**RHODE ISLAND DEPARTMENT OF LABOR AND TRAINING**
**REGULATIONS FOR IDENTITY THEFT PROTECTION**

**TABLE OF CONTENTS**



## I. PURPOSE

The Rhode Island Identity Theft Protection Act, R.I Gen. Laws §11-49.2, provides for the establishment of measures to protect the privacy of personal information of all Rhode Island residents. The purpose of the Act is to require businesses that own or license personal information about Rhode Island residents to provide reasonable security for that information. The Department of Labor and Training has access to said personal information and these regulations have been developed to protect same.

Personal information shall include an individual's first name or first initial and last name or number that may be used alone or in conjunction with any other identifying information when either the name or the data elements are not encrypted:

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

## II. REQUESTS FOR PERSONAL INFORMATION

All requests for personal information, as defined by RIGL 11-49.2-5 (c) (1-3), including by Subpoena Duces Tecum, under the Freedom of Information Act, under the Access to Public Records Act (R.I. Gen. Laws §38-2 et. seq.), by any other statutory authority or by any person or entity must be forwarded to the Office of Legal Counsel for review. Along with the request, information regarding the content and availability of the personal information should be detailed. The Office of Legal Counsel will determine the manner in which the request should be answered along with any actions to ensure confidentiality and compliance with this Act.

## III. CONFIDENTIALITY OF PERSONAL INFORMATION

All personal information maintained by this Department shall remain confidential. To that extent, all Department personnel having access to said information, whether it is written or electronic data, must assure its safety. All transmissions, which contain personal information, shall be secured by the use of appropriate safeguards including passwords for electronic transmittals. All documentation containing personal information shall be maintained in a secure place out of view of non-essential personnel or the public. When documents containing personal information are no longer to be maintained, they shall be stored and or destroyed pursuant the records retention law, R.I. Gen. Laws 38-1 et.seq.

If the Department in its normal course of business is required to provide personal information to other agencies or businesses as mandated by law, contract, or agreement the recipient agency or business must provide written assurance to the Department that it will maintain the confidentiality of said personal information so provided.

## III. NOTIFICATION OF BREACH

If at any time, the Department believes a breach of the confidentiality of personal information has occurred, the Director and the Office of Legal Counsel shall be notified immediately. A breach also includes the unauthorized disclosure of personal information not owned by the Department but its disclosure poses a significant risk of identity theft. The Office of Legal Counsel will initiate an investigation in order to determine the magnitude of the breach in the security of the data, contact the appropriate law enforcement agency to determine whether notification is necessary, determine the method of notification, and, monitor the notification process.

If the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired, notification of a breach to the affected individual(s) is not required. This shall be determined by the Office of Legal Counsel.

If the breach will likely result in a significant risk of identity theft to the individuals whose personal information has been acquired, the Office of Legal Counsel will implement the notification process. The notification process shall be implemented in the most expedient time possible without unreasonable delay.

If the cost of providing notice exceeds twenty-five thousand ($25,000) dollars or the affected class of subject persons required notification exceed fifty thousand (50,000) or there is insufficient contact information, substitute notice may be made by E-mail, posting on the agency's website and by statewide media. The Department shall make all reasonable efforts to restore the integrity to the data system.

## V. VIOLATIONS

Failure of department employees to maintain confidentiality of personal information and maintain identity theft protection may result in a civil violation for which a penalty of not more than a hundred dollars ($100.00) per occurrence and not more than twenty-five thousand dollars ($25,000.00) may be adjudged. In addition, disciplinary action up to and including termination may result.

## VI. EFFECTIVE

These regulations shall become effective twenty days after filing with the Secretary of State.