POLICY STATEMENT

Computing and Information Network Acceptable Use

SU Policy Number: 601-001.3

ORIGINATING OFFICE

Information Technology Services

PURPOSE

The following policy contains the governing philosophy for regulating the use of Shippensburg University's computing/information network facilities and resources. Access to the University's computing/information network facilities and resources is a privilege granted solely to Shippensburg University faculty, staff, registered students, those with special accounts, and individuals using public access computers. All users of the computing/information network facilities must act responsibly and maintain the integrity of these resources. The University reserves the right to limit, restrict, or extend computing/information network privileges and access to its resources.

SCOPE

This policy applies to the use of all computing and network activity at Shippensburg University.

POLICY

Use of Shippensburg University Computer Network services constitute agreement to this Acceptable Use Policy.

Disclaimer

No Warranties: To the extent permitted by applicable law, neither Shippensburg University ("SU"), nor any person, either expressly or implicitly, warrants any aspect of this service, including any output or results of this service. This service is being provided "as is," without any warranty of any type or nature, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, and any warranty that this service is free from defects.

Assumption of Risk: The risk of any and all loss, damage, or unsatisfactory performance of this service rests with you as the user. To the extent permitted by law, neither SU, nor any person either expressly or implicitly, makes any representation or warranty regarding the appropriateness of the use,

output, or results of the use of this service in terms of its reliability, availability, or otherwise. Nor do they have any obligation to distribute updates, or provide notification of any error or defect, known or unknown. If you rely upon this service, you do so at your own risk, and you assume the responsibility for the results. Should this service prove defective, you assume the cost of all losses, including, but not limited to, any necessary servicing, repair or correction of any property involved.

Disclaimer: In no event, unless required by applicable law or agreed to in writing, shall SU, or any person be liable for any loss, expense or damage, of any type or nature arising out of the use of, or inability to use this service, including, but not limited to, claims, suits or causes of action involving alleged infringement of copyrights, patents, trademarks, trade secrets, or unfair competition.

Indemnification: To the extent permitted by law through this agreement, you, the user, agree to indemnify and hold harmless SU, its officials and employees, and any person from and against all claims, liabilities, losses, causes of action, damages, judgments, and expenses, including the reasonable cost of attorney fees and court costs, for injuries or damages to the person or property of third parties, including, without limitations, consequential damages and economic losses, that arise out of or in connection with your use, of this service, its output, or any accompanying documentation.

Terms and Conditions

User Responsibility: The Shippensburg University Computer Network user is responsible for all use of their network connections. The Shippensburg University Computer Network user will be held accountable for any violations that occur involving their computer or network connections. Users should only allow others to use their device with the full understanding of the consequences of that action. It is the responsibility of all users to maintain reasonable security and anti-virus protection for their systems. This includes using a secure administrator password, maintaining the latest operating system security updates, and regularly updating anti-virus protection with the most recent virus definitions. Systems found to be vulnerable to compromise, infected by a virus, or otherwise insecure, may be disconnected from the campus network until steps have been taken to secure and/or disinfect the system, as required. Subscribers are responsible for all network usage associated with their computer and/or network connection. This includes all network traffic originating from off-campus for the purposes of connecting to or downloading from a computer, server, or other network device on the Shippensburg University Computer Network (such as occurs with file-sharing).

In addition to the policies described in this document, as a user of university resources you are subject to applicable local, State, and Federal laws, as well as all relevant university and Shippensburg University Computer Network policies. Violations of this policy may be prosecuted under the guidelines set forth by the Swataney. Violations will be referred to the Dean of Students Office, or to the appropriate SU body adjudicating academic integrity, and/or to the appropriate local, State, and Federal authorities, as required. Shippensburg University reserves the right to investigate suspected violations using all appropriate means. Furthermore, Shippensburg University may terminate or restrict any person's access to its resources, without prior notice, if such action is necessary to maintain availability, security, and/or integrity of operations for other users of those resources. All users of university resources are expected to be familiar with and to abide by these regulations.

Anti-Virus Software

Shippensburg University Computer Network users using Windows, macOS or Linux operating systems are required to use regularly updated anti-virus software on their computer(s). Shippensburg University Technology Services provide a list of recommended free anti-virus products for use on personal devices.

IP Address Usage

Shippensburg University Computer Network users are dynamically assigned IP addresses for use with their computers or other networkable devices. The use of any Shippensburg University Computer Network IP address other than that those that have been dynamically assigned by Shippensburg University is prohibited. Your registration to the Shippensburg University Computer Network service is transferable to any Residence Hall or Academic Building location. Use of "hard-coded" or unassigned IP addresses can cause conflicts, possibly resulting in a disruption or temporary suspension of service.

Network Devices

Any computer or other networkable device connected directly to the Shippensburg University Computer Network must be registered. The use of any unregistered device is prohibited. This includes, but is not limited to, game consoles, smartphones, tablets, smart device, and any other networkable device. Users can still use these devices, but they must be properly registered. Use of network switching equipment such as switches, cellular hotspots, WiFi extenders, routers (wireless or otherwise), etc. is strictly prohibited. Only one Ethernet connection per user per data port is permitted. Use of network switching equipment for the purpose of network expansion, bridging, and/or multi-device access may result in your Shippensburg University Computer Network connection being suspended or terminated with or without prior notice. Use of network devices in a "server" capacity is strictly prohibited. Use of such devices may result in your Shippensburg University Computer Network connection being suspended or terminated with or without prior notice.

