ENERSYS

SENSITIVE PERSONAL INFORMATION SECURITY POLICY

FOR NORTH AMERICA

Version: 8.2

Date: September 16, 2016

Approval: /s/ Joseph G. Lewis
Joseph G. Lewis, VP, General Counsel,
Corporate Compliance Officer and Secretary

Sensitive Personal Information Security Policy for North America (the "Policy")

1. OVERVIEW:

EnerSys Delaware Inc. and its affiliates and subsidiaries with operations in North America (the "Company") recognize the importance of safeguarding sensitive personal information of its employees and their families, customers and third-party vendors contained in both paper and electronic records handled by the Company. Safeguarding sensitive personal information is an undertaking that relies on a combination of common sense, good judgment, and sound discretion in addition to the implementation and use of software, hardware and other technologies. It also requires the cooperation of various stakeholders across the Company. The purpose of this Policy is to ensure the security and confidentiality of sensitive personal information in a manner fully consistent with a business of the Company's nature; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to the Company, its employees and their families, and the Company's customers and third-party vendors.

2. DEFINITIONS:

"Sensitive Personal Information" means the first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual, customer or third-party vendor: (a) Social Security or Federal Employer Identification Number; (b) driver's license number or state-issued identification card number; or (c) financial account number, credit or debit card number (with or without any required security code, access code, personal identification number or password) that would permit access to an individual's, customer's or third-party vendor's financial account. Sensitive Personal Information also includes any other health-related or financial information when associated with an identifiable individual, or any information associated with an individual's racial/ethnic status, sexual orientation, or religion.

3. SCOPE/PURPOSE:

The President of the Company has approved and adopted this Policy and it applies to all North America employees, third-party vendors and independent contractors who are granted access to Sensitive Personal Information on a need-to-know basis, as well as Authorized Visitors (defined below) (collectively referred to in this Policy as "Authorized Users"). This Policy is not intended to replace, undermine or conflict with other Company policies, such as the policies Management Information Systems ("MIS"), Human Resources ("HR"), Environmental Health and Safety ("EH&S") and Legal have implemented that may relate to the subject matter herein, nor is it intended to replace or supplement the use of common sense, good judgment and sound discretion. The purpose of this Policy is to establish administrative, technical and physical safeguards to (1) protect the security and confidentiality of Sensitive Personal Information; (2) protect against any anticipated threats or hazards to the security or integrity of such Sensitive Personal Information; (3) protect against unauthorized access of such Sensitive Personal Information in a manner that creates a substantial risk of identity theft or fraud; and (4) to comply with applicable laws.

4. POLICY

General: All Authorized Users are expected to maintain the security and confidentiality of personal and business information that is exchanged during their relationship with the Company, as well as after the relationship. All Authorized Users are subject to the requirements set forth in this Policy, as applicable. The effective date shall be the date set forth on the cover page of this Policy.

The Company's policy is to only collect and maintain records and files containing Sensitive Personal Information of the type reasonably necessary to accomplish the Company's legitimate business purposes, or as otherwise necessary for the Company to comply with local, state, or federal regulations or laws. The Company periodically reviews its records, files, and form documents to ensure that the Company is not gathering and retaining Sensitive Personal Information unless there is a reasonable and necessary business or legal reason to do so.

Storage and Disposal: Hard copies of records and files containing Sensitive Personal Information must be stored in a locked or otherwise secured desk, file cabinet, office, or in some form of controlled manner when unattended. Storage of electronic Sensitive Personal Information should always be kept to a minimum and, when the circumstances deem it appropriate, encrypted. This practice applies to both hard-copies and electronic copies of records and files containing Sensitive Personal Information. At the end of each business day, all hard-copies and electronic copies of records and files must be secured in a manner that is consistent with this Policy, common sense, good judgment and sound discretion.

All files, copies, and forms containing Sensitive Personal Information should be disposed of in a manner that ensures it cannot be reconstructed into a usable or readable format. For example, papers, slides, photographs, and film containing Sensitive Personal Information should be disposed of by cross-shredding. Removable storage media, such as flash drives, discs and tapes that contain Sensitive Personal Information should be overwritten or formatted in such a manner to cause destruction of the Sensitive Personal Information before being reused. In no event shall any files, copies, and forms containing Sensitive Personal Information be disposed of in regular waste containers without taking such necessary precautions.

Access, Sharing, Transmission and Disclosure: All visitors to the Company must be registered and when the circumstances (i.e. location, purpose, etc.) deem it appropriate, must be accompanied by an employee of the Company. The Company determines on an individual case-by-case basis who shall be deemed an authorized user (with an active user account) at the Company and which of these authorized users need such Sensitive Personal Information to perform their job duties (an "Authorized Visitor"), taking into consideration the need the Authorized Visitor has for such information and the associated risks. Visitors who have not been deemed an Authorized Visitor of the Company are prohibited from accessing any Sensitive Personal Information.

Hard copies of records and files containing Sensitive Personal Information must be stored in a locked or otherwise secured desk, file cabinet, office, or in some form of controlled manner. Workstations, computers, devices, documents and files that contain Sensitive Personal Information must not be left unattended for extended periods of time and made accessible to

others, whether at work or remotely. Users should logoff their workstations at the end of the workday. Sensitive Personal Information may not be removed or transported from the Company premises unless there is a legitimate business need to do so. Stolen or lost Company devices, documents, files, or other assets containing Personal Information should be immediately reported to the contact information appearing at the end of this Policy. For electronic Sensitive Personal Information, the Company and the MIS department have in place additional policies and procedures that ensure the security and confidentiality of Sensitive Personal Information, all of which are incorporated herein.

