MILTON AMERICAN BASEBALL, INC.
WRITTEN INFORMATION SECURITY POLICY

Milton American Baseball, Inc. ("MAB" or "We") is a not-for-profit charitable organization that provides and promotes youth baseball activities in the Town of Milton, Massachusetts. We have established a Written Information Security Program ("WISP") to outline our administrative, technical and physical safeguards for personal information under 201 CMR 17.00.
MAB has important reasons for handling personal information that include but are not limited to:
1. As required by law, we keep employment records, including payroll records, and tax forms (e.g., W-4,I-9, 1099 Misc.).
2. When an individual pays by check, we may ask to see a driver's license or passport, and record the number on the check. We may scan the check, endorse it, and deposit at our bank.
3. When an individual pays by credit card, we may examine the individual's driver's license or passport. We normally do not record the credit card number (we swipe the card through a reader or enter it directly into our information system), but if the reader is broken or the system not readily available, we might manually record the credit card number to enter into our information system at a later time.
4. As required by law, we gather the information required under the Criminal Offender Record Information ("CORI") law to screen all volunteers, employees, and contractors who may work with children.
5. As required by Babe Ruth League Baseball, we gather Social Security Numbers to permit Babe Ruth League Baseball's contractor, First Advantage, to conduct national background checks.
6. We may also collect birth certificates or passport information to confirm the age and residency requirements of the baseball leagues and tournaments in which our teams participate.
Manners in which we protect this information include but are not limited to:

Designating Our Information Security Manager

Our Information Security Managers ("ISM") are our IT designee on the MAB Board and our Legal Counsel. They keep this WISP updated, train board members, volunteers, and staff, if any, and audit compliance with the WISP.

Making Sure Our Vendors are Compliant

We may routinely share Personal Information (PI) in the form of the information outlined in 1-6 above with state and federal authorities (taxes, CORI/SORI), our payment processing service, our Audit firm, and our legal counsel and or CORI "need to know" personnel. Our computer networking company and in-house IT coordinators sometimes may see PI in the course of repair work and consulting. Each January beginning after the adoption of this WISP, we require any outside entity who assists us in these areas to

send us a letter, signed by their CEO or other authorized person, that they follow a WISP that fully complies with 201 CMR 17.00. The only exception is the state and federal authorities, which we assume are compliant, since they must comply with laws that are stricter than 201 CMR 17.00.

Ensuring That WE Follow our PI Policy

Our Information Security Managers (ISM) ensure that each new member of our organization are trained in his or her role in carrying out the WISP through, among other things, review of the WISP This training is refreshed annually. New members agree to follow our WISP, and understand that their continued association with our organization depends on their following the WISP. Individuals who fail to follow the WISP are disciplined appropriately.

A note about the paragraphs that follow: we talk about keeping paper records under lock and key, and computer records restricted to certain users. We use good common-sense practices about this. All restricted documents are kept in a locked space where it is reasonably safe from burglary and intrusion. If we need a document or a computer file, we hold it closely and do not share inappropriately, and put it back when we are done. For example, we do not leave checks lying out on our desk. Similarly, we do not leave file folders containing PI sitting on a table. When we walk away from a computer, we lock it, keep it locked, or logged off.

Protection and Disposal of Paper Records That Contain Personal Information (PI)

All paper records that have PI are kept under lock and key in appropriate locations. As a standard, we destroy obsolete records using an office-grade shredder. Records containing PI are only taken from our files when necessary for organizational reasons. If members do this, they must explain why this is necessary. PI may be faxed, mailed or delivered to compliant vendors and government agencies. All fax machines we use are located behind locked doors.

When checks are received from individuals, they are delivered to our treasurer who stores them in a safe location until they are then deposited in our bank.

If a Breach Occurs

If our ISM determines that PI has been accessed without authorization, they will notify the Office of Consumer Affairs & Business Regulation (OCABR) and the Attorney General’s Office, describing the breach in detail, and work with authorities to investigate the breach and to protect the victim’s identity and credit. To the extent possible, our ISM will also warn the victims of the breach so that they can protect their credit and identity.