Alice Lloyd College Information Technology Policies and Procedures And Information Systems Security Plan

Revised June 2022

Table of Contents

Purpose

To compile all of Alice Lloyd College's computing policies and create an Information Systems Security Plan that will put Alice Lloyd College in compliance with applicable statutes, federal and state laws, regulations, executive orders, guidelines, and mandates regarding the management and secure operation of agency systems. It will also strengthen the Alice Lloyd College computing system and better protect the data of the Alice Lloyd College network.

Scope

The policies and procedures set forth in this document make up the Alice Lloyd College Security Plan and are applicable to all members of the Alice Lloyd College community, faculty, staff, student, visitors, volunteers, contractors, computers, programs, applications, communications and all other hardware, including mobile devices.

Policy

This Security Plan is governed and maintained by Alice Lloyd College's Security Board and subject to an annual review.

Contingency

This plan will follow and adopt the NIST SP 800-171r1 Security Standards and shall be reviewed annually and updated as needed. All aspects of this program shall be audited and tested by the Alice Lloyd College Information Systems Security Board.

Threat Intelligence

Threat intelligence is the output of analysis based on identification, collection, and enrichment of relevant data and information.

Alice Lloyd College uses Beazley Breach Solutions (https://www.beazleybreachsolutions.com/) as a source for cybersecurity announcements. Alice Lloyd College also uses sources such as Whois Lookup, IP

Lookup, Reverse IP lookup, IP Location Finder and IP Location Finder Geolocation to gather information on data that may be considered a threat.

Glossary

Account: A username and password combination allowing authenticated access to the Alice Lloyd College network and applications.

Authentication: The process by which an individual is identified, usually with a user name and password.

Backup: To copy files to a second medium (a disk or tape) as a precaution in case the first medium (workstation or server) fails.

Restore: Move files back from a second medium to the first medium (workstation or server).

Boundary Hardware: Refers to the Alice Lloyd College firewall. Extended to its boundaries means internal access up to the firewall.

Cloud Computing: A model for enabling network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, users, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. These services provided over the internet support things including communication, collaboration, sharing, project management, scheduling and data analysis, data processing, and storage.

Information Security Board: Personnel responsible for coordinating the response to computer security incidents.

Encryption: A process that converts data from its original form to a form that can only be used by authorized users.

Exploit: A tool developed by hackers that is used to perform malicious attacks on computer systems. A security exploit is an unintended and unpatched flaw in software code that exposes it to potential unauthorized access or compromised integrity.

Firewall: Firewall systems prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls may also be referred to as a network boundaries.

File Sharing: The sharing of files in a network environment allowing multiple people to access the same file.

Hard Copy: Information in paper format, whereas a soft copy exists in electronic format. Electronic copy may also be referred to as a digital copy.

Information System Component: A discrete, identifiable information technology asset (i.e., hardware, software, firmware, or media (electronic and hardcopy)) that represents a building block of an information system. Information system components include commercial information technology products.

Information Systems: A discrete set of information system components (servers, switches, hubs, routers, access points, etc.) organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. These typically make up the Information Technology Network.

Local Area Network (LAN): A data communications network spanning a limited geographical area. It provides communication between computers and peripherals. A LAN is inside of the firewall.

Malware: Short for malicious software. Malware is software designed specifically to damage or disrupt an information system.

Media: In computers, storage media is any technology used to place, keep and retrieve data. Although the term media usually refers to hardware storage (CD-ROM, USB drives, hard drives and backup tapes). Media is also inclusive of hard copy media.

Media Destruction/Sanitization: The process of cleansing or destroying all or part of a storage device so that the data it contained is cannot be recovered.

Mobile Device: Any portable device capable of receiving and/or transmitting data that may also be capable of making phone calls and/or accessing any or all of the following: e-mail, internet, servers, documents or systems. These include, but are not limited to, laptops, tablets, and smart phones.

Offsite Storage: Storage of critical data away from the agency Data Center for data recovery and disaster recovery purposes.

Patch: A piece of software designed to update a computer program or its supporting data, in order to fix or improve it.

Personally Identifiable Information (PII): Protected information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Protected Information: Information protected by State and Federal Laws or State Policies. Examples include, but are not limited to employee, student, and teacher identifiable data. This also includes information covered under FERPA and HIPPA.

Removable Media: Any portable device capable of storing data including data categorized at a confidential or greater level. These include, but are not limited to, USB drives, CD-ROMs, DVDs, portable hard drives, smart phones or secure digital ("SD") cards.

Remote Access: The ability to remotely access an information system from outside the network.

Risk: The degree to which accidental or unpredictable exposure of information, or violation of operations integrity due to an oversight or the malfunction of hardware or software, that could affect Alice Lloyd College processes, functions or responsibilities.

Risk Assessment: The identification of risks through the examination of the potential harm that may result if the risk occurs.

Risk Management: The entire process of assessing risks, evaluating risks, and then deciding on priorities for mitigating actions so that resources are available and actions can be taken to manage the risk.

Security Incident: A change in the everyday operations of an information system, indicating that a security policy may have been violated or a security safeguard may have failed. These may be infestation, hacking or data breach, or a combination of any of the three.

Sensitive Information: Sensitive information is defined as information which, if made available to unauthorized persons, may adversely affect Alice Lloyd College, its programs, faculty, staff, students or other participants served by its programs. Examples include, but are not limited to, personal identifiers and financial information.

Social Engineering: A term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. Social engineers rely on the natural helpfulness of people as well as on their weaknesses.

Spam: Most spam is considered to be electronic junk mail or junk newsgroup postings that is unsolicited and sent to a mailing list or newsgroup.

Trojan: Software designed specifically to damage or disrupt an information system.

User: An individual, automated application, or automated process that accesses any component of the Alice Lloyd College network.

Vendor: An external authorized individual or organization that provides services or manages a component of the Alice Lloyd College network or data. May also be called a 3rd party or a service provider.

Virtual Private Network (VPN): A secure network technology connecting distant locations over a secure channel.

Virus: Software designed specifically to damage or disrupt an information system.

Vulnerability: Flaws or security holes in a program or IT system, often used by malware as a means of infection.

Worm: Software designed specifically to damage or disrupt an information system.

Gramm-Leach-Bliley Act

Purpose

The Gramm-Leach-Bliley Act ("GLB"), together with an implementing Federal Trade Commission ("FTC") "Safeguards Rule," regulates the security and confidentiality of customer information collected or maintained by or on behalf of financial institutions or their affiliates. Because Alice Lloyd College is classified as a financial institution under GLB, by virtue of processing or servicing student loans, or offering other financial products or services, the College has established this Information Systems Security Plan (the "Plan") to assure compliance with GLB and the Safeguards Rule. As required by the Safeguards Rule, the Plan is designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Scope

The contents of this policy apply to all the Alice Lloyd College community, its networking infrastructures, servers, firewalls and data.

Policy

Alice Lloyd College complies with and requires its employees and other agents to comply with, all applicable federal, state, and local laws and regulations, as well as College policies and procedures, that govern information security, confidentiality, and privacy. This Information Systems Security Plan incorporates, by reference, future and existing college-wide or departmental policies and procedures that address the security and confidentiality of data encompassed by the definition of "covered data" given below.

Definitions

Customer information is defined as any record containing non-public, personally identifiable financial information, whether in paper, electronic, or other forms, that the College obtains from a student, a student's parent(s) or spouse, employee, alumnus, or other third party, in the process of offering a financial product or service; or such information provided to Alice Lloyd College by another financial institution; or such information otherwise obtained by the College in connection with providing a financial product or service. Examples of customer information include names, address, phone numbers, bank and credit card account numbers, income and credit histories, as well as Social Security Numbers. In general, the financial products or services offered by a college or university, including student loan programs and other miscellaneous financial services as defined in 12 CFR & 225.28.

Covered data is defined as all information required to be protected under GLB. This includes customer information, as well as financial information that the College, as a matter of policy, has included within the scope of this Plan, whether or not such information is covered by GLB. This may include financial and personal identifying information obtained by the College outside of a financial service transaction covered by GLB. Service providers are defined as all third parties who are provided access to covered data. Examples of service providers include businesses retained to transport and dispose of covered data, collection agencies, and systems support providers.

Information Systems Security Plan Components

GLB requires financial institutions to develop, implement, and maintain a comprehensive Information Systems Security Plan that contains administrative, technical and physical safeguards appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information it handles. The five components of the plan require each institution to:

1. Designate one or more employees to coordinate the safeguards; (This individual will be referred to as the Security Officer, and will be the Officer of the Alice Lloyd College Security Plan Board)
2. Identify reasonably foreseeable internal and external risk to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of the current safeguards for controlling these risks;
3. Design and implement information safeguards to control the identified risks, and ensure that the effectiveness of these safeguards is regularly tested and monitored;
4. Select service providers that can maintain appropriate safeguards and require them, by contract, to implement and maintain such safeguards; and
5. Evaluate and adjust the Information Systems Security Plan based on the results of the testing and monitoring, any material changes to operations, or any other circumstances that have or may have a material impact on the Information Systems Security Plan.

Information Systems Security Plan Coordinator

The GLBA Information Systems Security Plan Coordinator will be referred to as the Security Officer of the Alice Lloyd College Information Systems Security Plan Board, a board implemented to assist the Security Officer with his or her duties to oversee the GLBA compliance and the Alice Lloyd College Information Systems Security Plan. This Board is discussed in the next policy - Security Board. The Security Officer, along with members of the Security Board, is responsible for implementing and maintaining this Plan. They are to work along with the Information Technology Office, the Center for Student Service, the Registrar's office, the Director of Financial Aid, Business Office, Human Resources, and all other relevant academic and administrative organizational units. The responsibilities of the Security Officer are lined out in the next section of policies, the Security Board.

Risk Identification and Assessment

Under the guidance of the Security Officer, the Security Board is to:

- Take steps to identify and assess internal and external risks to the security, confidentiality, and integrity of Alice Lloyd College data. At a minimum, this process is to consider the risks to covered data, and the safeguards currently in place to manage those risks, in each relevant area of college operations including: employee management and training; information systems, including network and software design; as well as information processing, storage, transmission, and disposal for both paper and electronic records; and security management, including threat, detection, and response to attacks, intrusions, or other system failures.
- Establish procedures for identifying and assessing risks in each relevant area of the College's operations outlined above.
- Perform the risk identification and assessment. Risk assessments are to include system-wide risks, as well as risks unique to each area with covered data. The Security Officer is to ensure risk assessments are conducted at minimum annually, and more frequently where required.

Information Safeguards and Monitoring

The Security Officer along with the Information Security Board is to design and implement reasonable safeguards to control identified risks to the security, confidentiality, and integrity of that data, and that the effectiveness of these safeguards is monitored regularly. Such safeguards and monitoring are to include the following:

Employee Management and Training Safeguards for information security are to include the management and training of those individuals with authorized access to covered data. In consultation with the Information Technology Office and other responsible organizational units, the Security Officer is to identify categories of employees and others with access to covered data. The Security Officer is to work with the Security Board to develop appropriate training and education programs for all affected current and new employees. These programs will be a component of the New Employee Orientation Program conducted by Human Resources. Training and education may also include brochures, websites, and other means of increasing awareness of the importance of preserving the confidentiality and security of covered data.

Information Systems Information systems include network and software design, as well as information processing, storage, transmission, and disposal. Each affected organizational unit is to implement and maintain in writing administrative, technical, and physical safeguards to control the risks to information systems, as identified through the unit's risk assessment process. Safeguards are to be designed and implemented in accordance with the nature and scope of a unit's activities and the sensitivity of the covered data to which it has access. The Security Officer, the Security Board, and the Information Technology Office, are to work on the design and implementation of safeguards. Safeguards may include: creating and implementing access limitations; using secure, password-protected systems, and encrypted transmissions within and outside the College for covered data; regularly obtaining and installing patches to correct software vulnerabilities; prohibiting the storage of covered data on transportable media (floppy drives, zip drives, etc.); permanently removing covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media prior to disposal; storing physical records in a secure area with limited access; protecting covered data and systems from physical hazards such as fire or water damage; disposing of outdated records under a document disposal policy; and other reasonable measures to secure covered data during the course of its lifecycle while in the College's possession or control.

Security Management and Managing System Failures In consultation with the Information Technology Office and the Security Board, the Security Officer is to develop and implement effective procedures for preventing, detecting, and responding to actual and attempted attacks, intrusions, and other systems failures. Such procedures may include implementing and maintaining current anti-virus software, maintaining appropriate filtering or firewall technologies, regularly obtaining and installing patches to correct software vulnerabilities, imaging documents and shredding paper records, regular data back up and off-site storage, implementing incident response plans, and other reasonable measures. The Security Board will assure that all incidents are reported by the Information Technology Department.

Monitoring and Testing In consultation with the Security Board and Information Technology Office, the Security Officer develops and implement procedures to test and monitor the effectiveness of information security safeguards. Monitoring may include sampling, sending Phishing emails, systems checks, systems access reports, and any other reasonable measures adequate to verify that the Plan's safeguards, controls, and procedures are effective.

Service Providers and Contract Assurances
The Security Officer is to identify service providers with access to covered data and the organizational units that provide this access. Working with these units, the Security Officer is to ensure that reasonable steps are taken to select and retain service providers that can maintain appropriate safeguards for covered data, and are to require service providers, by contract, to implement and maintain such safeguards. The security officer is to request a SOC2 report or its equivalent (SSAE18) from each service provider. If these are not made available, documented contact information for whom to contact in case of an incident shall be kept. SOC2 and equivalent reports that are made available shall be documented and evaluated for assurance of GLB compliance through a vendor review document geared towards GLB compliance. The institution is to take steps to ensure that all relevant future contracts incorporate a "GLB compliance clause" that requires service providers to implement and maintain safeguards for covered data.

Periodic Review and Adjustment of Plan
The Security Officer, working with the Information Technology Office and Information Security Board:

- Is to evaluate and adjust annually the Plan in light of the results of the testing and monitoring described above, as well as any material changes to operations or business arrangements, including changes in technology, the sensitivity of covered data, and the nature of internal and external threats to information security, and any other circumstances that may reasonably impact the Plan.

- Is to review the Plan annually to assure ongoing compliance with GLB and the FTC Safeguards Rule, as well as consistency with other existing and future laws and regulations.

The following policies defines the Information Systems Security Plan Board and defines policies to make up the Alice Lloyd College Information Systems Security Plan.

Security Board

Purpose
The purpose of this section is to compile a Security Board, name its Security Officer and list its responsibilities.

Scope
This applies to the Security Board and all aspects of the Alice Lloyd College Information Systems Security Plan.

Policy
Hospitals, colleges, and universities are increasingly targeted by cyber criminals, each looking for a way inside of your network and obtaining credentials and data. Due to this increase and to abide by governmental standards (GLBA, NIST SP 800), Alice Lloyd College has made protecting data and the integrity of the Alice Lloyd College network, users and computers a top priority.

This policy is to establish an Information Technology Security Board and to designate a security officer and layout the standards and responsibilities of the Board.

An Alice Lloyd College Information Security Board has been developed and made up of:

- VP of Finance at Alice Lloyd College
- The Director of Human Resources
- The Director of Financial Aid
- The Director of Enrollment Management
- The Director of Information Technology

The Human Resources director will be named the Information Security Officer. The Information Security Officer will be ultimately responsible for Alice Lloyd College's security plan strategy to ensure Alice Lloyd College assets and data is protected.

This position shall have extensive training in Information Security, has an understanding of the Alice Lloyd College data, the authority to perform certain functions within the security policy and be able to work closely with the Information Security Board.

The Security Board shall write up a set of policies and procedures that shall in a whole make up the Alice Lloyd College Security Plan, including this policy in its plan.

The Security officer's task, along with the assistance of the Security Board, shall consist of:

- Working with appropriate organizational units to ensure that adequate training and education programs are developed and provided to all employees with access to covered data, and that existing policies and procedures that provide for the security of covered data are reviewed and adequate. The Security Officer is to make recommendations for revisions to policy, or the development of new policy, as appropriate.
- Consult with responsible organizational units to identify service providers with access to covered data, ensure that all such service providers are included within the scope of this Plan, and maintain a current listing of these service providers.
- Develop, manage and improve a comprehensive information security risk-based program to ensure the integrity, confidentiality and availability of information assets.
- Ensures that organization maintains compliance with federal and state laws related to privacy, security, confidentiality, and protection of information resources.
- Performs ongoing risk assessments and audits to ensure that information is adequately safeguarded pursuant to applicable law and certification requirements.
- Establish and implement a process for incident management to effectively identify, respond, contain and communicate a suspected or confirmed incident.
- Identify, assess, and prioritize IT risks to data and systems, including external threats, cyber-crimes, internal threats and third-party risks. Advise relevant stakeholders on the appropriate courses of action to mitigate or eliminate risk.

The Security Board shall look at the threat landscape applicable to Alice Lloyd College and the existing Information Security Program to enumerate Key Risk Indicators (KRI) which can be used to determine how well the organization is managing its information security risk. A Key Risk Indicator (KRI) is a metric for measuring the likelihood that the combined probability of an event and its consequence will exceed the organization's threshold and have a profoundly negative impact on an organization's ability to be successful.

Identifying key risk indicators requires an understanding of the organization's goals. Each KRI should be able to be measured and accurately reflect the negative impact it would have on the organization's key performance indicators. Once these indicators have been determined, a process should be implemented or compiling data used and quantifying these indicators to measure Key Risk Indicators on a periodic basis to measure performance over time.

Examples of Key Risk Indicators are:

- Disasters, Outages, Disruption
- Resolution Time
- IT incidents/Investigations

The Director of Information Technology shall use this data to provide reports as needed that show statistics from these Key Risk Indicators.

Special reports may be asked to be submitted from the Director of Information Technology on occasion to submit to the Alice Lloyd College Board of Trustees.

What Data Must Be Protected?

Data that must be protected is described as Personally Identifiable Information (PII) (and referred to as Confidential Data, Sensitive Data or just "data" in these policies) and consist of:

- Social Security Number
- Driver's license number
- Credit/debit card numbers
- Passport number
- Bank account information
- Date of birth
- Medical information
- Biometric data (for example, fingerprints)
- Mother's maiden name
- E-mail/username in combination with password/security question and answer

Critical questions to answer:

- What type of PII data does Alice Lloyd College have?
    - Alice Lloyd College has PII data consisting of
        - Social Security Number
        - Driver's license number
        - Credit/debit card numbers
        - Passport number
        - Bank account information
        - Date of birth
        - Medical information

- How much PII data does Alice Lloyd College have?
    - Alice Lloyd College has PII data for its students, past students, prospective students, faculty, staff and donors.
- Who has access to the organization's PII and where it is stored?
    - Administrators, the Registrar's office, Business Office, Admissions, Financial Aid, Student Services, the Education Office, Dean's offices, Development and Alumni Offices have access to Alice Lloyd College's PII data.
    - The majority of this data is in SQL databases, while some is stored in password protected Excel documents.
- How is the organization protecting its PII data?
    - Alice Lloyd College is protecting its PII data with this Information Systems Security Plan.

