Misuse of internet policy final assignment

Misuse of the Internet Policy Introduction The Company provides access to the information resources of the Internet to support employee success with their Job function. The Internet is a tool, provided for employees. The Company expects its employees to use their Internet access primarily to research relevant topics and obtain useful information. Employees are expected to conduct themselves honestly and appropriately on the Internet, and respect copyrights, software licensing rules, property rights, privacy and rights of others. Unnecessary or unauthorized Internet usage causes network and server congestion.

Unlawful Internet usage may also garner negative publicity towards CB 603 Company and exposes significant legal liabilities. Employees must take special care to maintain the clarity, consistency and integrity of the Company image and posture. Employee actions on the Internet could be taken as representation of the Company. The CB 603 Company connection to the Internet offers a wealth of potential benefits, it also open the door to some significant risks to our data and systems if appropriate security discipline are not followed. The overriding principle is that security is to be everyone’s Job.

Company employees can be held accountable for any breaches of security or confidentiality. It is the employees due diligence to report any misuse of the Internet to the Company. Purpose. The purpose of the Misuse of the Internet Policy is to outline CB 603 Company’s acceptable use of the Internet. The Policy is in place to protect the CB 603 and its employees. Use of the Internet whether for good or malicious conduct exposes the Company to risks including but not limited to virus, attacks, denial of service, data

compromise, services and legal issues. Organizational Roles and Responsibilities.

Key personnel including the CIO, ISO and Legal Representatives are outlined and described in the Organizational Roles and Responsibilities section of the CYBER IT Policy. Additional roles and responsibilities specific to this Policy are as follows: Human resource representative is responsible for execution of appropriate company actions based on the violation of the Internet use policy. Human resources must file all Policy Agreement forms Users are all employees of the company that have been granted access to the Internet and have signed the Internet Use Policy Agreement.

Scope of the Policy. This Internet Usage Policy applies to all employees of the Company are granted access to computers and the Internet to be used to accomplish their work. Use of the Internet by employees of the Company is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet is a privilege and all employees must adhere to the policies concerning Computer and Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment.

Employees may also be held personally liable for damages caused by any violations of this policy. All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by this Policy. All employees must accept and sign the Internet use policy agreement, see enclosure ##. Unacceptable use of Internet Definitions. Unacceptable use of the Internet by the Company employees include, but are not limited to the

following: Social Networking, Media and Blobbing – CYBER has strict rules and regulation regarding the use of Social Networking, Media and Blobbing.

All employees refer to the CYBER Social Media policy for guidance. Downloading/ Uploading – Downloading or pirating electronic media and software without authorization is strictly prohibited and may be subject to prosecution. Company name use – Company name use is strictly prohibited unless otherwise explicitly used for Business. Software – Software may not be downloaded without the consent of CYBER ‘ SO. New required software to fulfill Job functions must submitted in writing and presented to the ISO and a review board consisting of Team and Department leads will determine its approval.

This includes software installation. Personal use – Internet may be accessed during work hours for personal reasons as long it does not interfere with daily tasks. Employees conducting online transactions, using personal information may do so at their own risk. CYBER is not responsible for any loss or damages of personal property from online transactions. Personal Identifiable Information – PI sharing is strictly prohibited. All employees must abide by the PI Policy. Spam/Spoofing/Denial of Service will not be tolerated and will be subject to immediate action up to termination.

Instant Messaging is strictly prohibited and may tot be installed in any system. Gambling – Gambling is not permitted on company property at any time including traveling on business, company functions and through Internet use. Contests or promotions may be subject for approval by the Human Resources Department of Legal Team. Bullying – Discrimination,

harassment or use of threatening messages on the Internet on any site or email is strictly prohibited. If an employee is unsure about what constitutes acceptable Internet usage, then he/ she should ask his/her supervisor for further guidance and clarification. Disciplinary Actions.

All CYBER employees are subject to monitoring as outlined in the Employee Monitoring Policy. To ensure compliance with this policy, all employees are expected to cooperate with any investigation. CYBER Employees violating this policy are subject one or more of the following: Loss of company computing, email and/or voice mail privileges Reassignment or termination from the company and/or suspension Prosecution under applicable civil or criminal laws Copyright Infringement Laws – Section 506 of Chapter 5 in Title 17 of US Code describes criminal offenses under the copyright laws with fines of up to $150, 000.