## New Jersey Pool Manager Policy on the Destruction of Personal Information

According to the law, personal information is defined as a person's first name or first initial and last name in combination with the following identifying information:

- Social security or employer taxpayer identification numbers.
- Drivers license, State identification card, or passport numbers.
- Checking account numbers.
- Savings account numbers.
- Credit card numbers.
- Debit card numbers.
- Personal Identification (PIN) Code.
- Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
- Digital signatures.
- Any other numbers or information that can be used to access a person's financial resources.
- Biometric data.
- Fingerprints.
- Passwords.
- Parent's legal surname prior to marriage.

Therefore, in response to this law, New Jersey Pool Managers Association is adopting the following Destruction of Personal Information Policy (Policy), which is designed to prevent unauthorized access to or use of personal information in connection with its disposal. The responsibility for managing the Policy is delegated to Treasure (the Policy Administrator). The Policy Administrator shall be responsible for auditing the purpose of, content of and compliance with this Policy and for interpreting any portions of the Policy as they may apply to specific situations.

The Policy Administrator shall be responsible for providing employees with written copies of the most current version of the Policy and circulating reminders to employees regarding compliance with the Policy if deemed necessary by the Policy Administrator. Employees shall abide and comply with the terms of the Policy, and all questions regarding the Policy and its application shall be submitted to the Policy Administrator for review and guidance. Employees promptly should report any possible violations or deviations from the Policy to the Policy Administrator.

When paper records containing personal information are disposed of, they must be shredded so that the information cannot practicably be read or reconstructed.

When electronic information containing personal information is disposed of, it must be destroyed or erased so that the information cannot practicably be read or reconstructed, simply deleting the files is not sufficient. We must ensure that all the information on the hard drive, computer disks and any other memory systems cannot be retrieved.

The Policy Administrator shall be responsible for supervising the process of document destruction that occurs under this policy and for monitoring compliance. No employee may

destroy any personal information records (paper or electronic) without prior approval from the Policy Administrator.

The Policy Administrator shall suspend the application of the Policy with respect to the destruction of any records or documents in the following scenarios if litigation or a government investigation is foreseeable or imminent or if the corporation's actions come under any type of outside scrutiny, including scrutiny in the press. Upon the occurrence of one of the above-referenced events, as determined by the corporation’s President with the advice of legal counsel, the Policy Administrator shall promptly notify employees via written communication of the suspension of the Policy until further notice.