1.1 Access Control

Account Access Policy

Purpose

The Account Access Policy is to establish rules for user accounts and define common across-the-board schemes.

Scope

This policy applies to all the Alice Lloyd College community users.

Policy

Only authorized users are granted access to Alice Lloyd College computing. Users are limited to specific applications and levels of access rights. Computer and application system access is to be achieved via password protected user IDs that are unique to each individual user to provide individual accountability and any user accessing the Alice Lloyd College network must be authenticated through this user ID.

All users shall abide by all the Alice Lloyd College Information Technology Policies and Procedures as set forth in this set of policies and laid out under General Responsibilities, Statement of Ethics and Copyright/Peer to Peer.

Faculty/Staff

After notification from the Human Resources office that there has been a new JBS/ALC employee, then the user ID(s) is/are created.

The Human Resource office provides the correct first and last name as well as the associated ID number and the corresponding department.

- The computer account will be created in the form of firstnamelastname (bobdoe). This account will also be their email login structure with the domain being @alc.edu, such as bobdoe@alc.edu. Needed exceptions are taken place if an account name of this format already exists.
- Passwords will be random, case sensitive, alphanumeric, and will consist of eight characters. Please contact the Information Technology office if you need assistance in having your password changed. Passwords will be changed from time to time to maintain the security of the Alice Lloyd College network. (Please see Password Complexity)
- Access to their "MY DOCUMENTS" will be set up on the data server for security and back-up purposes with access to no cached documents.
- Users will be assigned an EagleNet account, with the appropriate role, with the same firstnamelastname (bobdoe) structure as email and a password of the same complexity requirements.
- Users will be granted access to information/application/shares on a "need-to-know" basis or the principle of least privilege. That is, users will only receive access to the minimum applications and privileges required to perform their jobs other than what is specified by the new employee's direct supervisor. The direct supervisor will direct the IT department on what kind of "extra" access to assign to new employee such as:
    - Do they need Jenzabar access?
    - What modules? What permissions?
    - PowerFaids access?
    - Do they need access to a shared folder or to be part of an email distribution group?

- Jenzabar access will be assigned if needed, with a username of the lastname_firstname (doe_bob) structure. They will become a member of the appropriate group as needed. (Admissions, Development, etc.). The password will once again follow the eight-character password complexity.
- PowerFaids accounts will be given to new Financial Aid employees. These accounts will be in the format of the firstnamelastname (bobdoe). Passwords will follow the PowerFaids password complexity to the minimal.
- All employees with a desk will receive an IP phone, Long Distance Code, and computer workstation. Workstations will be named firstinitiallastname (bdoe) and set as:
  - Account lockout after 3 attempts of invalid password. Account will auto unlock after 15 minutes.
  - Computer sessions lock with a password protected screensaver after 15 minutes of inactivity. To gain access again, the employee will need to enter their password.
  - They will have a logon session of 10 hours. After that, they will be automatically logged off the workstation.
  - The user will be a domain user and will not have access to administrator abilities on the local workstation. This will protect the integrity of the computer by not allowing malware to be written to the registry and help keep software installations down.
  - Local administrator account will be disabled.
- Any special equipment will be provided as needed such as laptop, phone, tablet, etc. as specified by the direct supervisor.
- Remote Access will be given to employees upon the request of the direct supervisor. (Please see Remote Access Policy)

Students

- Student accounts are created after notice from the Admissions department of the student's acceptance into Alice Lloyd College.
- The computer login account will be created in the form of firstinitialmiddleinitial_lastname (bk_doe). This account will also be their email login structure with the domain being @alicelloyd.edu, such as bobdoe@alicelloyd.edu. Needed exceptions are taken place if an account name of this format already exists.
- Passwords are generated in the form of the last four digits of their Social Security number followed by their initials. From time to time, random special characters are included for security purposes to throw off the "form" of the password.
- Student accounts are restricted and only get access to a shared folder that contains course syllabi and lecture copies as made available by faculty. They do not have access to save their documents to a computer, nor do not get any kind of remote access.
- No new student accounts will be created for the fall semester any earlier than the 2nd Saturday in June, or the week of fall finals for incoming spring students.
- Certain departmental student workers receive Jenzabar accounts. This layout will be the same form as Alice Lloyd College employees. Jenzabar accounts are examined every semester and those that no longer need access will be purged.

Other/Vendor

Accounts are not given to volunteers but are given to those receiving a stipend. From time to time, special accounts may be generated to suit the purpose of an application. These are named accordingly as best as they can to match what they are detailed for and follow the same eight-character password.

Email

- Will be provided via Office365
    - Can be accessed through Outlook, Webmail or your mobile device (see Mobile Device Policies)
- Email shall be used primarily for Business.
- Represent yourself in a professional manner.
- No forwarding rules will be sat by the Alice Lloyd College Information Technology Office and this practice is discouraged.
- Email shall not be used for chain letters, spam, profit, harassment, phishing, pornographic material, etc.
- Accessing or attempting to access someone else's email is prohibited.
- Do not attempt to pose as someone else when sending email, except when specifically authorized to do so.
- An email user must not give the impression that he/she is representing, giving opinions, or otherwise making statements on behalf of Alice Lloyd College unless appropriately authorized.
- Protected information should not be sent or received via Alice Lloyd College email or as an email attachment in clear text. The information must be protected in a way that prevents access to anyone other than the intended recipient.
- Employee email requires MFA.

Deactivation (see Termination process)

- Staff accounts are deactivated upon the day of departure from Alice Lloyd College or as the need for the application/access is no longer there. This applies to computer accounts, email, remote access, PowerFaids and Jenzabar and will also take effect on any share that the user had access to.
- Computer and email accounts for departing faculty will be terminated 2 weeks following graduation, or two weeks after the planned graduation date if the graduation event is not held for some reason. The only exception to this is if the faculty member will be providing services for Alice Lloyd College that will take longer than the two allotted weeks, and the request will need to come from the Academic Dean. Other accounts (Jenzabar, etc.) will be deactivated upon the day of graduation or when the need for the application/access is no longer there.
- Student graduates are given 30 days from the last day of finals before their accounts are purged. No exceptions, nor any forwarding rules will be sat by the Alice Lloyd College Information Technology Office.
- Students whom withdraw will have their email account purged the day the Registrar's office notifies of the student withdrawal.
- Students whom simply don't return will have their accounts purged upon receiving notice of non-returning students from the Alice Lloyd College Registrar's Office.
- Accounts cannot be recreated for any reason.
- Certain issues may require that accounts and access be deactivated before the notice of any termination to protect the data and assets of Alice Lloyd College, or accounts may need to be terminated before the set termination time. This notice would need to come from the employee's direct supervisor or line officer and should be made in writing.

Statement of Ethics

The Information Technology policy is in accordance with Alice Lloyd College Guidelines on the Ethical Use of Information Technology and comprise a portion of the Standards of Employee Conduct. Where there is any question, the more restrictive policy will apply. This statement of ethics in the use of computers applies to all faculty, staff, and students. The Office of Information Technology provides service to all personnel at Alice Lloyd College and June Buchanan School. All users have the responsibility to use computing technology resources in an effective, efficient, ethical and lawful manner. The ethical and legal standards that are to be maintained are derived directly from standards of common sense and common decency that applies to the use of any public resource. Violation of any of the conditions is considered to be unethical and possibly unlawful. In accordance with established College practices, violations may result in disciplinary review, which could result in legal action. Access to any Alice Lloyd College/June Buchanan data shall kept confidential.

It is the responsibility of all Users to read and follow this policy and all applicable laws and procedures. In addition, when using the Alice Lloyd College Computing Resources, Users must adhere to the following rules:

General Responsibilities

1. Use of data records and computer hardware must be employed only for the purpose in which they are intended. This is governed by the Federal Computer Fraud and Abuse Act 1986. ALC-supported computing includes authorized research, word processing, instructional, and administrative activities and only for the purpose of supporting the needs of the institution. Do not use the institution's Computing Resources to violate other policies or laws. Computing resources cannot be used for commercial purposes or monetary gain. **All data is to be kept confidential and cannot be shared. Do not leave sensitive data laying around for others to see**.
2. Computer users must not search for, access, print or copy directories, programs, files, disks, or data not belonging to them or attempt to do so unless they have specific authorization to do so. Programs and data provided on ALC central computers cannot be downloaded or taken to other computers without permission. ALC equipment or software may not be used to violate the terms of any License Agreement (See Peer-to-Peer and Copyright). Do not use any of the Company's Computing Resources for inappropriate purposes.
3. Individuals should not encroach on others' use of the computer. This includes such activities as trivial applications, sending frivolous or excessive messages or email either locally or over the networks or running inefficient programs. Honor the privacy of other Users.
4. **Keep your passwords secure**. Do not lend them to anyone nor ask anyone else for their passwords. Do not allow anyone else to sit down at your signed-on sessions. Do not allow another user to access your accounts. Use only the institution's account(s) you are authorized to use.
5. Individuals must not attempt to modify systems, system facilities, or attempt to crash the system or attempt to subvert the restrictions associated with computer account or the networks of ALC. This includes no hacking, phishing, network sniffing, port scanning, spoofing, denial of service, spamming, introduction of malicious software/virus, etc. Proxy servers, VPNs, and other ways of attempting to hide your identity may not be used. Personal networking equipment shall not be joined to the Alice Lloyd College network.
6. Surfing peer-to-peer sites (see peer-to-peer policy), adult oriented sites and other non-ethical sites are against policy. Pornographic material is a violation of Alice Lloyd College's sexual harassment policies.

Avoid phishing emails and other types of email and attachments that may be harmful to the Alice Lloyd College network.

Disclaimers

Alice Lloyd College has a firewall which will ensure content filtering. (Blocking inappropriate Internet sites and protocols). Please note that any site you access will be logged and the Information Technology Director will be able to see the sites you have visited in these log files. Alice Lloyd College is not intentionally tracking what you do, but it is a part of the software and would be something that could be subpoenaed for legal purposes should anything criminal or illegal ever happen regarding the Alice Lloyd College campus. If information is ever needed for legal or law enforcement purposes, you will be held accountable for what was accessed from your computer.

To ensure the continuity and safety of the Alice Lloyd College network and its data, the Information Technology office has the right to perform a password change and/or access a mailbox for cleanup without your knowledge as needed due to virus infection, a compromised mailbox, a compromised account, breached password, etc. You will be notified of the change time permitting and you will be given a new password when it can be verified that your computer/mailbox is clean.

Peer-to-Peer and Copyright

Purpose

To implement a policy on copyright laws and the use of peer-to-peer software.

Scope

This policy applies to all the Alice Lloyd College community users.

Policy

Unauthorized distribution of copyrighted material by any means including peer-to-peer file sharing is against Alice Lloyd College policy. Downloading or sharing copyrighted materials, such as music and movies, without the owner's permission is a violation of federal copyright law and a violation of Alice Lloyd College's Computer and Network Policy. Alice Lloyd College is required by law to provide this notice to you each year.

Copyright violations may result in College disciplinary action and even criminal prosecution. Per the requirements of the Digital Millennium Copyright Act (DMCA), when copyright holders or industry groups like the Recording Industry Association of America contact the College about specific incidents of infringement, the College must respond by removing or disabling access to the infringing material. Per College policy disciplinary action may include loss of network access privileges or even dismissal, and the College will cooperate fully with any criminal investigation. Unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject you to civil and criminal liabilities. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at no less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq. Copyright applies to all unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, movies, software and the installation of any copyrighted Software for which Alice Lloyd College does not have an active license is strictly prohibited.

Separation of Duties / Dual Control

Purpose

To compose a policy of separation of duties to cut down on malevolent and unlawful activity.

Scope

This scope applies to the employees of Alice Lloyd College.

Policy

The "separation of duties" is defined as the assignment of responsibilities such that no one individual or function has control over an entire process. The principle of "separation of duties" manages conflict of interest, the appearance of conflict of interest, and potential fraud.

Dual Control is a control procedure whereby the active involvement of two people is required to complete a specified process. Such control may be physical, e.g. two persons required to unlock the Data Safe, or logical, as in the case of a higher-level authorization password required to permit the entry of data created or amended by another person.

Dual Control is one of the foundations of Information Security as it is based upon the premise that, for a breach to be committed, then both parties would need to be in collusion and, because one should always alternate the pairs of people, it would require a much greater level of corruption in order to breach dual control procedures; especially is such procedures require nested dual control access, such that two pairs of people are required to enable access.

To help reduce the risk of malevolent activity and addressing the potential of abuse of authorized privileges, this Separation of Duties Policy was designed.

Whenever possible, Alice Lloyd College will separate duties when it comes to Alice Lloyd College's network, systems, applications, processes and data, meaning that at least two individuals will have access to any system or application where malevolent activity may occur.

Jenzabar/PowerFaids houses data such as Social Security Numbers, Alice Lloyd College ID numbers, payroll, grades, loan information, etc. This is an area that could result in highly unlawful activity, such as changing a grade or changing payroll. In each of Alice Lloyd College's major groups of these applications, there are at least two individuals to attempt to prevent this activity. These groups listed below are malevolent areas and always have double duties as needed:

- Registration
- Payroll
- Human Resources
- Financial Aid
- PowerFaids
- Admissions

A security board has been composed of and a security officer appointed. This position will not be a member of the Information Technology Department, thus separating the duties of overseeing the compliance of the security plan from the duties of the Alice Lloyd College Information Technology Department.

Least Privileged and Privileged Accounts

The principle of least privileged should be followed, including for specific security functions and privileged accounts. This means that a privileged account should not be used for every day task, such as word processing and web browsing.

Elevated user privileges

The user shall follow these rules:

- Users must be aware of potential problems that can occur when accessing web sites
- Users must not download programs through untrusted sources
- Users must read warnings carefully when accessing web sites or installing programs
- Users must research alerts that warn against certain sites or programs before downloading content
- Users must keep anti-virus programs up to date
- Users must keep the operating system up to date (patched), and configure the workstation for automatic updates
- If a user with "elevated user privileges" misuses the access privileges, disciplinary actions will be taken. At a minimum, repeat offenders will lose "elevated privileges."
- Users will not have a privileged account on their local workstations.

Session Management

Purpose

This policy defines the requirements for local or remote sessions.

Scope

The policy applies to all individuals accessing any Alice Lloyd College computing.

Account Lockout Policy

All Alice Lloyd College accounts (faculty, staff and students) are subject to the account lockout policy.

If the password is entered wrong 3 times in a row, then the account will lock out for 15 minutes. After the 15 minutes are up, the account will automatically unlock. A support call can be placed before the 15 minutes and a member of the Alice Lloyd College IT department will assist in unlocking, once they are verified to be the owner of the account.

This applies to initial log in, unlocking a locked screen, webmail email access, wireless access and attempting to log into Jenzabar and PowerFaids.

Session Lockout policy

All Alice Lloyd College computers are joined to the domain and are subject to session lock out. After 15 minutes of screen inactivity, the computer will lock, and a screensaver of a black screen will occur. Before the user can regain access to their computer, they will need to enter their password to continue their session.

This will also apply to the connection for Jenzabar and PowerFaids.

Session Time Outs
Session timeouts for computer log-on are set to 10 hours. VPN sessions time-outs are set to 3 hours.

Remote Access

Purpose
To define a policy for the use of Remote Access.

Scope
This policy applies to Alice Lloyd College potential and current Remote Access users.

Policy
Remote access is a privilege and is granted only to remote users who have a defined need for such access, and who demonstrate compliance with Alice Lloyd College's established safeguards which protect the confidentiality, integrity, and availability of information resources.

Remote Access for an employee must be requested by the employee's direct supervisor and approved by the Director of Information Technology.

Multifactor authentication is required for VPN users, authenticating against the DUO app on smart phones. Requiring a second form of authentication will help secure VPN accounts and connections. MFA will be required upon logging into the laptop as well as connecting the VPN for any employee that has access to Social Security numbers, thus protecting the use of the laptop as well as the VPN account.

Remote Access accounts are not to be shared with others.

A VPN account will be created, and the credentials given to the employee. The VPN software will be installed on an Alice Lloyd College owned piece of equipment. To ensure that adequate updates, patches and virus/malware protection is accounted for, **VPN software will not be installed on a personal computer**. In some special, but rare cases, an alternative to a VPN account may be given, such as RDP with firewall rules or a temporarily TeamViewer Session. The procedure is decisive upon the choice of the Director of Information Technology.

All individuals connecting remotely shall only connect to or have access to machines and resources they have permission and rights to use.

Vendors play an important role in the support of hardware, software, management, and operations for Alice Lloyd College so at times Remote Access may be given to such vendors (see Vendor Management and Logical Access).

Alice Lloyd College employees and authorized third parties/vendors using the remote access must ensure that unauthorized users are not allowed access to internal Alice Lloyd College networks and associated information/data. If you have an active remote access session established, no one else is to use the computer, including family members and please do not leave the computer unattended.

Alice Lloyd College Employees and authorized third parties/vendors shall comply with all applicable policies, procedures, and agreements including but not limited to policies in the following areas:

- Safety
- Privacy
- Security

- Auditing
- Software Licensing
- Acceptable Use

Remote Access users shall not try to infringe on other parts of the network or try to use other applications other than what they have access to. Unethical browsing, such as adult material, peer to peer, and crack sites is unaccepted through remote sessions. Individuals must not attempt to modify systems, system facilities, or attempt to crash the system or attempt to subvert the restrictions associated with computer account or the networks of ALC. This includes no hacking, phishing, network sniffing, port scanning, spoofing, denial of service, spamming, introduction of malicious software/virus, etc. Proxy servers, other VPNs, and other ways of attempting to hide your identity may not be used

Alice Lloyd College employees found in violation of this policy may be subject to disciplinary action, up to and including termination.

Authorized 3rd party users/vendors found in violation of this policy may be subject to dismissal of the vendor relationship of Alice Lloyd College.

Some organizations or hotspots (hotels, restaurants, etc.) may have the required ports blocked needed for remote access, and if this is a case, there is nothing that Alice Lloyd College Information Technology can do to address this issue.

Data through the remote access session is encrypted through the IKE protocol.

Remote Access terminates after 180 minutes and you will have to re-authenticate with your password.

