DATA SECURITY AGREEMENT

This Data Security Agreement (Agreement) is agreed upon effective 12th Oct 2021 by and between the **Missionaries of the Sacred Heart of Jesus and Mary** (Client) and **Bosco Soft Technologies** (Service Provider).

# Use of, Storage of, or Access to, Client Data

Service Provider shall only use, store, or access Client Data:

* 1. In accordance with, and only to the extent permissible under this Agreement and the Contract; and
  2. In full compliance with any and all applicable laws and regulations, only to the extent applicable to the Service Provider.
  3. Any transmission, transportation, or storage of Client Data outside of the main server in the to the local desktop / laptop computers in the parish office is prohibited except on prior written authorization by the Client.

# Safeguarding Client Data

Service Provider agrees that use, storage, and access to Client Data shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices. Service Provider shall implement and maintain safeguards necessary to ensure the confidentiality, availability, and integrity of Client Data. Service Provider shall also implement and maintain any safeguards required to be implemented by applicable state and federal laws and regulations.

Such safeguards shall include as appropriate, and without limitation, the following:

* 1. System Security. A System that is owned or operated by Service Provider and contains Client Data shall be secured as follows:
     1. Service Provider shall implement controls reasonably necessary to prevent a breach.
     2. The System shall use secure protocols and encryption to safeguard Client Data in transit.
     3. Service Provider shall:
        1. Limit administrative access to the System,
        2. Limit remote access to the System,
        3. Limit account access and privileges to the least necessary for the proper functioning of the System
        4. Use named user accounts and not generic or shared accounts,
        5. Enable an appropriate level of auditing and logging for the operating system and applications.
     4. The System shall allow the changing of System and user passwords.
  2. Product Maintenance and Support
     1. Service Provider shall have a process for the timely review, testing, and installation of patches essential for safeguarding the confidentiality, integrity, or availability of the System or Client Data.
     2. Change management procedures shall be followed.
     3. Service Provider shall ensure that the product is supported, provided that Client maintains the requisite subscriptions. Service Provider shall provide Client with notice 12 months before the product becomes unsupported.
     4. If necessary, and provided that Client maintains the requisite subscriptions, Service Provider shall provide remote support via a secure connection method that includes an audit log of events. Remote access shall be limited to an as needed or as requested basis.
  3. Data Protections
     1. Service Provider shall only use, store, disclose, or access Client Data:
        1. In accordance with, and only to the extent needed to provide services to Client; and
        2. In full compliance with any and all applicable laws, and regulations
     2. Service Provider shall implement controls reasonably necessary to prevent unauthorized use, disclosure, loss, acquisition of, or access to Client Data. This includes, but is not limited to personnel security measures, such as background checks.
     3. All transmissions of Client Data by Contractor shall be performed using a secure transfer method
  4. Service Provider access to Client systems

Client login credentials may be given to Service Provider requiring access to secured computer equipment located on-site at the Client for the purposes of scheduled troubleshooting, maintenance, or updates to software provided or supplied by Service Provider and installed on Client-owned computer equipment. In this case, the Client will provide the Service Provider with credentials for logging in locally or through a secured Virtual Private Network (VPN), if required.

As a condition of the Service Provider’s access to the Client’s computing equipment the Service Provider represents that they will not attempt to access any system(s) other than the one(s) absolutely necessary nor will the Service Provider use any computer equipment for any purpose that is unlawful.

All work performed by the Service Provider while connected to Client computing equipment is subject to monitoring by Client staff and verification by the Client Department or Division requesting the access.

# Oversight

The Client reserves the right to request information and relevant reports related to the Service Provider’s internal data security standards and practices and that of any data center in which Client’s Data is stored.

# Data Breach

If Service Provider becomes aware that Client Data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this Agreement or the Contract, Service Provider shall use reasonable efforts to alert the Client of any Data Breach within one business day, and shall immediately take such actions as may be necessary to preserve forensic evidence and

eliminate the cause of the Data Breach. Service Provider shall give highest priority to immediately correcting any Data Breach and shall devote such resources as may be required to accomplish that goal. Service Provider shall provide the Client information necessary to enable the Client to fully understand the nature and scope of the Data Breach. If required by applicable law, Service Provider shall provide notice and credit monitoring to parties affected by any Data Breach. Upon request, Service Provider shall provide Client information about what Service Provider has done or plans to do to mitigate any deleterious effect of the unauthorized use or disclosure of, or access to, Client Data. In the event that a Data Breach requires Service Provider’s assistance in reinstalling software, such assistance shall be provided at no cost to the Client. The Client may discontinue any services or products provided by Service Provider until the Client, in its sole discretion, determines that the cause of the Data Breach has been sufficiently mitigated.

# No Surreptitious Code

Service Provider warrants that, to the best of its knowledge, the System is free of and does not contain any code or mechanism that collects personal information or asserts control of the System without Client’s consent, or which may restrict Client’s access to or use of Client Data. Service Provider further warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, or other code or mechanism designed to permit unauthorized access to Client Data, or which may restrict Client’s access to or use of Client Data.

# Compelled Disclosure

If Service Provider is served with any subpoena, discovery request, court order, or other legal request or command that calls for disclosure of any Client Data, Service Provider shall promptly notify the Client in writing and provide the Client sufficient time to obtain a court order or take any other action the Client deems necessary to prevent disclosure or otherwise protect Client Data. In such event, Service Provider shall provide Client prompt and full assistance in Client’s efforts to protect Client Data. Where Service Provider is prohibited by law from notifying the Client of a legal request for Client Data, Service Provider will comply with all applicable laws and regulations with respect to the requested Client Data.

# Termination Procedures

Upon expiration or termination of the Contract, Service Provider shall ensure that no Data Breach occurs and shall follow the Client’s instructions as to the preservation, transfer, or destruction of Client Data. The method of destruction shall be accomplished by “purging” or “physical destruction”, in accordance with industry standard norm. Upon request by the Client, Service Provider shall certify in writing to Client that return or destruction of data has been completed. Prior to such return or destruction, Service Provider shall continue to protect Client Data in accordance with this Agreement.

# Survival; Order of Precedence

This Agreement shall survive the expiration or earlier termination of the Contract. However, upon expiration or termination of the Contract, either party may terminate this Agreement. In the event the provisions of this Agreement conflict with any provision of the Contract, or Service Provider’ warranties, support contract, or service level agreement, the provisions of this Agreement shall prevail.

# Definitions

* 1. Client Data: Client Data is any and all data that the Client has disclosed to Service Provider. For the purposes of this Agreement, Client Data does not cease to be Client Data solely because it is transferred or transmitted beyond the Client’s immediate possession, custody, or control.
  2. Data Breach: The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of confidential or sensitive personal information

maintained by the Client as part of a database of personal information regarding multiple individuals and that causes or the Client reasonably believes has caused or will cause loss or injury to any Client constituent.

* 1. System: An assembly of components that supports an operational role or accomplishes a specific objective. This may include a discrete set of information resources (network, server, computer, software, application, operating system, or storage devices) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
  2. Change Management: A formal process used to ensure that changes to a system are introduced in a controlled and coordinated manner. This reduces the possibility that unnecessary changes will be introduced to a system, that faults or vulnerabilities are introduced to the system, or that changes made by other users are undone.
  3. Contract. Shall mean Contractors terms and conditions of sale and service.

|  |  |
| --- | --- |
| CLIENT | SERVICE PROVIDER |
| Signature: | Signature: |
| Printed Name: | Printed Name: |
| Job Title: | Job Title: |
| Date: | Date: |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |