FILE: EHAA

Computer Security

Written Information Security Policy (WISP)

Introduction

The objective of Bristol Warren Regional School District (BWRSD) in the development and implementation of this comprehensive Written Information Security Program (WISP) is to create effective administrative, technical and physical safeguards for the protection of Personally Identifiable Information (PII). The WISP sets forth BWRSD's procedure for evaluating its electronic methods of accessing, collecting, storing, using, transmitting and protecting PII.

The purpose of the WISP is to comply with regulations issued by the State of Rhode Island entitled, "Identity Theft Protection Act of 2015" [R.I. Gen. Laws 11-49.3.2]. This policy applies to all BWRSD faculty, staff, hired consultants, interns and students.

In accordance with state laws and regulations, BWRSD is required to take measures to safeguard PII and to provide notice about security breaches of protected information at BWRSD to affected individuals and to appropriate state agencies.

BWRSD is committed to protecting the confidentiality of all sensitive data, as defined below, that it maintains, including information about students, families and employees.

Definitions

- **Data:** For the purposes of this document, data (classifications defined below) refers to PII collected, stored, archived or maintained electronically under the management of BWRSD whether stored on premises or within a third-party service.
- **Encryption** is the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.
- **Personally Identifiable Information (PII)**: Under the Identity Theft Protection Act of 2015 [R.I. Gen. Laws 11-49.3.2], PII means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format:

    1. Social security number;
    2. Driver's license number, Rhode Island identification card number, or tribal identification number;
    3. Account number, credit or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account(s);

4. Medical or health insurance information;
5. E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account(s); or
6. Passport number, alien registration number or other government-issued identification number.

Responsibilities

Bristol Warren Information Technology Department (BWIT) shall be responsible for all data stored centrally on BWRSD servers and administrative systems, and are responsible for the security of such data. For distributed data stored on departmental systems, the department head or their designee shall be responsible.

The Human Resources Department will alert BWIT at the conclusion of a contract for BWRSD employees and approved consultants to terminate access to BWRSD accounts.

All members of BWRSD are responsible for maintaining the privacy and integrity of all PII as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members are required to access, store and maintain records containing PII in compliance with this policy.

Data Security Coordinator

BWRSD has designated the Information Technology Director to implement, supervise and maintain the WISP. That designated employee will be responsible for:

- Initial implementation of the WISP;
- Training employees using an industry standard Security Awareness Training Program;
- Regular testing of the WISP's safeguards;
- Evaluating the ability of each of BWRSD's third-party service providers to implement and maintain appropriate security measures for PII to which BWRSD has permitted them access, consistent with the regulations; and requiring such third-party service providers by contract to implement and maintain appropriate security measures;
- Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in BWRSD's business practices that may implicate the security or integrity of records containing PII; and
- Conducting training sessions for all owners, managers, employees and independent contractors, including temporary and contract employees, who have access to PII, on the elements of the WISP.

Risks

BWRSD implements improvements and compliance to align with nationally recognized standards to minimize risks (Internal and External).

NIST Cybersecurity Framework

CIS Critical Security Controls (CIS Controls)

Risk Assessment-BWRSD consistently evaluates security practices to determine areas of improvement to limit risks, including, but not limited to:

- Ongoing employee training
- Employee compliance with security policies and procedures,
- Employ technological safeguards to protect and prevent PII disclosure.

This Risk Assessment is used to recommend and make modifications to limit risks.

Internal Risks

To combat internal risks to the security, confidentiality, and/or integrity of any electronic records containing PII, and evaluating and improving the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

- BWRSD shall only collect PII of students, their parents/guardians, vendors, staff or employees that is necessary to accomplish legitimate operational needs.
- Access to records containing PII is limited to employees whose duties, relevant to their job descriptions, constitute a legitimate need.
- Any PII stored shall be disposed of when no longer needed for business purposes or required by law for storage. Electronic records (including records stored on hard drives or other electronic media) containing PII shall be disposed of only in a manner that complies with the regulations and as follows:
    - Electronic media and other non-paper media containing PII shall be destroyed or erased upon disposal so that PII cannot be practically read or reconstructed.
- A copy of this WISP will be posted and each current and new BWRSD employee with access to PII will be required to comply.
- All employees with access to PII shall participate in BWRSD's training program on the detailed provisions of the WISP. Immediate retraining of BWRSD's employees shall occur to the extent the Data Security Coordinator determines a need.
- All security measures shall be reviewed at least annually, or whenever there is a material change in BWRSD 's business practices that may reasonably implicate the security or integrity of records containing PII. The Data Security Coordinator shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.

- BWRSD 's employees are required to immediately report suspicious or unauthorized use of PII to the Data Security Coordinator.
- Whenever there is an incident that requires notification under any state or federal breach notification statute or regulation, there shall be an immediate mandatory post-incident review of events to determine whether changes in BWRSD 's security practices are required.

External Risks

To combat external risks to the security, confidentiality, and/or integrity of any electronic records containing PII, and evaluating and improving the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

- To the extent technically feasible, firewall protection, operating system security patches and all software products shall be reasonably up-to-date and installed on all BWRSD computers.
- To the extent technically feasible, all system security software including, but not limited to, anti-virus, anti-malware, internet security, device management and backup shall be reasonably up-to-date and installed on all BWRSD computers.
- To the extent technically feasible, all PII shall be encrypted. There shall be secure user authentication protocols in place.
- PII shall not be removed from the premises in any form absent a legitimate need.
- All BWRSD computers, systems and infrastructure shall be monitored for unauthorized use or access to PII.
- BWRSD staff may have administrative access to the operating system, databases, applications or infrastructure being supported as part of their job responsibilities. This access may only be used in support of BWRSD and consistent with the roles and responsibilities of the staff member as prescribed by BWRSD management. BWRSD periodically reviews administrator access to the systems it is responsible for managing.

Contact in Case of Loss/Theft or Suspected Loss/Theft

If you have reason to believe that any PII has been lost or stolen or compromised, report the incident immediately by contacting the Information Technology Department at 401-253-4000 x 5200.

Policy Owner

Information Technology Department

References: [R.I. Gen. Laws 11-49.3.2]

Policy Adopted: June 24, 2024

Bristol Warren Regional School District, Bristol, Rhode Island