Information acquired by the vendor during a remote session cannot be used for any other purposes other than those specified in maintenance/service agreement and shall not be divulged to others. Devices belonging to a vendor connecting to Alice Lloyd College through remote access shall keep their device patches, have current anti-virus software and a sufficient firewall. Vendors may be asked for a copy of their policies regarding this issue if it is not outlined in the vendor/Alice Lloyd College contract.

Vendor Remote Access will be initiated by Alice Lloyd College Information Personnel as needed, by either enabling the remote access account, creating a remote access session or powering on an RDP box. Vendor remote access sessions shall be logged, monitored and terminated at the end of the session.

Upon termination (see termination) of an employee or a support engagement, all Remote Access accounts shall be terminated.

Alice Lloyd College personnel shall immediately report a theft of a device that has been configured for Alice Lloyd College Remote Access.

No remote access is given to students.

Remote Support Access

Alice Lloyd College uses a secure remote support platform called SolarWinds TakeControl for remote support of Alice Lloyd College owned computers. The client must launch an app before a member of the IT department may connect and control the computer. No other remote software is to be used or implemented without approval of the Alice Lloyd College Director of Information Technology. Any new remote software must be evaluated.

Wireless

Purpose

To compose a policy on the use of Alice Lloyd College wireless networks.

Scope

This scope pertains to all Alice Lloyd College wireless users.

Policy

Alice Lloyd College has 802.11 A/B/G/N Wireless Technology with a gigabit backbone throughout campus with redundant Ruckus wireless controllers with corresponding Ruckus Access Points.

Faculty, staff and students may access the internet using their wireless devices throughout campus by providing their Alice Lloyd College credentials – the same credentials that they would use for computer log-on.

Faculty, staff and students shall not use their credentials to get someone else's device logged on to the Alice Lloyd College Wireless Network as this may compromise their password or compromise their individuality of accountability.

The wireless bandwidth is shared across campus, so depending on the load will depend on what type of connection you may have at any given time.

There is an open, throttled, wireless for Guest access. Guess access has ACL rules in place for network segmentation to restrict it from accessing the sever network, so some applications that require server access will not run on the Guest network. The guest network is intended for general internet access only. Upon connecting to the guest wireless, there is a "good ethics" claim that must be acknowledged.

The Information Technology Department would like to request that all students please keep their anti-malware/anti-virus as well as windows patches up to date on computer platforms.

Printing to the Alice Lloyd College printers from student personal devices through the Alice Lloyd College wireless will not be available.

Although the Alice Lloyd College IT department does not support student owned computers, the Information Technology Department will do what they can to get their device on the wireless network, and to protect the Alice Lloyd College network the IT department will help with malware software installations and general malware/virus removal.

Alice Lloyd College employees wanting to do ALC work will be required to use an Alice Lloyd College owned laptop to connect with.

The Alice Lloyd College Information Technology Department will not assist in getting gaming consoles, streaming devices and other types of equipment like these on the network.

As laid out in the peer to peer polices, peer to peer usage is against Alice Lloyd College policy. Surfing pornographic material and other potentially unsafe sites is against policy. Individuals must not attempt to modify systems, system facilities, or attempt to crash the system or attempt to subvert the restrictions associated with computer account or the networks of ALC. This includes no hacking, phishing, network sniffing, port scanning, spoofing, denial of service, spamming, introduction of malicious software/virus, etc. Proxy servers and other ways of attempting to hide your identity may not be used. Personally owned wireless routers and network extenders are prohibited.

Mobile Device Management

Purpose

This policy is to establish mobile device guidelines for Alice Lloyd College mobile device users.

Scope

The Alice Lloyd College Mobile Device Policy applies to all individuals utilizing mobile devices for Alice Lloyd College purposes.

Policy

A mobile device is a computing device that is carried on the individual. They operate wirelessly from towers or a wireless network. They have their own power source (battery) and can be taken anywhere. They generally have some type of storage. They can be used for phone calls, emails, texts, camera, calendar, web surfing and many other things with the addition of apps.

These mobile devices can be phones, tablets, EPUB readers, etc. and generally use IOS, Android or Windows operating systems.

Alice Lloyd College email can be accessed on these devices using the operating systems native mail clients (Exchange or Cooperate) or can be accessed by using a number of apps that the user may have downloaded (Outlook).

If the mobile device is lost or stolen, the Alice Lloyd College data may be in danger of breach of data if any of these examples exist:

- There may be a file attachment in the email.
- There may be files saved to the device's local storage.
- There may be files saved to the cloud that the mobile device has access to.
- There may be photos of screenshots that the user has taken that details sensitive data.
- The browser may still be logged into the campus portal.
- Various other possibilities

Alice Lloyd College highly recommends that if you do use a mobile device for any Alice Lloyd College functionality that:

- You have a passcode set up on the device or use other methods of securing the device such as thumbprint, face recognition, etc.
- Set the screen lock time down to a minimum
- Use an app such as Find My iPhone if it's lost or stolen
- If it is lost or stolen and there is no passcode on it and there may be sensitive files on your ALC email, please contact the Alice Lloyd College IT department to have your password changed.

To protect the data of the Alice Lloyd College network, **ALL** Mobile devices that access Alice Lloyd College email through any app or any other method besides through the browser will be managed through the Office365 portal. Through this portal the following can be performed:

- Require a four-digit passcode - this is active. If you do not use a passcode, your device will not access the email server.
- Stop email from updating - once the device is found, this can be reversed.
- Remove the email account from the phone
- Remotely wipe device

If you are an Alice Lloyd College employee and you have Alice Lloyd College email sat up on your mobile device, and the device is misplaced/lost or stolen, you are encouraged to contact the Alice Lloyd College Information Technology Department to have your email disconnected from the device and your phone wiped.

Students are encouraged to abide by this request as well if they feel that they may have sensitive information in their Alice Lloyd College email.

Data Loss Prevention

Purpose

This policy establishes minimal planning, preparation, and deployment requirements needed to protect and secure confidential data.

Scope

This policy applies to all individuals employed by Alice Lloyd College, its students, and vendors.

Policy

This policy was developed to help defer data loss and covers aspects with regular account management/responsibilities.

Alice Lloyd College defines data loss as any process or event that results in data being corrupted, deleted and/or made unreadable by a user and/or software or application or data that is stolen or shared or made available to other individuals or computing systems that should not have access to the data.

Alice Lloyd College shall manage and ensure the confidentiality, availability, and integrity of protected information.

Alice Lloyd College has Data Loss Prevention rules implemented to check for Social Security numbers being emailed to internal and external email addresses. In composing an email that contains Social Security numbers, an email tip may pop up telling them that there is an item that conflicts with an organizational policy but will still let them send. However, after they send the email, it will be blocked and they will get a notification that the email was blocked due to Social Security Number Data Loss policies. The Director of Information Technology will also receive a copy of this blocked email notification. The recipient will receive nothing. Users will not have the option of overriding. The policy will look for a combination of the Social Security number format as well as a keyword such as SSN or Social Security to apply the block.

Mobile Device Polices and Removeable Media Policies are also sat up as Data Loss Prevention polices and are in their own section.

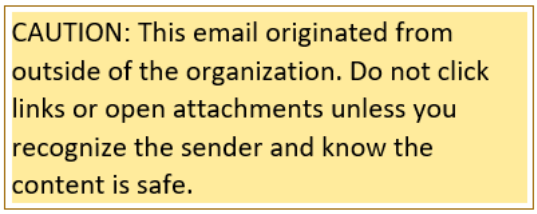
Data Loss Prevention also shall consist of the following:

- Require passwords for all users. This will stop unauthorized users from logging onto a computer and gaining access to data.

- Do not share passwords allowing access of others to items they should not have access to. If you have these written down, keep them in a safe place.
- Give appropriate access to individuals. If they do not need access to certain applications and data, do not give them access to it. Start out with basic access and expand this as needed.
- Do not allow someone else to sit down at your console with your login.
- Do not allow someone to watch over your shoulder.
- Visitor access into offices should always be accompanied by Alice Lloyd College personnel.
- Session time out. Computers will lock after a certain time of inactivity. This will keep an individual from accessing a computer that had been previously logged onto as another individual.
- Do not put sensitive data in shared folders unless you're sure that others in the share are permitted to have access to the given data. Make sure there are sufficient backups in place for these certain files in case they are accidentally deleted or overwritten. Give access to these shares as needed.
- Data **should not be** emailed to other individuals and do not allow others access to your email. If others need the data, they should be able to pull the data needed on their own.
- If checking Webmail from an off-site location, please remember to log off from your email session, and if possible, restart the computer after logging off.
- Personal email should not be checked on your Alice Lloyd College workstation. This would allow another method of malware to be introduced to the Alice Lloyd College network.
- Do not save documents that include sensitive data unless it is necessary. If you do save these types of documents, they are advised to be password protected.
- Do not store sensitive data on a removable drive (jump drive, memory card, burn to CD). (See Removable Drive section)
- Empty your recycle bin routinely.
- Be aware of phishing emails that may appear to be legit and are intended to gain information or have you to click on an infected link.
- Be aware of unknown attachments. If you are not expecting an attachment from someone and do not recognize what it may be, you are advised to delete it.
- Do not fall for the various "ransom" emails wanting payment or for the popups that you are instructed to call Microsoft or other popups trying to solicit money from fake anti-virus or computer help.
- Data should not be accessed from personal computers, even with remote access privileges. Under remote access circumstances, an Alice Lloyd College owned laptop shall be furnished so they can be maintained with anti-virus/anti-malware programs.
- Avoid surfing sites that would be considered "potentially unsafe," such as crack sites or adult oriented sites where there would be a likelihood of picking up malware.

- Do not use Peer to Peer software (See peer to peer policy)
- Keep a clean desk policy. Avoid printing sensitive data and leaving it around for others to see. If it really does not need to be printed, do not do so. Do not delay picking up prints from the copier/printer. Any prints should be securely disposed of by placing in the Shred-All bins.
- Hard copies of sensitive data should be locked up in a filing cabinet.
- Faxing solution requires each department to have their own username and password to log on to a designated site to retrieve faxes. This username and password shall not be shared with other departments.
- All employees should take a class on Data Security awareness.
- Student workers that work in offices with access to sensitive data should take a data awareness class as well as fill out an Alice Lloyd College Statement of Confidentiality form each semester.
- Don't discuss information with sensitive data to others that are not entitled to access such information.
- Only discuss confidential information with the individual that it pertains to.
- Any removable device with data stored on it should be disposed of securely when no longer needed. Any removable media is wiped clean if it can be done and then physically defaced before being disposed of. This same process applies to hard drives. Removable devices can be turned over to the Alice Lloyd College Information Technology office for disposal. CDs are broken in half so they can't be used and read.
- Any computer that has been reassigned will be reformatted and then reimaged before going out to another user.
- Maintain a sufficient firewall with intrusion detection preventions.
- Use a combination of antivirus/anti-malware programs. This will help against system crashes, ransomware, etc. corrupting files.
- Keep updates and patches installed. This will close any vulnerabilities.
- Maintain good backups:
    - Everyone's "my-documents" folder is a redirect to a server. This keeps them backed up from loss and more secured as they are not cached in the event that a computer is stolen.
    - Backups are done twice a day to on-site and then backed up off-site nightly.
    - Backups can be easily restored in case of a bad ransomware outbreak.
- Wireless guest access should be restricted from "seeing" servers that may host data and should be used for standard web surfing only.
- Assure that any vendor that has access or host any sensitive/crucial information has policies in place to protect the data, their computing devices, and obtain SOC reports from them if they are available.

- A ruleset is defined to mark external email as external, cautioning the users that it is an external email and to take caution in opening attachments or clicking links. The caution box appears as below:



Removable Media

Purpose

To define a policy for the use of removable media on the Alice Lloyd College network, explaining its definition and suggested use.

Scope

This scope applies to all Alice Lloyd College network users.

Policy

This policy is to protect the integrity of the private and confidential data that resides on the Alice Lloyd College network and to prevent this data from being deliberately or inadvertently moved outside the Alice Lloyd College network where other individuals can access it and to protect the integrity of the network by cutting down the risk of virus/malware infection.

Removable media is defined as devices or media that is readable and/or writable by the end user and can be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs, removable hard drives, optical disks, such as CD and DVD disks, and even cell phones.

Removable media may be used on the Alice Lloyd College network and in Alice Lloyd College computers. However, sensitive information should never be stored on removable media.

For Alice Lloyd College work, files shall not be taken back and forth from Alice Lloyd College computers to home computers on removable media. Furthermore, removable drives from Alice Lloyd College offices should not be taken home at all.

Be cautious in inserting removable media if it is used and you are not sure of its origination. If in doubt, please contact the Alice Lloyd College Information Technology Office.

When removable media starts giving error issues when attempting to access, permanently deface the drive, trash it, and obtain a new one (or give to the Information Technology Office for disposal). When they get in this state, they are undependable.

When the Information Technology Office trashes removable media, it is formatted when it can be and it is securely destructed.

Information Technology has public access computers that have an application installed called Deep Freeze. This software protects the hard drive, and any changes on installations and configurations and such are removed after reboot. It is Information Technology policy to remove these computers from the network and test potential infected drives and documents on these computers. With them removed from the network, any malware cannot spread, and with the hard drives being protected, any virus or malware that they pick up will be erased upon reboot.

External Systems

Controls shall be in place to limit connections to External Systems belonging to Alice Lloyd College. Cloud storage and cloud sites are examples of External Systems. Measures that can be taken to protect these from the public include accounts and passwords, firewall rules and IP Range Access Limitations

Public vs. Non-Public Information

Controls in the matter of an overseer shall be in place to assure that no non-public information is posted to an external public system for the public to see. This can be any information that is protected under the Privacy Act, or any data that is considered confidential. Individuals authorized to post onto publicly accessible systems shall review the content if information prior to posting it.

1.2 Awareness and Training

Awareness and Training

Purpose

Alice Lloyd College recognizes that security and data compliance start with awareness, that every user plays a role in security, and users need to be informed on the most current security issues.

Scope

This policy applies to all the Alice Lloyd College community, its employees, students, and vendors.

Policy

Colleges and universities are increasingly targeted by cyber criminals, each looking for a way inside of the network and obtaining credentials and data. The knowledge of security awareness is the key aspect of preventing this.

Managers, system administrators, and users shall be made aware of the security risk associated with their activities on the Alice Lloyd College network and its applications.

All Alice Lloyd College employees shall complete an Information Systems Data Security Awareness Class.

Alice Lloyd College student workers whom work in an area where they will have access to sensitive data will be required to take a one-time class in Data Awareness. Any new student workers shall take this class upon being assigned to these areas. These areas have been classified as Financial Aid, Admissions, Registrar's Office, and Student Services.

The Data Awareness class shall consist of the following topics:

- Passwords including security and sharing
- Privacy and proper handling of sensitive information
- Physical security
- Social engineering
- Identity theft avoidance and action
- Email usage
- Internet usage
- Malware
- Software usage, copyrights and file sharing
- Portable devices
- Proper use of encryption devices
- Reporting of suspicious activity and abuse
- Social media usage

* Security Awareness and Data Security & Privacy Training shall be offered through an online learning management system. Attendance of the trainings shall be tracked with successful completion to be documented and retained.

Information Technology staff, the Security Board Officer and the members of the Security Board shall be held to a higher degree and shall complete more advanced awareness classes as they are made available.

Overall awareness is covered by policies and procedures and email advisories that are sent out on a need to basis, letting the Alice Lloyd College community know of any major outbreaks of phishing/malware attacks.

General promotion of cybersecurity is encouraged in ways such as emails, posters, and free promotional items with security reminders, etc.

Alice Lloyd College uses a software platform called Knowbe4 to provide additional training to higher end staff as needed. This software will also allow the IT department to conduct phishing test scenarios. Reports are provided on whom accessed the links as well as those whom reported it as a phishing email through a Phishing button located in Outlook. This will help Alice Lloyd College understand how the employees as a whole understand the importance of addressing Phishing emails appropriately.

1.3 Audit and Accountability

Audit and Accountability

Purpose

This policy establishes requirements for the collection, maintenance and review of audit logs for Alice Lloyd College applications and computers, in support of identity management and threat monitoring.

Scope

All Alice Lloyd College system users are impacted by this policy. It is the responsibility of staff employed to maintain and manage IT systems to understand and comply with this policy.

Policy

An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity.

Audit Logs

Audit logs should be maintained and audited to look for these types of events.

Audit logs should be reviewed and analyzed as often as needed.

Inspections should be made to ensure audits/logs are being generated and not being deleted for any reason.

To match a user account to a person, each employee is assigned their own workstation. To protect the deleting and manipulation of auditing logs of workstations, users are restricted from access to this by having the role of a non-admin user on their workstations.

Important types of logs to look at can include password changes, failed logons, and failed access to shares.

Audit logs and records of an incident should be kept to help with monitoring, analysis, investigation and reporting of unlawful or unauthorized system access. Do a report on unlawful, unauthorized, suspicious or unusual activity.

Server audit logs are maintained by Netwrix Auditor.

If there is an incident; date, time, incident, how incident was found, whom incident involved, and what was impacted are bare minimal of what should be recorded, so logs should represent event date, time, source, and description. This section relates to Incident Response.

There should be a method in place that should track user log-on to which computer.

Date and time service can be critical to security capabilities such as access control and identification and authentication. In order to ensure that Windows has the latest and most accurate time data, Microsoft continuously monitors DST and TZ changes announced by governments around the world. Microsoft makes an effort to incorporate these changes to Windows, and publishes an update through Windows Update (WU). Each DST/TZ update released through WU will have the latest time data and will also supersede any previously issued DST/TZ update

REN-ISAC

Alice Lloyd College is a member of the REN-ISAC organization. The Research and Education Networks Information Sharing and Analysis Center (REN-ISAC) is integral to higher education's strategy to improve cybersecurity. By forming a trusted coalition, members are better equipped to analyze and respond to threats and incidents.

REN-ISAC member institutions benefit from Security Event System (SES) threat intelligence and other automated data collection and sharing tools to enable informed decisions about threats and events, as well as peer assessment services to improve the institution's overall security posture. They offer members daily cybersecurity news reports, alerts and advisories, analysis reports of cybersecurity threats and mitigation, and an active, interested community of subject matter experts who provide feedback on practices and standards

REN-ISAC and its affiliates searches the internet for .edu credential (usernames and passwords) dumps. If found, ALC will be notified with the name of the account, the password thats included and if possible, where the dump originated from. With the passwords, ALC can test to see if it is a working ALC account to determine if a password change is in order.

