TOOELE TECHNICAL COLLEGE

Information Systems Plan

(ensuring the privacy, safety and security of data within the technical infrastructure)

Purpose

To ensure the confidentiality, integrity and availability all IT systems within the college's custody. This includes all data contained in these systems, whether the location is on-campus or off-campus through a contractual arrangement. The three areas of confidentiality, integrity and availability are a commonly used framework to guide policies for information security within an organization. This framework provides a solid base to ensure all elements of a successful information system are covered. Having a higher level of accomplishment in these three areas, enables the college to ensure technology is a help, not a hindrance, to student success.

Definitions

Confidentiality - A set of rules that limits access to information and ensures privacy, safety and security of the data maintained by the institution. Data must be safeguarded from theft and misuse.
Integrity - The assurance that the information is trustworthy and accurate. This includes comprehensive backups of all electronic data to ensure business continuity in case of emergency or other incident. Data must be safeguarded from abuse and damage of any form.
Availability - A guarantee of reliable access to the information by authorized people: staff or student. This includes network reliability and redundancy at all levels of the technical infrastructure.

1. Goal Area 1: Confidentiality
    a. Objective: Limit access of information systems to authorized people
        i. Strategy: Maintain good password health by all users especially by employees that have access to financial or sensitive information.
            1. The computer use agreement was updated to require complex passwords by all users
            2. Ongoing training must be implemented to help employees following good password habits, such as not writing down their passwords, using separate passwords for home and work accounts, and not using common dictionary words as part of the password.
            3. Password auditing should be performed on accounts where possible to verify that passwords are not easily hackable.
        ii. Strategy: Help foster security awareness for all employees, because this is the single most important key in keeping IT data and systems secure. Most data breaches are caused human errors.

   1. Hold ongoing security awareness training with staff members during Inservice meetings, email communication, and in person communication to increase awareness.
   2. Make sure new staff members understand the Computer Resource Acceptable Use Policy that covers the password requirements in detail.
   3. Have new employees go through FERPA training that covers what student information can and can’t be given out to the public.

iii. Strategy: Monitor network traffic to help determine if there are any unauthorized users trying to access institutional data.

iv. Strategy: The Information security policy specifies the minimum requirements for disposal of electronic media to ensure that data does not get into the hands of unauthorized individuals.

v. Strategy: When the college uses an off-site IT systems through a contractual agreement, the Director of Information Technology does research to verify that the company and systems they provide have adequate confidentiality.

2. Goal Area 2: Integrity
   a. Objective: Data must be trustworthy and accurate
      i. Strategy: An adequate backup plan must be in place for all data
         1. The Information security policy specifies what data is backed up and how often.
         2. The Director of Information Technology constantly verifies that backups are taking place and that these backups are working.
      ii. Strategy: When the college uses an off-site IT systems through a contractual agreement, the Director of Information Technology does research to verify that the company and systems they provide have adequate integrity.

3. Goal Area 3: Availability
   a. Objective: Guarantee of reliable access to the information by authorized people
      i. Strategy: Provide as much physical redundancy as possible for onsite technical infrastructure, to ensure reliable access.
         1. Examples of full redundancy currently in place:
            a. 2 sources of power for all Datacenter equipment: electric grid and generator power
            b. 3 different A/C units in main Datacenter that run off both power sources
            c. 2 uninterruptible power supplies for all Datacenter equipment with full failover
            d. 2 Firewalls with full failover
            e. 2 core switches with full failover

f. 2 Datacenter rooms at opposite ends of the building with replicated equipment and data between each room

i. 2 synchronous SANs with full failover

ii. 3 physical servers that run all the the virtual servers

iii. 2 iscsi switches with full failover

g. 2 sources of power for each distribution switch

ii. Strategy: Use of email alerts to notify Network Admin before problems create a business disruption

1. Examples include:

a. Hard drive running out of space

b. Physical Memory being exhausted on a server

c. CPU going beyond a certain threshold for a period of time on a server

d. Battery going bad on a UPS

e. Physical server going offline

f. Power supply dying

iii. Strategy: Use of cloud computing to increase availability for core systems

1. Even with all the redundancy and planning put in place for onsite technical infrastructure, it will never be able to provide the level of availability that a hosted cloud provider can guarantee. With that in mind the following critical systems have been moved to the cloud:

a. Email and some staff data files (Google Apps)

b. Phone system (Masergy)

c. Learning management system (Canvas)

iv. Strategy: When the college uses an off-site IT systems through a contractual agreement, the Director of Information Technology does research to verify that the company and systems they provide have adequate availability.

4. Goal Area 4: To ensuring that IT systems in place meet the needs of students and staff and that any difficulties with these systems are resolved in a timely manner.

a. Objective: To ensure IT systems used at the college are adequate in helping the end users to accomplish the mission of providing rewarding, competency-based, affordable, and accessible career preparation for youth and adults.

i. Strategy: Regularly review the IT systems including: plans, budget, needs, risks, etc.

1. Identify and plan for current and future IT needs inside of each educational program with the Instructors, Director of Information Technology, and Executive staff in the annual program planning meetings.

a. Develop a prioritized budget based off of these meetings.

2. The Director of Information Technology meets regularly with the Executive staff to discuss areas such as:

a. Risk assessment and mitigation
b. IT system health
c. Data restoration testing
d. Employee access to IT systems
e. Staff security awareness training
f. Planning, budget, and priorities
g. IT system documentation.

b. Objective: Removing technological barriers, especially ones that directly hinder student support or learning.

i. Strategy: Any technological barriers or issues are brought to the attention of the Director of Information Technology through: email, text, phone, or in-person communication. These issues are usually resolved quickly by the Director of Information Technology as he/she works directly with the staff member or students being affected.

1. IT support for issues that directly hinder students support or progress are always given first priority.
2. For ongoing issues the Director of Information Technology may use additional resources such as outside consulting firms, to get to the bottom of the issue.
3. Extra budget is put aside each year to purchase additional hardware to solve any unanticipated hardware related problems.