Information Technology Policies and Procedures
Information Security Policy
Effective Date: June 3, 2015
Board Approval: Nov 2, 2016
Amended: Oct 24, 2016

1. Purpose

1.1. To protect the organization's business information and any student information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability

1.2. To establish safeguards to protect the organization's information resources from theft, abuse, misuse and any form of damage

1.3. To establish responsibility and accountability for Information Security in the organization

1.4. To encourage management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimize the occurrence and severity of Information Security incidents

1.5. To ensure that the organization is able to continue its business activities in the event of significant Information Security incidents

2. Policy

2.1. IT personnel shall meet annually with the institutional leadership to review and discuss the following items:

2.1.1. Review IT risk assessment and discuss risk mitigation strategies
2.1.2. Report on the overall IT systems health
2.1.3. Report results of the yearly data restoration testing
2.1.4. Review of employee access to IT systems
2.1.5. Plans to continually train staff on IT security awareness
2.1.6. Discuss IT plans, budget and priorities
2.1.7. Review changes made in the last year and explain how proper documentation has taken place

2.2. Electronic Data Backup, and Disposal

2.2.1. The following data is backed up and retained:
2.2.1.1. Staff Documents and Desktop folders
2.2.1.2. Staff shared drive
2.2.1.3. Staff Google apps data
2.2.1.4. Student information database

2.2.1.5. Financial information databases

2.2.2. Backup of this data consists of the following:

2.2.2.1. All data whether onsite or in the cloud is backed up daily

2.2.3. Offsite Storage of Backups

2.2.3.1. Backups of onsite data are automatically replicated to offsite storage

2.2.3.2. All offsite backups are password protected and encrypted

2.2.3.3. All cloud data is backed up to another cloud provider

2.2.4. The offsite backup contains current documentation of all IT systems including:

2.2.4.1. All passwords, configuration files, and details on how to restore each IT system

2.2.4.2. All data necessary to rebuild the network on new hardware

2.2.5. Restoration testing of data files is performed at least annually to ensure data integrity and recoverability

2.2.6. All electronic media is wiped before being disposed or sent to a certified disposal center

2.2.6.1. The following standard or greater is used: Standard DoD 5220.22-M

2.3. Process to create, change or suspended a user account in any IT system:

2.3.1. Any account changes require a supervisor level or higher electronic notification requesting the creation, change, or suspension

2.3.2. The IT Staff is responsible to make these changes after electronic notification and document that they have taken place