ALC feels that subscribing to this service is a benefit to the ALC network and its Cybersecurity Policy.

1.4 Configuration Management

Baseline Configuration

Purpose

The purpose of this policy is to establish a policy on Baseline Configurations for Alice Lloyd College computing.

Scope

This policy applies to the Alice Lloyd College Information Technology Department and its entire assets**.**

Policy

A Baseline Configuration is a documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. This includes hardware, software, firmware and documentation. Documentation can include establishing and enforcing security configuration settings for information technology products employed in Alice Lloyd College systems.

Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture.

Baseline configurations of systems reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration.

Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (such as system association, system owner). Information deemed necessary for effective accountability of system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

Alice Lloyd College shall maintain a set of Baseline Configurations for its servers, workstations, hardware peripherals, software, operating systems, phones, firewall and networking pieces such as wireless access points, cameras, switches, etc.

When applicable, baseline settings for configuration change settings that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system will be kept.

Security parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security requirements. Security parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive

specific configuration settings for systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides) provide recognized, standardized, and established settings that stipulate secure configuration settings for specific information technology products and instructions for configuring those system components to meet operational requirements.

Change Control/Management

Purpose

This policy is intended to ensure changes to Alice Lloyd College IT systems are managed in a documented and predictable manner so that staff and other agency constituents can plan accordingly.

Scope

This policy applies to all production systems that are maintained by, on behalf of, or involve, the IT resources of Alice Lloyd College.

Policy

To ensure the quality delivery of Information Technology services and monitor any changes in the Alice Lloyd College Information Systems environment that may have an impact of the security of the network, its data or applications and platforms, a Change Control policy has been adapted. This is adapted to ensure the effective management of change while reducing risk and is part of the overall security plan.

Information Technology Change Management is the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. The Change Management process begins with the creation of a Change Request within the company's selected technology platform. It ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

It is essential that requests for change are submitted and approved in a timely manner. This will allow completion of accurate documentation, change processing and obtaining the approvals in sufficient time prior to the requested implementation date, and also provide for conflict resolution for scheduling of changes.

Changes will need to follow Alice Lloyd College Information Technology guidelines to assure that the change is acceptable. Many times, the 2nd approver will also be the requester.

Once a change has been implemented, the end user or the Information Technology Office will test the change.

Goals of this policy are:

- Establish clearly defined best practice processes to ensure compliance with across the board requirements.
- Improve efficiency through the use of automated tools and a centralized data depository.
- Improve communication through automated escalations and notifications.
- Ensure proper level of approvals.

- Reduce risk associated with completing changes.
- Reduce the impact of changes on IT organizations.

The process shall consist of:

- Accurate documentation
- Formal approval process – the majority can be approved by the director of IT
- Scope – What kind of Information System changes will this apply to?
- Reasoning
- Categorize and prioritize if needed
- Schedule if needed
- Plan
- Completion and review

Information to collect is:

- Date
- Request
- Category
- Requester
- Priority
- Impact/Risk level
- Approver
- Title
- 2nd approver (if needed) - Many times the 2nd approver will also be the requester.
- Title
- Completion date
- Performed by
- Reversible
- Reviewed/followed up date/Testable

Items that need to be logged are:

- Firewall ruleset change
- Firewall firmware upgrades
- Firewall allotted bandwidth change
- Change to backup schedule
- Any other change not listed that would impact the integrity/security of the Alice Lloyd College network, its data or its users

Items not covered in the Change list above are considered daily IT tasks and should be logged in help desk software and not covered in Change Management.

Access

Any changes to the hardware, software or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, only qualified and authorized individuals may access the systems for purposes of initiating change.

Access restrictions are set and included in this set of policies as Physical and Logical access.

Change Window

A change window is set for Friday evenings at 4:30pm in case this time allotment is needed. This will be the window that the Information Technology Department may need to implement any changes that may require a downtime, such as a configuration change or a system restart. However, emergencies arise and these changes may have to take place any time of the day. Notification will be given with as much notification time as possible.

Software

All software should be explicitly identified, inventoried, documented and maintained and clear definitions of the legal use of software and information systems, to ensure copyright is not violated.

Software should follow the guidelines of:

End users

- Do not purchase or install software without consulting with the Alice Lloyd College Information Technology department.
- Do not attempt to make copies of software.
- Do not attempt to take any Alice Lloyd College software home.
- Do not bring any software from home and attempt to install on an Alice Lloyd College computer.
- To prevent the installation of software by the end user, workstation users will be a non-admin user and will not have the credentials to install software since they do not have administrator access.

Information Technology

- Record and provide evidence of ownership of licenses
- Controls to ensure maximum number of users – permitted within the license - are not exceeded
- Know what is installed where
- Have knowledge of any type of data that the software may use (any unique identifiers)
- Keep an inventory of software. Software is inventoried by OCS's software inventory page.

Firewall

A set of redundant checkpoint firewalls are in place that are used to block unlawful applications and sites such as adult oriented material, peer to peer, proxy and stealth.

Following the principle of least functionality, all ports are blocked by default, with only allowing surfing ports and various ports that are needed for day-to-day operations at Alice Lloyd College.

The firewall is referred to as the Alice Lloyd College boundary, as it is where the inside meets the outside.

1.5 Identification and Authentication

Identification and Authentication

Purpose

To set a set of policies for Alice Lloyd College Identification purposes.

Scope

This scope applies to all the Alice Lloyd College users, vendors and networking systems.

Identification

All users, workstations, servers, printers, access points and other devices are named accordingly.

Users are limited to specific applications and levels of access rights. Computer and application system access is to be achieved via password protected user IDs that are unique to each individual user to provide individual accountability and any user accessing the Alice Lloyd College network must be authenticated through this user ID.

Usernames, passwords and any other information that would be considered protected information will not be given to any other individual but the owner. The only exception to this would be if the student had a Student Information Release Form on file in the Deans office. If a request for confidential information is through a telephone call or email, all efforts must be taken to assure the person at the other end is whom they are supposed to be. A student may be asked random questions such as of whom their instructor was for a certain class, what dorm they stayed in, the personal email that ALC has on file, their DOB or the last 4 digits of their SSN. Confidential information shall not be sent to a non-ALC email account if there is any doubt that the email didn't come from the subject in question.

Multifactor Authentication

Multifactor authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user *knows*, such as a password and what the user *has*, such as a security token; MFA may also be referred to a 2FA, meaning there are two ways of authentication.

Multifactor authentication is required for

- VPN users, authenticating against the DUO app on smart phones. Requiring a second form of authentication will help secure VPN accounts and connections. MFA will be required upon logging into the laptop, as well as connecting the VPN for any employee that has access to Social Security Numbers, thus protecting the use of the laptop, as well as the VPN account. If the employee is not issued an ALC owned mobile phone, it is up to the employee to provide one for the DUO app.
- All employee email accounts. Employees have a choice of the method they choose, whether it be a phone call, a text verification code, or using an app to approve the sign in. If the employee is not issued an ALC owned mobile phone, it is up to the employee to provide one if they want to use the text or app authentication method.
- Privileged accounts are protected by MFA using the DUO app. If the employee is not issued an ALC owned mobile phone, it is up to the employee to provide one for the DUO app.
- Remote assistance tool: *Solawinds: Take Control*. MFA is used against Authy App.

Employee Termination

Staff accounts are deactivated upon the day of departure/termination from Alice Lloyd College or as the need for the application/access is no longer there. This applies to computer accounts, email, remote access, file shares, PowerFaids and Jenzabar.

Computer and email accounts for departing faculty will be terminated 2 weeks following graduation, or two weeks after the planned graduation date if the graduation event is not held for some reason. The only exception to this is if the faculty member will be providing services for Alice Lloyd College that will take longer than the two allotted weeks, and the request will need to come from the Academic Dean. Other accounts (Jenzabar, etc.) will be deactivated upon the day of graduation or when the need for the application/access is no longer there.

ID card physical access assignments are deactivated upon departure from Alice Lloyd College.

Certain issues may require that accounts and access be deactivated before the notice of any termination to protect the data and assets of Alice Lloyd College, or accounts may need to be terminated before the set termination time. This notice would need to come from the employee's direct supervisor or line officer and should be made in writing.

Any laptop, tablet, phone, etc. that is assigned to an employee must be returned upon departure from Alice Lloyd College/June Buchanan. Failure to do so may resort in holding of funds of the last pay period.

There is a checkout form through the Human Resource department that an employee has to pick up, fill out, and have signed by various departments, allowing the IT department to know of the termination so they can terminate the appropriate accounts.

Monthly, Human Resources will send out an email that caps the previous month's employee departure.

FMLA

Employees on FMLA leave will not have access to their computer account, email access or Jenzabar/PowerFaids during the leave time. Certain departments may need to have the *out of office assistant* turned on for the employee on leave instructing individuals on whom they shall contact for the time being, as well as requesting that email forwarding be turned on so future emails will go to a designated individual. The max time that this will be set is 12 weeks. To ensure the continuity of Alice Lloyd College business, the employee's mailbox may need to be accessed by the Information Technology Office or by Alice Lloyd College personnel if requested by the division head.

Password Complexity

Accounts are not to be shared and passwords are to be kept private. Passwords will randomly be changed from time to time as needed but have a life span of 170 days. Passwords will consist of eight characters minimum, cannot contain part of the account name, and will require at least three of the following:

- Uppercase
- Lowercase
- Number
- Special character

Please contact the Alice Lloyd College Information Technology Office if you need assistance with changing your password.

Users will have to roll through a new password at least 5 times before they may reuse an original.

Obscure Feedback

Obscure feedback is referred to as the effect you get when someone may be looking over your shoulder as you input data. This can be brought to a minimum by using items such as smaller monitors, smaller keyboards, displaying feedback for a short amount of time, and using asterisks in place of passwords.

1.6 Incident Response

Incident Response

Purpose

The Alice Lloyd College Information Technology Security Incident Management Policy describes guidelines for identifying, tracking, and dealing with information security incidents.

Scope

This policy applies to all the Alice Lloyd College Community and it is up to the Information Technology Security Plan Board and Department of Information Technology to understand and enforce it.

Policy

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

An Incident Response Plan should include procedures for detecting, responding to, and limiting the effects of a data security breach

Incident response plans usually include instructions on how to respond to potential attack scenarios, including data breaches, denial of service/distributed denial of service attacks, network intrusions, virus, worms or malware outbreaks or insider threats.

Any incident that is not properly contained and handled can escalate into a bigger problem that can ultimately lead to a damaging data breach or system collapse. Responding to an incident quickly will help an organization minimize losses, mitigate exploited vulnerabilities, restore services and processes, and reduce the risks that future incidents pose.

Cybersecurity Threats

Cybersecurity Technical Threats	Cybersecurity Human Threats
Ransomware	Malware
Network probing	Spyware
Intrusion	Phishing
Alteration/Corruption of Data	Gain system access
Theft of data	Gain administrator access
Blocking system access	Leaving workstation accessible
Hijacking system control	Insecure password storage
Hijacking system resources	Insecure password practices

This policy lays out the policy and procedures for Incident Response.

Preparation

- Keep the Security Plan up-to-date with adequate policies and procedures.
- Keep the Alice Lloyd College community aware of the dangers of an outbreak.
- Require data awareness training.
- Keep workstation computers up to date with antivirus and malware. Campus computers run McAfee antivirus, McAfee MVision and Malwarebytes/Spybot for anti-malware. McAfee has web control and email scan enabled. Alice Lloyd College Checkpoint firewalls have antivirus and antimalware blades enabled.

- Keep computer systems patched.
- Point out items that the community can do to cut down the risk.
    - Use a complex password and don't share it with others.
    - Employees are constantly reminded about emails that can cause potential issues. They are encouraged to delete any email that has an unknown attachment or if it is from a sender that they are not familiar with.
    - They are advised to watch out for phishing emails and to not reply with any of their ID credentials or to use their credentials to attempt to log onto any non-legitimate site.
    - They are advised against surfing potential "bad sites" where they may pick up malware, trojans, etc.

Incident Process

All incidents should go through the following process**:**

- **Preparation**
    - Training for your Information Security Board
    - Tabletop exercises for pretend incidents
    - Spread awareness to the Alice Lloyd College campus
- **Identification**
    - What was the outbreak?
    - How was the outbreak noticed?
    - Does the outbreak spread?
        - What does it do?
    - Is data corruption/thief involved?
- **Containment**
    - How can we contain this outbreak? To a subnet? To a building?
- **Source**
    - Where did it come from? What area of campus did it effect? Where is the original source from?
- **Communication**
    - Reported, logged and tracked
- **Recovery**
    - What needs to be done? Are there legitimate backups?

Types of Incidents

Infestation

1. Notify any personnel that needs notified such as the Information Technology Director and Security Officer. If a data breach was suspected, then the Security Officer shall be notified and procedures under the Data Breach followed.
2. Attempt to contain it.
    - If the incident seems to be isolated to a certain building, pull the fiber from that building from either the server room or the building's network closet. If it seems to be isolated to a certain VLAN (faculty/staff computers or student access computers), then the appropriate switch can be taken off-line and the other VLAN brought back up.
    - If the incident is spreading thorough Wi-Fi, terminate the session to the wireless controllers.
    - If it seems to be spreading through email, then the connection to the outside world should be disconnected.

    - If spreading through removable media, removable media can be restricted from being read in GPO policies.
3. Run McAfee to see what it picked up. Look at the MVision logs in the EDR EPO cloud. If McAfee does not pick up anything, follow up with AVG Free and Windows Defender. Next follow up with Spybot. Now go through the same steps on a 2nd, and possibly a 3rd looking for similarities. What is being looked for here is the specific item that is the outbreak. Check McAfee's repository to find information on any item was found, identifying any issues, such as stolen data/corrupted data/spreading worm to cause denial of service, etc.
4. Once again, if a data breach was suspected, then the Information Systems Security Board Officer shall be notified.
5. Once identified, scan all computers to identify all infected computers.
6. Pull all infected computers offline.
7. Monitor the network/other building computers for activity of the issue
8. If there are no issues seen, reinstate connection to building/VLAN/Wi-Fi/email as needed.
9. Monitor all network activity, exclusively the infected building/VLAN.
10. Record any evidence as needed (logs, screenshot, keep the hard drive, etc.)
11. Reimage infected computers, updating antivirus/antimalware. Restore documents from backup. No backups or anything should be pulled from infected computer(s).
12. Return computes to network.
13. Monitor for signs of re-infestation.

*This is considering it is an actual outbreak and not a general infestation of one computer. If it is involving one computer, look for signs of hacking or a data breach and cleanup\reimage\restore backups as see fit.

Hacking

1. If this was a case of hacking:
    a. The infected computers(s) shall be identified. How was it noticed?
    b. The computer shall be taken off-line and gone over to attempt to determine what the hacker was attempting to accomplish. What were they hoping to get access to?
    c. If a data breach was suspected, then the Security officer shall be notified and procedures under the data breach section followed.
    d. Attempt to find the method of attack. If it was through the firewall, attempt to locate and close any vulnerabilities.
    e. Record any evidence as needed (logs, screenshot, keep the harddrive, Etc.)
    f. Change passwords to any accounts that may have assessed this computer(s), such as login, Jenzabar and PowerFaids or to any other application that may house other sensitive information.
    g. Reimage computer(s) and return to network, restoring files from the backup server.
    h. Monitor for signs of any suspicious activity

Data Breach

A data breach is an incident that may require multiple incident responses in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. Data breaches may involve personal health information, personally identifiable information (credit card numbers, Alice Lloyd College ID number, Social Security Number, etc.), financial, address, or other sensitive information.

If anyone who is not specifically authorized to do so views such data, the organization charged with protecting that information is said to have suffered a data breach. If a data breach results in identity theft

and/or a violation of government or industry compliance mandates, the offending organization may face fines or other civil litigation.

Cybersecurity insurance must be carried by the data owner to cover these fines or litigations.

Data breaches may result from:

- Hacking and stealing data
- Email Phishing
- Malware
- Virus
- Unpatched software/operating system that leaves a vulnerability access hole
- Indirect access by viewing over someone's shoulder
- Printing that has been left around
- Word of mouth
- Weak Passwords – someone else accessed someone's account
- Stolen computers/mobile device
- Emailing wrong individuals
- Allowing others use of your email or computer system
- Sharing of removable device

Data breaches may also fall under HIPPA and FERPA guidelines, so the data breach could also result in a HIPPA/FERPA incident.

When there is a suspected, potential or actual breach incident, the Information Systems Security Board's Security Officer shall be notified. The Information Security Officer will gather all information that is possible at that time and then bring forth a meeting of the Information Security Board. The individual reporting the incident may be brought into the meeting if they are personnel other than someone on the Security Board.

The Board shall investigate for Who, What, Where, When and How as the medium standards.

- What was leaked? Any unique identifiers?
- Is it a true breach?
- Who did it effect? All students? Employees?
- Where did this happen? What office?
- When did this take place? Date? Time?
- Who was it leaked to, and do we know approximately how many the information was leaked to?
- How was it leaked? Was it leaked through an email, a stolen list, a missing removable drive, etc.?
- Has any action been taken?
- Is there any immediate action that should be taken at this time? Changing a password? Terminating an account? Shutting down a system?

Any evidence shall be collected, such as screen shots, print of an email, etc.

Any process that was terminated should be reinstated if applicable and safe to do so.

