Purpose: This annex will outline how the college will respond in the event of an IT cyber-attack or disruption of IT services.

Sinclair’s Information Technology (IT) Department has extensive policies in place to prevent cyber-attacks and respond to disruptions in the IT process. Many of these policies are outlined at the following website: http://IT.Sinclair.edu.

The IT Policy Manual contains the Sinclair College Information Security Policy. This policy is necessary to ensure that the College:

- Establishes a college-wide approach to information security, including appropriate security awareness training and education for constituents.
- Complies with federal and state statutes and regulations regarding the collection, maintenance, use, and security of information assets.
- Establishes and implements prudent, reasonable and effective practices for the protection and security of information assets, including protection of sensitive and confidential information against accidental or deliberate unauthorized disclosure, modification or destruction.
- Develops effective mechanisms for responding to real or perceived incidents involving breaches of information security.

The policy includes information on roles and responsibilities, key information concepts and principles, identification and assessment of assets and risk, controls/safeguards to mitigate identified risk, and auditing, monitoring and adjusting the program.

The vice president of each college division is responsible for ensuring appropriate and auditable information security controls are practiced within their division. Each division also appoints an information security officer to partner with the IT Department’s Chief Information Security Officer (CISO) to develop, implement, and maintain appropriate and effective information security practices.

Preventing attacks includes making computer users aware of personal cybersecurity. On the above mentioned website, there is a tab for Information Security. In that section, it provides a PowerPoint Presentation for all users outlining confidentiality (PII Exposure, Fraud/ID Theft, Privacy); Integrity (Deletion, Changing); and Availability (Deletion, Lockout, and E-mail Blocking). Since users can also access Sinclair’s network from their personal computers and smart phones, the IT Department also provides information on Anti-Malware Options for Home Computers at the same website.

The college has a formal “Acceptable Use of Information Technology Policy” available on-line to all users. Such principles will assure that:

- The Sinclair College community is informed about the applicability of policies and laws as related to information technology services.
- Information technology resources are used in compliance with those policies and laws.
- Users of information technology services are informed about how concepts of privacy and security apply to these services.
- Disruptions to College information technology resources and activities are minimized.
The IT Department has a formal *Computer Incident Handling Procedure* that provides direction for preliminary activities, detection and initial reporting, containment, eradication, recovery, and post-incident activities. The IT Department has a formal *Document Incident Response Form* and flowchart which dictates the exact procedure for responding to a disaster incident.

All college computing devices have up-to-date virus protection. There are systems in place to automatically monitor all computing devices to assure that the latest virus protection is installed on each of them. If a status report reveals that proper virus protection is not installed properly on a given computing device, immediate remediation is put into effect.

The IT Department tests all of their disaster recovery systems at specified intervals. In addition, each department has its own Business Continuity Plan (BCP) aka Continuity of Operations Plan (COOP) about how it would continue operations if the main IT infrastructure was unavailable. This plan is maintained and approved by the IT Department.

The IT Department is located in a secure area in the basement of one of our buildings. Access is only available via a token – except for the server area – which requires two types of authentication. Logs are kept for everyone entering these highly restricted areas.

IT systems are continually monitored for any signs of hacking and those issues are addressed immediately.

Servers are protected by dual power inputs into each unit in the event one power system fails. Server locations are cooled by dedicated cooling systems to avoid temperature fluctuations. The IT Department is protected by dual emergency backup generators (secured) that are dedicated just to that department. If one fails, the other backup generator is automatically started. In addition, the IT Department is also protected by dedicated dual Uninterrupted Power Supply (UPS) units. These systems are tested by the Facilities Department at specified intervals. In addition, the Dayton Campus’ IT equipment is protected by its own FM200 clean agent fire suppression system and the offsite backup system is protected by the Sapphire fire suppression system. Both fire suppression systems are tested at specified intervals by the manufacturer.

Back-up computer systems are in place at Sinclair’s offsite location. Should the Dayton Campus’ servers and equipment become inoperable for any reason, the back-up system is able to run a limited version of IT processes that are necessary to meet the College’s basic IT needs. Back-up Information is available on media (at the offsite location) for a six month period and is available on media for one year at Iron Mountain.

In the event of a system failure which would require significant replacements of equipment, the IT Department has a list of equipment that will require immediate replacement and coordinates with the Business Services Department to identify appropriate vendors/ordering procedures.

The College also has Cyber Liability Insurance to provide financial protection for the College in the event of a data breach.

The IT Department classifies data by the type of information, the primary repository or owner, the confidentiality classification, and the applicable legislation or standard that applies to the data.
classification. All data classifications are restricted to those with a need-to-know, and access to data is only permitted consistent with applicable law or standard.

Events covered in this threat annex may require detailed procedures involving evacuation, accounting for all persons, communication and notification, medical care, security and recovery to follow when normal college operations are disrupted. The functional annexes that are contained in Sinclair College’s complete Emergency Management Plan contain the necessary details as outlined below:

1. For details of the evacuation procedure, see the Evacuation Functional Annex of this Manual.
2. In each of the hazards listed above, after there has been sufficient time to move to appropriate shelter areas, it will be necessary to account for persons displaced from their original locations. For details of this process, see the Accounting for All Persons Functional Annex of this Manual.
3. For details of communication about this event and for notifications procedures, see the Communications and Notification Functional Annex of this Manual.
4. Should college operations be disrupted in a significant manner as a result of these events, see the Continuity of Operations Functional Annex of this Manual.
5. Procedures for handling injuries to persons are addressed in Public Health/Medical Functional Annex of this manual.
6. For details of security procedures, see the Security Functional Annex of this Manual.
7. For details of the recovery procedures necessary for these events, see the Recovery Functional Annex of this Manual.