NRS 603A COMPLIANCE CHECKLIST

The Bureau of Consumer Protection has compiled this checklist and guide to help data collectors (NRS 603A.030) in their effort to comply with NRS 603A. **This Checklist is not a substitute for compliance with 603A**. Instead, it is designed as a useful tool to aid in the development of a written information security program for data collectors that handle "personal information." Each item requires proactive attention in order for a plan to be comprehensive. **While following these guidelines should assist a data collector in its efforts to adequately protect the personal information of its employees and customers, it is the responsibility of the data collector to review NRS 603A in its entirety and implement the most appropriate practices and procedures for its business.**

1. Assessment Checklist

The following checklist is designed to help data collectors identify any gaps that may exist in their current information security program. **This checklist is not exhaustive and should not be relied upon as a definitive authority for compliance with NRS 603A. Each data collector should retain the assistance of legal and/or technical consultants, as necessary, to formally assess the adequacy of the data collector's current practices.**

I. Characterization and Usage of the Information

☐ A natural person's first name or first initial and last name in combination with any one or more of the following data elements is considered personal information ("PI"): ☐ Social security number ☐ Driver's license number, driver authorization card number or identification card number ☐ Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account ☐ A medical identification number or a health insurance identification number ☐ A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account
☐ Is PI collected and stored by paper and electronically?
☐ Is PI that is collected and stored necessary and relevant to the corresponding transaction? ☐ If not, can PI be properly disposed of? (NRS 603A.200) ☐ If not, is the maintenance, retention, or disposal of PI governed by a particular statute?
☐ Does data collector require the use of all PI marked above?
☐ Does data collector use PI in any other manner?
☐ Do third party businesses have on-site or remote access to PI stored with or used by data collector? ☐ If so, does data collector know how PI is accessed, retained and used by the third party? ☐ Is data collector notified each time a third party gains remote access to its system?
☐ Does data collector have use and retention policies for PI?
☐ Does data collector comply with the current version of Payment Card Industries ("PCI") Data Security Standard? (NRS 603A.215)
☐ Does data collector store sensitive authentication data after authorization?

II. Retention

☐ Do the employees, with or without knowledge, handle PI?
☐ Does data collector physically store PI in any other manner?
☐ Does data collector store PI in any other format(s)?
☐ Can the data collector identify all connections between the data network in your business?
☐ Does data collector destroy media when it is no longer needed for business or legal reasons?
☐ Does data collector have a procedure for consumers requesting a copy of their PI?
☐ Do employees understand and abide by the processes for retaining and disseminating PI?
☐ Does data collector encrypt any PI stored on its computer network, disks, or portable storage devices? ☐ Is PI sent internally or externally encrypted?

III. Notification and Redress

☐ Does data collector notify consumers concerning updates to policies or procedures in a timely manner?
☐ Does data collector notify consumers concerning changes to usage in PI or dissemination of PI in a timely manner?
☐ Does data collector have a policy or plan ready to implement when a data breach has been detected or identified? (NRS 603A.020)
☐ Does data collector have a policy or process that will notify persons affected by a data breach? (NRS 603A.220)
☐ Does data collector have a risk assessment process in place?
☐ Does data collector regularly implement the established risk assessment process at least once every six months?
☐ Does data collector have a procedure for customers wishing to file a grievance or complaint?
☐ Does data collector offer different avenues for redressability of a grievance or complaint?
☐ Does data collector record and document all investigations and findings?

IV. Controls on Access

☐ Is the internal network secure from unauthorized electronic access?
☐ Is the internal system appropriately restricting inbound and outbound traffic?
☐ Does the data collector collect and store PI that includes payment card data? ☐ If so, is the PI protected by requiring the use of a token, “smart card,” thumb print, or other biometric—as well as a password—to access the central computer?
☐ Does data collector, specialized employee, or third-party IT company regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network?
☐ Does data collector restrict the use of laptops or work-related electronic devices to those employees who need them to perform their jobs? ☐ Does data collector require employees to store work-related laptops and electronic devices in a secure place? ☐ Does data collector restrict laptop use to only network access of PI and not storage? ☐ Are all work-related laptops and electronic devices encrypted?

