# New England Teamsters and Trucking Industry Pension Fund
# Comprehensive Written Information Security Program

## I. Program Overview

New England Teamsters and Trucking Industry Pension Fund (the "Fund") has developed this comprehensive written information security program (the "Program") in order to create effective administrative, technical, and physical safeguards for the protection of Personal Information (defined below), and to comply with the Fund's obligations under the Massachusetts regulations found at 201 C.M.R 17.00 *et seq.* (the "Regulations"). This Program sets forth the Fund's policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing Personal Information stored for the sole purpose of tracking and administering pension benefits to members covered in the New England Teamsters Pension Plan.

For purposes of this Program, "Personal Information" means any Pension Fund member's first name and last name, or first initial and last name, in combination with anyone or more of the following data elements that relate to such resident: (a) Social Security Number, (b) driver's license number or state-issued identification card number, or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account. "Personal Information" does not, however, include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

This Program has been approved and adopted by the Executive Director, Fund Manager and Board of Trustees of the New England Teamsters Pension Fund. This Program may be amended, suspended, or terminated from time to time by the Fund, with the approval of the Executive Director the Fund Manager or the Board of Trustees.

## II. Purpose and Scope

The purpose of this Program is to establish administrative, technical, and physical safeguards to protect Personal Information that is owned, licensed, stored, or maintained by the Fund, whether such information is contained in paper or electronic records or in any other form. This Program is designed to ensure the security and confidentiality of Personal Information, to protect against anticipated threats or hazards to the security or integrity of Personal Information, and to protect against unauthorized access to or use of Personal Information in a manner that creates a substantial risk of identity theft or fraud.

## III. Administration of Information Security Program

A. Program Administration. The Fund's Information Systems Manager Brian Stafford will be the "Information Security Coordinator" for this Program.

B. Responsibilities of Information Security Coordinator. The Information Security Coordinator will be responsible, with the support of the Fund and the Board of Trustees, to perform each of the following responsibilities, among others:

1. Develop, implement, administer, monitor, review, and update this Program from time to time, consistent with the requirements of the Regulations;

2. Oversee ongoing employee training and any communications involving this Program;

3. Address any information security issues, including employee compliance, that may arise, and provide input to Fund Management regarding the imposition of disciplinary measures for violations of the Program; and

4. Take all reasonable steps to verify that any third-party service provider with access to the Fund's personal information has the capacity to protect such personal information in the manner consistent with this Program and the requirements of the Regulations and that any such third party service provider applies protective security measures at least as stringent as those required by the Regulations.

## IV. Compliance With Program

A. Compliance. All employees (whether full-time, part-time, substitute, seasonal, or temporary) and independent contractors, and consultants are subject to the applicable requirements set forth in this Program.

B. Non-Compliance. Instances of non-compliance with this Program must be reported immediately to the Information Security Coordinator. Violations may result in disciplinary action by the Fund, up to and including termination of employment.

C. Non-Retaliation. It is unlawful and against Fund policy to retaliate against anyone who reports a violation of this Program or who cooperates in an investigation regarding non-compliance with this Program. Any such retaliation will result in disciplinary action by the Fund, up to and including termination of employment.

## V. Record Retention

A. Retention. The Fund only collects and maintains records and files containing Personal Information of the type, and for the length of time, reasonably necessary to accomplish the Fund's legitimate business purposes, or as otherwise necessary for the Fund to comply with other local, state, or federal regulations or requirements. The Fund periodically reviews its records, files, and form documents to ensure that the Fund is not gathering and retaining Personal Information unless there is a compelling need to do so.

B. Return of Records. All employees and consultants of the Fund are required upon termination or resignation from the Fund for any reason, or earlier, if upon the request of the Fund or the Information Security Coordinator, to return or destroy all records and files containing Personal Information of current or former members of the Fund, in any form that may at the time of such termination be in their possession or control, including all such information stored on laptops, portable devices (such as thumb drives, zip drives, CDs, DVDs, cell phones, or blackberries), or other media, or in files, records, notes, or papers.

## VI. Handling of Personal Information

Personal Information must be created, stored, disclosed, transmitted, and disposed of in the following manner

A. Creation. Upon creation of paper and electronic documents and files that contain Personal Information, such documents and files must be treated as "Confidential"

B. Storage. Paper documents containing Personal Information must be stored in a locked or otherwise secured desk, file cabinet, office, or controlled area when unattended.

C. Access, Sharing, and Disclosure. Access to, sharing, and disclosure of records or files containing Personal Information is limited to those persons who are reasonably required to know such information in order to accomplish the Fund's legitimate business purposes or to enable the Fund to comply with other local, state, or federal regulations or requirements.