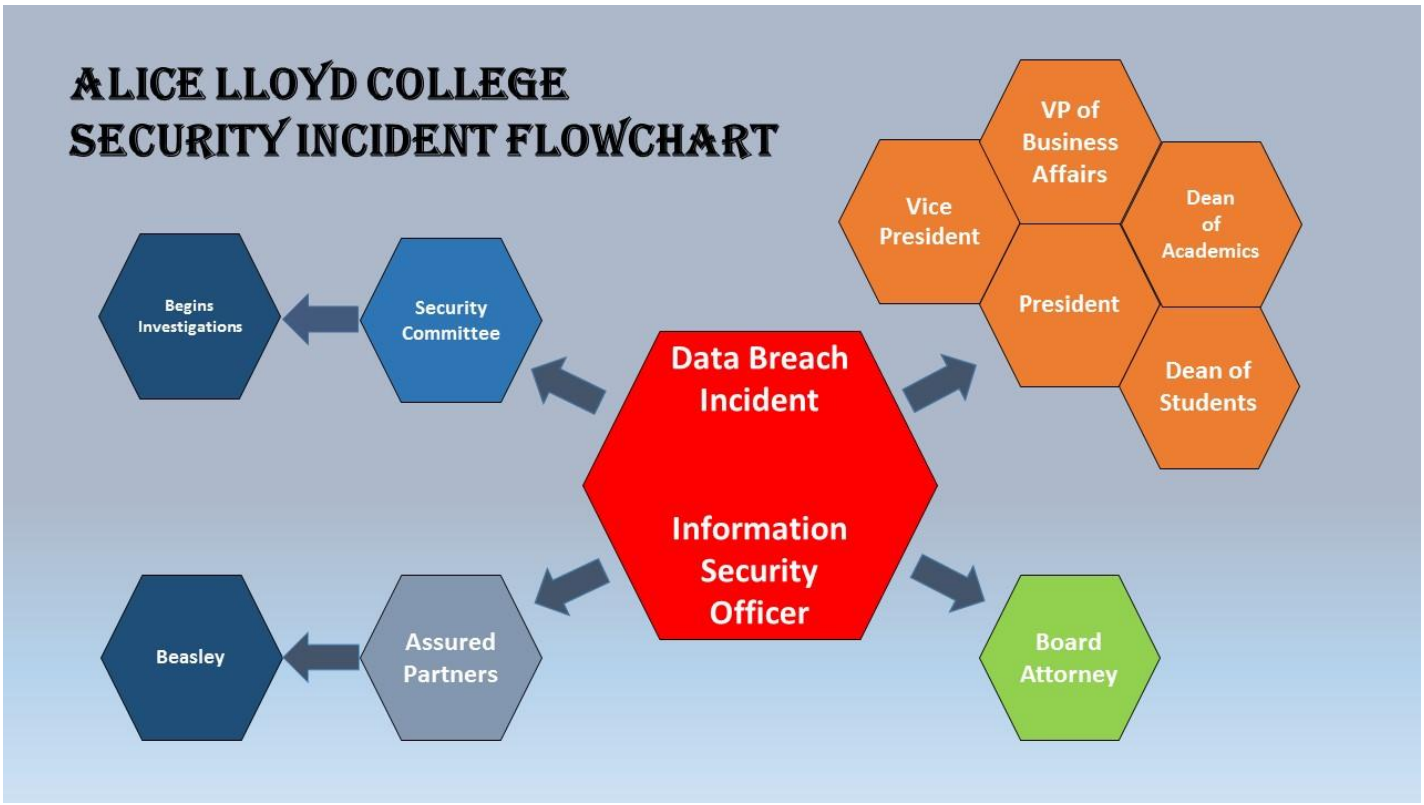
After all this information is obtained, the Information Security Officer shall:

- Report the incident to assured partners whom will report to Wright Beasley Breech Response Solutions
- Report the incident and turn over the information to the Alice Lloyd College attorney whom will discuss with cybersecurity attorneys.

The Security Officer will notify administrative members of the institution as needed, such as the President, the Vice President, the Dean of Students and the Dean of the College.

The attorney will then advise Alice Lloyd College on how to handle the matter. This could consist of several things, from notifying the individuals, change of operations, or a settlement from cybersecurity insurance.

The Security Board will meet to discuss the attorney's recommendations and take the actions proposed and discuss any needed follow-up actions, such as change in office tactics, application permissions, more awareness training, or any change of policy, etc.



The incident reporting individual shall be kept informed of the progress and happenings.

All procedures shall be documented.

Conclusion

An incident could include all three of these types. For instance, the Alice Lloyd College network could be hacked, a trojan released, and data could have been compromised. Thus, do not overlook one aspect while concentrating on another.

A complete, detailed report should be generated and stored for any information security incident that the organization experiences. This report should include all details of the incident discovered through forensic analysis, how was it detected, and what did it consist of. The steps taken in the containment and eradication stages, and recommendations for improving security and preventing future incidents. Reports of the incident should be prepared and sent to the appropriate parties both internally and externally. This should be kept on file by the Information Technology Director as well as the Security Officer of the Security Board.

1.7 Maintenance

Asset Maintenance

Purpose

To set and maintain a set of policies that covers the maintenance of Alice Lloyd College assets, protecting their integrity on the Alice Lloyd College network.

Scope

This policy applies to the maintenance and upkeep of all Alice Lloyd College networking infrastructure as well as client workstations.

Policy

Alice Lloyd College shall employ qualified, in-house staff for operations of production systems containing protected information or contract for managed support.

These employees shall maintain and upkeep the Alice Lloyd College assets. These assets cover hardware, software, firmware, and other assets that are not directly associated with data such as copiers, scanners, printers, etc.

These maintenance repairs and related task shall be logged in help desk software.

All Information Systems Maintenance shall be approved by the Alice Lloyd College Director of Information Technology.

Alice Lloyd College shall configure critical information systems to be fault tolerant. Data on those systems shall be restorable to a known secure state of operations while annually confirming the restoration process.

Routine Maintenance shall be logged.

Any networking tools (software) that is used for monitoring and scanning shall be tested for their accuracy and non-existence of malware. In the event that the tools contain malicious code, the incident shall be handled and documented as in Incident.

In case that Information Systems Maintenance is employed by a 3rd party, that maintenance will be performed by remote (logical) access or performed in-house. The Alice Lloyd College assets will never be sent off-site for maintenance. In the case that this was to happen though, all data shall be stripped from the asset.

Remote Access and Physical Access policies will be maintained in these scenarios, meaning that all access be logged and all activities shall be monitored. The Data Center access form shall be filled out. Remote Access shall be established when needed, performed in a secure way, monitored and terminated.

Records shall be kept for warranty and maintenance information. These types of records can be kept in Asset Management.

1.8 Media Protection

Media Protection

Purpose

The purpose of the Media Policy is to establish standards to provide safeguards for protected information.

Scope

The scope of this policy includes anyone with physical access to the Alice Lloyd College offices or work areas.

Policy

The policy is as follows:

- Alice Lloyd College shall restrict physical access to media that contains data categorized at a confidential or greater level to authorized personnel only.
- Media that contains protected information shall be stored securely within a controlled area and physical access to that controlled area shall be restricted to authorized personnel.
- Appropriate safeguards shall be utilized when media containing protected information is transported by authorized personnel outside of a controlled area.
- All work areas shall be categorized as publicly accessible or as work areas potentially containing protected information.

Backup Media

Backups are first backed up on-site then replicated off site. There are no tapes to change out, so due to this, there is no need for the secure storage of backup media.

Installation Media

Any installation media belonging to Alice Lloyd College that is furnished on CD is digitalized and a secure digital copy is made and saved and is backed up with the backup process. The original CD is maintained in a secure location by the Information Technology Department. Copies of any original digital installations are also backed up with in the backup server.

Removable Media

Removable media is a well-known source of malware/virus infections and can cause loss of data and a campus wide malware outbreak.

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs, removable hard drives, optical disks, such as CD and DVD disks, and even cell phones.

This policy is to protect the integrity of the private and confidential data that resides on the Alice Lloyd College network and to prevent this data from being deliberately or inadvertently moved outside the Alice Lloyd College network where other individuals can access it and to protect the integrity of the network by cutting down the risk of virus/malware infection.

Removable media may be used on the Alice Lloyd College network and in Alice Lloyd College computers. However, sensitive information should never be stored on removable media. This is part of the Data Loss plan.

Employees: Files shall not be taken back and forth from Alice Lloyd College computers to home computers on removable media. Furthermore, removable drives from Alice Lloyd College should not be taken home at all.

Be cautious in inserting removable media if it is used and you are not sure of its origination. If in doubt, please contact the Alice Lloyd College Information Technology Office.

When removable media starts erroring when attempting to access, permanently deface the drive, trash it, and obtain a new one (or give to the Information Technology Office). When they get in this state, they are undependable.

When the Information Technology office trashes removable media, it is formatted when it can be and it is securely destructed.

In case of needing to restrict individual computers from the use of removable media, this process can be performed in the User or Computer Section of a GPO > Admin templates > System > Removable Storage Access where the choices of Deny Read Access or Deny Write Access may be performed.

Data Destruction

Avoid printing sensitive data and leaving it around for others to see. If it really does not need to be printed, do not do so. Do not delay picking up prints from the copier/printer. **Any prints should be securely disposed of by placing in the Shred-All bins**. Only appropriate personnel have access to the locks for the bin. Do not place data prints in your trash can.

Any removable device with data stored on it should be disposed of securely if the time comes to do so. Any removable media is wiped clean if it is able to be done, and then physically defaced before being disposed of.

Hard drives that are to be trashed are formatted when possible and then removed from the system and physically defaced before being placed in the garbage. They are trashed separately from the CPU.

Any computer that has been reassigned will be reformatted and then reimaged before going out to another user.

CDs are broken in half so they cannot be used and read.

Please empty the recycle bin frequently.

1.9 Personnel Security

Personnel Security

Purpose

This policy is to establish guidelines for personnel security.

Scope

This policy applies to all individuals of the Alice Lloyd College Community.

Policy

Each information system will have standardized data classification and corresponding security controls associated to it.

Based on the system's data classification, appropriate user roles shall be defined.

A user's category is based on their job duties within their assigned division.

Alice Lloyd College shall assign information system authorizations to users based on user categorization, classifications and departments.

System roles will be reviewed annually, and updated if required.

At the beginning of their employment, all Alice Lloyd College employees will be required to sign Alice Lloyd College computing access agreements. With their signature, the user agrees to abide by all signed agreements. As policies and agreements are updated new signatures may be required.

Users changing their job duties or their assigned divisional team who still work at Alice Lloyd College shall have their access and operational privileges reviewed immediately and where required, updated. This review and update will focus equally on eliminating access privileges no longer required as well as providing new/enhanced access privileges required of the user's new category.

Access accounts for all systems roles will be immediately suspended or terminated upon the termination of employment of Alice Lloyd College. Suspended accounts may be maintained for a pre-defined period of time to allow for the extraction and retention of necessary information; thereafter, all accounts of the terminated individual shall be permanently deleted.

Exit interviews shall be completed by Human Resources for each exiting Alice Lloyd College employee. As part of the exit interview there will be a confirmation that all of the agency property has been returned.

*See Termination Process

1.10 Physical & Environmental Protection

Physical, Logical and Environmental Protection of the Alice Lloyd College Information Technology Data Center

Purpose

The purpose of the Alice Lloyd College Physical Access and Environmental Policy is to establish standards for granting and monitoring physical access to the areas of Alice Lloyd College networking and to provide safeguards for protected information.

Scope

The scope of this policy includes anyone with physical access to the Alice Lloyd College Information Technology offices and Data Center, also may be referred to as the "Server room".

Physical Access and Environmental Policy

The Alice Lloyd College Data Center is in the McGaw Library located in the Baum Technology Center along with the Information Technology offices and computer labs. The main door accessing the Baum Technology Center is equipped with a card lock that locks nightly at 11pm. This door has a security alarm on it if opened after hours. The Data Center is equipped with a card lock and stays locked 24/7. Only the IT department, President of the College, and the maintenance department have access to the Data Center.

Besides the personnel listed above, no one else is permitted in the Data Center unless accompanied by the IT or maintenance department.

There is a camera on the door entering the Technology Center, as well as a camera on the Data Center door and a camera in the Data Center.

The Data Center is equipped with a monitoring device that monitors for temperature, humidity, smoke and liquidity. If these items are detected or goes above the thresh hold, texts and emails are sent out for notification purposes.

The Data Center has its own air conditioning and humidifier unit and is equipped with a Halon unit in event of a fire episode.

The Data Center is protected by battery backup as well as a natural gas generator. The generator is tested for error codes and started every Friday and runs for five minutes. A physical inspection is performed for types of clogs or physical damage. Logs of inspection are kept.

The generator will also keep up the wireless access points and cameras for the McGaw building.

Visitors to the Alice Lloyd College Data Center

Alice Lloyd College does not have any remote campuses and only has one Data Center.

The purpose of this policy is to ensure the safety and security of visitors/vendors to the Data Center and to protect and secure the assets and data located in the Data Center.

No food, drink, or tobacco use is to occur in the Data Center.

In order to track visits/work performed in the IT Data Center, Alice Lloyd College shall consider this as a visitor policy.

All visitors to the Alice Lloyd College Data Center shall be attendance tracked with an attendance sheet left on a clipboard in the Data Center logging individual, company, date, and reason. Individuals need to be accompanied by IT personnel.

Any individual with physical access does not need to be logged/accompanied (Alice Lloyd College Maintenance Dept. for example) and shall gain entry by swiping their ID card. This will be their "log." Any individual with physical access may be the "accompanied by" individual in case they are bringing in a vendor such as a contractor, electrical, etc. If there is more than one maintenance personal, they both shall swipe their pass.

Remote access from a vendor is considered a visitor to the Alice Lloyd College Data Center as well. Their information shall be logged by an Alice Lloyd College IT personnel the same as a physical vendor. Remote Access policies for vendors are covered in the Remote Access section.

Logical Access

Purpose

The purpose of this policy is to define Logical Access and to lay out a policy on it, defining its difference between Physical Access.

Scope

This policy applies to any individual connecting remotely to the Alice Lloyd College networking systems.

Policy

Logical access in Information Technology is often defined as interactions with hardware through remote access. This type of access generally features identification, authentication, and authorization protocols. This is often contrasted with the term "physical access," which refers to interactions with hardware in the physical environment, where equipment is stored and used.

Logical access may be provided from part of a vendor agreement or Information Technology Support to hardware, software, etc. This policy coincides with the Physical and Remote Access Policy.

Physical access describes any time a user can reach a computer's hardware. Conversely, logical access refers to every other type of computer use, where a user connects to a computer system without being in the same room as the machine.

Logical access controls who or what process is to have access to a specific information resource but also the type or level of access that is permitted, such as use, change, or view for:

- PCs
- Software
- Databases
- Networks

Programs such as Windows' Remote Desktop Connection, as well as commercial alternatives including TeamViewer, GoToMyPC and LogMeIn, provide a type of logical access to computers that mimics physical access. Unlike logging in to a website, these programs allow a remote user to interact with a PC as if sitting

in front of its monitor and keyboard. Some remote-control programs also include features such as file transfers and presentation tools. Though these programs have security features, such as passwords and restrictions, you should only let individuals you trust connect to your machine through remote access -- a malicious user can very quickly damage a system when given remote control over it.

Hackers can break into a system through logical access. For example, a virus spread through an email attachment can grant its creator the ability to connect to infected computers, stealing or erasing their data. Physical access, however, poses a far greater security risk. With physical access and the right expertise, someone can completely bypass security systems on a computer, such as by using a system install disc to reset the password or attaching a key logger. Direct access to a computer also makes it possible for a data thief to simply steal the hard drive.

Businesses, organizations and other entities use a wide spectrum of logical access controls to protect hardware from unauthorized remote access. These can include sophisticated password programs, advanced biometric security features, or any other setups that effectively identify and screen users at any administrative level.

Information acquired by the vendor during a remote session cannot be used for any other purposes other than those specified in maintenance/service agreement and shall not be divulged to others. Devices belonging to a vendor connecting to Alice Lloyd College through remote access shall keep their devices patched, have current anti-virus software and a sufficient firewall. Vendors may be asked for a copy of their policies regarding this issue if it is not outlined in the vendor/Alice Lloyd College contract.

Logical access to any system will be granted based on least privilege and the method of connecting will be decided upon by the Director of Information Technology and the desired method of connecting will need to be established before the remote access procedure started by either enabling the remote access account, creating a remote access session or powering on an RDP box. That is, logical access cannot be obtained by an individual anytime they wish. Any accounts used for logical access should remain disabled until the need for the access.

Access shall be monitored, looking out for the installation of malicious software and key loggers, or attempting to add/edit user permissions or copy data from one area to another, perhaps a place off site.

A guest form shall be filled out for the procedure by the Information Technology Department. The individual's company shall make available on request an SOC report or something of that nature ensuring that they keep their equipment secure, that is up to date with patches, malware and virus software.

Upon termination (see termination for Employees) of an employee or a support engagement, all Remote Access accounts shall be terminated.

1.11 Risk Assessment

Risk Management

Purpose

As a college that receives student federal aid, Alice Lloyd College is considered a banking agency. Alice Lloyd College gathers and distributes a significant amount of confidential information. Alice Lloyd College must ensure that proper protocols are in place to properly protect the resources and maintain the integrity of the data for which Alice Lloyd College has been entrusted. Risk Management is the process of identifying and assessing risk, realizing the limitations in reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.

Scope

This scope applies to all the Alice Lloyd College community.

Policy

A risk management policy should address all issues of information security, from personnel screening and the insider threat to physical security and firewalls.

The Information Security Board shall

- Ensure that Restricted-Use Information Assets are identified
- Review the classifications of Restricted-Use Information Assets
- Direct the investigation, mitigation and acceptance of risks
- Compile a list of risk
- Ensure that risks are assessed
- Ensure that tabletop exercises are performed
- Process and approve variances from requirements in this document based upon risk and mitigating controls
- Define an acceptable level of risk, as it is impossible to have a system or environment that is 100% secure
- Document risk

To minimize risk, the Information Technology Department shall:

- Perform periodic scans of the network are to take place to look for
    - Unknown devices that are active on the major VLANs
    - Open shares
- Have an annual vulnerability scan performed by an outside agency on the external boundaries
- Perform periodic risk assessments by vulnerably scanning in house, checking for missed patches, out of date DAT files for anti-virus software, etc.
- See that account maintenance is performed regularly, ensuring that accounts for terminated employees have been terminated
- File shares shall be inspected regularly to inspect shares for incorrect privileges
- Implement network segmentation
- Monitoring for constant account lock-outs shall be performed. This may point to brute force attacks of an account(s) or a presence of a Trojan.
- Document Change Control process to ensure that changes do not introduce new vulnerabilities

The Alice Lloyd College community shall:

- Be instructed to not share their passwords, be advised on ethical surfing, watch out of phishing emails, etc.
- Be made aware of the risk of incidents such as data loss, virus outbreaks, data breach, etc.
- Be offered training on data awareness

Risk need to be identified, classified by category, and evaluated to calculate their potential loss. Real risk is hard to measure, and accept, but prioritizing the potential risks in order of which risk needs to be addressed first is attainable.

Categories of Risks

- Physical damage – fire, water, vandalism, power loss, and natural disasters
- Human interaction – accidental or intentional action or inaction that can disrupt productivity
- Equipment malfunction – failure of systems and peripheral devices
- Inside and outside attacks – hacking, cracking, and attacking
- Misuse of data – sharing confidential information, fraud, espionage, and theft
- Loss of data – intentional or unintentional loss of information through destructive means
- Application error – computation errors, input errors, etc.