The Company has and will continue to maintain reasonable up-to-date firewall protection and software security patches on all systems maintaining Sensitive Personal Information that are reasonably designed to maintain the integrity of such information.

The Company uses secure user authentication protocols, including (i) control of user IDs and other identifiers; (ii) a reasonable secure method of assigning and selecting passwords; (iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect. The Company requires that computer or network passwords be changed every 90 days. Network passwords must meet the following minimum requirements: (i) must contain at least eight characters; (ii) may not be re-used (password history) for a minimum of ten changes; (iii) must contain one (1) uppercase letter, one (1) lowercase letter and one (1) number; (iv) cannot contain more than three (3) repeating characters in a row (example: aaaa, AAAA or 1111); (v) cannot contain any properties of the users account (examples: first name, last name, email address, location, etc); cannot contain a word on the list of prohibited words. Passwords may not be shared with anyone, even if that person is also an Authorized User. Passwords should not be stored on easily accessible papers or electronic programs.

When the circumstances deem it appropriate, the Company's policy is to encrypt all Sensitive Personal Information stored on laptops or other portable devices of employees who possess Sensitive Personal Information in order to fulfill the Company's legitimate business purposes. The Company utilizes reasonably up-to-date versions of system security agent software which includes malware protection and reasonably up-to-date patches and virus definitions. Any actual or suspected breaches of security shall be immediately reported to the contact information appearing at the end of this Policy.

The Company's policy is to terminate and restrict access to Sensitive Personal Information by formerly Authorized Users who are no longer deemed Authorized Users. This includes voicemail access, e-mail access, network access, internet access, as well as access to papers, documents, and other physical files. Formerly Authorized Users who are no longer deemed Authorized Users shall have their access to workstations and other devices revoked within one (1) day of notification of termination, resignation, or expiration of their relationship to the Company, or sooner if the Company deems appropriate. When applicable, the Company may consider additional controls on preventing such disclosures of Sensitive Personal Information, such as non-disclosure and confidentiality agreements. The Company and its North American operations are committed to receiving and protecting data in accordance with the laws of foreign countries. Where applicable, Authorized Users will be required to process Sensitive Personal

Information in accordance with the Company's Data Transfer Agreement and other requirements.

Independent Contractors/Third-Party Service Providers: The Company conducts reasonable due diligence to assess whether a prospective independent contractor/third-party service provider will have access to Sensitive Personal Information and be deemed an Authorized User. If a prospective independent contractor/third-party service provider will have access to Sensitive Personal Information, the Company will assess whether they are capable of safeguarding the Sensitive Personal Information in a manner consistent with this Policy. Due diligence efforts may include, but are not limited to, discussing with the prospective independent contractor/third-party service provider's personnel, reviewing their privacy and/or information security policies; or requesting they complete a security questionnaire or otherwise answer security related questions. Prospective independent contractors/third-party service providers that will have access to Sensitive Personal Information should represent and warrant to the Company (by contract or otherwise) that it maintains safeguards as stringent as those outlined in this Policy.

5. ADMINISTRATION

The **Office of General Counsel** for the Company is responsible for overseeing the Company's compliance with this Policy. The **Office of General Counsel** is responsible for overseeing the following:

- Development and implementation of this Policy;
- Ongoing training of employees on the importance of the security of Sensitive Personal Information security and ensuring that all employees, third-party vendors and independent contractors, including temporary and contract employees who have access to Sensitive Personal Information are aware of this Policy and/or that they have certified their awareness;
- Regular monitoring and testing of the Policy's safeguards for effectiveness in limiting internal and external risks;
- Evaluating the ability of each of the Company's independent contractors and third party service providers to implement and maintain reasonable and appropriate security measures;
- Reviewing the scope of the security measures in this Policy and its relation to the policies of MIS, HR, Legal and other Company policies on a reasonable basis, or whenever there is a material change in the Company's business practices;
- Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Sensitive Personal Information;
- Ensure that all former employees, third-party vendors and independent contractors – including temporary and contract employees – who have had access to Sensitive Personal Information, no longer have access to Sensitive Personal Information and have returned or destroyed any Sensitive Personal Information previously in their possession.

Any instances of non-compliance or suspected non-compliance with this Policy must be reported immediately to the **Office of the General Counsel** of the Company **at (610) 208-1970 or at Joseph.Lewis@enersys.com**. **Any violations of this Policy by a Company employee may result in disciplinary action by the Company, up to and including termination of employment, and in the case of third party vendors, independent contractors, and Authorized Visitors, the immediate termination of the business relationship and if the circumstances are appropriate, legal action according to applicable laws (including criminal prosecution) and contractual agreements**. It is against the Company's policy to retaliate against anyone who reports a violation of this Policy or who cooperates with an investigation regarding non-compliance with this Policy. Any such retaliation will not be tolerated and will result in disciplinary action by the Company, up to and including termination of employment with the Company or the immediate termination of the business relationship.

Any questions or concerns regarding this Policy should be directed to the **Office of General Counsel** for the Company **at (610) 208-1970 or at Joseph.Lewis@enersys.com**.