CHAPTER 603A - SECURITY AND PRIVACY OF PERSONAL INFORMATION

SECURITY OF INFORMATION MAINTAINED BY DATA COLLECTORS AND OTHER BUSINESSES

GENERAL PROVISIONS

APPLICABILITY

REGULATION OF BUSINESS PRACTICES

REMEDIES AND PENALTIES

NOTICE REGARDING PRIVACY OF INFORMATION COLLECTED ON INTERNET FROM CONSUMERS

SECURITY OF INFORMATION MAINTAINED BY DATA COLLECTORS AND OTHER BUSINESSES

General Provisions

NRS 603A.010 Definitions. As used in NRS 603A.010 to 603A.290, inclusive, unless the context otherwise requires, the words and terms defined in NRS 603A.020, 603A.030 and 603A.040 have the meanings ascribed to them in those sections.

(Added to NRS by 2005, 2503; A 2017, 4079; 2021, 1353)

NRS 603A.020 "Breach of the security of the system data" defined. "Breach of the security of the system data" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. The term does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.

(Added to NRS by 2005, 2503)

NRS 603A.030 "Data collector" defined. "Data collector" means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.

(Added to NRS by 2005, 2504)

NRS 603A.040 "Personal information" defined.

1. "Personal information" means a natural person'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 data elements are not encrypted:
   (a) Social security number.
   (b) Driver's license number, driver authorization card number or identification card number.
   (c) 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.
   (d) A medical identification number or a health insurance identification number.
   (e) 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.
2. The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records.

(Added to NRS by 2005, 2504; A 2005, 22nd Special Session, 109; 2007, 1314; 2011, 2411; 2015, 241)

Applicability

NRS 603A.100 Applicability; waiver of provisions prohibited.

1. The provisions of NRS 603A.010 to 603A.290, inclusive, do not apply to the maintenance or transmittal of information in accordance with NRS 439.581 to 439.595, inclusive, and the regulations adopted pursuant thereto.
2. A data collector who is also an operator, as defined in NRS 603A.330, shall comply with the provisions of NRS 603A.300 to 603A.360, inclusive.
3. Any waiver of the provisions of NRS 603A.010 to 603A.290, inclusive, is contrary to public policy, void and unenforceable.

(Added to NRS by 2005, 2506; A 2011, 1762; 2017, 4079; 2019, 1172; 2021, 1353, 1673)

Regulation of Business Practices

NRS 603A.200 Destruction of certain records.

1. A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records.
2. As used in this section:

(a) "Business" means a proprietorship, corporation, partnership, association, trust, unincorporated organization or other enterprise doing business in this State.

(b) "Reasonable measures to ensure the destruction" means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation:

(1) Shredding of the record containing the personal information; or

(2) Erasing of the personal information from the records.

(Added to NRS by 2005, 2504)

NRS 603A.210 Security measures.

1. A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

2. If a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable, with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of Standards and Technology of the United States Department of Commerce.

3. 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.

4. 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.

5. The Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration shall create, maintain and make available to the public a list of controls and standards with which the State is required to comply pursuant to any federal law, regulation or framework that also satisfy the controls and standards set forth in subsection 2.

(Added to NRS by 2005, 2504; A 2019, 2574)

NRS 603A.215 Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability.

1. 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.

2. 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, its data storage contractor or, if the data storage device is used by or is a component of a multifunctional device, a person who assumes the obligation of the data collector to protect personal information, unless the data collector uses encryption to ensure the security of the information.

3. A data collector shall not be liable for damages for a breach of the security of the system data if:

(a) The data collector is in compliance with this section; and

(b) The breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents.

4. The requirements of this section do not apply to:

(a) A telecommunication provider acting solely in the role of conveying the communications of other persons, regardless of the mode of conveyance used, including, without limitation:

(1) Optical, wire line and wireless facilities;

(2) Analog transmission; and

(3) Digital subscriber line transmission, voice over Internet protocol and other digital transmission technology.

(b) Data transmission over a secure, private communication channel for:

(1) Approval or processing of negotiable instruments, electronic fund transfers or similar payment methods; or

(2) Issuance of reports regarding account closures due to fraud, substantial overdrafts, abuse of automatic teller machines or related information regarding a customer.

5. As used in this section:

(a) "Data storage device" means any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives and optical computer drives, and the medium itself.

(b) "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using:

(1) An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data;

(2) Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology; and

(3) Any other technology or method identified by the Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration in regulations adopted pursuant to NRS 603A.217.

(c) "Facsimile" means an electronic transmission between two dedicated fax machines using Group 3 or Group 4 digital formats that conform to the International Telecommunications Union T.4 or T.38 standards or computer modems that conform to the International Telecommunications Union T.31 or T.32 standards. The term does not include onward transmission to a third device after protocol conversion, including, but not limited to, any data storage device.

(d) "Multifunctional device" means a machine that incorporates the functionality of devices, which may include, without limitation, a printer, copier, scanner, facsimile machine or electronic mail terminal, to provide for the centralized management, distribution or production of documents.

(e) "Payment card" has the meaning ascribed to it in NRS 205.602.

(f) "Telecommunication provider" has the meaning ascribed to it in NRS 704.027.

(Added to NRS by 2009, 1603; A 2011, 2002)

NRS 603A.217 Alternative methods of and technologies for encryption: Adoption of regulations. Upon receipt of a well-founded petition, the Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration may, pursuant to chapter 233B of NRS, adopt regulations which identify alternative methods or technologies which may be used to encrypt data pursuant to NRS 603A.215.

