 Data Breach Investigation Report

In the event of a Data Breach that discloses Client Data to an unauthorized party, SameGoal will provide written notice to the Client that includes a "Data Breach Investigation Report" (DBIR) once the investigation has concluded and steps have been taken to prevent further disclosure of Client Data.

The DBIR is a written report, including any supporting documentation, that identifies:

- The nature of the Data Breach
- Steps SameGoal has taken to investigate the Data Breach

- What Client Data, including PII, was disclosed or used
- Who or what was the cause of the Data Breach
- What SameGoal has done or shall do to remediate any deleterious effect of the Data Breach
- What corrective actions SameGoal has taken or shall take to prevent a future Data Breach

6.4 Effect of Data Breach

If a Data Breach results in downtime of SameGoal Services, the Client may be entitled to a license fee credit per the SameGoal Service Level Agreement. If the Client chooses to terminate its use of SameGoal Services following a Data Breach, the Client may request a refund of remaining prepaid SameGoal license fees.

Note: SameGoal has had no known Data Breach since 2008 (founded). A Client has never terminated use of SameGoal Services due to SameGoal's failure to comply with its security obligations.

7. Legal Orders, Demands or Requests for Data

7.1 Received by SameGoal

Except as otherwise expressly prohibited by law, SameGoal will:

- Immediately notify the Client of any subpoenas, warrants, other legal orders, or demands or requests received by SameGoal seeking Client Data;
- Consult with the Client regarding response; and
- Upon Client request, provide the Client with a copy of SameGoal's response.

7.2 Received by Client

If the Client receives a subpoena, warrant, or other legal order, demand or request seeking Client Data maintained by SameGoal, the Client has many end-user availabile tools it may use to facilitate a response. For example:

- Within the SameGoal web application, administrative Users may access all documents. Any deleted document can be undeleted.
- Within the SameGoal web application, administrative Users may access the document history panel for any document when using SameGoal Pro Edition. This shows document edits, as well as key document events such as document creation, completion, incompletion, amendment, deletion, undeletion, etc. Each document edit and event is associated with a date, time and User who performed the change.
- The Client can download and restore a full database backup.

If the Client needs further assistance or information in formulating a response, the Client may contact SameGoal. SameGoal will take reasonable efforts to assist the Client in producing requested information.

7.3 Parent Request

If a parent, legal guardian or student contacts SameGoal with a request to review or correct Client Data or PII, SameGoal will direct this individual to instead contact the Client.

If a parent, legal guardian or adult student contacts the Client with a request to review or correct Client Data or PII, the Client may contact SameGoal. At the direction of the Client, SameGoal will use reasonable and good faith efforts to assist the Client in fulfilling such requests within ten (10) calendar days of being contacted by the Client.

8. Compliance with Applicable Law

SameGoal abides by applicable state and federal laws. Examples of federal laws SameGoal abides by relevant to the provision of SameGoal Services includes:

- **Family Educational Rights and Privacy Act** (FERPA)
- **Protection of Pupil Rights Amendment** (PPRA)

Examples of federal laws that may apply to Client's other services but do not apply to SameGoal Services include:

- **Children's Online Privacy and Protection Act** (COPPA) - SameGoal Services are not directed to children under 13.
- **Health Insurance Portability and Accountability Act** (HIPPA) - Except in an extremely narrow set of cases, data entered in Special Programs documents by educational institutions are considered Education Records covered under FERPA, rather than Personal Health Information (PHI) covered by HIPPA. Any potential or existing Client that determines their particular data would be considered PHI and covered by HIPPA should not use, or should cease use, of SameGoal Services. A HIPAA business associate agreement (BAA) is not required between the Client and SameGoal. See HHS/USDOE Joint Guidance
- **Payment Card Industry Data Security Standards** (PCI DSS) - SameGoal collects all payments by check or wire transfer.

9. Termination

9.1 Termination by Client

The Client may terminate SameGoal Services at any time and request a refund of remaining prepaid SameGoal license fees.

9.2 Termination by SameGoal

SameGoal may terminate provision of contracted SameGoal Services with a Client at any time if any of the events below occur. See Data and Privacy Agreement, 8. Ending your Relationship with SameGoal

- A Client's User breaches any provision of SameGoal's Terms of Service or has acted in a manner which clearly shows that the User does not intend to, or is unable to comply with the provisions of SameGoal's Terms of Service
- SameGoal is required to do so by law
- The partner with whom SameGoal offered SameGoal Services to the Client with has terminated its relationship with SameGoal, or ceased to offer SameGoal Services to the Client
- SameGoal is transitioning to no longer providing SameGoal Services to Users in the state in which Users are residents or from which Users use SameGoal Services
- The provision of SameGoal Services to the Client by SameGoal is, in SameGoal's opinion, no longer commercially viable

10. Data Handling Upon Termination

10.1 Transfer of Client Data

The Client is responsible for extracting desired data collected through SameGoal Services upon termination. Some options include:

- Download PDFs for each student in bulk from the SameGoal web interface
- Download a full database backup from Client's SFTP account
- Executing and downloading reports to extract key data
- Use SameGoal's document viewer integration for one year to continue displaying effective plan documents in the Client's student information system during a switchover process

If the Client plans to terminate use of SameGoal Services via non-renewal for an upcoming school year, and notifies SameGoal at least one month in advance of the current license term ending, SameGoal offers a 6 month window of free access to SameGoal Services in order to allow the Client a smoother transition. If after this free service window the Client decides to continue use of SameGoal Services, the Client is then responsible for the full cost of the annual subscription.

SameGoal allows Clients to securely access and extract data from SameGoal Services. The Client is responsible for securely transfering any Client Data from SameGoal to another third-party provider. The Client and/or third-party providers are responsible for any post-processing and import of Client Data extracted from SameGoal Services. SameGoal does not offer custom development services to provide Client Data in a custom data format.

10.2 Destruction of Client Data

Upon Client's termination of use of SameGoal Services, the Client's SameGoal environment is inactivated. SameGoal will Securely Destroy Client's data within 60 days of

receipt of written request. See Data and Privacy Agreement, 6. Data Ownership

This process includes:

- Deletion of Client's database and directories from SameGoal servers
- Deletion of all Client database backups
- Deletion of all Client data from Client's SFTP account
- Use of DBAN and physical destruction of drives when decommissioned

SameGoal will confirm to the Client in writing once the Client's data has been permanently deleted.

11. Liability

By accessing and using SameGoal Services, Users agree not to sue or institute any cause of action or legal proceeding of any nature against SameGoal or any of its affiliates, or its or their respective officers, directors, employees, representatives, agents, licensors, licensees, successors and assigns (collectively the "Released Parties") for, and agree to release, acquit, forever discharge and compensate and hold harmless the Released Parties from and against, any and all costs, damages (actual, consequential, special, incidental, indirect, exemplary, punitive or otherwise), losses, liabilities, claims or expenses (including attorneys' fees) of any kind and nature, known and unknown, suspected and unsuspected, disclosed and undisclosed (collectively, "Damages"), arising out of, relating to, or in any way connected with User access or use of SameGoal Services. See Data and Privacy Agreement, 10. Release and Limitation of Liability.

12. Insurance

SameGoal maintains professional liability coverage. Coverage includes:

- Media, tech, data & network liability
- Breach response
- Regulatory defense & penalities
- First party data & network loss, including:
    - Business interruption loss
    - Dependent business interruption loss
    - Cyber extortion loss
    - Data recovery costs
- eCrime
- Criminal reward

A certificate of insurance (COI) can be provided upon Client request.