Accetable usage policy for Our Company:

1. **Overview** Infosec’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Group XX company’s established culture of openness, trust and integrity. Infosec is committed to protecting 's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, Peer-to-Peer communication, and FTP, are the property of . These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.
2. **Purpose** The purpose of this policy is to outline the acceptable use of computer equipment at Group XXX company. These rules are in place to protect the employee and Group XXX company. Inappropriate use exposes to risks including virus attacks, compromise of network systems and services, and legal issues.
3. **Scope** This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by Group XXX company, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Group XXX company and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Group XXX company policies and standards, and local laws and regulation.
4. **Policy**

4.1 General Use and Ownership

* 1. 4.1.1 Group XXX company proprietary information stored on electronic and computing devices whether owned or leased by Group XXX company , the employee or a third party, remains the sole property of Group XXX company. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
  2. 4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.
  3. 4.1.3 You may access, use or share Group XXX company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
  4. 4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
  5. 4.1.5 For security and network maintenance purposes, authorized individuals within Group XXX company may monitor equipment, systems and network traffic at any time, per Infosec's Audit Policy.
  6. 4.1.6 Group XXX company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. 4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.
2. 4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
3. 4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
4. 4.2.4 Postings by employees from a Group XXX company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Group XXX company , unless posting is in the course of business duties.
5. 4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Software and application acceptable usage and licensing

1. Software may only be used in compliance with applicable license and purchasing agreements. Only authorized copying of files or programs and authorized program utilization are ethical and legal. The Information Technologies Department is charged with the responsibility for enforcing software licensing compliance for the Group XXX company. Please refer to the[IT Support Standards](http://www.css.edu/Administration/Information-Technologies/Computing-Policies/IT-Support-Standard.html) for detailed information.

**4.4 Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Group XXX company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Group XXX company -owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4.1 System and Network Activities: The following activities are strictly prohibited, with no exceptions:

a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Group XXX company.

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Group XXX company or the end user does not have an active license is strictly prohibited.

c. Accessing data, a server or an account for any purpose other than conducting Group XXX company business, even if you have authorized access, is prohibited.

d. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

e. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

f. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

g. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

**4.5 Peer to Peer Policy**

It is the policy of Group XXX company that the company’s network connections may not be used to violate copyright laws. The unauthorized reproduction of copyrighted materials is a serious violation of Group XXX company’s Internet Acceptable Use Policy, as well as U.S. Copyright Laws, as discussed above. In order to ensure compliance with the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), and law enforcement, peer-to-peer file sharing has been restricted by the company. All peer-to-peer file sharing network activity will be monitored and usage tracked. Network activity that utilizes peer-to-peer applications that have a high prevalence for distributing copyrighted material will be blocked.