* 1. **NRS 603A**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NRS 603A Requirement** | **Reporting Instruction** | **Assessor’s Response** | | **Control Effectiveness** |
| **NRS 603A.200 Destruction of certain records.** | | | | |
| **D1** | | | | |
| Take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records. | **Identify the data-retention and disposal documentation** examined to verify policies, procedures, and processes define the following for all confidential data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements for data retention. * Specific requirements for retention of confidential data. * Processes for secure deletion of confidential data when no longer needed for legal, regulatory, or business reasons. * A quarterly process for identifying and securely deleting stored confidential data that exceeds defined retention requirements. |  |  | |
| **NRS 603A.210 Security measures.** | | | | |
| **S1** | | | | |
| Implement and maintain reasonable security measures to protect personal information from unauthorized access, acquisition, destruction, use, modification or disclosure. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  | |
| **S2** | | | | |
| A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s confidential data or sensitive authentication data, or manages the customer's confidential data environment on behalf of a customer. |  |  | |
| **S3** | | | | |
| If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident of this State which are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section. | **Identify** how the data collection company is in compliance with state or federal law. |  |  | |
| **NRS 603A.215 Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability.** | | | | |
| **C1** | | | | |
| If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization. | **Identify** the current PCI DSS version the data collection company is compliant with. |  |  | |
| **C2** | | | | |
| A data collector doing business in this State to whom subsection 1 does not apply shall not:  (a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission; or  (b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information. | **Identify** all locations where confidential data is transmitted or received over open, public networks. |  |  | |
| **Identify** **the documented standards** examined. |  |
| **Describe how** the documented standards were examined and compared to system configurations to verify the use of: | |
| * Security protocols observed in use |  |
| * Strong cryptography for all locations |  |
| **NRS 603A.220 Disclosure of breach of security of system data; methods of disclosure.** | | | | |
| **B1** | | | | |
| Disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. * Communication strategies. * Requirement for notification of the payment brands. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage for all critical system components. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  |  | |
| **B2** | | | | |
| Notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. * Communication strategies. * Requirement for notification of the payment brands. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage for all critical system components. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  |  | |