Security Awareness Policy

1.0 Purpose

- To educate employees on cyber-attack strategies/tactics and increase awareness
- To improve cybersecurity awareness
- To minimize the risk of loss or exposure of sensitive information maintained by Drake State Community and Technical College Information Technology to cyber-attack.

Drake State Community and Technical College Information Technology department utilizes NEOED to deliver cybersecurity awareness training. The cybersecurity course contains various topics related to information technologies and cybersecurity. At a minimum, the security awareness training will be delivered and required annually. If DSCTC IT deems necessary, supplemental training may be required in addition to the annual training.

2.0 Scope

This policy applies to all college employees, including, but not limited to, faculty, staff, consultants, or other third-party representatives, using DSCTC IT-provided computing devices in public or unsecured areas. It also applies to the same population using non-DSCTC IT-provided devices on a DSCTC IT provided network in public or unsecured areas.

3.0 Policy

All individuals within scope must participate in and complete, cybersecurity awareness training as provided by DSCTC IT.

This policy is in accordance with the following regulations:
FERPA: 34 CFR Part 99 [Family Educational Rights and Privacy Act], GLB: 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (‘‘GLB Act’’), USA Patriot Act, HIPAA Security rule 45 CFR 164.312(a)(2)(iii) Implementation Specification for Access Control Standard, HIPAA Security rule 45 CFR 164.312(a)(2)(iii)]

4.0 Enforcement

Employee participation is monitored via NEOED reporting. Any college employees, including, but not limited to, faculty, staff, consultants, or other third-party representatives, found to have violated this policy may be subject to disciplinary action.