Ways to deal with Risk

There are four basic ways of dealing with risks:

- Transfer it: If a company's total or residual risk is too high and it purchases an insurance then it is transfer of risk to the insurance company
- Reject it: If a company is in denial about its risk or ignore it, it is rejecting the risk
- Reduce it: If a company implements countermeasures, it is reducing the risk
- Accept it: If a company understands the risk and decides not to implement any kind of countermeasures it is accepting the risk. And this is actually what all computer systems boil down to. There is no way to mitigate the risk if the system is going to connect to the internet. Having only one user without any networking with other computer systems is the closet you can ever get to not having any risks.

Risk Assessments

Purpose

Performing risk assessments will allow the Alice Lloyd College Information Security Board to allocate its resources with maximum efficiency. Through the risk assessment, the agency determines the amount and nature of risk to which a system faces and this drives the security planning to mitigate the identified risks with proper mitigation controls.

Scope

This policy applies to all the Alice Lloyd College community.

Policy

Risk Assessment is a method of identifying vulnerabilities and threats and assessing the possible damage to determine where to implement security safeguards. This is done to help integrate the security plan and to prepare for what risk are out there.

Risk assessments shall be performed as early in the life cycle of a system as possible on any Alice Lloyd College system that holds or transmits data regardless of the hosting environment or classification of the data. If the assessment cannot be completed prior to acquisition, documented approval to delay must be acquired from the Security Officer as part of the procurement process and an assessment scheduled.

A Risk Assessment shall be completed on all information systems prior to implementation, whenever a significant change is made, and at least once every year thereafter.

The Risk Assessment shall be performed by the Information Systems Security Board. The Assessment shall consist of the following:

- Identify and document the assets.
- Identify and document the potential threats.
- Each potential threat shall be reviewed and the likelihood and impact of the threat being realized shall be documented.
- Identify if Alice Lloyd College has proper technology to mitigate each potential threat or if agency resources are inadequate.
- An overall Risk Determination will be calculated for each system.
- The Security Officer is responsible to verify that the Risk Determination is acceptable for each system, and that the controls and mitigations identified are sufficient.
- The most recent Risk Assessment shall be retained and stored within the project documentation.
- Alice Lloyd College shall implement a process of validation to ensure that a dynamic security plan is properly implemented.
- The security plan shall consist of the following:
    - Requirements and security controls that will be implemented to achieve the determined security stance.
    - Document how the security controls mitigate the organizational risks.
    - Create a risk monitoring threshold.
    - Alice Lloyd College will document how the agency security plan addresses the identified risks and if unique controls will be utilized to mitigate the risk.
- Risk implies uncertainty. If something is guaranteed to happen, it is not a risk.

Here are some common ways you can suffer financial damage:

- **Data loss.** Theft of trade secrets could cause you to lose business to your competitors. Theft of customer information could result in loss of trust and customer attrition.
- **System or application downtime.** If a system fails to perform its primary function, customers may be unable to place orders, employees may be unable to do their jobs or communicate, and so on.
- **Legal consequences.** If somebody steals data from one of your databases, even if that data is not particularly valuable, you can incur fines and other legal costs because you failed to comply with the data protection security requirements of HIPAA, PCI DSS or other compliance.

To perform an assessment:

1. **Collect a database of all hardware and softwar**e. This will be the Alice Lloyd College assets. This includes users, vendors, support personnel, networks, servers, wireless routers, access points, desktops, laptops, software applications, websites, IOS devices, personal mobile devices, physical security, logical security, environmental issues, equipment backup, file backup, credit card machine, etc. It includes any asset that it takes to perform a daily task.
2. **Identify Threats that can exist from these assets**. Prepare a list of all potential threats that Alice Lloyd College could face based on past experiences, experiences of your peers, and expected threats. These are your risks. Identify gaps (shortfalls) in your system that these threats could potentially exploit.

   Classify these threats. Classifications may consist of:
   - Physical damage – fire, water, vandalism, power loss, and natural disasters
   - Human interaction – accidental or intentional action or inaction that can disrupt productivity
   - Equipment malfunction – failure of systems and peripheral devices
   - Inside and outside attacks – hacking, cracking, and attacking
   - Misuse of data – sharing confidential information, fraud, espionage, and theft
   - Loss of data – intentional or unintentional loss of information through destructive means
   - Application error – computation errors, input errors, etc.

3. **Estimate the Impact**. What would the impact/consequences be of these risks? The impact could be in monetary terms, legal action, data loss, and system or application downtime. Categorize the impact of the risk as *High*, *Medium* or *Low*, based on its severity or cost.
4. **Determine the likelihood**. Categorize the likelihood that each potential risk would happen as *High*, Medium or *Low*. The risk level increases if the likelihood is high.
5. **Plan the Controls**. List the existing control system in place and outline further actions that can help mitigate the identified risk. Depending on the level of Risk, the following guidelines can be used for each level if there is no plan of action:
   - **High**- A plan for corrective measure should be developed as soon as possible if there is none.
   - **Medium**- A plan for corrective measure should be developed within a reasonable period of time.
   - **Low**- The security board must decide whether to accept the risk or implement corrective actions.
6. Document the results

Example:

RISK	What asset does it involve	What is the impact	What is the likelihood	What are existing controls	What other controls can we implement	Notes:
Power to server room will go out	All networking components, Jenzabar, web surfing email, PowerFaids	HIGH	Medium	Server room is on a battery backup that is in turn powered by a natural gas generator.	NA	We fill that existing controls are adequate.

Rating:

		Tech Performance	Cost	Schedule
HIGH	A risk event, that if it occurs, will have a severe impact on achieving desired results to the extent that one or more if its critical outcome objectives will not be achieved.	Performance unacceptable	Significant cost and down time. May result in data loss or loss of work.	Daily workload delayed
MEDIUM	A risk event, that if it occurs, will have a moderate impact on achieving desired results to the extent that one or more stated outcome objectives will fall well below goals but above minimum levels.	Performance below goal	Does not require significant cost or reserves	Moderate schedule slip
LOW	A risk event that, it if occurs, will have little or no impact on achieving outcome objectives.	No Impact	Not affected	Schedule not affected.

The below template can be used for assessments:

IMPACT	LIKELIHOOD		
	HIGH	MEDIUM	LOW
HIGH			
MEDIUM			
LOW			

Vulnerability Scanning

Alice Lloyd College shall implement a vulnerability management solution to identify weakness in information systems on the network. The solution should include performing vulnerability assessments for hardware and software on the network, and basic vulnerability scanning to identify potential risks that can be exploited, including missing patches and unnecessary open ports on servers and workstations.

Alice Lloyd College shall use an automated tool to perform vulnerability scanning. These scans will be performed on a periodic basis, mostly random, at minimum annually. The department of Information Technology should evaluate the results of the scans and determine mitigating controls or corrective actions for the detected vulnerabilities. These vulnerabilities should be reviewed and tracked in a vulnerability management document from inception through mitigation, correction, or acceptance

Alice Lloyd College will have an external scan and penetration test performed by an outside source annually.

Reports on the internal and external scans will be made available as needed.

1.12 Security Assessment

Security Assessment

Purpose

Establish a procedure and process to evaluate security standards on a periodic bases to meet regulatory compliance objectives.

Scope

This scope applies to Alice Lloyd College's Department of Information Technology, its Information Systems Security Board, and its Information Systems Security Plan.

Policy

Alice Lloyd College has implemented these set up policies and procedures to be called the "Alice Lloyd College Information Technology Policies and Procedures and Information Systems Security Plan." The policies listed in it are referred to as its "Safe Guards".

This Security Plan is governed and maintained by Alice Lloyd College's Security Board and subject to an annual review. The board is made up of the Alice Lloyd College Director of Information Technology and various members of the Alice Lloyd College community.

This plan will follow and adopt the NIST SP 800-171r1 Security Standards.

This plan will be reviewed annually, or more often as needed in the event of an Incident.

By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in this set of plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

Alice Lloyd College ensures that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the life cycle.

A plan of action should be designed to correct deficiencies and reduce or eliminate vulnerabilities in the Security Plan. The plan of action should describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented.

1.13 Systems & Communication Protection

Systems and Communications

Purpose

This policy establishes processes to ensure a secure and reliable information systems.

Scope

This policy applies to all Alice Lloyd College information systems.

Policy

- All network protocols that connect to external networks, such as the internet shall be protected by boundary protection systems that monitor and control communications, aka firewall.
- Alice Lloyd College shall establish network segmentation to create additional security layers between buildings.
- Alice Lloyd College shall perform security assessments against all information systems prior to installation on production environments and scheduled thereafter at least annually thereafter to meet the security requirements of the system.
- All information systems will receive scheduled vulnerability scans with the frequency being associated to their data classification. Once corrective actions are in place the vulnerability assessment process will be re-initiated for confirmation of mitigation.
- Information technology staff shall monitor for security alerts and advisories relative to the technologies that Alice Lloyd College has implemented in production.
- Alice Lloyd College shall implement a patch management process that includes testing, validation and configuration management prior to enterprise deployment for all high and critical level patches at a minimum. Lower level patches are independently assessed based on their impact to the Alice Lloyd College computing environment
- Alice Lloyd College shall, at a minimum, implement tools which monitor and report the health and integrity of systems that contains protected information. Alerts by the monitoring tool shall be mitigated.
- Maintain a high-level security profile and do modify any operational practice at the request of a third-party auditor. All auditing parameters require the IT Directors approval before proceeding. All physical and logical security control testing is to be highly documented
- Risk shall be identified and evaluated yearly.

Encryption

Data from the Jenzabar and PowerFaids SQL databases are encrypted by the following standards:

- AES-256
- FIPS 140-2
- FISMA
- HIPAA
- PCI
- Basel II
- California Security Breach Information Act (SB1386)
- EU Data Protection Directive 95/46/EC

These are protected at rest and in transit.

Such data from these databases consist of the following and is the main source of sensitive data belonging to Alice Lloyd College:

- Student names
- Student ID numbers for Alice Lloyd College
- Social Security Numbers
- Addresses
- Alumni names
- Donor names
- Student Loan amounts and their student loan IDs

Local files on the Alice Lloyd College network are not encrypted.

1.14 System & Information Integrity

System and Information Integrity

Purpose

The purpose of this policy is to set a policy that will protect the integrity of the Alice Lloyd College network, its peripherals and its data.

Scope

This policy applies to all Alice Lloyd College computing platforms, including its workstations and servers.

Policy

Integrity

- Integrity of data is protected when the assurance of accuracy and reliability of information and system is provided, and unauthorized modification is prevented.
- Threat sources
    - Viruses
    - Logic bombs
    - Backdoors
- Countermeasures
    - Strict access control
    - Intrusion detection
    - Hashing

Availability

- Availability ensures reliability and timely access to data and resources to authorized individuals.
- Threat sources
    - Device or software failure.
    - Environmental issues like heat, cold, humidity, static electricity, and contaminants can also affect system availability.
    - Denial-of-service (DoS) attacks
- Countermeasures
    - Maintaining backups to replace the failed system
    - IDS to monitor the network traffic and host system activities
    - Use of certain firewall and router configurations

Antimalware/Antivirus

Alice Lloyd College uses McAfee Security Suite for antivirus software. This is installed on all Alice Lloyd College IBM compatible computers. It is configured to do a scan on startup and is constantly doing a background scan as well as doing an email scan. Web Control is enabled, giving a security check and site report for any URL that is accessed. Pornography and other unsafe sites are blocked by the Web Control.

Alice Lloyd College uses McAfee MVision for malware detection. This is EPO cloud based.

Random routine checks of DAT updates shall be performed and logged. These random checks will be performed approximately every two weeks.

The set of redundant Checkpoint firewalls does virus inspection.

Monitoring

Alice Lloyd College uses Netwrix Auditor to confirm that every change in their Active Directory and Group Policy is performed according to the internal security policy, as well as using the same line of software to monitor shares and windows servers. This software provides comprehensive compliance reporting and simplify the process of gathering audit data and well as alerting to changes. Netwrix Auditor is a visibility and governance platform that enables control over changes, configurations and access in hybrid cloud IT environments to protect data at rest regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Email Notification Reports

Notifications are sent from Office 365 that notify of:

- suspicious email sending patterns
- Elevation of admin privileges
- Email reported as Spam or malware
- Email sending exceeded
- Creation of forwarding or redirect rules
- User restricted from sending email

Deep Freeze Protection

The public access computers have an application called Deep Freeze installed. This is meant to protect the hard drives from becoming permanently infected from virus and malware.

Windows Updates

Windows updates and other recommended updates for faculty and staff computers are configured through a GPO.

They are set for auto download and install every Thursday at 1:00 AM.

Updates are then scheduled to check again every 22 hours. This is designed to install any missed updates or any that may have been skipped because of errors.

If a restart is needed, the system will prompt the user to restart now or postpone. They should be prompted for these three times and on the third time it will go ahead and restart.

Intrusion and Detection

Alice Lloyd College has a set of redundant Checkpoint firewalls that Information Technology has Intrusion Detection-Threat Prevention-IPS running on that uses the vulnerabilities/threats that Checkpoint provides in their definition files, which are downloaded from Checkpoints repository. The College uses the recommended actions from Checkpoint on whether it is blocked or not. If any item is blocked and needed, then it is revisited and allowed as needed. Reports can be ran daily, last 24 hours, seven days, or custom timeframes and there is a dashboard that shows a weeks' worth of hits.

Patch Management

With the increase of worms and viruses on the Internet, operating system updates are now a part of daily life. In order to reduce the amount of time individuals need to spend managing the security of their systems, and to improve the overall security posture at the College, Information Technology has taken additional steps to improve the security of college owned computers. Through a centrally managed system, Information Technology will "harden" operating systems by applying critical patches released by Microsoft. Applying these patches will limit the vulnerabilities that a worm or virus can take advantage of, reducing the chances of a user becoming infected. This process is monitored through Microsoft's WSUS platform. With WSUS, reports can be generated showing number of updates needing per computer. Spot checks are also performed every Friday.

Secure Credentials

A secure password vault is used for the storage of secure credentials. The host is *Solarwinds PassPortal*. This method is more secure than having the passwords stored in a document on a computer. This platform uses multi-factor authentication and used by the IT department

Network admin credentials are stored in the Alice Lloyd College safe in an envelope marked Network Credentials. Only the Business Affairs employees have access to this safe, and it is behind a locked door.

Awareness

Extreme caution is encouraged on any suspicious attachments that come in through email. Please contact the IT department if you are uncertain about an attachment.

Extreme caution is encouraged about surfing any potential unsafe site. Pornographic and Peer to Peer sites are blocked for the purpose of malware/ethical and copyright decisions.

Caution and potential risk awareness is encouraged about swapping jump drives and spreading email

1.15 Vendor Program

Vendor Program

Purpose

To define a policy for vendor, cloud, 3rd parties and service providers and address their need and security issues. This policy provides resources to assist in conducting due diligence on Alice Lloyd College vendors, negotiating and contracting with them, and managing risk in ongoing vendor relationships.

Scope

This policy applies to all Alice Lloyd College employees and its vendors/3rd parties/external relationships.

Policy

Vendors play an important role in the support of hardware, software, management, and operations for Alice Lloyd College. Many organizations rely on vendors to perform all kinds of services, which can help reduce overall costs and administrative burdens. Setting appropriate limits and controls on what can be seen, copied, modified, and controlled by vendors reduces the risk of exposure, breach, liability, loss of trust and other security risk to Alice Lloyd College.

Alice Lloyd College has to ensure that vendors have the appropriate security and privacy protections in place, so that when data is entrusted to them, they continue to meet the legal and regulatory obligations to keep that data secure.

According to the PCI Data Security Standard (PCI DSS) v3.0, "A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers." But doing so does not remove the burden of cybersecurity and may involve new risk.

Vendors and their contracted employees shall comply with all applicable Alice Lloyd College policies, procedures, and agreements including but not limited to policies in the following areas:

- Privacy
- Security
- Auditing
- Software licensing
- Acceptable use

Vendors often use personal information supplied by their clients in order to provide services. Shared personal information can include information on a retailer's employees, customers, business partners and other parties.

Information acquired by the vendor during the course of contract execution cannot be used for any other purposes other than those specified in the contract and shall not be divulged to others.

Alice Lloyd College must ensure that the following data is secure if it is being handled, transcribed or hosted for Alice Lloyd College:

- Social Security number
- Driver's license number
- Credit/ debit card numbers
- Passport number
- Bank account information

- Date of birth
- Medicalinformation
- Biometric data (e.g., fingerprints)
- Mother's maiden name
- E-mail/username in combination with password/security question andanswer

*This data is what is referred to from now on when data or confidential items or confidential information is mentioned.

This can be accomplished by:

- Conducting privacy and security due diligence when selecting a Vendor
- Ensuring that the Vendor agreement contains the appropriate safeguards for personal data
- Monitor Vendors to verify that they comply with their privacy and security obligations throughout the life of the relationship

Some questions to bring to surface before contracting with 3rd party include:

- Does the service provider maintain an information security management program?
- How often does the service provider conduct security assessments, including vulnerability scans and penetration tests?
- How does the service provider validate its workforce? Do they perform background checks?
- How does the service provider control logical, as well as physical, access to cardholder data?
- Are there adequate controls in place to protect against malware?
- What identification and authentication methods does the service provider use? Is each individual assigned unique credentials?

Vendor Agreement Clauses shall be uses to establish a standard of care to reduce the risk and liabilities that may arise from a vendor's data security breach, a malware outbreak orientating from a vendor or any other Cybersecurity issue. This agreement clause may exist of:

- Define the scope of information protected
- If duties will be extended to other parties
- Require incident reporting by the vendor
- Confidentiality clauses
- Restrictions on use or further disclosure of information
- Limitations of liability
- Survivability clauses
- Data retention requirements
- Insurance requirements
- Termination clause

Vendor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the data, ensuring in each case that access is strictly limited to those individuals who need to know/access the data, as strictly necessary for the purposes of the agreement, and to comply with laws in the

context of that individual's duties, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Vendor shall notify Alice Lloyd College without delay upon becoming aware of a data breach affecting data, providing Alice Lloyd College with sufficient information to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

Vendor states that it will not engage in any transfer of Alice Lloyd College data.

Vendor shall implement appropriate measures designed to ensure the confidentiality and security of Data, protect against any anticipated hazards or threats to the integrity or security of such information, protect against unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm.

Even if the vendor does not have any involvement with Data, the vendor can still expose a risk if they provide remote assistance from an unpatched/un-kept computer.

Vendor should have a SOC2 report or an equivalent such as a "Standard of Care" and shall me made available to Alice Lloyd College upon request or upon an incident. SOC 2 is the Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy, formed under the AICPA Trust Services Principles and Criteria. A SOC 2 report or an improved equivalent shall be requested and kept on file for each vendor.

