Written Information Security Program

I. Objective

In order to protect personal information of residents of the State of Rhode Island (R.I.G.L. § 11-49.3-1), and if applicable, residents of the Commonwealth of Massachusetts (201 CMR § 17.00), and in compliance with any other applicable law or regulation (the "Regulations"), Chariho Regional School District ("Chariho") has developed the following Written Information Security Program (the "Program") to address the requirements of the Regulations.

The Program's goal is to set forth effective administrative, technical and physical safeguards applicable to personal information, to provide an outline for the ongoing compliance with the Regulations, to protect personal information from unauthorized access, use, modification, destruction or disclosure, and to position Chariho to comply with future privacy and security regulations as they may develop.

Personal information for purposes of this Program shall mean: the first name and last name or first initial and last name of an individual in combination with any one or more of the following data elements that relate to such individual:

(a) Social Security number;

(b) driver's license number, state-issued identification card number, passport number, tax payer identification number, alien registration number, or tribal identification number; or

(c) financial account number, credit card number, 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 financial account, or deposit or savings account number, or medical information or health insurance information;

(d) medical information or health insurance information;

(e) unique biometric information (e.g. fingerprint, retinal scan); and/or

(f) a username or email address in combination with security code, access code or password or security question and answer that would permit access to an online account; provided however, that "personal information" shall not 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.

The safeguards set forth in this Program are meant to protect the security and confidentiality of personal information, and to protect against any anticipated threats or hazards to the security or integrity of personal information.

II. Information Security

In order to comply with applicable Regulations, we have appointed the Director of Information Technology and Information Systems and Human Resource Administrator who will be responsible for the following:

- Implementing the initial Program.
- Training employees who have exposure to personal information through their work at Chariho on the various aspects of the Program at least annually.
- Obtaining certification of attendance to and understanding of such training by the employees.
- Conducting regular testing and evaluation of the Program's safeguards.
- Verifying the ability of third-party recipients of personal information to comply with the Regulations.
- Reviewing the Program, its scope and its effectiveness at least annually or at such time as a material change in business practice occurs that implicates the security of personal information and upgrading information safeguards as necessary to limit risk.

III. Risk Assessment

The Director of Administration and Finance will conduct a risk assessment or will supervise an outside entity to perform the risk assessment. The initial risk assessment will seek to reveal the following potential and actual risks to the security and privacy of personal information:

- Unauthorized access of personal information by an employee not entitled to the information.
- Compromised system security as a result of unauthorized access by a third party.
- Interception of personal information during transmission.
- Unauthorized access to paper files containing personal information.
- Unauthorized access to personal information through mobile personal devices, removable media or other means.

The Director of Information Technology and Information Systems and Human Resource Administrator will discuss findings and recommendations resulting from the periodic reviews with relevant Chariho personnel.

The Director of Information Technology and Information Systems and Human Resource Administrator will evaluate Chariho's security practices to determine where improvement is necessary to limit risks, including, but not limited to, ongoing employee training, employee compliance with security policies and procedures, means for detecting and preventing security system failures, and the upgrade of safeguards, if necessary, to limit risks.

IV. Safeguards

In an effort to address the internal and external risks to personal information, Chariho has implemented the following policies and procedures:

A. General Safeguards

Chariho will limit the amount of personal information collected to that necessary to achieve legitimate business goals and to comply with state and federal laws and regulations. Chariho will limit access to personal information to those people with a need to know to accomplish legitimate business goals and to comply with state and federal laws and regulations. Chariho will monitor its security systems for breaches of security.

Upon the occurrence of an incident requiring notification under state law, the Director of Administration and Finance will assemble an Incident Response Team and applicable incident response procedures will be followed. Post-incident review by Chariho following any actual or suspected breach of security and documentation of the actions Chariho takes in response to such breach, including any changes Chariho makes to its business practices relating to the safeguarding of personal information, will be conducted and documented.

Chariho will restrict visitor access where personal information is stored. Visitors will be prohibited from visiting unescorted any area within Chariho's premises that contains personal information.

B. Employee Safeguards

Chariho will post a copy of the Program on the district website. Each employee will participate in employee training about the Program and upon successful completion of the training, certify to attending training and understanding the terms of the Program and the importance of protecting personal information.

Employee training will, among other things, address issues relating to:

- Proper access, use, and disclosure of personal information.
- Proper disposal of personal information.
- Proper safeguards for maintaining, transmitting and storing personal information.
- Logging-off computers.
- Locking files and doors.
- Limiting access to offices.
- Properly handling and protecting mobile devices and removable media.
- Password management.

