**The Following are Relevant Laws:**

* Copyright Act of 1976
* Foreign Corrupt Practices Act of 1977
* Computer Fraud and Abuse Act of 1986
* Computer Security Act of 1987
* The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
* Georgia Computer Systems Protection Act

Since HAL is headquartered in Atlanta, GA, the above laws are noted as a reference. These laws impact HAL’s computer use for all employees, as applicable under jurisdictional interpretations.

# Georgia Computer Systems Protection Act

The "Georgia Computer Systems Protection Act" is an act enacted by the 1991 Georgia General Assembly and signed into law by the Governor effective July 1, 1991 which repealed and replaced an act having the same name enacted by the 1981 Georgia General Assembly and signed into law by the Governor effective July 1, 1981. This act establishes certain acts involving computer fraud or abuse as crimes punishable by defined fines or imprisonment or both. A modification to this Act, [HB1630](http://www.usg.edu/oiit/policies/hb1630.phtml), was passed by the 1996 session of the Georgia General Assembly.

AN ACT

To amend Chapter 9 of Title 16 of the Official Code of Georgia Annotated, relating to crimes involving forgery and fraudulent practices, so as to repeal the existing "Georgia Computer Systems Protection Act" and enact a new "Georgia Computer Systems Protection Act"; to provide for legislative intent; to provide for definitions; to provide for criminal liability and penalties for the crimes of computer theft, computer trespass, computer invasion of privacy, computer forgery, and computer password disclosure; to provide for civil remedies and damages; to provide for venue; to provide for other related matters; to provide an effective date; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

Section 1. Chapter 9 of Title 16 of the Official Code of Georgia Annotated, relating to crimes involving forgery and fraudulent practices, is amended by repealing in its entirety Article 6, the "Georgia Computer Systems Protection Act," and inserting in its place a new Article 6 to read as follows:

"ARTICLE 6

16-9-90. This article may be cited as the 'Georgia Computer Systems Protection Act.'

16-9-91. The General Assembly finds that:

(1) Computer related crime is a growing problem in the government and in the private sector;

(2) Such crime occurs at great cost to the public, since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime; (3) The opportunities for computer related crimes in state programs, and in other entities which operate within the state, through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets are great;

(4) Computer related crime operations have a direct effect on state commerce;

(5) Liability for computer crimes should be imposed on all persons, as that term is defined in this title; and

(6) The prosecution of persons engaged in computer related crime is difficult under previously existing Georgia criminal statutes.

16-9-92. As used in this article, the term:

(1) 'Computer' means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device or system performing computer operations with or on data and includes any data storage facility or communications facility directly related to or operating in conjunction with such device; but such term does not include an automated typewriter or typesetter, portable hand-held calculator, household appliance, or other similar device that is not used to communicate with or to manipulate any other computer.

(2) 'Computer network' means a set of related, remotely connected computers and any communications facilities with the function and purpose of transmitting data among them through the communications facilities.

(3) 'Computer operation' means computing, classifying, transmitting, receiving, retrieving, originating, switching, storing, displaying, manifesting, measuring, detecting, recording, reproducing, handling, or utilizing any form of data for business, scientific, control, or other purposes.

(4) 'Computer program' means one or more statements or instructions composed and structured in a form acceptable to a computer that, when executed by a computer in actual or modified form, cause the computer to perform one or more computer operations. The term 'computer program' shall include all associated procedures and documentation, whether or not such procedures and documentation are in human readable form.

(5) 'Data' includes any representation of information, intelligence, or data in any fixed medium, including documentation, computer printouts, magnetic storage media, punched cards, storage in a computer, or transmission by a computer network.

(6) 'Financial instruments' includes any check, draft, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction-authorizing mechanism or marketable security, or any computer representation thereof.

(7) 'Property' includes computers, computer networks, computer programs, data, financial instruments, and services.

(8) 'Services' includes computer time or services or data processing services.

(9) 'Use' includes causing or attempting to cause:

(A) A computer or computer network to perform or to stop performing computer operations;

(B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program, or data; or

(C) A person to put false information into a computer.

(10) 'Victim expenditure' means any expenditure reasonably and necessarily incurred by the owner to verify that a computer, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by unauthorized use.

(11) 'Without authority' includes the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network.