(Added to NRS by 2011, 2002)

NRS 603A.220 Disclosure of breach of security of system data; methods of disclosure.

1. Any data collector that owns or licenses computerized data which includes personal information shall 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.

2. Any data collector that maintains computerized data which includes personal information that the data collector does not own shall 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.

3. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation.

4. For purposes of this section, except as otherwise provided in subsection 5, the notification required by this section may be provided by one of the following methods:

(a) Written notification.

(b) Electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq.

(c) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information. Substitute notification must consist of all the following:

(1) Notification by electronic mail when the data collector has electronic mail addresses for the subject persons.

(2) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website.

(3) Notification to major statewide media.

5. A data collector which:

(a) Maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data.

(b) Is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., shall be deemed to be in compliance with the notification requirements of this section.

6. If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as that term is defined in 15 U.S.C. § 1681a(p), of the time the notification is distributed and the content of the notification.

(Added to NRS by 2005, 2504)

Remedies and Penalties

NRS 603A.260 Violation constitutes deceptive trade practice. A violation of the provisions of NRS 603A.010 to 603A.290, inclusive, constitutes a deceptive trade practice for the purposes of NRS 598.0903 to 598.0999, inclusive.

(Added to NRS by 2021, 1353)

NRS 603A.270 Civil action. A data collector that provides the notification required pursuant to NRS 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification.

(Added to NRS by 2005, 2506)—(Substituted in revision for NRS 603A.900)

NRS 603A.280 Restitution. In addition to any other penalty provided by law for the breach of the security of the system data maintained by a data collector, the court may order a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of such breach to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the notification required pursuant to NRS 603A.220, including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification.

(Added to NRS by 2005, 2506)—(Substituted in revision for NRS 603A.910)

NRS 603A.290 Injunction. If the Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of NRS 603A.010 to 603A.290, inclusive, the Attorney General or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.

(Added to NRS by 2005, 2506; A 2017, 4079)—(Substituted in revision for NRS 603A.920)

NOTICE REGARDING PRIVACY OF INFORMATION COLLECTED ON INTERNET FROM CONSUMERS

NRS 603A.300 Definitions. As used in NRS 603A.300 to 603A.360, inclusive, unless the context otherwise requires, the words and terms defined in NRS 603A.310 to 603A.337, inclusive, have the meanings ascribed to them in those sections.

(Added to NRS by 2017, 4077; A 2019, 1172; 2021, 1674)

NRS 603A.310 "Consumer" defined. "Consumer" means a person who seeks or acquires, by purchase or lease, any good, service, money or credit for personal, family or household purposes from the Internet website or online service of an operator.

(Added to NRS by 2017, 4077)

NRS 603A.320 "Covered information" defined. "Covered information" means any one or more of the following items of personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator or a data broker in an accessible form:

1. A first and last name.
2. A home or other physical address which includes the name of a street and the name of a city or town.
3. An electronic mail address.
4. A telephone number.
5. A social security number.
6. An identifier that allows a specific person to be contacted either physically or online.
7. Any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator or data broker in combination with an identifier in a form that makes the information personally identifiable.

(Added to NRS by 2017, 4078; A 2021, 1674)

NRS 603A.323 "Data broker" defined. "Data broker" means a person whose primary business is purchasing covered information about consumers with whom the person does not have a direct relationship and who reside in this State from operators or other data brokers and making sales of such covered information.

(Added to NRS by 2021, 1672)

NRS 603A.325 "Designated request address" defined. "Designated request address" means an electronic mail address, toll-free telephone number or Internet website established by an operator or data broker through which a consumer may submit to an operator or data broker a verified request.

(Added to NRS by 2019, 1171; A 2021, 1674)

NRS 603A.330 "Operator" defined.

1. "Operator" means a person who:

(a) Owns or operates an Internet website or online service for commercial purposes;

(b) Collects and maintains covered information from consumers who reside in this State and use or visit the Internet website or online service; and

(c) Purposefully directs its activities toward this State, consummates some transaction with this State or a resident thereof, purposefully avails itself of the privilege of conducting activities in this State or otherwise engages in any activity that constitutes sufficient nexus with this State to satisfy the requirements of the United States Constitution.

2. The term does not include:

(a) A third party that operates, hosts or manages an Internet website or online service on behalf of its owner or processes information on behalf of the owner of an Internet website or online service;

(b) An entity that is subject to the provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended, and the regulations adopted pursuant thereto;

(c) A manufacturer of a motor vehicle or a person who repairs or services a motor vehicle who collects, generates, records or stores covered information that is:

(1) Retrieved from a motor vehicle in connection with a technology or service related to the motor vehicle; or

(2) Provided by a consumer in connection with a subscription or registration for a technology or service related to the motor vehicle; or

(d) A person who does not collect, maintain or make sales of covered information.

(Added to NRS by 2017, 4078; A 2019, 1172; 2021, 1674)

NRS 603A.333 "Sale" defined.

1. "Sale" means the exchange of covered information for monetary consideration by an operator or data broker to another person.