Employee training will also include training to report any suspicious or confirmed unauthorized access, use or disclosure of personal information, to comply with the Program at all times, and understand that they are subject to disciplinary action for violation of the Program. Employees will be prohibited from storing, accessing or transporting personal information outside the premises of the business, unless in accordance with Chariho policies.

Access to personal information by terminated employees will be revoked as soon as possible following termination and terminated employees will be required to return all personal information in their possession; moreover, all passwords to computer systems will be promptly disabled, all access to electronic files, physical files, email, voicemail and internet access will be promptly blocked, all keys will be surrendered and all forms of identification that permit access to Chariho's premises or information will be returned. Terminated employees will, as a condition of severance, be required to execute an agreement whereby they agree to honor all obligations with respect to maintaining the confidentiality of personal information handled during the course of their employment, to the extent not already contractually bound to do so.

C. Non-Electronic File Safeguards

All tangible files containing personal information will be in a locked room or cabinet or stored securely offsite. The Chariho Regional School District Administrative Team will control the distribution of the keys and will keep track of the number of keys issued. Chariho will limit access to offsite storage facilities containing personal information to those employees with a need to access the files, and Chariho will periodically request an access log to monitor who is accessing such files. When sending personal information via carrier, Chariho will use overnight carriers with tracking and, if sending electronic information, encrypt the information to the extent technically feasible.

D. Electronic File Safeguards

Access to all electronic files maintained on Chariho's servers or Chariho's hardware that contain personal information will be limited to those employees with a need to know.

Moreover, Chariho understands that the following protocols further protect personal information in electronic form. Chariho will, to the extent technically feasible:

- Secure the services of a contract consultant or with internal resources, annually run intrusion testing.
- Install firewall protection and operating system patches on all computers with personal information.
- Install up-to-date versions of security agency software.
- Encrypt personal information that is transmitted across public networks.
- Encrypt all personal information stored on a laptop or other mobile or removable device.
- Limit access to the computer system using complex logins and alphanumeric passwords that require changing periodically and require passwords and limited access to e-files containing personal information.
- Require re-logging after passage of inactive time.
- Prohibit posting or sharing of passwords by employees.
- Lock users out after (3) failed log-in attempts.
- Check websites and software vendor websites for alerts about new problems and implement such vendor approved patches as soon as practical.
- Maintain control of user IDs and other identifiers.
- Maintain passwords in a location and/or format that does not compromise the security of the data the password protects.

- Prohibit the continued use of default passwords by employees (i.e. force employee to change passwords).
- Maintain a reasonably secure method of assigning and selecting passwords or the user of unique identifier technologies such as biometric s or security tokens.
- Terminate any access to personal information by terminated employees.
- Use secure computer and Internet user authentication protocols (i.e. control of user identifications and other identifiers).

E. Third-Party Vendors

When using third-party vendors for services that necessitate the sharing of personal information, Chariho will:

- Obtain, when possible and practical, a copy of the third-party vendor's written information security program designed to comply with the Regulations.

- Require a written contract that the Third-Party Vendor implement and maintain privacy and security measures appropriate to the size and scope of the organization; describes the nature of the information; the purpose for which the information was collected; and a Written Information Security Program by the third-party vendor that complies with R.I.G.L. § 11-49.3-1 et. seq.

F. Disposal

When disposing of files containing personal information, Chariho will follow its policy and records retention schedule, (if applicable) which will include:

1. Shredding all hardcopies of files containing personal information when such information is no longer required or needed to be maintained by Chariho,

2. Destroying all electronic files containing personal information when such information is no longer required or needed to be maintained by Chariho, including the destruction of residual electronic data on computers and other electronic devices.

V. NOTIFICATION OF BREACH

Upon confirmation of any disclosure of personal information or any breach of the security of the safeguards or information system that poses a significant risk of identity theft or disclosure of personal information to an unauthorized person notice shall be given as follows:

A. Notification Procedure

Notification shall be made in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained below. In the event that more than 500 Rhode Island residents are to be notified, the school shall notify the Attorney General and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals.

A notification may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation.

B. Notification Requirements

The Notification shall contain:

a. A general and brief description of the incident, including how the security breach occurred and the number of affected individuals;

b. The type of information that was subject to the breach;

c. Date of breach, estimated date of breach, or the date range within which the breach occurred;

d. Date that the breach was discovered;

e. A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact: (i) The credit reporting agencies; (ii) Remediation service providers; (iii) The Attorney General; and

f. A clear and concise description of the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

Adopted and effective 2-9-21