Bandwidth Utilization: Shippensburg University sizes and acquires Internet bandwidth and network resources based on past usage statistics. While every effort is made to assure ample bandwidth is available to all campus network users, unexpected peak demand may cause degradation of services to all users until additional bandwidth is installed. To manage the impact at these times, traffic may be prioritized to assure critical communications are not adversely impacted.

Scanning & Network Security: Shippensburg University collects network usage statistics about all direct connections between Shippensburg University Computer Network computers and external addresses (the Internet). This data is similar to the data collected for telephone connections: it consists of the information required to transfer the data (IP addresses, protocols, port numbers, and other routing information), the number of packets and bytes transferred, as well as a time stamp. Shippensburg University reserves the right to conduct regular security scans to check for vulnerabilities, Trojan software, or other system compromises which could be exploited by other users. All computers and networkable devices connected to the Shippensburg University Computer Network will also be subjected to initial and periodic security scans. Any systems found to be insecure or otherwise vulnerable to compromise may be refused access, disconnected from the campus network, or have access restricted until such time as the user takes the necessary steps to secure their system.

General Usage: University-owned computers and networks are governed by policies and codes as well as federal, state, and local laws. In addition, all non-university computers and servers using these networks are governed by the same policies. Among other restrictions, the operation of any commercial or for-profit enterprise, crypto-currency mining or advertising is prohibited, along with any re-sale of access or services. Illegal activities -- including, but not limited to, such practices as fraud, harassment, software piracy, and copyright infringement -- are, of course, also prohibited. In addition, IP spoofing, packet sniffing, virus distribution, or any activity that disrupts the network are violations of Shippensburg University computer abuse policies. The university reserves the right to place limited restrictions on the use of its computers and network systems in response to complaints presenting evidence of violations of university policies or codes, or state or federal laws. Once evidence is established, computers involved in alleged violations may be disconnected from the network until the situation is resolved. In the event that campus, local, state, or federal authorities request records, logs, or any other service-related data on any given user, Shippensburg University will make every reasonable effort to furnish the requested information with or without notice given to the user. Shippensburg University allows access to University servers, library resources, e-mail, and the Internet. The Shippensburg University Computer Network is designed and maintained for academic use only. Shippensburg University does not specifically bar use of network resources for additional, legal uses (such as gaming/streaming), but neither supports nor devotes network resources for such activities.

Service Interruptions: Network service may be interrupted on occasion. Shippensburg University will work to restore service as soon as practicable; however, Shippensburg University is not responsible for any losses or damages caused by service interruptions or other failures in Shippensburg University Computer Network equipment.

Statement on Peer-To-Peer (File Sharing/"P2P") Applications and Use

Shippensburg University does not specifically bar the installation or use of P2P applications on student machines. The University does not, however, support or devote resources to such applications. Use of these applications is at the user's own risk. Use of P2P applications for the purpose of "serving" content is prohibited, as this constitutes the use of your computer or networkable device in a server capacity. Any use of P2P or similar applications for the purpose of serving or trafficking protected content (i.e. copyrighted materials) may result in the suspension or termination of service without prior notice. All notices of such activity or alleged activity presented to the Shippensburg University Computer Network office will be investigated and referred to the appropriate adjudicating body in accordance with the terms set forth in this agreement.

Statement on Gaming Software

Shippensburg University does not specifically bar the installation or use of gaming consoles, devices or software on student machines used to connect to gaming platforms and/or gaming servers. The University does not, however, support or devote resources to such applications. Use of these applications is at the user's own risk.

Change of Acceptable Use Policy (AUP)

This Acceptable Use Policy is subject to change without notice. Shippensburg University may also make improvements and/or changes in the services described in this agreement at any time

without notice. The terms and conditions contained in this legal notice are subject to change without notice, and you should visit the Shippensburg University Computer Support website periodically to determine if any such changes have been made.

RESPONSIBILITIES

Technology Services and the President should be notified about violations of laws and policies governing information use, intellectual property rights, or copyrights, as well as about potential loopholes in the security of the University's computer systems and networks. The user community is expected to cooperate with Technology Services in its operation of computer systems and networks as well as in the investigation of misuse or abuse. Should the security of a computer system or information network be threatened, suspected user files may be examined under the direction of the University President or his/her designee.

While the university recognizes the role of privacy in an institution of higher learning, and will endeavor to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned IT resources, except as required by law. For example, the university may be required to provide information stored in IT resources to someone other than the user as a result of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.). In order to provide system reliability, copies of all files are maintained on backup storage devices so that even the deletion of files by a user will not guarantee their destruction. The need for system maintenance and reliability may require University personnel to have access to user's files.

Those who do not abide by the policies listed above are subject to suspension of computer/information network privileges, disciplinary actions that may result in suspension or dismissal, and possible referral to the appropriate judicial process.

Offenders may also be subject to criminal prosecution under federal or state law, and should expect the University to pursue such action. As an example, under Pennsylvania law, it is a felony punishable by a fine up to $15,000 and imprisonment up to seven years for any person to access, alter or damage any computer system, network, software, or database, or any part thereof, with the intent to interrupt the normal functioning of an organization [18Pa.C.S.3933(a)(1)]. Disclosing a password to a computer system, network, etc., knowingly and without authorization, is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software [18Pa.C.S.3933(a)(2) and (3)].

PROCEDURES

Not applicable.

RECISSION

Not applicable.

APPROVALS

President's Cabinet April 29, 2004 (Revision 1.1)

President's Cabinet August 31, 2009 (Revision 1.2)
Executive Management Team October 10, 2023 (Revision 1.3)

DISTRIBUTION:
Public