2. The term does not include:

(a) The disclosure of covered information by an operator or data broker to a person who processes the covered information on behalf of the operator or data broker;

(b) The disclosure of covered information by an operator to a person with whom the consumer has a direct relationship for the purposes of providing a product or service requested by the consumer;

(c) The disclosure of covered information by an operator to a person for purposes which are consistent with the reasonable expectations of a consumer considering the context in which the consumer provided the covered information to the operator;

(d) The disclosure of covered information by an operator or data broker to a person who is an affiliate, as defined in NRS 686A.620, of the operator or data broker; or

(e) The disclosure or transfer of covered information by an operator or data broker to a person as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the person assumes control of all or part of the assets of the operator or data broker.

(Added to NRS by 2019, 1171; A 2021, 1675)

NRS 603A.337 "Verified request" defined. "Verified request" means a request:

1. Submitted by a consumer to an operator or data broker for the purposes set forth in NRS 603A.345 or 603A.346, as applicable; and

2. For which an operator or data broker can reasonably verify the authenticity of the request and the identity of the consumer using commercially reasonable means.

(Added to NRS by 2019, 1171; A 2021, 1675)

NRS 603A.338 Applicability of provisions. The provisions of NRS 603A.300 to 603A.360, inclusive, do not apply to:

1. A consumer reporting agency, as defined in 15 U.S.C. § 1681a(f);

2. Any personally identifiable information regulated by the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq., and the regulations adopted pursuant thereto, which is collected, maintained or sold as provided in that Act;

3. A person who collects, maintains or makes sales of personally identifiable information for the purposes of fraud prevention;

4. Any personally identifiable information that is publicly available;

5. Any personally identifiable information protected from disclosure under the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721 et seq., which is collected, maintained or sold as provided in that Act; or

6. A financial institution or an affiliate of a financial institution that is subject to the provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., or any personally identifiable information regulated by that Act which is collected, maintained or sold as provided in that Act.

(Added to NRS by 2021, 1672)

NRS 603A.340 Notice regarding covered information collected by operator: Operator required to make available to consumers; contents; exception.

1. Except as otherwise provided in subsection 2, an operator shall make available, in a manner reasonably calculated to be accessible by consumers whose covered information the operator collects through its Internet website or online service, a notice that:

(a) Identifies the categories of covered information that the operator collects through its Internet website or online service about consumers who use or visit the Internet website or online service and the categories of third parties with whom the operator may share such covered information;

(b) Provides a description of the process, if any such process exists, for an individual consumer who uses or visits the Internet website or online service to review and request changes to any of his or her covered information that is collected through the Internet website or online service;

(c) Describes the process by which the operator notifies consumers who use or visit the Internet website or online service of material changes to the notice required to be made available by this subsection;

(d) Discloses whether a third party may collect covered information about an individual consumer's online activities over time and across different Internet websites or online services when the consumer uses the Internet website or online service of the operator; and

(e) States the effective date of the notice.

2. The provisions of subsection 1 do not apply to an operator:

(a) Who is located in this State;

(b) Whose revenue is derived primarily from a source other than the sale or lease of goods, services or credit on Internet websites or online services; and

(c) Whose Internet website or online service has fewer than 20,000 unique visitors per year.

(Added to NRS by 2017, 4078; A 2021, 1675)

NRS 603A.345 Submission of verified request to operator not to sell covered information collected by operator; response to verified request.

1. Each operator shall establish a designated request address through which a consumer may submit a verified request pursuant to this section.

2. A consumer may, at any time, submit a verified request through a designated request address to an operator directing the operator not to make any sale of any covered information the operator has collected or will collect about the consumer.

3. An operator that has received a verified request submitted by a consumer pursuant to subsection 2 shall not make any sale of any covered information the operator has collected or will collect about that consumer.

4. An operator shall respond to a verified request submitted by a consumer pursuant to subsection 2 within 60 days after receipt thereof. An operator may extend by not more than 30 days the period prescribed by this subsection if the operator determines that such an extension is reasonably necessary. An operator who extends the period prescribed by this subsection shall notify the consumer of such an extension.

(Added to NRS by 2019, 1171)

NRS 603A.346 Submission of verified request to data broker not to sell covered information purchased by data broker; response to verified request.

1. Each data broker shall establish a designated request address through which a consumer may submit a verified request pursuant to this section.

2. A consumer may, at any time, submit a verified request through a designated request address to a data broker directing the data broker not to make any sale of any covered information about the consumer that the data broker has purchased or will purchase.

3. A data broker that has received a verified request submitted by a consumer pursuant to subsection 2 shall not make any sale of any covered information about that consumer that the data broker has purchased or will purchase.

4. A data broker shall respond to a verified request submitted by a consumer pursuant to subsection 2 within 60 days after receipt thereof. A data broker may extend by not more than 30 days the period prescribed by this subsection if the data broker determines that such an extension is reasonably necessary. A data broker who extends the period prescribed by this subsection shall notify the consumer of such an extension.

(Added to NRS by 2021, 1673)

NRS 603A.347 Data broker authorized to remedy first failure to comply with requirements concerning verified request.

1. A data broker who has not previously failed to comply with the provisions of NRS 603A.346 may remedy any failure to comply with the provisions of NRS 603A.346 within 30 days after being informed of such a failure.

2. A data broker described in subsection 1 who remedies a failure to comply with the provisions of NRS 603A.346 within 30 days after being informed of such a failure does not violate NRS 603A.346 for the purposes of NRS 603A.360.

(Added to NRS by 2021, 1673)

NRS 603A.348 Operator authorized to remedy first failure to comply with notice requirements.