Vendor agrees at all times to maintain commercially reasonable network security that, at a minimum, includes: network firewall provisioning, intrusion detection/prevention, and periodic third-party penetration testing.

Vendor agrees to protect and maintain the security of data with protection security measures that include maintaining secure environments that are patched and up to date with all appropriate security updates and to provide appropriate Data Storage and Backup when applicable.

Vendor agrees that upon termination of the Agreement, it shall return all data to Alice Lloyd College in a useable electronic form, and erase, destroy, and render unreadable all data in its entirety.

Vendor agrees that, as required by applicable state and federal law, auditors from state, federal, shall have the option to audit the outsourced service.

Vendor acknowledges that unauthorized disclosure or use of the data may irreparably damage Alice Lloyd College in such a way that adequate compensation could not be obtained from damages in an action at law.

All present and new vendors will be complied along with the data that they may transcribe, provide or host, or services that they provide along with a risk rating. If obtainable, a SOC2 report or Standard of Care (*Defines the standard of care a Vendor must take, requires the Vendor to conduct risk assessments and keep their systems secure and patched*) shall be requested and kept with this vendor compilation along with any other maintenance/service agreements.

Remote Access

Remote vendor access must be uniquely identifiable and password management must comply with Alice Lloyd College password standards. Alice Lloyd College reserves the right to determine applicable virtual private network, remote access and encryption technologies used to access their systems and network. Remote access will be granted with least privilege principal. The remote access ability and remote access accounts will remain disabled until they are ready to be used and must be activated and monitored by the

Alice Lloyd College Information Technology Department. Remote Access is covered in the Logical Access and Remote Access areas of this set of policies.

Cloud Use

Alice Lloyd College employees should not use a self-provisioned cloud service to process, share, store, or otherwise manage crucial Alice Lloyd College protected data. Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. Self-provisioned agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice.

Risks with using self-provisioned cloud services which will need to be addressed before any service is approved include:

- Unclear, and potentially poor access control or general security provisions
- Sudden loss of service without notification
- Sudden loss of data without notification
- Data stored, processed, or shared on cloud service is often mined for resale to third parties that may compromise people's privacy
- The exclusive intellectual rights to the data stored, processed, or shared on cloud service may become compromised.

All Alice Lloyd College proposed cloud services will be reviewed and approved by the Director of Information Technology to ensure agreements with cloud service providers are clearly defined and well known by the agency.

Example Vendor Clause:

Business and Other Proprietary Information Clause – *Defines the scope of the information protected.*

> Vendor agrees that business and other proprietary information of any type generated in connection with work is confidential. Such information may include business discussions and deliberations, compliance related information, meeting minutes, documents, network transmissions, data/records, and personal information related to the Retailer's employees or customers.
>
> Business and other proprietary information obtained or learned during the course of Vendor's relationship will not be disclosed to any unauthorized party; or used or disclosed after termination of the relationship. Vendor promises to return or destroy all business and other proprietary information to the Retailer within 14 days after termination of the relationship between the parties.

Vendor's Reasonable Security Measures Clause – *Defines the standard of care a Vendor must take, requires the Vendor to conduct risk assessments, and allows a Retailer to confirm Vendor's compliance.*

> Vendor promises to conduct an internal, data security risk assessment and implement reasonable administrative, technical, and physical safeguards designed to protect the Retailer's business and

other proprietary information from unauthorized disclosure. Vendor promises to update the risk assessment and related safeguards at least annually. Upon request by the Retailer, Vendor agrees to provide documentation sufficient to demonstrate Vendor's compliance with the terms of this paragraph.

Vendor's Reporting of Instances of Noncompliance Clause – *Requires Vendor to notify of any noncompliance with the Agreement within a defined period.*

Vendor agrees to report within 24 hours to the Alice Lloyd Colleges contact any violations of this agreement, violations of the Acceptable Use Policy, or data security incidents that may result in the unauthorized disclosure of the Retailer's business and other proprietary information.

Vendor Employees, Agents, and Subcontractors Clause – *Extends the standard of care to parties within Vendor's control.*

Vendor will require its employees, agents, and subcontractors to observe and comply with the terms of this agreement. To the extent necessary, Vendor will provide training to such employees, agents, and subcontractors to promote compliance with this agreement.

Vendor's Requirement to Maintain Insurance Clause – *Ensures Vendor maintain sufficient insurance amounts for costs that may be necessary to adequately respond to a data security event.*

Indemnification Clause – *Provides a contractual avenue for the Retailer to recover damages it may have had to pay as a result of Vendor's unauthorized disclosure of the Retailer's information.*

1.16 Business Continuity Plan

Business Continuity Plan

Purpose

To establish a policy to keep day to day business needs secure.

Information Technology includes many components such as networks, servers, hubs, switches, workstations, wireless devices and many applications.

If a facility is damaged or technology services is disrupted, business is impacted and the financial losses can begin to grow. Recovery strategies for Information Technology should be developed so technology can be restored in time to meet the daily needs of the business. These strategies shall be labeled as the Disaster and Recovery Plan. Recovery strategies are alternate means to restore business operations to a minimum acceptable level following a business disruption and are prioritized by recovery time objectives. Manual workarounds should be part of the plan when needed so business can continue while computer systems are being restored.

Recovery of a critical or time-sensitive process requires time, planning and resources. The Information Systems Security Board should include disaster recovery of their risk assessments. Completed assessments can be used to determine the resource requirements for recovery strategies.

Following an incident that disrupts business operations, resources will be needed to carry out recovery strategies and to restore normal business operations. Resources can come from within the business or be provided by third party vendors. Since all resources cannot be replaced immediately following a loss, the Director should estimate the resources that will be needed in the hours, days and weeks following an incident. Extra personnel may need to be employed during this recovery process.

Recovery strategies require resources including people, facilities, equipment, materials and technology equipment (servers, hubs, switches, firewalls routers). An analysis of the resources required to execute recovery strategies should be conducted and should be included in the disaster plan.

Possible alternatives to recovery should be explored and the best scenario implemented.

Data Center operations may be relocated to an alternate site. This strategy assumes that the new site has the resources and capacity to assume the roles of the Data Center, thus as much planning and setup that can happen should take place in the time that the Recovery and Disaster Plan is developed.

The Recovery and Disaster plan should cover aspects from data loss and recovery to a standalone server crash and recovery to a system wide Data Center disaster and recovery. Steps of how to achieve these task and test performed on recovery processes shall be documented with the plan.

The core requirements for the Alice Lloyd College network and the minimum for recovery in a complete disaster consist of:

1. Internet Access with the required IP Address
2. Firewall with appropriate rules
3. An Active Directory server with DHCP and DNS

Business Impact Assessment

Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuance plan; it includes a planning component to develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied. One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, a business may be able to continue more or less normally if the cafeteria has to close, but would come to a complete halt if the information system crashes.

Alice Lloyd Colleges Impact analysis is as follows:

RISK	What asset does it involve	What is the impact	What is the likelihood	What are existing controls	What other controls can we implement	Notes:
Power to Data Center will go out	All networking components, Jenzabar, web surfing email, PowerFaids	HIGH	Low	Data Center is on a battery backup that is in turn powered by a natural gas generator.	NA	We feel that existing controls are adequate.
Firewall to crash.	Connection to outside world, no web, no email and no Jenzabar.	High	Low	We have redundant firewalls. If one crashes the other will take its place, just need to power the bad one down.	NA	We feel that this adequate.
DHCP server to crash	No computers would get an IP, meaning no connection.	High	Medium	There is a virtual backup of the DHCP server. It would just need brought online once the main one		

				is taken down.		
Active Directory server to crash	Computers or users could not log on	High	Medium	There is more than one domain controller to take place of one that goes down and a virtual backup of one that can be brought online.		
DNS Server to crash	Computers can't get web pages	Medium	Medium	There is more than one DNS Server. Also, a virtual back up of one that can be brought online.		If used a secondary DNS, would have to change the IP address for DNS on each DHCP scope in DHCP server.
Data Center to catch fire	All IT infrastructure	HIGH	Low	There is a halon fire suppression system that hopefully would put the fire out. It also has its own smoke detector.		
Complete Data Center disaster	All IT infrastructure	HIGH	Low	All critical components of a network would need to be set up somewhere and made a networking infrastructure.	Having a firewall and a Domain Controller with DHCP and DNS in place in	

				Would need an Internet Connection, a firewall, a server with DHCP, DNS and Active Directory.	another building would better prepare a Data Center disaster.	

1.17 Social Engineering

Social Engineering Policy

Social Engineering is defined as a form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites. In addition, hackers may try to exploit a user's lack of knowledge; thanks to the speed of technology, many consumers and employees don't realize the full value of personal data and are unsure how to best protect this information.

Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.

For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password. Almost every type of attack contains some kind of social engineering, from the classic email "phishing" to virus scams. Phishing emails attempt to convince users they are in fact from legitimate sources, in the hopes of procuring even a small bit of personal or company data. Emails that contain virus-filled attachments, meanwhile, often purport to be from trusted contacts or offer media content that seems innocuous, such as "funny" or "cute" videos.

In some cases, attackers use more simple methods of social engineering to gain network or computer access. Some attacks, meanwhile, rely on actual communication between attackers and victims where the attacker pressures the user into granting network access under the notification of a serious problem that needs immediate attention. Anger, guilt and sadness are all used in equal measure to convince users their help is needed and they cannot refuse. Finally, it's important to beware of social engineering as a means of confusion.

Protection against social engineering starts with education and training — users must be trained to never click on suspicious links and always keep their log-in credentials in a secure place at the office or at home. In the event that social tactics are successful, however, the likely result is a malware infection. To combat rootkits, Trojans and other bots, it's critical to employ a high-quality Internet security solution that can both eliminate infections and help track their source.

Worm Attacks--The cybercriminal will aim to attract the user’s attention to the link or infected file – and then get the user to click on it.

Malware Link delivery channels-- Links to infected sites can be sent via email, ICQ and other IM systems – or by Internet chat rooms. Mobile viruses are often delivered by SMS message.

Whichever delivery method is used, the message will usually contain eye-catching or intriguing words that encourage the unsuspecting user to click on the link. This method of penetrating a system can allow the malware to bypass the mail server’s antivirus filters.

Peer-to-Peer (P2P) network attacks

P2P networks are also used to distribute malware. A worm or a Trojan virus will appear on the P2P network, but will be named in a way that’s likely to attract attention and get users to download and launch the file

Victims may respond to a fake offer of a free utility or a guide that promises:

- Free Internet or mobile communications access
- The chance to download a credit card number generator
- A method to increase the victim's online account balance… or other illegal benefits

Once attacked and infected, Cybercriminals may then:

- Steal access codes to bank accounts
- Advertise products or services on a victim's computer
- Illegally use an infected computer's resources – to develop and run:
    - Spam campaigns
    - Distributed Network Attacks (also called DDoS attacks)
    - Blackmailing operations
    - Email from a friend
    - Email from another trusted source
    - Baiting Scenarios
    - Response to a question you never had
    - Creating distrust

Some social engineering is all about creating distrust, or starting conflicts; these are often carried out by people you know and who are angry with you, but it is also done by disgruntled people just trying to wreak havoc. This form of social engineering often begins by gaining access to an email account or another communication account on a messenger client, social network, chat, forum, etc. They accomplish this either by hacking, social engineering, or simply guessing really weak passwords.

The malicious person may then alter sensitive or private communications (including images and audio) using basic editing techniques and forwards these to other people to create drama, distrust, embarrassment, etc. They may make it look like it was accidentally sent, or appear like they are letting you know what is 'really' going on.

Alternatively, they may use the altered material to extort money either from the person they hacked or from the supposed recipient.

There are literally thousands of variations to social engineering attacks, and you may see multiple forms of exploits in a single attack. Then the criminal is likely to sell your information to others so they too can run their exploits against you, your friends, your friends' friends, and so on as criminals leverage people's misplaced trust.

Tips to Remember:

- Slow down. Spammers want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- Research the facts. Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.

- Don’t let a link be in control of where you land. Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.
- Email hijacking is rampant. Hackers, spammers, and social engineers taking over control of people’s email accounts (and other communication accounts) has become rampant. Once they control an email account, they prey on the trust of the person’s contacts. Even when the sender appears to be someone you know, if you aren’t expecting an email with a link or attachment check with your friend before opening links or downloading.
- Beware of any download. If you don’t know the sender personally AND expect a file from them, downloading anything is a mistake.
- Foreign offers are fake. If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.

Ways to Protect Yourself:

- Delete any request for financial information or passwords. If you get asked to reply to a message with personal information, it’s a scam.
- Reject requests for help or offers of help.
- Set spam filters to high
- Secure computing devices. Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn’t automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks.

Training

- Publish Phishing announcements
- Review exiting processes, procedures and separation duties, adding add extra controls if needed.
- Consider new policies as needed
- Review, refine and test your incident management and phishing systems

1.18 Social Media

Social Networking Policy

Purpose

The policy is to establish specific guidelines for the Alice Lloyd College community's use of social networking sites.

Scope

This policy applies to all individuals of the Alice Lloyd College community. This policy applies to all social networking sites such as, but not limited to Facebook, Twitter, Instagram and similar services.

Policy

Alice Lloyd College permits surfing social media sites on its network. Its use by Alice Lloyd College employees during work hours may be infringed upon, so different departments may enforce rules upon its use.

Social media sites use in the public access computing areas should come second to any activity related to classwork. There is a lab rule pertaining to this:

- The computer labs throughout campus are set up for education use only. Lab attendants may ask non-educated users to relinquish their computer if the computer is needed by a student wishing to use it for educational purposes. This applies to all student-computing areas.

Alice Lloyd College Owned Social Media

Alice Lloyd College will have only one social networking presence per platform which will be managed by the Marketing Department.

Use of social networking sites by Alice Lloyd College shall be consistent with applicable federal and state laws, regulations, and policies including ethics, privacy, disclosure of protected information, and all information technology security and data privacy policies.

Privacy Policy

This Privacy Policy describes Alice Lloyd College's current policies and practices regarding information collected through the Alice Lloyd College website. This Privacy Policy is subject to change; please review this policy regularly to note any changes.

Google Analytics

Alice Lloyd College uses Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses cookies; these cookies are used to track the use and performance of the Alice Lloyd College website and services. Google has a Privacy Policy which can be reviewed.

Use of Third-Party Services

Alice Lloyd College will sometimes share information gathered from its donors with select third-party vendors who assist other parties and Alice Lloyd College with promoting and marketing products. You may request that Alice Lloyd College not share your information for these purposes by contacting margosparkman@alc.edu.

Contact Information

If you have questions or concerns about this policy, please contact us at webmaster@alc.edu.

Website Content

Content uploaded to the official website, including images and official college documents, belongs to Alice Lloyd College and will be maintained by Alice Lloyd College. Updates to the content on the Alice Lloyd College website must be approved by the Marketing and Communications department.

Social Media

All official Alice Lloyd College social media accounts are owned by the College. The Marketing Department has sole authority to manage, administer, and post to these accounts. All content, including images and video, published to any of the official social media accounts are owned by Alice Lloyd College. At this time, these accounts include the following:

- Twitter: @ALCeagles
- Facebook: Alice Lloyd College, Alice Lloyd College Athletics
- YouTube: Alice Lloyd College
- LinkedIn: Alice Lloyd College
- Instagram: @alicelloydcollege

The Marketing Department reserves the right to remove comments published on any of the above listed social media accounts that defame the college and/or subsequent members thereof.

Any social media accounts not listed above are not owned or operated by the Marketing Department at the College. Accounts using the Alice Lloyd College, any official ALC logo, or any college-owned image, will be reported if the content posted on the account does not match the views of the College.

In order to add content to the official Alice Lloyd College social media accounts, the Marketing and Communications Department must feel that the content is beneficial for the social media account and approve all aspects of the post.

Confidentiality

Controls are in place to assure that no non-public information is distributed or uploaded to the College's website or social media accounts. Additionally, Alice Lloyd College will comply with all applicable federal, state, and local laws regarding the privacy and security of visitor information.

When an Alice Lloyd College staff member that manages a social networking account leaves Alice Lloyd College, the account passwords will be changed to rule out the chances of unauthorized postings.

1.19 Assets

Assets

Purpose

This policy is to ensure Alice Lloyd College's assets are inventoried.

Scope

This policy applies equally to the Information Technology Department.

Policy

The Alice Lloyd College Information Technology Department shall assign each piece of IT hardware purchased that is valued at $250.00 and above a unique inventory asset number. This number will be on an asset tag and will be placed on the device.

All Alice Lloyd College technology inventoried items will be maintained in a searchable inventory system for the life of each item. Assigned to every inventory item there must be an Alice Lloyd College staff member identified as the primary person, which is held accountable for the location tracking of the asset. The inventory shall document at least each items description (brand, make and model), asset number, purchase date, purchase price, location and assigned staff member.

Software shall be inventoried in a database stating title, purchase date, purchase amount and number of licenses with updates of how many are in use. Copy of licenses shall be kept.

1.20 Purchasing

Purchasing Policy

Purpose

This policy is to ensure Alice Lloyd College's information technology security requirements are addressed in the acquisition process, ensuring only authorized software is purchased and that all purchases follow the baseline configurations.

Scope

This policy applies equally to all Alice Lloyd College individuals involved in the acquisition of information systems, system components, software, or contracted services.

Policy

All purchases must be approved through the Information Technology Office to assure software and hardware meet baseline configurations and that security requirements are met.

The Alice Lloyd College Information Technology Department shall process all technology purchases for the Alice Lloyd College community. Exceptions to this are keyboards, mice, speakers, toner and ink.

All Alice Lloyd College technology purchases must be addressed through the department head and an account number obtained before being submitted to the Alice Lloyd College Information Technology Department.

All new purchases shall be inventoried before delivery/setup.

Quotes for hardware and software shall be obtained for a purchase of multiple items.

Records shall be maintained in the form of quote, purchase order and invoice.

1.21 Key Scan/Card Access/Card program

Alice Lloyd College Card Program and Card Access

ID cards are made in the Information Technology Office and distributed to Faculty, Staff and Students.

These serve as:

- The official Alice Lloyd College ID card
- Lunch Card and Library card for students
- Keycard to certain buildings and rooms.

