8279 Mayfield Rd,
Unit 12
Chesterland, OH 44026

# Client Data Protection

By executing a contract with Main Sail, LLC, you and/or your company, if applicable, agree to comply with all applicable rules, laws, regulations and contractual requirements that address the protection and handling of sensitive information.

1. **I understand that Client Data includes the following types of information:**
    - Personal Information – Information that can be used to locate or identify an individual, such as a name, alias, Social Security number, biometric record, or other personal information linked or linkable to an individual. In most circumstances, this data relates to the client's customers or personnel, although it may include personal data submitted to the client on behalf of Main Sail personnel or its Contractors. Loss of such information may lead to identity theft or other fraudulent use of information, resulting in substantial harm, embarrassment, and inconvenience to individuals.
    - Business Data – Non-personal business information the client considers confidential or sensitive (e.g., pricing information, trade secrets, financials, mergers, acquisitions or other strategic plans).
    - Intellectual Property (IP) – Generally includes copyrighted, trademarked, or other protected materials, processes, designs, or trade secrets owned or licensed by the client.

    **Exceptions: The requirements of this policy do not apply to the following information:**

    a. Information identified by Executive Order as national security information ("Classified Information"), which must be protected in accordance with applicable rules, regulations and security classification guidance provided by the US government;

    b. Attorney-Client or Attorney Work Product Privileged Information; or

    c. Information protected under court order.

2. **I will access Client Data using only approved methods, locations and devices.** Client Data may not leave the client project environment unless explicitly permitted by the project. Using a contractor-owned computer to access highly confidential client data is not permitted unless it is approved beforehand by both the client and Main Sail.

3. **I will use care to become and remain aware of accessed or stored Client Data, including information located on:**
    - Main Sail owned electronic equipment (e.g. computers, external hard drives, personal files on shared servers, etc.)
    - Client-owned electronic equipment
    - Contractor computers (if approved by both the client and Main Sail )
    - Portable data storage devices (e.g., CDs, DVDs, flash drives, etc.)
    - Old and archival data and backups, and
    - Hard copy (e.g. paper files, day planners, etc.).

4. **I will not bring or use any data owned by the client onto a different engagement.** At the end of my involvement with a project, I will remove all Client Data associated with that project from the hardware and media under my control. If, during my current project, I find Client Data that appears to be from a different client, I will notify my Main Sail supervisor immediately. If I support multiple engagements concurrently using my Main Sail approved laptop, I will segregate the information so as not to co-mingle one client's data with another's.

8279 Mayfield Rd,
Unit 12
Chesterland, OH 44026

5. **I will access, use, disclose and retain Client Data only as necessary to provide services for the data owner.** I will not access Client Data that I do not need to perform my duties. I will use good judgment when collecting, using or disclosing Client Data in order to keep it secure and confidential. I will observe the "rule of least privilege" by not disclosing Client Data under my control except to an individual who has a legitimate need for it, is assigned to my project, and has been approved for such access. I will never use or disclose Client Data for personal purposes, or transfer such information to systems controlled by individuals or entities unless expressly permitted by Main Sail.
6. **I will inform my Main Sail supervisor, if I have access to Client Data I do not need to do my job.** I will contact my supervisor or an available member of the Main Sail, project leadership team if the client requests me to handle sensitive Client Data outside of my defined responsibilities.
7. **I will take all reasonable steps to protect Client Data in my custody.** I will follow all client and Main Sail, requirements related to information security and will implement those requirements with respect to Client Data under my control (e.g. use and protection of passwords, use of encryption for mobile storage devices, etc.). I will escalate threats to Client Data, or concerns about the adequacy of controls, to my supervisor.
8. **I will securely transmit and store Client Data.** I will use a secure transmission method when sending confidential client information to the client. This may include linking to client-managed SharePoint sites, using only client-provided email, or encryption. I will not use a personal email account or third-party email service to transmit Client Data unless explicitly approved by the client. All portable or removable storage devices needed for Client Data must be encrypted and be either client- or Main Sail owned. Personally-owned devices will not be used to store Client Data.
9. **I will delete or destroy all Client Data appropriately.** I will not retain unnecessary copies of Client Data for any longer than needed to perform services for the client who owns the data, and will delete it when it is no longer needed. I will securely delete and overwrite Client Data from electronic media. I will submit official hardcopies to the appropriate Main Sail or Client supervisor, as required and will shred or otherwise permanently destroy hard copies that are not official records.
10. **I will request permission from my project's lead before removing Client Data from the project environment.** All requests to copy or share project files outside the project environment, must be submitted in writing to the project's lead. The lead will work with the appropriate parties to consider Client and Main Sail ownership rights and confidentiality before permitting any project files to be transmitted, shared or copied outside the project or client environment.
11. **I will follow established incident reporting procedures to identify and escalate security breaches involving Client Data.** I will report known or suspected data breaches immediately to the Main Sail Facilities Security Officer (FSO) 216-283-6981, the Assistant Facilities Security Officer (AFSO), and also as directed within the project. I will follow up a called in report with a detailed email, to include dates, times and names of all individuals involved with a full description of the incident. A security breach includes any loss of control of Client Data, whether intentional or accidental, and can include lost or stolen portable data storage devices, misdirected data, computer hacking, or intentional misuse of Client Data.
12. **I will consider the privacy of individuals when designing systems that utilize Personal Information.** I will seek to create privacy-protective systems and services consistent with client objectives. I will consider the privacy impact of my work and will take a conservative approach to the collection, use, and disclosure of Personal Information when developing solutions.
13. **I will review Client Data Protection materials provided to me by my project and will complete all required related training.** Prior to accessing any Client Data, I will complete the appropriate level of required Main Sail and Client training, for my role.
14. **I understand my responsibilities regarding the retention of project-related records.** I understand that Main Sail must be able to produce certain types of records in their original form in order to respond to audit and legal inquiries, and that failure to do so can subject Main Sail to serious penalties. I understand that if I have actual knowledge of a dispute, threatened lawsuit, potential or actual government investigation, or

8279 Mayfield Rd,
Unit 12
Chesterland, OH 44026

audit relating to the project, I must notify the Main Sail and the project lead before disposing of any documents.

15. **I am responsible for complying with these rules of behavior and Main Sail policies, procedures and practices, as applicable.** I understand that complying with Main Sail policy also means complying with laws and client instructions. I understand that preserving the confidentiality and privacy of Client Data is a critical part of my job duties. I will conform to applicable Main Sail and Client policies, procedures and practices with respect to the management of Client Data. Main Sail or the Client may monitor my compliance with these rules of behavior. Failure to abide by these rules may result in disciplinary action, up to and including dismissal, as well as referral to law enforcement authorities, if appropriate. My signature affixed below acknowledges that I have read this document, understand its requirements and confirms I will make my best efforts to comply with these rules.

**In Addition to Client Data Protection**

16. In accordance with the Federal Information Security Management Act of 2002 (FISMA) and DFARS clause 252.204-7012, when applicable, employee or contractor agrees to fully comply with the National Institute of Standards and Technology (NIST) SP800-171 which outlines basic IT security requirements concerning the storage, processing, or transmitting of Controlled Unclassified Information (CUI) and the required security protection for such systems. At all times, the contractor will adhere to required IT security guidelines and protocols outlined in the NIST and adhere to all applicable information protection and handling procedures of all U.S. government and client supplied, collected or transmitted data.