1. An operator who has not previously failed to comply with the applicable provisions of subsection 1 of NRS 603A.340 may remedy any failure to comply with the applicable provisions of subsection 1 of NRS 603A.340 within 30 days after being informed of such a failure.

2. An operator described in subsection 1 who remedies a failure to comply with the applicable provisions of subsection 1 of NRS 603A.340 within 30 days after being informed of such a failure does not violate NRS 603A.340 for the purposes of NRS 603A.360.

(Added to NRS by 2021, 1673)

NRS 603A.349 Operator authorized to remedy first failure to comply with requirements concerning verified request.

1. An operator who has not previously failed to comply with the provisions of NRS 603A.345 may remedy any failure to comply with the provisions of NRS 603A.345 within 30 days after being informed of such a failure.

2. An operator described in subsection 1 who remedies a failure to comply with the provisions of NRS 603A.345 within 30 days after being informed of such a failure does not violate NRS 603A.345 for the purposes of NRS 603A.360.

(Added to NRS by 2021, 1673)

NRS 603A.350 Unlawful acts. An operator violates NRS 603A.340 if the operator:

1. Has not previously failed to comply with the applicable provisions of subsection 1 of that section and knowingly fails to remedy a failure to comply with such provisions within 30 days after being informed of such a failure;

2. Knowingly fails to comply with the applicable provisions of subsection 1 of that section after having previously failed to comply with such provisions; or

3. Makes available a notice pursuant to that section which contains information which constitutes a knowing and material misrepresentation or omission that is likely to mislead a consumer acting reasonably under the circumstances, to the detriment of the consumer.

(Added to NRS by 2017, 4079; A 2021, 1676)

NRS 603A.360 Enforcement by Attorney General; civil penalty for violation or injunction; no private right of action against operator; provisions not exclusive.

1. The Attorney General shall enforce the provisions of NRS 603A.300 to 603A.360, inclusive.

2. If the Attorney General has reason to believe that an operator, either directly or indirectly, has violated or is violating NRS 603A.340 or 603A.345, the Attorney General may institute an appropriate legal proceeding against the operator. The district court, upon a showing that the operator, either directly or indirectly, has violated or is violating NRS 603A.340 or 603A.345, may:

(a) Issue a temporary or permanent injunction; or

(b) Impose a civil penalty not to exceed $5,000 for each violation.

3. If the Attorney General has reason to believe that a data broker, either directly or indirectly, has violated or is violating NRS 603A.346, the Attorney General may institute an appropriate legal proceeding against the data broker. The district court, upon a showing that the data broker, either directly or indirectly, has violated or is violating NRS 603A.346, may:

(a) Issue a temporary or permanent injunction; or

(b) Impose a civil penalty not to exceed $5,000 for each violation.

4. The provisions of NRS 603A.300 to 603A.360, inclusive, do not establish a private right of action against an operator.

5. The provisions of NRS 603A.300 to 603A.360, inclusive, are not exclusive and are in addition to any other remedies provided by law.

(Added to NRS by 2017, 4079; A 2019, 1172; 2021, 1676)

CHAPTER 242 - INFORMATION SERVICES

GENERAL PROVISIONS

DIVISION OF ENTERPRISE INFORMATION TECHNOLOGY SERVICES

SERVICES

MISCELLANEOUS PROVISIONS

GENERAL PROVISIONS

NRS 242.011 Definitions. As used in this chapter, unless the context otherwise requires, the words and terms defined in NRS 242.013 to 242.068, inclusive, have the meanings ascribed to them in those sections.
(Added to NRS by 1969, 930; A 1973, 975; 1977, 1183; 1981, 1145; 1993, 1540; 2011, 1858, 2949)

NRS 242.013 "Administrator" defined. "Administrator" means the Administrator of the Division.
(Added to NRS by 2011, 2948)

NRS 242.015 "Board" defined. "Board" means the Information Technology Advisory Board.
(Added to NRS by 1993, 1538)

NRS 242.031 "Department" defined. "Department" means the Department of Administration.
(Added to NRS by 1981, 1143; A 1993, 1540; 1997, 3083; 2011, 2949)

NRS 242.045 "Division" defined. "Division" means the Division of Enterprise Information Technology Services of the Department.
(Added to NRS by 2011, 2948)

NRS 242.051 "Equipment" defined. "Equipment" means any machine or device designed for the automatic handling of information, including but not limited to recording, storage, transmission and retrieval.
(Added to NRS by 1969, 930; A 1981, 1146; 1993, 1540)

NRS 242.055 "Information service" defined. "Information service" means any service relating to the creation, maintenance, operation, security validation, testing, continuous monitoring or use of an information system.
(Added to NRS by 1993, 1538; A 2011, 1858)

NRS 242.057 "Information system" defined. "Information system" means any communications or computer equipment, computer software, procedures, personnel or technology used to collect, process, distribute or store information.
(Added to NRS by 1993, 1538; A 2011, 1859)

NRS 242.059 "Information technology" defined. "Information technology" means any information, information system or information service acquired, developed, operated, maintained or otherwise used.
(Added to NRS by 1993, 1539; A 2011, 1859)

NRS 242.061 "Local governmental agency" defined. "Local governmental agency" means any branch, agency, bureau, board, commission, department or division of a county, incorporated city or town in this State.

(Added to NRS by 2011, 1858)

NRS 242.063 "Security validation" defined. "Security validation" means a process or processes used to ensure that an information system or a network associated with an information system is resistant to any known threat.