Rules and Responsibilities:

- Cards are not to be lent.
- If your ID card is lost/stolen, please notify the IT department as soon as possible so the card can be deactivated.
- There is a $10.00 replacement cost for lost, stolen, name change or abused cards.
- If you are caught with someone else's card, you will be reported to the Pippa Passes Police Department.
- Department heads/direct supervisors must request access for their employees unless it's an area that they will have default access to. The doors will be on a need for use basis.
- Some doors will be on a time schedule while others stay locked 24/7. Classrooms will stay locked 24/7 and all faculty will have access to these areas 24/7.
- Dorms are locked 24/7. Males will have access to all male dorms, while females will have access to all female dorms. Commuters will not have access to dorms.
- The ID card will be used for convocation access. Please scan your card upon entering convocation to show convocation attendance.
- Please do not prop the doors open, as some of the doors have an auditable alarm that will sound if open for more than a minute. If caught propping the doors open, you will be fined $50.00 to your student account.
- Please do not try to yank the doors open. If you are a student and caught doing so, you will be fined $50.00 to your student account. There are cameras on the doors. If doors are damaged, you may be fined part or up to the entire amount of repair cost.
- Ensure that all doors used are secured when leaving a locked room or building and do not allow anyone that is not permitted in access with you.

Employees: Building Access through the ID card is terminated upon your departure/termination and employees are asked to turn their ID card over to IT at this time. Deactivation may happen sooner in special circumstances. This must be submitted in a written request from the direct supervisor, security or a line officer of Alice Lloyd College.

Students: Building access is terminated on the following Monday from the last day of finals. Winter or summer work access will be given following the recipient of a list of workers from the Alice Lloyd College Student Work Office. Students who have completed the withdrawal process will have their access terminated upon notification from the Registrar's office.

1.22 Printing

Student Printing

At the start of every semester, each student starts with a credit of $10.00 for printing.

The cost of printing is:

- Black/white print is .05 per page
- Color print is .020 per page.

Additional funds may be added to the account by paying the desired amount in the Business Office and then bringing the receipt to the Information Technology Offices where the funds will then be placed on your account.

The funds and amount printed are reset every semester. Any added funds will not be carried over.

It is your responsibility to keep your account password secure. Funds will not be credited back to your account from unknown printing that was performed from your account.

Funds used from printer jams, etc. can be reimbursed by seeing a member of the Alice Lloyd College Information Technology Office.

1.23 Other Policies and Procedures

Voice over IP Telephone (VOIP)

Alice Lloyd College provides telephone service to Alice Lloyd College offices and common areas in the dormitories by *Avaya IP Office* and *Voice over IP Telephones*. Telephone service is not available in individual dormitory rooms. No one is permitted to bring in your own VOIP telephone. Students are unable to make long distance calls on phones that are located in the dormitory common areas.

Voice Mail

Voicemail is provided for all Alice Lloyd College employees that have a phone extension. Voice mail can be checked on campus by pressing the ENVELOPE button on your Avaya phone. Voicemail can be accessed off campus by dialing 606-368-6400 but has to be password activated by the employee from within the office. Voicemail is intended for the individual user and accessing someone else's voicemail without their consent is against Alice Lloyd College policy.

Personal Items and the Alice Lloyd College Network

Individuals (faculty, staff or students) may not bring any network equipment from home and place it on the Alice Lloyd College network. This includes wireless routers, extenders, repeaters, switches, hubs, etc. Any device found on the Alice Lloyd College network will become the property of Alice Lloyd College.

Windows Server Edition operating systems or Linux/Unix computers are not to be joined to the network.

Faculty and staff bringing any personal hardware in to Alice Lloyd College is not permitted and will not be supported (scanners, printers, etc.).

Alice Lloyd College Information Technology **does not** support personally owned computers.

Student computer support is limited to assisting in getting on the campus network.

Support will not be given in attempt to join to the network for gaming consoles, streaming devices, etc.

Alice Lloyd College does not support student owned hardware such as printers, scanners, tablets, cell phones, etc.

Alice Lloyd Owned Equipment

Laptops and projectors may be checked out from the Information Technology offices for special occasions by Alice Lloyd College employees and must be signed for. These are not intended for long time use and must be returned within seven days unless otherwise noted at checkout. Individuals will be responsible for the repair/replacement of any damaged, lost or stolen items that are in their possession.

Alice Lloyd College employees are responsible for the repair or replacement of any equipment assigned to them such as a laptop, tablet, phone, etc. These items must be returned upon request and must be accounted for during the annual inventory process. These items must be returned upon the employee's departure or termination from Alice Lloyd College/June Buchanan School. Failure to do so may resort in holding of funds of the last pay period.

Fire damaged or stolen equipment needs to be reported and a fire/police report submitted to the Information Technology department.

Students may not check out equipment.

Software

Microsoft Office:

- Is available to students and is self-installed by the student by logging onto their student email from the computer they wish to install the Microsoft Office Suite on. From the main screen, there will be an install option. The Microsoft Office subscription will be current as long as the student is currently enrolled.
- Microsoft Office is not available to faculty/staff.

Windows operating systems cannot be provided to employees or students.

Although Alice Lloyd College cannot provide it, the Alice Lloyd College Information Technology Department recommends SPYBOT and MALWARE BYTES to students. These can be found at www.downloads.com.

No one is to install any software on Alice Lloyd College computers without the knowledge and approval of the Alice Lloyd College Information Technology Department.

Equipment Disposal

Any technology equipment must be turned over to the Information Technology offices for disposal. Exceptions are keyboards, mice, and speakers. Any media must be defaced following the Alice Lloyd College media destruction policy.

e2Campus

Alice Lloyd College uses a program called e2Campus to notify users of incidents, closures, postponements and other important notices. This is available to faculty, staff and students. This is a self-sign up service and can be accessed by visiting the Alice Lloyd College website at www.alc.edu and choosing e2Campus under the *Student Life* tab.

Computer Lab Information

- The computer labs throughout campus are set up for education use only. Lab attendants may ask non-educated users to relinquish their computer if the computer is needed by a student wishing to use it for educational purposes. This applies to all student-computing areas.
- The computers throughout campus will not allow you to save items to them so students will need to use a flash drive.
- Students are not granted permission to download or install any program to a lab computer or copy anything from the computer that may be a copyright infringement.
- Food, drinks, and tobacco products are not permitted in any ALC computer lab and students found in violation may be asked to leave the lab.
- Please clean up after yourself while in the labs. When finished, clean work area, log off the computer, and push the seat under the table.
- No surfing of pornographic or other offensive material. No surfing for hacking, phishing, network sniffing, port scanning, spoofing, denial of service, spamming or any other topic that may be used against the network by ALC.
- Please be considerate of others by not being loud or rude.
- Students are not to be in classrooms using computers and technology after hours. This is what the computer labs are designed for. Any student caught in the McGaw Lab after hours will be fined $25.00. This will be charged to their accoun**t.**

Dormitory Internet Access

Student dormitory rooms are equipped with wireless internet and two Network Data Ports for accessing the campus Local Area Network (LAN). Any student bringing a computer to campus and that want to use the wall ports must have a **10/100/1000 Base-T Ethernet Network Interface Card (NIC)** installed in the computer. Some modern-day computers do not have a network card installed, and in this case a USB Network device may be used.

Once again, the Alice Lloyd College Information Technology Department ask that you keep your computing device updated with patches and installations of antivirus and antimalware.

Alice Lloyd College Information Technology will not assist in getting gaming consoles, streaming devices and other types of equipment like these on the network.

EagleNet

Alice Lloyd College has on online portal called EagleNet. The URL to this portal is https://eaglenet.alc.edu. Faculty, staff and students have logins to this. Please keep your password secure and do not share it with anyone. If you have issues logging in, there is a "forgot password" option. This option is best to be used with Internet Explorer and a regular computer. For further issues you may email support@alc.edu.

Faculty and staff will find items such as paystubs, time off accrual, time card submittal, etc. on the EagleNet portal. Students can access things such as grades, schedules, account statements, etc.

Alice Lloyd College Faculty and Staff EagleNet accounts will be terminated 15 days after the employee termination date. For faculty, this will be August 15th since their termination date is July 31st and Staff it will be 15 days after the official termination/resignation. Please prepare for this and print what you may need before this deadline. Restrictions and modules may be removed from EagleNet beforehand, when the need for the application is no longer there.

Individuals on FMLA may EagleNet access restricted to certain access, allowing them to see pay stubs, time off accrual etc.

BYOD/Mobile Devices

Computers/laptops should be well maintained with updates and patches. Antivirus and anti-malware software are to be installed and kept up to date before joining the Alice Lloyd College network.

Alice Lloyd College office staff shall not use their own computer/laptop to perform their Alice Lloyd College job duties.

Mobile devices that have access to Alice Lloyd College email should be kept confidential and secure. Alice Lloyd College Information Technology department has policies implemented to require any mobile device (phone, tablet) that has Alice Lloyd College email configured on it to require a passcode.

Faxing

Alice Lloyd College uses fax services through eFax.com. Each department has their own fax number as well as their own password to go to a designated website to retrieve their faxes. Passwords shall not be shared with other departments. Departments are notified by email when they have a fax awaiting in their secure fax mail box. Passwords must be updated every 90 days with an 8-digit password that consist of 1 digit, 1 special character and 1 upper case letter.

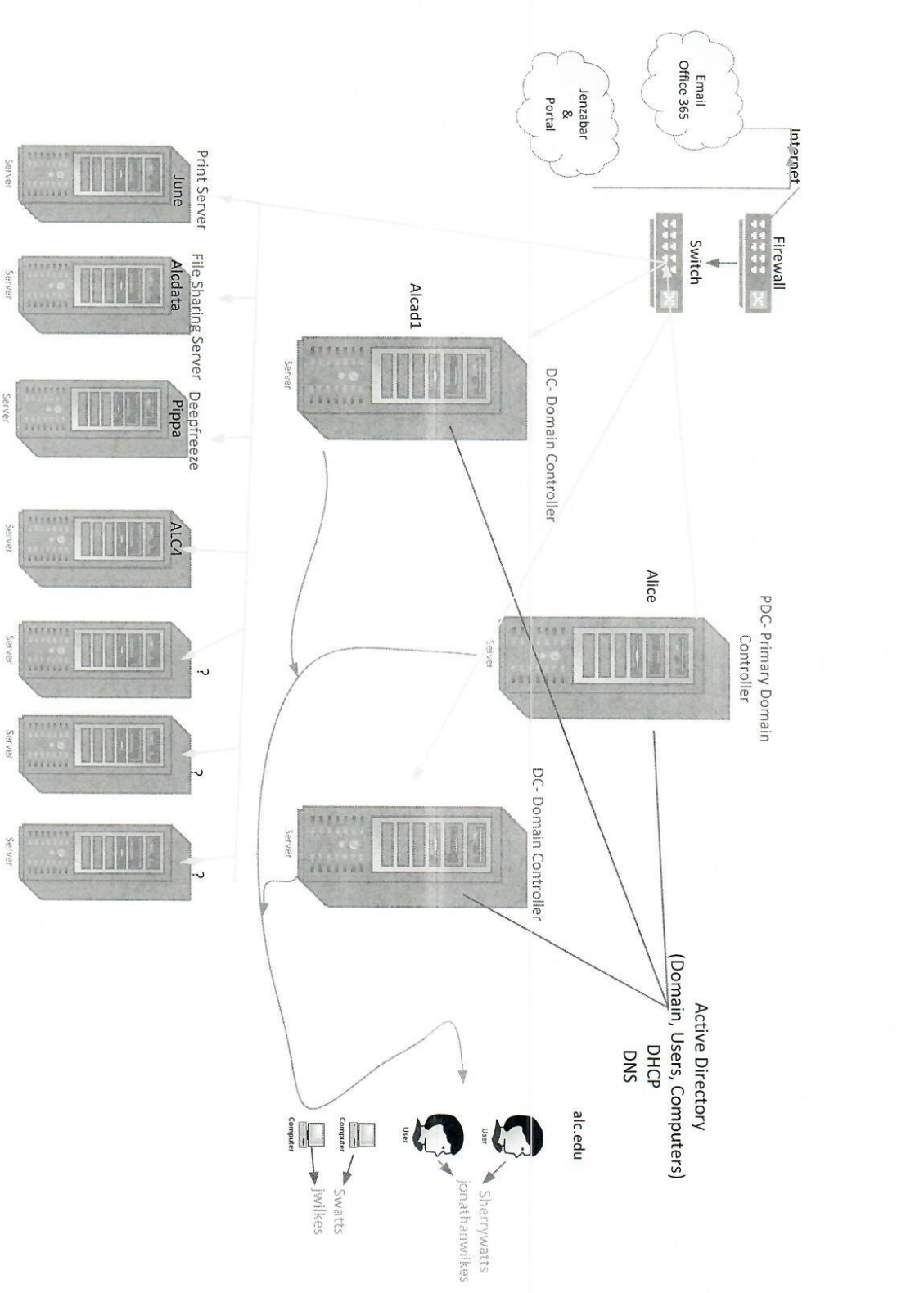
Gaming

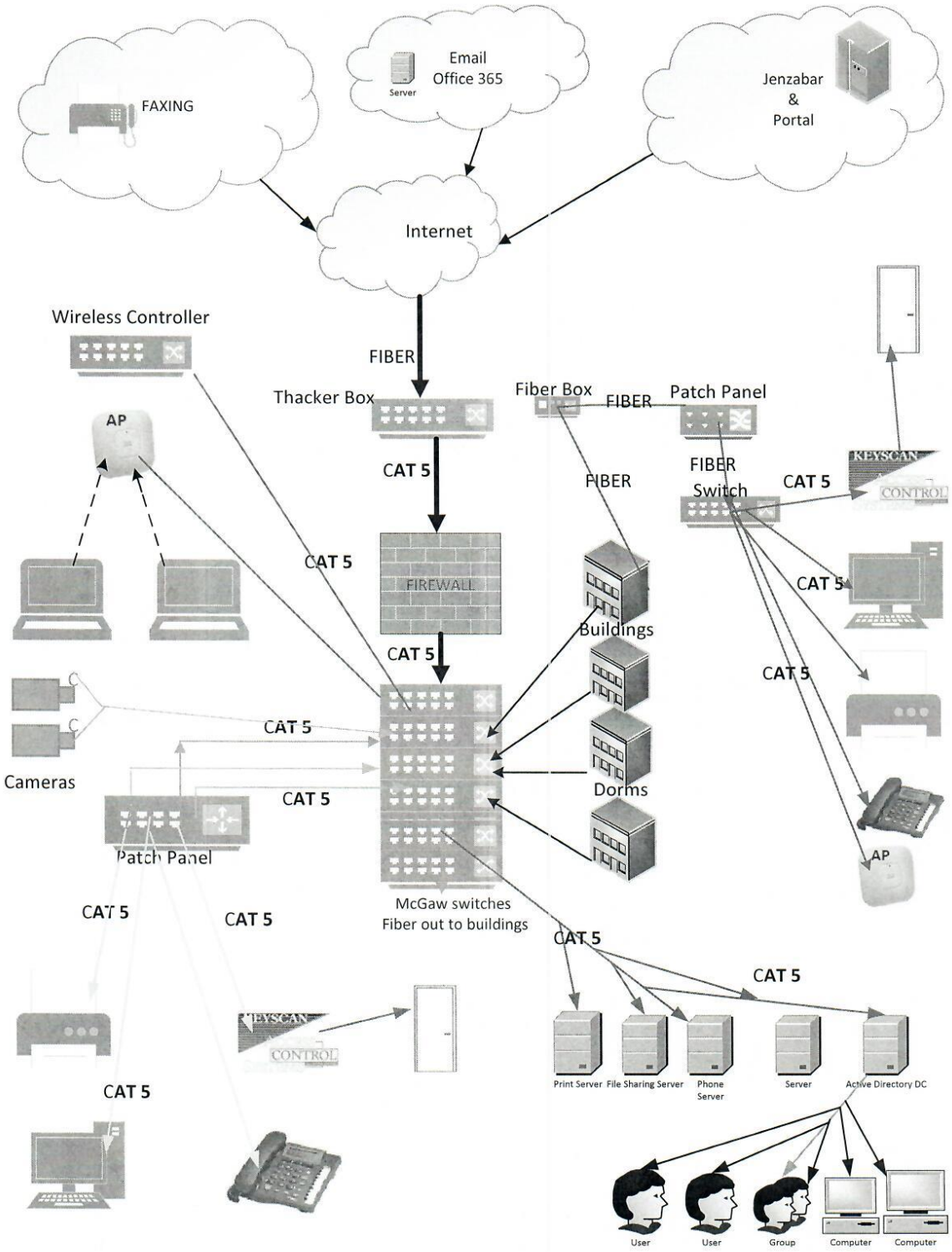
Gaming applications are allowed on the ALC LAN network. Gaming will not work on WIFI. Support will not be given in attempting to join gaming consoles to the ALC network.

PHONE DIRECTORY

Academic Dean	**6061**		**Library Front Desk**	**6112**
Admissions	**6036**		**Library Secretary**	**6132**
Alumni Office	**6044**		**Maintenance**	**6006**
Alumni Work Room	**6116**		**Marketing/Comm.**	**6055**
Athletic Director	**6105**		**Miss Irma's Café**	**6023**
Bookstore	**6135**		**Physical Education**	**6070**
Business Office	**6032**		**Pioneer Food Service**	**6021**
Business Resource Center	**6096**		**Post Office**	**6053**
Career Placement	**6136**		**President's Office**	**6027**
Conference Room	**6010**		**Print Shop**	**6047**
Craft Shop	**6451**		**Radio Station**	**6150**
Daycare	**6124**		**Registrar's Office**	**6041**
Education Department	**6003**		**Science/Math Dept.**	**6077**
English Tutoring Center	**6100**		**Security Office**	**6060**
Financial Aid	**6058**		**SGA Office**	**6069**
Humanities Dept.	**6099**		**Social Science Dept.**	**6095**
Hunger Din	**6021**		**Student Affairs**	**6120**
Infirmary	**6122**		**Student Work Office**	**6063**
Inst. Advancement	**6454**		**TGM Board Room**	**6084**
JBS Athletics Dept.	**6138**		**Weight Room**	**6025**
June's Guest House	**6052**			

Appendix A: Network Maps




FAXING
Email
Office 365
Server
Jenzabar
&
Portal
Internet
Wireless Controller
FIBER
Thacker Box
Fiber Box
FIBER
Patch Panel
AP
CAT 5
FIBER
FIBER
Switch
CAT 5
KEYSCAN
CONTROL
CAT 5
FIREWALL
Buildings
CAT 5
CAT 5
CAT 5
Cameras
CAT 5
Dorms
Patch Panel
AP
McGaw switches
Fiber out to buildings
CAT 5
CAT 5
CAT 5
CAT 5
KEYSCAN
CONTROL
CAT 5
Print Server
File Sharing Server
Phone
Server
Server
Active Directory DC
User
User
Group
Computer
Computer