D. Transmission. Voice communications involving Personal Information must be kept to a minimum and performed in closed or secured locations. Transmission of Personal Information in paper or hard-copy form outside of the Fund, or other removal of Personal Information from the Fund's premises, must be done with reasonable precaution and in accordance with any applicable Fund procedures and/or rules to ensure the security of such information and to prevent unauthorized disclosure. Transmission of electronic Personal Information must be encrypted, and must likewise be done with reasonable precaution to ensure the security of such information and to prevent unauthorized disclosure.

E. Disposal. Personal Information must be disposed of when no longer needed by the Fund where appropriate, paper documents and other hard-copies of records or files containing Personal Information determined by the Fund to be no longer needed should be disposed of by cross-cut shredding, so that Personal Information cannot practicably be read or reconstructed. Electronic Personal Information determined by the Fund to be no longer needed must be destroyed or erased so that Personal Information cannot practicably be read or reconstructed.

## VII. Physical and Environmental Controls

A. Use and Storage of Files. Employees, consultants, and volunteers of the Fund must not keep open documents or files containing Personal Information on their desks when they are not at their desks or in any other unsecured, unattended place. This policy applies to both hard-copies and electronic copies of records and files containing Personal Information. At the end of the work day, all files and other records containing Personal Information must be secured in a manner that is consistent with this Program and the requirements of the Regulations.

B. Blocked Physical Access. The Fund prohibits and blocks physical access to records and files containing Personal Information by any individual without authorization to access such records as follows:

1. Physical access to the Fund office located at 1 Wall Street Burlington MA is controlled by an America Alarm Security System which allows the Information Security Coordinator to control and monitor all access to the Fund Office. The software allows adding changing and deleting user access to specific areas by day or time depending on the level of security needed.

2. Access to electronic data via desktop computers:

    a. PC Passwords. Controlled by the employee only all windows based PC's are scheduled to timeout in 30 minute intervals of inactivity with a password necessary to re-sign on. All employees are required to sign off nightly and shut down on Fridays. Employees are to protect pc passwords, do not write them down and do not share them with others.

    b. Main Server Passwords. Controlled by the employee, expire every 90 days, max password is 10, minimum password is 6 positions, numeric is required on the password, cannot be the same as the previous four passwords, after 3 unsuccessful attempts the user profile will be disabled and can only be reset by the Information Security Coordinator. Employees are to protect their main server passwords, do not write them down and do not share them with others.

    c. Access Control to Menu Options. Menu options are controlled by a menu security program which allows or disallows users to view Personal Information. The options are given according to employee need as determined by the employee's supervisor. The Information Security Coordinator is responsible to oversee and monitor this process.

Employees, of the Fund are required, upon termination, resignation or any reason, upon the request of the Fund or the Information Security Coordinator, to surrender all keys, IDs, access codes, badges, business cards, and the like, that permit access to the Fund's premises or to records of the Fund containing Personal Information. The Information Security Coordinator upon termination or resignation of an employee will facilitate the removal of "All Access" to the Facility and Data.

C. Visitors. All visitors to the Fund must be received at the Front Desk and be given authorization to enter through the locked door and must be accompanied by an approved employee or other service provider of the Fund. Visitors of the Fund are prohibited and blocked from accessing any records or files of the Fund containing Personal Information.

## VIII. IT Policies and Procedures

A. Electronic Access.

1. The Fund has in place secure user authentication protocols, including (i) control of user IDs and other identifiers, (ii) a reasonably secure method of assigning and selecting passwords; and (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.

2. The Fund assigns unique identifications plus passwords that are designed to maintain the integrity of the security of the access controls, and prohibits the use of vendor supplied default passwords, to each authorized active user.

3. The Fund restricts access to authorized users and active user accounts only. Such restrictions allow access to records and files containing Personal Information only to users with a need to access such Personal Information in order to perform their job duties. The Information Security Coordinator determines in tandem with the employee's supervisor who shall, in order for them to perform specific job duties, be an authorized user at the Fund.

4. The Fund requires that current computer or network passwords are changed above periodically. The Fund blocks access to users after multiple unsuccessful attempts to gain electronic access to records or files containing Personal Information.

5. The Fund blocks electronic access to Personal Information by former employees, other former service providers of the Fund, and other individuals who are no longer authorized users with an active user account.

6. The Fund promptly terminates and prohibits electronic access by former employees, other former service providers of the Fund, and other individuals who are no longer authorized users with an active user account to records and files containing Personal Information. Voicemail access, email access, Fund internet access, and passwords are also promptly disabled or blocked.

B. Network Security.

1. The Fund monitors all computer systems for unauthorized use of or access to records and files containing Personal Information. Logs are monitored and where applicable modifications to strengthen security are continually implemented.