(Added to NRS by 2011, 1858)

NRS 242.068 "Using agency" defined. "Using agency" means an agency of the State which has a function requiring the use of information technology, information services or an information system.

(Added to NRS by 1981, 1143; A 1993, 1540)

NRS 242.071 Legislative declaration; purposes of Division of Enterprise Information Technology Services.

1. The Legislature hereby determines and declares that the creation of the Division of Enterprise Information Technology Services of the Department of Administration is necessary for the coordinated, orderly and economical processing of information in State Government, to ensure economical use of information systems and to prevent the unnecessary proliferation of equipment and personnel among the various state agencies.

2. The purposes of the Division are:

(a) To perform information services for state agencies.

(b) To provide technical advice but not administrative control of the information systems within the state agencies and, as authorized, of local governmental agencies.

(Added to NRS by 1965, 972; A 1969, 933; 1973, 352; 1981, 1143; 1993, 1540; 1997, 3083; 2011, 1859, 2949)

DIVISION OF ENTERPRISE INFORMATION TECHNOLOGY SERVICES

NRS 242.080 Creation; composition.

1. The Division of Enterprise Information Technology Services of the Department is hereby created.

2. The Division consists of the Administrator and the:

(a) Enterprise Application Services Unit.

(b) Communication and Computing Unit.

(c) Office of Information Security.

3. A Communications Group and a Telecommunications Group are hereby created within the Communication and Computing Unit of the Division.

(Added to NRS by 1981, 1143; A 1993, 1541; 1997, 3083; 2007, 915; 2009, 1163; 2011, 2949; 2013, 3825)

NRS 242.090 Administrator: Appointment; classification; other employment prohibited.

1. The Director of the Department shall appoint the Administrator in the unclassified service of the State.

2. The Administrator:

(a) Serves at the pleasure of, and is responsible to, the Director of the Department.

(b) Shall not engage in any other gainful employment or occupation.

(Added to NRS by 1981, 1143; A 1983, 641; 1985, 413; 2011, 2949)

NRS 242.101 Administrator: General powers and duties.

1. The Administrator shall:

(a) Appoint the Chief of the Office of Information Security who is in the classified service of the State;

(b) Administer the provisions of this chapter and other provisions of law relating to the duties of the Division; and

(c) Carry out other duties and exercise other powers specified by law.

2. The Administrator may form committees to establish standards and determine criteria for evaluation of policies relating to informational services.

(Added to NRS by 1981, 1143; A 2011, 1859, 2949; 2015, 2756)

NRS 242.105 Confidentiality of certain documents relating to homeland security: List; biennial review; annual report.

1. Except as otherwise provided in subsection 3, records and portions of records that are assembled, maintained, overseen or prepared by the Division to mitigate, prevent or respond to acts of terrorism, the public disclosure of which would, in the determination of the Administrator, create a substantial likelihood of threatening

the safety of the general public are confidential and not subject to inspection by the general public to the extent that such records and portions of records consist of or include:

(a) Information regarding the infrastructure and security of information systems, including, without limitation:

(1) Access codes, passwords and programs used to ensure the security of an information system;

(2) Access codes used to ensure the security of software applications;

(3) Procedures and processes used to ensure the security of an information system; and

(4) Plans used to re-establish security and service with respect to an information system after security has been breached or service has been interrupted.

(b) Assessments and plans that relate specifically and uniquely to the vulnerability of an information system or to the measures which will be taken to respond to such vulnerability, including, without limitation, any compiled underlying data necessary to prepare such assessments and plans.

(c) The results of tests of the security of an information system, insofar as those results reveal specific vulnerabilities relative to the information system.

2. The Administrator shall maintain or cause to be maintained a list of each record or portion of a record that the Administrator has determined to be confidential pursuant to subsection 1. The list described in this subsection must be prepared and maintained so as to recognize the existence of each such record or portion of a record without revealing the contents thereof.

3. At least once each biennium, the Administrator shall review the list described in subsection 2 and shall, with respect to each record or portion of a record that the Administrator has determined to be confidential pursuant to subsection 1:

(a) Determine that the record or portion of a record remains confidential in accordance with the criteria set forth in subsection 1;

(b) Determine that the record or portion of a record is no longer confidential in accordance with the criteria set forth in subsection 1; or

(c) If the Administrator determines that the record or portion of a record is obsolete, cause the record or portion of a record to be disposed of in the manner described in NRS 239.073 to 239.125, inclusive.

4. On or before February 15 of each year, the Administrator shall:

(a) Prepare a report setting forth a detailed description of each record or portion of a record determined to be confidential pursuant to this section, if any, accompanied by an explanation of why each such record or portion of a record was determined to be confidential; and

(b) Submit a copy of the report to the Director of the Legislative Counsel Bureau for transmittal to:

(1) If the Legislature is in session, the standing committees of the Legislature which have jurisdiction of the subject matter; or

(2) If the Legislature is not in session, the Legislative Commission.

