DRAKE STATE
COMMUNITY & TECHNICAL COLLEGE

Computer and Network Security Policy

1.0 Purpose

The purpose of this policy is to establish conditions for use of, and requirements for appropriate security Drake State Community and Technical College computer and network resources.

1.1 Security Statement

Drake State Community and Technical College Information Technologies has taken and continues to take all reasonable measures to secure their IT infrastructure and data resident on that infrastructure. Although it is against Drake State policy to disclose specific manufacturer and model of in-place security solutions, Drake State does rely on Stateful Packet Inspection technology that can perform Network Address Translation for both ingress and egress. Likewise, Drake also relies on Inline Intrusion Detection and Prevention with Malware filtering and blacklist capabilities. Independent Security Audits supplement the IT security position of Drake by providing insight into other security risks. These audits provide prioritized security items, thereby giving Drake additional focus on areas of concern and solutions to those concerns.

2.0 Scope

This policy applies to all Drake State Community and Technical College employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing the Drake State network.

3.0 Policy

Appropriate security shall include, but is not limited to: protection of the privacy of information, protection of information against unauthorized modification or disclosure, protection of systems against denial of service, and protection of systems against unauthorized access.

Drake State Community and Technical College computer and network resources may be accessed or used only by individuals authorized by the college. Issuance of an account to a system user must be approved by an authorized college representative. Any question with regard to whether a specific use is authorized must be referred to Drake State Community and Technical College Information Technology. (DSCTC IT).

In order to protect the security and integrity of computer and network resources against unauthorized or improper use, and to protect authorized users from the effects of such abuse or negligence, DSCTC IT reserves the rights, at its sole discretion, to limit, restrict, or terminate any account or use of computer and network resources, and to inspect, copy, remove or otherwise alter any data, file, or system resources which may undermine authorized use. DSCTC IT also reserves the right to inspect or check the configuration of computer and network resources for compliance with this policy, and to take such other actions as deemed necessary to protect college computer and network resources. DSCTC IT further reserves the right to enforce these provisions without prior notice to the user.

Drake State shall not be liable for, and the user assumes the risk of, inadvertent loss of data or interference with files or processes resulting from DSCTC IT's efforts to maintain the privacy, integrity and security of the college's computer and network resources.

3.1 Responsibilities

DSCTC IT is responsible for:

1. Implementing campus-wide security policies to protect the college's computer and network resources from intentional or inadvertent modification, disclosure or destruction.
2. Monitoring user adherence to these policies.
3. Authorizing security audits or security scans affecting computer and network resources.
4. Coordinating response to computer and network security incidents to include, but not be limited to, notification of incidents to campus security, internal auditors, and other college administrators as appropriate.
5. Requiring regular updates of all college computer and network resource software, especially those for which demonstrated security exposures are repaired.
6. Requiring strong encryption and secure authentication techniques throughout all college computer and network resources.
7. Providing services (i.e., notifications, FAQs, patches, virus software updates, instruction, security alerts, etc.) to assist individuals to maintain security on their computer and network resources.
8. Developing additional security policies as needed as technology and infrastructure mature and change.

S**ystem users** are responsible for:

1. Understanding, agreeing to and complying with all security policies governing college computer and network resources and with all federal state and local laws, including laws applicable to the use of computer facilities, electronically encoded data and computer software.
2. Safeguarding passwords and/or other sensitive access control information related to their own accounts or network access. Such information must not be

transmitted to, shared with, or divulged to others. Similarly, system users must recognize the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share or divulge such information, nor convert the same from encrypted or enciphered form to unencrypted form or legible text. Any attempt to conduct such actions by a system user is a violation of this policy.

3. Taking reasonable precautions, including personal password maintenance and file protection measures, to prevent unauthorized use of their accounts, programs or data by others.
4. Ensuring accounts or computer and network access privileges are restricted to their own use only. System users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorized computer and network access privileges to others.
5. Ensuring the secure configuration and operation of network services (e.g., WWW, anonymous ftp, shared directories, files, and printers) they may establish on machines connected to college computer and network resources.
6. Conducting or attempting to conduct security experiments or security probes or scans involving or using college computer and network resources without the specific authorization of DSCTC IT is prohibited. The intentional or negligent deletion or alteration of information or data of others, intentional or negligent misuse of system resources, intentionally or negligently introducing or spreading computer viruses, and permitting misuse of system resources by others are prohibited.
7. Respecting the privacy of electronic communication. System users must not obtain nor attempt to obtain any electronic communication or information not intended for them. In particular, system users must not attempt to intercept or inspect information (e.g., packets) en route through college computer and network resources, nor use college computer and network resources to attempt to intercept or inspect information en route through networks elsewhere.
8. Respecting the physical hardware and network configuration of college-owned networks. System users must not extend the physical network on which their system resides (e.g., wiring, jacks, wireless connections, routing devices) without proper authorization.
9. Abiding by all security measures implemented on college computer and network resources. System users must not attempt to defeat or subvert security measures. System users must not use any other network address (e.g., IP address) for a computer or network resource than has been properly assigned by an authorized system or network administrator.
10. Treating non- DSCTC computer and network resources in accordance with this policy. College computer and network resources must not be used to attempt to breach the security or security policy of other sites (either willfully or negligently). An action or attempted action affecting non- DSCTC computer and network resources that would violate this policy if performed on a Drake State campus or utilizing computer and network resources is prohibited.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History