16-9-93. (a) Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

(2) Obtaining property by any deceitful means or artful practice; or

(3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

(b) Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or

(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

(c) Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

(d) Computer Forgery. Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery.

The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

(e) Computer Password Disclosure. Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

(f) Article not Exclusive. The provisions of this article shall not be construed to preclude the applicability of any other law which presently applies or may in the future apply to any transaction or course of conduct which violates this article.

(g) Civil Relief; Damages.

(1) Any person whose property or person is insured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, 'damages' shall include loss of profits and victim expenditure.

(2) At the request of any party to an action brought pursuant to this Code section, the court shall by reasonable means conduct all legal proceedings in such a way as to protect the secrecy and security of any computer, computer network, data, or computer program involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(3) The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(4) A civil action under, this Code section must be brought within four years after the violation is discovered or by exercise of reasonable diligence should have been discovered. For purposes of this article, a continuing violation of any one subsection of this Code section by any person constitutes a single violation by such person.

(h) Criminal Penalties.

(1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.

(2) Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.

16-9-94. For the purpose of venue under this article, any violation of this article shall be considered to have been committed:

(1) In the county of the principal place of business in this state of the owner of a computer, computer network, or any part thereof; and,

(2) In any county in which any person alleged to have violated any provision of this article had control or possession of any proceeds of the violation or of any books, records, documents, or property which were used in furtherance of the violation; and,

(3) In any county in which any act was performed in furtherance of any transaction which violated this article; and,

(4) In any county from which, to which, or through which any use of a computer or computer network was made, whether by wires, electro-magnetic waves, microwaves, or any other means of communication."

Section 2. This Act shall become effective on July 1, 1991.

Section 3. All laws and parts of laws in conflict with this Act are repealed.

[HB1630](http://www.usg.edu/oiit/policies/hb1630.phtml), an amendment to this act

Computer or telephone network; transmitting misleading data  
  
Enacted by the 1996 Georgia General Assembly  
Effective 1 July 1996

Description

**HB 1630** amends the [**Georgia Computer Systems Protection Act**](http://www.usg.edu/oiit/policies/proact.phtml), thus making it unlawful for any person or organization knowingly to transmit certain misleading data through a computer or telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank; and for other purposes.

HB 1630

Computer or telephone network; transmitting misleading data

HB 1630

A BILL to amend Article 6 of Chapter 9 of Title 16 of the OfficialCode of Georgia Annotated, known as the "Georgia Computer Systems Protection Act," so as to provide that it shall be unlawful for any person or organization knowingly to transmit certain misleading data through a computer or telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank; and for other purposes.

HB 1630 HB 1630/FSFA

A BILL TO BE ENTITLED

AN ACT

To amend Article 6 of Chapter 9 of Title 16 of the Official Code of Georgia Annotated, known as the "Georgia Computer Systems Protection Act," so as to provide that it shall be unlawful for any person or organization knowingly to transmit certain misleading data through a computer or telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank; to provide for a penalty; to provide that civil actions are allowed; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

**SECTION 1**.

Article 6 of Chapter 9 of Title 16 of the Official Code of Georgia Annotated, known as the "Georgia Computer Systems Protection Act," is amended by adding, following Code Section 16-9-93, a new Code Section 16-9-93.1 to read as follows:

"16-9-93.1.

(a) It shall be unlawful for any person, any organization, or any representative of any organization knowingly to transmit any data through a computer network or over the transmission facilities or through the network facilities of a local telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data or which would falsely state or imply that such person, organization, or representative has permission or is legally authorized to use such trade name, registered trademark, logo, legal or official seal, or copyrighted symbol for such purpose when such permission or authorization has not been obtained; provided, however, that no telecommunications company or Internet access provider shall violate this Code section solely as a result of carrying or transmitting such data for its customers.

(b) Any person violating subsection (a) of this Code section shall be guilty of a misdemeanor.

(c) Nothing in this Code section shall be construed to limit an aggrieved party's right to pursue a civil action for equitable or monetary relief, or both, for actions which violate this Code section."

**SECTION 2**.

Nothing contained herein shall prohibit a member of the General Assembly from using the state seal or the Georgia flag which contains the state seal on a home page that is clearly identified with the name of the member as the home page of that member.

**SECTION 3**.

All laws and parts of laws in conflict with this Act are repealed.