5. As used in this section, "act of terrorism" has the meaning ascribed to it in NRS 239C.030.

(Added to NRS by 2003, 2461; A 2005, 268; 2011, 2950)

NRS 242.111 Regulations. The Administrator shall adopt regulations necessary for the administration of this chapter, including:

1. The policy for the information systems of the Executive Branch of Government, excluding the Nevada System of Higher Education and the Nevada Criminal Justice Information System, as that policy relates, but is not limited, to such items as standards for systems and programming and criteria for selection, location and use of information systems to meet the requirements of state agencies and officers at the least cost to the State;

2. The procedures of the Division in providing information services, which may include provision for the performance, by an agency which uses the services or equipment of the Division, of preliminary procedures, such as data recording and verification, within the agency;

3. The effective administration of the Division, including, without limitation, security to prevent unauthorized access to information systems and plans for the recovery of systems and applications after they have been disrupted;

4. The development of standards to ensure the security of the information systems of the Executive Branch of Government; and

5. Specifications and standards for the employment of all personnel of the Division.

(Added to NRS by 1965, 973; A 1973, 1462; 1981, 1145; 1989, 2154; 1993, 369, 1541; 1995, 585; 1997, 3084; 2007, 915)

NRS 242.115 Development of policies, standards, guidelines and biennial state plan for information systems of Executive Branch of Government.

1. Except as otherwise provided in subsection 2, the Administrator shall:

(a) Develop policies and standards for the information systems of the Executive Branch of Government;

(b) Coordinate the development of a biennial state plan for the information systems of the Executive Branch of Government;

(c) Develop guidelines to assist state agencies in the development of short- and long-term plans for their information systems; and

(d) Develop guidelines and procedures for the procurement and maintenance of the information systems of the Executive Branch of Government.

2. This section does not apply to the Nevada System of Higher Education or the Nevada Criminal Justice Information System used to provide support for the operations of law enforcement agencies in this State.

(Added to NRS by 1989, 2153; A 1993, 370, 1541; 1995, 586; 1997, 3084; 2007, 916; 2009, 1163)

NRS 242.122 Information Technology Advisory Board: Creation; members; Chair.

1. There is hereby created an Information Technology Advisory Board. The Board consists of:

(a) One member appointed by the Majority Floor Leader of the Senate from the membership of the Senate Standing Committee on Finance.

(b) One member appointed by the Speaker of the Assembly from the membership of the Assembly Standing Committee on Ways and Means.

(c) Two representatives of using agencies which are major users of the services of the Division. The Governor shall appoint the two representatives. Each such representative serves for a term of 4 years. For the purposes of this paragraph, an agency is a "major user" if it is among the top five users of the services of the Division, based on the amount of money paid by each agency for the services of the Division during the immediately preceding biennium.

(d) The Director of the Department or his or her designee.

(e) The Attorney General or his or her designee.

(f) Five persons appointed by the Governor as follows:

(1) Three persons who represent a city or county in this State, at least one of whom is engaged in information technology or information security; and

(2) Two persons who represent the information technology industry but who:

(I) Are not employed by this State;

(II) Do not hold any elected or appointed office in State Government;

(III) Do not have an existing contract or other agreement to provide information services, systems or technology to an agency of this State; and

(IV) Are independent of and have no direct or indirect pecuniary interest in a corporation, association, partnership or other business organization which provides information services, systems or technology to an agency of this State.

2. Each person appointed pursuant to paragraph (f) of subsection 1 serves for a term of 4 years. No person so appointed may serve more than 2 consecutive terms.

3. At the first regular meeting of each calendar year, the members of the Board shall elect a Chair by majority vote.

(Added to NRS by 1993, 1539; A 2011, 1859)

NRS 242.123 Information Technology Advisory Board: Meetings; compensation.

1. The Board shall meet at least once every 3 months and may meet at such further times as deemed necessary by the Chair.

2. Members of the Board who are officers or employees of the Executive Department of State Government serve without additional compensation. Members who are not officers or employees of the Executive Department of State Government are entitled to a salary of $80 for each day or part of a day spent on the business of the Board. All members of the Board are entitled to receive the per diem allowance and travel expenses provided for state officers and employees generally.

(Added to NRS by 1993, 1539)

NRS 242.124 Information Technology Advisory Board: Duties; powers.

1. The Board shall:

(a) Advise the Division concerning issues relating to information technology, including, without limitation, the development, acquisition, consolidation and integration of, and policies, planning and standards for, information technology.

(b) Periodically review the Division's statewide strategic plans and standards manual for information technology.

(c) Review the Division's proposed budget before its submission to the Budget Division of the Office of Finance created by NRS 223.400.

2. The Board may:

(a) With the consent of the Division, recommend goals and objectives for the Division, including periods and deadlines in which to achieve those goals and objectives.

(b) Upon request by a using agency, review issues and policies concerning information technology to resolve disputes with the Division.

(c) Review the plans for information technology of each using agency.

(Added to NRS by 1993, 1539)

NRS 242.125 Consultation and coordination with state agencies not required to use services or equipment of Division. Regulations, policies, standards and guidelines adopted pursuant to the provisions of this chapter must be developed after consultation and coordination with state agencies that are not required to use the services or equipment of the Division.

(Added to NRS by 1989, 2154)

SERVICES

NRS 242.131 Services provided for agencies and elected officers of State: Negotiation; withdrawal; contracts to provide services.

1. The Division shall provide state agencies and elected state officers with all their required design of information systems. All agencies and officers must use those services and equipment, except as otherwise provided in subsection 2.

2. The following agencies may negotiate with the Division for its services or the use of its equipment, subject to the provisions of this chapter, and the Division shall provide those services and the use of that equipment as may be mutually agreed:

(a) The Court Administrator;

(b) The Department of Motor Vehicles;

(c) The Department of Public Safety;

(d) The Department of Transportation;

(e) The Employment Security Division of the Department of Employment, Training and Rehabilitation;

(f) The Department of Wildlife;

(g) The Housing Division of the Department of Business and Industry;

(h) The Legislative Counsel Bureau;

(i) The State Controller;

(j) The Nevada Gaming Control Board and Nevada Gaming Commission; and

(k) The Nevada System of Higher Education.

