512.4 Computer Usage: It is critical to ensure the provision of computer and telecommunications resources and services to Grant County employees for the purpose of conducting business. This policy section applies to all users of Grant County computer and telecommunications resources and services. Violations of this policy may result in corrective action, up to and including termination of employment; it is also possible that, depending upon the nature of the violation(s), criminal charges and/or legal action may result.

512.4.1 Specifics

a. The Department of Technology Services provides computer users with technical resources. All computer users have the responsibility to use County computer resources in an efficient, effective, ethical, and lawful manner. This Policy 500, Standards of Conduct, sets forth the requirements and expectations of employee conduct and usage of County resources.
b. All computer usage is to be in conformance with Section 512 and its subsections; applicable and binding policies set forth hereinabove are not duplicated in this subsection 512.4.
c. Viewing of any internet site of a sexual nature is strictly prohibited and could result in disciplinary action, up to and including termination of employment.

512.4.2 Security and Monitoring

a. Grant County seeks to protect computer-based information, recognized as a primary administrative, educational and research asset, from accidental or intentional/unauthorized modification, misuse, destruction, disruption, or disclosure. In order to make every reasonable effort to protect the integrity of its computing systems, workstations, networks, etc., Grant County has the right and responsibility to monitor its computing resources.
b. All County computer users must read and sign an acknowledgement of having received and read Policy 500, Standards of Conduct, Section 512, *Use of County Resources*, prior to authorization for use. This form is provided by the Human Resources Department at employee orientation. Refusal to read and sign the policy may be grounds for discipline, up to and including termination of employment.
c. Grant County has the right to monitor any and all aspects of a system, including individual login sessions to determine if a user is acting in violation of County policy, state, and/or federal laws. The issuance of a password of other means of access is to assure appropriate confidentiality of County files and information, and does not guarantee privacy for personal or improper use of County equipment or facilities.

d. All user Internet activity is monitored, tracked, and documented. Reports and documentation stemming from Internet activity monitoring is a matter of public record, with the exception of certain law enforcement matters. In addition, it is available to management as a tool to assist in determining an office's, departments, or individual's use of County time, resources, and adherence to related County policies.
e. All users are assigned an individual log on with password protection.
    1. Each user is responsible for safeguarding his or her user identification and password.
    2. Users should not print, store on-line, or provide their password(s) to others.
    3. The user is responsible to make authorized usage of the ID for its intended purpose only.
    4. Each user is responsible for all transactions made under the authorization of his or her ID.
    5. Any user who suspects a breach of password protection should report their concern immediately to his/her supervisor and immediately make arrangements with Technology Services for the ability to select a new password.
f. Computer users shall not intentionally view, provide, or modify information in or obtain copies of files, programs, keystrokes, or passwords belonging to other computer users. This includes all system files and accounts.
g. The copying or sharing of copyrighted materials, software, video and audio files (including MPEG files) is prohibited.
h. Due to risks of electronically transmitted viruses, it is suggested that software upgrades, installation files, and other executable files (*.exe files) should only be downloaded and installed from the internet after consultation with or instruction from Technology Services staff. This includes executable files (*.exe) attached to electronic mail messages, but does not include document files such as Word (*.doc) and Excel (*.xls). Individual users who do not conform to this policy must take responsibility for all problems and issues that may subsequently arise.

512.4.3 Site Access – Federal/Other

a. *Criminal Justice Information System (CJIS) Requirements:* Certain County offices/departments work under Criminal Justice Information System (CJIS) requirements as prescribed by the Washington State Patrol and the Federal

Bureau of Investigation (FBI). Access to the CJIS site includes the following requirements:

1. Agencies must conduct a state of residency and fingerprint-based background check for all personnel within 3 days of employment or assignment.
2. The agency's Technical Agency Coordinator (TAC) must retain the State Identification Number (SID) of each employee who uses **A Central Computerized Enforcement Service System** (ACCESS) or maintains the application or network connection. Below is a list of personnel that will fall under the background check requirements:
    i. Law enforcement officers
    ii. Corrections
    iii. Court personnel
    iv. Probation personnel
    v. Technical staff
    vi. Technical vendors for applications/network assistance
    vii. Contractors
3. Terminal locations must be secure from unauthorized access and all employees authorized to access files must be instructed on proper use and dissemination of information.
4. All visitors to computer centers and/or terminal areas must be escorted by authorized personnel at all times. This would include:
    i. The public
    ii. Prospective employees
    iii. Contractors
    iv. Vendors
5. The FBI requires all personnel who manage or have access to FBI CJIS systems (including technical staff) must receive security awareness training every three years. The technical point of contact must keep a record of training completion dates and provide ACCESS a copy of the employee's signature sheet. ACCESS requires agencies to conduct a background re-investigation every five years for all personnel who use or work on the connection to ACCESS.