☐ Is the network protected by requiring the use of a token, "smart card," thumb print, or other biometric—as well as a password—to access the central computer?
☐ Does data collector require an employee's user name and password to be different? ☐ Do employees have unique strong passwords—the longer, the better—that use a combination of letters, symbols, and numbers? ☐ Do employees change their passwords regularly or at least once every three months?
☐ Does data collector, specialized employee, or third party IT company regularly check for patches that address new vulnerabilities? ☐ Does data collector have an implementation policy—addressing time, manner, and training—in place for installing new patches?
☐ Are employees trained to handle PI? ☐ Are employees provided with written policies and procedures on how to safeguard personal information? ☐ Are such policies and procedures updated regularly and at least every six months?
☐ Are key employees certified by PCI to assess risk to PI in the normal course of business?
☐ Do employees have regular access to PI in the normal course of business?
☐ Do employees who are authorized to access PI have a unique ID?
☐ When data collector receives or transmits PI, does data collector protect the information in transit using a secure connection?

2. Implementation and Goals

After identifying any gaps in your current infrastructure, or if you are developing an information security program for the first time, the following guide may be useful. This guide identifies some of the public policies served by implementing a comprehensive information security program and, with those goals in mind, offers some suggestions for its development. **This guide is not exhaustive and should not be relied upon as a definitive authority for compliance with NRS 603A. Each data collector should familiarize itself with all obligations imposed by NRS 603A, and retain the assistance of legal and/or technical consultants, as necessary, to implement the most appropriate practices and procedures for its business.**

Data Collector's Responsibilities:

<u>Accountability at the beginning</u>

- Determine if you collect or use Personal Information, as described in NRS 603A.040.
- Commit to compliance with NRS 603A.200.
- Commit to compliance with NRS 603A.210.
- Commit to compliance with NRS 603A.215, and if applicable, PCI data security standards.
- Appoint an individual (or individuals) to be responsible for your organization's compliance, and determine if an Information Security manager is needed.
- Establish an internal hierarchy that identifies what security issues should be escalated to the data collector's board of directors or chief executive officer(s).
- Protect all personal information held by your organization or transferred to a third party for processing.
- Develop and implement personal information policies, procedures and practices.

- Review all written policies and procedures regularly, at least every 6 months, and update them as necessary to guard against emerging security threats.
- Inform customers, clients and employees that you have policies and practices for the management and security of personal information.
- Make these policies and practices understandable and easily available.

Data Collecting Boundaries and Purposes

- Before or when any personal information is collected, identify why it is needed and how it will be used.
- Document why the information is collected.
- Inform the individual from whom the information is collected why it is needed.
- Identify any new purpose for the information and obtain the individual's consent before using it, or provide the individual with a reasonable opportunity to deny any new uses of such information.

Consent

- Specify what personal information you are collecting and why in a way that your customers and clients can clearly understand.
- Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal information.
- Obtain the individual's consent before or at the time of collection, as well as when a new use of their personal information is identified.

Collection Practices

- Do not collect personal information indiscriminately.
- Do not deceive or mislead individuals about the reasons for collecting personal information.

Restrictions on use, disclosure, and retention

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by law.
- Keep personal information only as long as necessary to satisfy the purposes.
- Put guidelines and procedures in place for retaining and destroying personal information.
- Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.
- Securely destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

Accuracy

- Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

Safeguards

- Protect personal information against loss or theft.
- Safeguard the information from unauthorized access, disclosure, copying, use or modification.
- Protect personal information regardless of the format in which it is held.

Access

- Give individuals access to their information.
- Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in law.
- An organization should note any disagreement on the file and advise third parties where appropriate.

Redressability

- Develop simple and easily accessible complaint procedures.
- Inform complainants of their avenues of recourse.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.