3. Any state agency or elected state officer who uses the services of the Division and desires to withdraw substantially from that use must apply to the Administrator for approval. The application must set forth justification for the withdrawal. If the Administrator denies the application, the agency or officer must:

(a) If the Legislature is in regular or special session, obtain the approval of the Legislature by concurrent resolution.

(b) If the Legislature is not in regular or special session, obtain the approval of the Interim Finance Committee. The Administrator shall, within 45 days after receipt of the application, forward the application together with his or her recommendation for approval or denial to the Interim Finance Committee. The Interim Finance Committee has 45 days after the application and recommendation are submitted to its Secretary within which to consider the application. Any application which is not considered by the Committee within the 45-day period shall be deemed approved.

4. If the demand for services or use of equipment exceeds the capability of the Division to provide them, the Division may contract with other agencies or independent contractors to furnish the required services or use of equipment and is responsible for the administration of the contracts.

(Added to NRS by 1965, 972; A 1969, 933; 1973, 1462; 1979, 1789; 1981, 1144, 1521, 1831; 1985, 1981; 1991, 1577; 1993, 370, 1542; 1995, 586; 1999, 1662, 1811; 2001, 2591; 2003, 1559, 2194)

NRS 242.135 Employment of one or more persons to provide information services for agency or elected officer of State.

1. The Administrator may recommend to the Governor that a state agency or elected officer that is required to use the Division's equipment or services be authorized to employ one or more persons to provide information services exclusively for the agency or officer if:

(a) The Administrator finds that it is in the best interests of the State to authorize the employment by the agency or elected officer;

(b) The agency or elected officer agrees to provide annually to the Division sufficient information to determine whether the authorized employment continues to be in the best interests of the State; and

(c) The agency or elected officer agrees to ensure that the person or persons employed comply with the provisions of this chapter and the regulations adopted thereunder.

2. The Administrator may recommend to the Governor the revocation of the authority of a state agency or elected officer to employ a person or persons pursuant to subsection 1 if the Administrator finds that the person or persons employed have not complied with the provisions of this chapter or the regulations adopted thereunder.

(Added to NRS by 1989, 2153; A 1993, 1543)

NRS 242.141 Services provided for agencies not under Governor's control and local governmental agencies. To facilitate the economical processing of data throughout the State Government, the Division may provide service for agencies not under the control of the Governor, upon the request of any such agency. The Division may provide services, including, without limitation, purchasing services, to a local governmental agency upon request, if provision of such services will result in reduced costs to the State for equipment and services.

(Added to NRS by 1965, 973; A 1981, 1144; 2011, 1860)

NRS 242.151 Administrator to advise agencies. The Administrator shall advise the using agencies regarding:

1. The policy for information services of the Executive Branch of Government, as that policy relates, but is not limited, to such items as standards for systems and programming and criteria for the selection, location and use of information systems in order that the requirements of state agencies and officers may be met at the least cost to the State;

2. The procedures in performing information services; and

3. The effective administration and use of the computer facility, including security to prevent unauthorized access to data and plans for the recovery of systems and applications after they have been disrupted.

(Added to NRS by 1969, 930; A 1981, 1147; 1989, 2154; 1993, 1543)

NRS 242.161 Managerial control of equipment owned or leased by State.

1. All equipment of an agency or elected state officer which is owned or leased by the State must be under the managerial control of the Division, except the equipment of the agencies and officers specified in subsection 2 of NRS 242.131.

2. The Division may permit an agency which is required to use such equipment to operate it on the agency's premises.

(Added to NRS by 1969, 931; A 1981, 1147)

NRS 242.171 Responsibilities of Division; review of proposed applications of information systems.

1. The Division is responsible for:

(a) The applications of information systems;

(b) Designing and placing those information systems in operation;

(c) Any application of an information system which it furnishes to state agencies and officers after negotiation; and

(d) The security validation, testing, including, without limitation, penetration testing, and continuous monitoring of information systems,

➥ for using agencies and for state agencies and officers which use the equipment or services of the Division pursuant to subsection 2 of NRS 242.131.

2. The Administrator shall review and approve or disapprove, pursuant to standards for justifying cost, any application of an information system having an estimated developmental cost of $50,000 or more. No using agency may commence development work on any such applications until approval and authorization have been obtained from the Administrator.

3. As used in this section, "penetration testing" means a method of evaluating the security of an information system or application of an information system by simulating unauthorized access to the information system or application.

(Added to NRS by 1969, 931; A 1973, 680; 1981,1147; 1993, 1543; 2011, 1860)

NRS 242.181 Adherence by using agencies and elected officers of State to regulations; reporting of certain incidents; uniformity of services.

1. Any state agency or elected state officer which uses the equipment or services of the Division shall adhere to the regulations, standards, practices, policies and conventions of the Division.

2. Each state agency or elected state officer described in subsection 1 shall report any suspected incident of:

(a) Unauthorized access to an information system or application of an information system of the Division used by the state agency or elected state officer; and

(b) Noncompliance with the regulations, standards, practices, policies and conventions of the Division that is identified by the Division as security-related,

➥ to the Office of Information Security of the Division within 24 hours after discovery of the suspected incident. If the Office determines that an incident of unauthorized access or noncompliance occurred, the Office shall immediately report the incident to the Administrator. The Administrator shall assist in the investigation and resolution of any such incident.

