

Effective 5/10/2016

**Part 1
Computer Abuse and Data Recovery Act**

63D-3-101 Title.

- (1) This chapter is known as "Unauthorized Access to Information Technology."
- (2) This part is known as "Computer Abuse and Data Recovery Act."

Enacted by Chapter 209, 2016 General Session

63D-3-102 Definitions.

As used in this part, the term:

- (1) "Authorized user" means, for a protected computer:
 - (a) the protected computer's owner; or
 - (b) an individual who has permission to access the protected computer under Section 63D-3-103.
- (2)
 - (a) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or storage functions.
 - (b) "Computer" includes any data storage device, data storage facility, or communications facility that is directly related to or that operates in conjunction with the device described in Subsection (2)(a).
- (3)
 - (a) "Damage" means, for a protected computer's owner, the cost associated with an individual's unauthorized access to information stored on a protected computer.
 - (b) "Damage" includes:
 - (i) the cost of repairing or restoring a protected computer;
 - (ii) economic damages;
 - (iii) consequential damages, including interruption of service; and
 - (iv) profit by the individual from the unauthorized access to the protected computer.
- (4) "Harm" means any impairment to the integrity, access, or availability of:
 - (a) data;
 - (b) a program;
 - (c) a system; or
 - (d) information.
- (5) "Owner" means a person who:
 - (a) owns or leases a protected computer; or
 - (b) owns the information stored in a protected computer.
- (6)
 - (a) "Protected computer" means a computer that:
 - (i) is used in connection with the operation of a business, state government entity, or political subdivision; and
 - (ii) requires a technological access barrier for an individual to access the computer.
 - (b) "Protected computer" does not include a computer that an individual can access using a technological access barrier that does not, to a reasonable degree of security, effectively control access to the information stored in the computer.
- (7) "Technological access barrier" means a password, security code, token, key fob, access device, or other digital security measure.

- (8) "Traffic" means to sell, purchase, or deliver.
- (9) "Unauthorized user" means an individual who, for a protected computer:
 - (a) is not an authorized user of the protected computer; and
 - (b) accesses the protected computer by:
 - (i) obtaining, without an authorized user's permission, the authorized user's technological access barrier; or
 - (ii) circumventing, without the permission of the protected computer's owner, a technological access barrier on the protected computer.

Enacted by Chapter 209, 2016 General Session

63D-3-103 Permission to access a protected computer -- Revocation.

- (1) Subject to Subsections (2) and (3), an individual has permission to access a protected computer if:
 - (a) the individual is a director, officer, employee, agent, or contractor of the protected computer's owner; and
 - (b) the protected computer's owner gave the individual express permission to access the protected computer through a technological access barrier.
- (2) If a protected computer's owner gives an individual permission to access the protected computer, the permission is valid only to the extent or for the specific purpose the protected computer's owner authorizes.
- (3) An individual's permission to access a protected computer is revoked if:
 - (a) the protected computer's owner expressly revokes the individual's permission to access the protected computer; or
 - (b) the individual ceases to be a director, officer, employee, agent, or contractor of the protected computer's owner.

Enacted by Chapter 209, 2016 General Session

63D-3-104 Prohibited acts.

- (1) An unauthorized user of a protected computer may not, knowingly and with intent to cause harm or damage:
 - (a) obtain information from the protected computer and, as a result, cause harm or damage;
 - (b) cause the transmission of a program, code, or command to the protected computer, and, as a result of the transmission, cause harm or loss; or
 - (c) traffic in any technological access barrier that an unauthorized user could use to access the protected computer.
- (2) An individual who violates Subsection (1) is liable to a protected computer's owner in a civil action for the remedies described in Section 63D-3-105.

Enacted by Chapter 209, 2016 General Session

63D-3-105 Remedies.

- (1) A person who brings a civil action against an individual for a violation of Section 63D-3-104 may:
 - (a) recover actual damages, including the person's:
 - (i) lost profits;
 - (ii) economic damages; and

- (iii) reasonable cost of remediation efforts related to the violation;
- (b) recover consequential damages, including for interruption of service;
- (c) recover, from the individual, the individual's profit obtained through trafficking in anything obtained by the individual through the violation;
- (d) obtain injunctive or other equitable relief to prevent a future violation of Section 63D-3-104; and
- (e) recover anything the individual obtained through the violation, including:
 - (i) misappropriated information or code;
 - (ii) a misappropriated program; and
 - (iii) any copies of the information, code, or program described in Subsections (1)(e)(i) and (1)(e)(ii).
- (2) A court shall award reasonable attorney fees to the prevailing party in any action arising under this part.
- (3) The remedies available for a violation of Section 63D-3-104 are in addition to remedies otherwise available for the same conduct under federal or state law.
- (4) A person may not file a civil action under Section 63D-3-104 later than three years after the day on which:
 - (a) the violation occurred; or
 - (b)
 - (i) the person discovers the violation; or
 - (ii) the person should have discovered the violation if the person acted with reasonable diligence to discover the violation.

Enacted by Chapter 209, 2016 General Session

63D-3-106 Exclusions.

- (1) This section does not prohibit a lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency, regulatory agency, or political subdivision of this state, another state, the United States, or a foreign country.
- (2) This part does not apply to a provider of:
 - (a) an interactive computer service as defined in 47 U.S.C. Sec. 230(f); or
 - (b) an information service as defined in 47 U.S.C. Sec. 153.

Enacted by Chapter 209, 2016 General Session