2. The Fund has and will continue to maintain reasonably up-to-date firewall protection and operating system security patches on all systems maintaining Personal Information, that are reasonably designed to maintain the integrity of such information. The Fund uses a ZyXel USG 310 Internet Security Appliance to protect intrusion. The Fund's main server is an IBM 8202-E4D Power 7 Server, running the most current operating system with continual updates. The Fund is committed to using the absolute best equipment and software to protect Personal Information. IBM servers offer a highly scalable and virus resistant architecture with a proven reputation for exceptional business resiliency, this is a main reason the Fund continues to use this product as the backbone of the operation.

3. The Fund has and will maintain reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing Personal Information. The fund uses a Microsoft Exchange Server using McAfee software for antivirus protection of email. The Fund also uses an additional layer at the client layer for antivirus protection using Kaspersky software on all personal computers.

C. Encryption.

1. To the extent technically feasible, the Fund encrypts all records and files of the Fund containing Personal Information transmitted across public networks. The Fund's will continue to keep the 128 bit encryption of data submitted via the Data Transfer Support website for Contributing Employers submitting reports containing Personal Information for the sole purpose of administering the members pension benefits. The Fund will continue to keep up to date the process of verifying that the Web Site can receive 128-bit encrypted information to ensure personal data is protected. The current Secure Site Certificate issued by Network Solutions is Valid through June 20 2016 and will be validated again well in advance of that date.

2. The Fund will encrypt all Personal Information stored on laptops or other portable devices. The Fund will require that limited amounts of Personal Data will be stored on laptops. The Fund will utilize a third party software package to access Personal information via the web when necessary. The Fund will use the product "GoToMyPC" which has 128-bit Advanced Encryption Standard (AES) encryption built in. All data including screen images, file transfers, keyboard and mouse input and chat text is fully encrypted from end to end. The encryption key is unique for each connection and is based on the PC's access code and a random bit sequence.

## IX. Security Awareness

A. Training. The Fund provides education and training regarding this Program to all employees who will have access to Personal Information through their employment to the Fund.

B. Consultants and Third-Party Service Providers. The Fund communicates its relevant policies and procedures under this Program to its consultants and third party service providers who will have access to Personal Information through their services to the Fund.

## X. Third-Party Service Providers

A. Evaluation Process. Before engaging a third-party service provider who will have access to Personal Information, the Fund conducts reasonable due diligence to assess whether a prospective third-party service provider is capable of safeguarding Personal Information in the manner required by this Program. Due diligence efforts may include, but are not necessarily limited to, discussions with the prospective third-party service provider's personnel, reviewing the prospective third-party service provider's privacy and/or information security policies, and/or requesting the prospective third-party service provider to complete a security questionnaire or otherwise answer security-related questions. The Fund may also enter into a contractual agreement with its third-party service providers to protect Personal Information disclosed to such service providers by the Fund.

B. Monitoring. The Fund periodically reviews and monitors the performance of its third-party service providers who have access to the Fund's systems and/or Personal Information in order to ensure that each such third-party service provider is applying protective security measures at least as stringent as those required by this Program to be applied to such information.

## XI. Risk Assessment and Incident Management

A. Identifying Records and Files Containing Personal Information. The Fund will regularly evaluate its paper, electronic, and other records, electronic systems, and storage media (including laptops and portable devices used to store Personal Information) to determine which records, files, and systems contain Personal Information.

B. Ongoing Risk Assessment. The Fund will, on a periodic basis, (i) conduct a review to identify reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of any electronic, paper, or other records containing Personal Information; (ii) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Information; (iii) evaluate the sufficiency of this Program to control those risks; and (iv) revise this Program to minimize those risks, consistent with the requirements of the Regulations. This risk assessment will include, but may not be limited to, an assessment of internal and external risks associated with ongoing employee training, employee compliance with this Program, and means for detecting and preventing security system failures.

C Review of Program. The Fund conducts a formal review of this Program at least annually and whenever there is a material change in the Fund's business practices that may reasonably implicate the security or integrity of records or files containing Personal Information.

D. Reporting Obligation. Employees, consultants, and volunteers are required to report any security violations, breaches of security, or suspicious or unauthorized use of Personal Information contained in records or files of the Fund to the Information Security Coordinator.

E. Incident Review. The Fund documents any responsive actions taken in connection with each security incident. The Fund conducts a prompt review of any security incident, including incidents that require notification under the Regulations, and determines whether any changes in this Program are required to improve the security of records and files containing Personal Information.

Attached is a copy of the Massachusetts Regulations Contained at 201 CMR 17.00, et seq.
Available at: http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf