Technology Reliability Plan 2019-2023

Woodmont College's technology system consists of a single server hosting our Wordpress-based websites, a Student Information System - Ampeducator and the Moodle Learning Management System. All are current and up-to-date.

To maintain reliability, Woodmont College follows the following technology reliability plan.

Maintenance:

Woodmont College has contracted with LiquidWeb to provide server hosting, support, backup and maintenance. Backups of data on the server are also downloaded onto a secure in-house computer for backup redundancy. This contract involves automatic updates and server maintenance.

Critical issues that may arise are emailed immediately to the college. Logs and reports are run to determine adequate disk space in relation to disk usage and system processes. LiquidWeb provides 24/7 support.

Regarding WordPress, Ampeducator, and Moodle, Woodmont College maintains a staff which reviews and updates the platform regularly. The Moodle community releases updates and bug fixes which are then integrated into the Woodmont College's Moodle platform. Wordpress plugins and updates are constantly being released, and the Woodmont Technology team tests and selects the appropriate plugins and features to enhance reliability and functionality. Ampeducator is a third-party system that is regularly updated, and also develops customizations based on the college's specific needs. Students may contact technical support via email anytime for support with any issues.

Data is stored on secure, cloud-based platforms such as Dropbox and Ampeducator. As cloud based servers, they provide backup capabilities

In addition, the IT department provides on-going maintenance via:

- adding or deleting users from a system
- modifying user rights and properties
- Security for users and the server

The Woodmont College IT Director and Educational CAO are responsible for the contact with LiquidWeb, Ampeducator and MoodleCloud and to ensure the continued reliability of all systems.

Annual Review:

At the end of the year the IT department performs a yearly review updating or upgrading hardware and software, and ensuring all links on the websites function properly. In addition, as part of the program review, internal and external stakeholders, rate their satisfaction, either through a survey or during meetings. The stakeholders suggest additions and customizations to the Moodle platform, which serve to enhance and develop the functionality of the LMS. The IT department moves to integrate those suggestions through additional plugins and/or custom code. As part of the IT review, the logs are reviewed as well as user issues that emerged during the year. IT develops solutions for these issues to prevent them from occurring the following year.

Monitoring and Assessing User Needs:

Moodle, WordPress, Apeducator and LiquidWeb, have tracking mechanisms and reports. Reports include user use, number of sessions, daily and weekly data usage.

Student satisfaction surveys measure student satisfaction with the institution's Learning Management System. Staff and faculty provide feedback during meetings and through their own faculty surveys.

Business Continuity:

Woodmont College keeps data up-to-date and reliable through proper security measures. Below is the institutions Data Security Policy:

Data Security

Purpose:
This Policy describes the responsibilities of Woodmont College staff for ensuring that sensitive data is kept secure. Failure to follow acceptable security protocols could lead to breaches that result in legal penalties and loss of important data. Controls are set to minimize risks. This policy seeks to provide a structure to identify security threats and measures needed to prevent any breach of Woodmont College Information Security Systems.

Roles:
Users: Users include any member of the Woodmont College community. Each user has a responsibility to protect all sensitive data to which the College has provided them access. All users must comply to the College's Data Security Policy.
Administrators: Administrators possess administrator rights to data systems. Administrators manage the users within their data systems.
IT department: The IT department is the staff that oversees the computer and information systems. For purposes of this policy the IT department creates the security controls that protect all sensitive information.

Data Security Manager: Data Managers oversee the classification of users and administrators and determines the college's security policies.

Classification:
Woodmont College bases the confidential classification on FERPA requirements.

Data Access:

1. Users access is kept at a minimum to only that which the user requires to perform his or her College tasks.
2. Administrators shall not alter user rights without approval by the Data Security Manager.
3. The Data Manager assigns user classifications and grant specific access to administrators and users.
4. The Data Manager supervises users access, modifying rights when necessary.
5. The IT Department will assign and maintain the access to the College computer infrastructure.

Password Control:

1. Users must create strong passwords to access confidential data.
2. Users are forbidden to share passwords including other members of the Woodmont College staff.
3. Users should not store passwords on paper.

Storage of Data:
Confidential data must be securely stored at all times.

a. Secured Data must reside on Woodmont College secured information systems and computers and not on personal computers even if password protected.
b. All access to computers which are connected to Naaleh College Information Systems must be password protected.
c. Portable devices possessing confidential data must remain with the user at all times.
d. Mobile Devices must be password protected and the device cannot be left unattended.

Transmission Data:

1. Confidential information must not be distributed to any person who does not possess the proper authorization to access that information. Any transmission must be protected from unauthorized interception.
2. Emails containing confidential information must be sent using the secure Woodmont College email system.
3. Conversations must occur in areas that unauthorized persons cannot overhear.

Physical Security

1. The Woodmont College offices and rooms containing confidential information must remain locked at all times when all personnel exist the office.

Security Incidents Reporting

1. Any suspected or actual breach to sensitive data must be reported to the Data Security manager.
2. The Data Security Manager will investigate the suspected or actual breach with the IT department.
3. The Data Security Manager will take steps to contain any loss of data and correct the situation.

Periodic Review:

1. The Data Security Manager, together with the IT department will conduct an annual review of the policy and implementation.
2. The Data Security Manager will report to the COO of the College
3. The Data Security Manager will improve the policy and modify as needed