3. The Division shall provide services to each state agency and elected state officer described in subsection 1 uniformly with respect to degree of service, priority of service, availability of service and cost of service.

(Added to NRS by 1969, 931; A 1981, 1148; 1993, 1544; 2011, 1861)

NRS 242.183 Investigation, resolution and notification of certain breaches or applications of information systems or certain unauthorized acquisitions of computerized data.

1. The Chief of the Office of Information Security shall investigate and resolve any breach of an information system of a state agency or elected officer that uses the equipment or services of the Division or an application of such an information system or unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of such an information system.

2. The Administrator or Chief of the Office of Information Security, at his or her discretion, may inform members of the Technological Crime Advisory Board created by NRS 205A.040, the Nevada Commission on Homeland Security created by NRS 239C.120 and the Information Technology Advisory Board created by NRS 242.122 of any breach of an information system of a state agency or elected officer or application of such an information system or unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of such an information system.

(Added to NRS by 2011, 1858)

NRS 242.191 Amount receivable for use of services of Division: Determination; itemized statement.

1. Except as otherwise provided in subsection 3, the amount receivable from a state agency or officer or local governmental agency which uses the services of the Division must be determined by the Administrator in each case and include:

(a) The annual expense, including depreciation, of operating and maintaining the Communication and Computing Unit, distributed among the agencies in proportion to the services performed for each agency.

(b) A service charge in an amount determined by distributing the monthly installment for the construction costs of the computer facility among the agencies in proportion to the services performed for each agency.

2. The Administrator shall prepare and submit monthly to the state agencies and officers and local governmental agencies for which services of the Division have been performed an itemized statement of the amount receivable from each state agency or officer or local governmental agency.

3. The Administrator may authorize, if in his or her judgment the circumstances warrant, a fixed cost billing, including a factor for depreciation, for services rendered to a state agency or officer or local governmental agency.

(Added to NRS by 1969, 931; A 1973, 680; 1979, 68; 1981, 1148; 1997, 3085; 2011, 1861)

NRS 242.211 Fund for Information Services: Creation; source and use.

1. The Fund for Information Services is hereby created as an internal service fund. Money from the Fund must be paid out on claims as other claims against the State are paid. The claims must be made in accordance with budget allotments and are subject to postaudit examination and approval.

2. All operating, maintenance, rental, repair and replacement costs of equipment and all salaries of personnel assigned to the Division must be paid from the Fund.

3. Each agency using the services of the Division shall pay a fee for that use to the Fund, which must be set by the Administrator in an amount sufficient to reimburse the Division for the entire cost of providing those services, including overhead. Each using agency shall budget for those services. All fees, proceeds from the sale of equipment and any other money received by the Division must be deposited with the State Treasurer for credit to the Fund.

(Added to NRS by 1965, 973; A 1979, 103; 1981, 255, 1145; 1989, 1470; 1993, 1544; 2003, 627)

NRS 242.221 Approval and payment of claims; temporary advances.

1. All claims made pursuant to NRS 242.122 to 242.241, inclusive, must, when approved by the Division, be paid as other claims against the State are paid.

2. If the State Controller finds that current claims against the Fund for Information Services exceed the amount available in the Fund to pay the claims, the State Controller may advance temporarily from the State General Fund to the Fund the amount required to pay the claims, but no more than 25 percent of the revenue expected to be received in the current fiscal year from any source authorized for the Fund. No amount may be transferred unless requested by the Chief of the Budget Division of the Office of Finance created by NRS 223.400.

(Added to NRS by 1969, 932; A 1981, 1148; 1987, 150, 415; 1989, 1470; 1993, 1544; 2003, 627)

NRS 242.231 Payment by state agency or officer for services. Upon the receipt of a statement submitted pursuant to subsection 2 of NRS 242.191, each state agency or officer shall authorize the State Controller by transfer or warrant to draw money from the agency's account in the amount of the statement for transfer to or placement in the Fund for Information Services.

(Added to NRS by 1969, 932; A 1979, 69; 1981, 1148; 1989, 1471; 1993, 1545; 2011, 1861)

NRS 242.241 Repayment of costs of construction of computer facility.

1. Until the construction costs of $535,600 for the computer facility in Carson City, Nevada, have been paid, the Administrator shall pay annually from the Fund for Information Services to the State Treasurer for deposit in the State General Fund 2 percent of the facility's original acquisition cost.

2. For any subsequent capital additions to the computer facility, the Administrator shall pay annually from that Fund to the State Treasurer for deposit in the State General Fund 2 percent of the original cost of such capital additions, until this cost has been fully paid.

(Added to NRS by 1969, 932; A 1973, 681; 1981, 1148; 1989, 1471; 1993, 1545)

MISCELLANEOUS PROVISIONS

NRS 242.300 Policy of state agency for appropriate use of computers by employees of agency.

1. A state agency that uses at least one computer in the course of its work shall:

(a) Create a written policy setting forth the appropriate uses of the computers of the state agency; and

(b) Provide all employees of the state agency with a copy of the written policy.

2. As used in this section, "state agency" means an agency, bureau, board, commission, department, division or any other unit of the Executive Department of the government of this State.

(Added to NRS by 1999, 2714)