TECHNOLOGY COMPLIANCE 2.51

I. PURPOSE

Producing, exchanging, and retrieving information electronically by taking advantage of computer technology presents valuable opportunities for Allied Services. While employees are encouraged to use technology, its use carries important responsibilities. Allied Services' employees are expected to exhibit a high level of ethical and business standards when using this technology are consistent with applicable law and Allied Services policy.

Computers, computer systems, and electronic media equipment (including, but not limited to computer accounts, laptop computers, printers, networks, software, electronic mail, and Internet) at Allied Services are provided for the use of Allied Services' employees and contractors for Allied Services' business-related use. It is the responsibility of Allied Services' employees and contractors to see that these information systems are used in an efficient, ethical, and lawful manner.

The use of information systems is a privilege extended by Allied Services, which may be withdrawn at any time. An employee's use of computer systems may be suspended immediately upon the discovery of a possible violation of these policies. A violation of the provisions of this policy may result in disciplinary action up to and including termination, as outlined in Allied Services Discipline and Discharge Policy 2.07.

II. RESPONSIBLE USE OF COMPUTERS AND COMPUTER SERVICES

The following policies relate to the responsible use of computers and computer services and electronic media resources at Allied Services:

1. These resources are Allied Services property and are to be used solely for business purposes. Access by employees requires written authorization from a supervisor/manager to the Information Systems Department. This authorization can be revised, restricted, or revoked at any time.

2. Fraudulent, harassing, threatening, discriminatory, sexually explicit, or obscene messages and/or materials are not to be transmitted, printed, requested, or stored. "Chain letters", solicitations, and other forms of mass mailings are not permitted.

3. Employees are responsible for protecting their own passwords. Sharing user ID's, passwords, and account access codes or numbers is forbidden. Employees may be held responsible for misuse that occurs through such unauthorized access.

Issued: 12/97
Re-issued: 3/10, 7/19

4. Allied Services provides an electronic mail system and network connections for internal and external business communication and data exchange purposes. Although employee passwords are required for access, these systems cannot guarantee confidentiality. In fact, use and access is monitored and tracked by management at any time. Even though files, data, or messages may appear to be "deleted," procedures by the company to guard against data loss may preserve material for extended periods of time.

5. In order to maintain and assure company access to company data, no employee is permitted to use encryption devices on a company computer without express written authorization. Any employee authorized to use encryption coding devices and other security protection devices must provide the applicable keys and codes in a sealed envelope to the Information Systems Department Administrator where they will be retained in a secure environment.

6. Introducing or using software designed to destroy or corrupt the company's computer system with viruses or cause other harmful effects is prohibited. Employees are required to use the company-provided anti-virus software.

7. Intentional virus infection by an employee is grounds for immediate dismissal.

III. INTERNET USE

The Internet can be described as a union of the telephone, mail, TV, or radio, in short, any type of remote communications can be carried out via the Internet. When Allied Services' employees are using the internet they should follow a few simple rules in regard to their conduct: don't break the law, be civil, and please use good judgment.

Accounts based on the Allied Services Internet connection should not be considered confidential in accordance with Allied Services policy. This also includes the possibility of inspection of any mail and/or files.

INTERNET ACCESS ORIGINATION AT ALLIED SERVICE IS A PRIVILEGE EXTENDED BY ALLIED SERVICES WHICH MAY BE WITHDRAWN AT ANY TIME.

When using the Allied Services Internet connection, you are a representative of Allied Services in the Internet community. Users must be aware of their responsibilities including, but not limited to the following:

1. Irresponsible use of system resources. Resources include bandwidth (the pipeline for the data both coming into Allied Services and going out of Allied Services) and storage (for downloaded files). A finite amount of data can travel across our network at any given time; downloading large files during business hours can compromise the performance of the entire system. Prior to working with a large file, please consider the impact you will have on all other Allied

Services network users. Large files should be downloaded after business hours of operations.

2. Any activity that is contrary to applicable, including distributing or obtaining copyrighted software or information without proper authorization from the copyright holder.

3. All Allied Services employees using the Allied Services Internet connections must respect all copyright issues regarding software, information, and attributions of authorship. In respect to software: copying copyrighted software to an Allied Services computer without proper licensing is not only illegal, but it makes you and Allied Services liable for copyright infringement. Any employee who has unlicensed software on Allied Services equipment that has been provided for his or her use will be held accountable for the consequences.

4. Downloaded software may have viruses or worms; scan any programs with a virus detection program prior to executing them. If you are unsure how to use detection software, please contact the Information Systems Department Help Desk.

5. Regarding copyright in general: “Allied Services expects its employees to respect all of the intellectual property rights of others.”

6. Any activity that could damage Allied Services reputation or potentially put you and Allied Services at risk for legal proceedings by any party (such as libelous or harassing communications or unfair competitive practices). In other words, please remember that the message you post to a mailing or newsgroup, or even send directly to another person outside the company, can end up on the screens of thousands of readers. Please use good judgment.

7. Any activity that could be construed as hostile to another company or institution. An example of this is making attempts to gain unauthorized access to another company’s systems and/or information.

8. When posting, blogging, using social networking or other similar communication technologies, unless authority is specifically tracked by Allied Administration, you do not have the authority to communicate on behalf of Allied Services any such post that monitors your affiliation or employment must specifically include a disclaimer to that fact

9. Any communication that could be construed as an official response from the company should be referred to the Communications Department for response. Frequently, messages are posted to Bulletin Boards or Mailing Lists that require a response and in order to handle these messages most efficiently all employees should direct that correspondence to the Communications Department.

10. Communication of commercial nature, solicitations, advertisements, and similar commercial postings are unwelcome in many Internet forums. Prior to posting any such communications, please contact senior management for advice.

11. Communication of Allied Services proprietary information. Methods and materials developed by Allied Services, including marketing information, developmental plans, and technological development are only a few examples of proprietary information held as confidential and which are not to be shared outside the company. If you have any questions in this regard please contact the Human Resources Department.