northwest
CAREER COLLEGE

Information Security Manual

IT Department

We are the first step in a student's journey toward a successful future.

~Dr. John Kenny

Table of Contents

Student Information Security Relevant Standards

Procedure Description

Safeguarding student information is a priority of Northwest Career College (NCC). NCC manages the Information Security Program of the institution in compliance with the standards laid out by the Federal Trade Commission's regulations for implementing the Gramm-Leach-Bliley Act.

Required Procedures

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

(1) Retain responsibility for compliance with this part;

(2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and

(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

(b) Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks 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 assesses the sufficiency of any safeguards in place to control these risks.

(1) The risk assessment shall be written and shall include:

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

(2) You shall periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks 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 reassess the sufficiency of any safeguards in place to control these risks.

(c) Design and implement safeguards to control the risks you identity through risk assessment, including by:

(1) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

(i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

(ii) Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

(3) Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;

(4) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;

(5) Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

(6)

(i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and

(ii) Periodically review your data retention policy to minimize the unnecessary retention of data;

(7) Adopt procedures for change management; and

(8) Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

(d)

(1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

(2) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

(i) Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;
(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;
(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and
(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(f) Oversee service providers, by:
(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
(2) Requiring your service providers by contract to implement and maintain such safeguards; and
(3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

(g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

(h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:
(1) The goals of the incident response plan;
(2) The internal processes for responding to a security event;
(3) The definition of clear roles, responsibilities, and levels of decision-making authority;
(4) External and internal communications and information sharing;
(5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
(6) Documentation and reporting regarding security events and related incident response activities; and
(7) The evaluation and revision as necessary of the incident response plan following a security event.

(i) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such a report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:
(1) The overall status of the information security program and your compliance with this part; and
(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

A. Designated Individual(s) to Coordinate Information Security Program

Procedure Description

Northwest Career College (NCC) has a designated individual(s) to coordinate the institution's Information Security Program.

Procedure Details

The Information Security Program at NCC is managed by the institution's Information Security Council and coordinated by the Information Security Program Coordinator. The CEO of the institution is responsible for the direction and oversight of the Information Security Program Coordinator. The Information Security Council of the institution consists of the following individuals:

- Tony Madero – Information Security Program Coordinator
- Patrick Kenny – CEO
- Dr. Thomas Kenny – CIO
- Mark Brunton – Dean of Education
- Jonathan Hill – Network Administrator I

B. Risk Assessment

Procedure Description

NCC ensures that a written risk assessment is in place that is reviewed/reassessed periodically, and is supported by safeguards that control the risks identified.

Procedure Details

On a quarterly basis, the Information Security Program's risk assessment is updated to ensure that any reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. At this time, the Information Security Council also assesses the sufficiency of any safeguards in place to control these risks.

The Risk Assessment includes:

- Evaluation of Identified Security Risks
    - Each quarter, all members of the Information Security Council are required to review our existing policies and procedures and identify new risks.
    - These individuals bring the identified risks to the quarterly Information Security Meeting, so that they can be evaluated with the group.
- Categorization of Identified Security Risks Criteria
    - Risks are categorized into one of the following categories:
        - Employee Training, Management, and Access Control Review
        - Information Systems
        - Detection, Prevention, and Response to Attacks
- Assessment Criteria of New and Existing Risks
    - At the Quarterly Information Security Meeting, the Information Security Council assesses all identified risks and classifies them as either (1) Low-Risk, (2) Moderate-Risk, or (3) High-Risk.
    - The risk profile is determined by reviewing the impact on confidentiality, integrity, and availability of the information systems and customer information, including the adequacy of the existing controls in the context of the identified risks.
- Mitigating or Accepting Risks
    - Once all risks are classified, the following steps will be taken to mitigate or accept the risk, including specifics of how the risk will be addressed.
        - Low-Risk - risk has no or low potential to impact the network's security significantly.
            - This level of risk may be classified as a known, acceptable risk, or this risk will be addressed with a non-urgent timeline.
        - Moderate-Risk - risk has a moderate chance of significantly impacting the network's security.
            - This level of risk will be addressed with a moderate level of urgency.
        - High-Risk - risk has a strong chance of significantly impacting the network's security.
            - This level of risk will be addressed aggressively and resolved as soon as possible.

- Tracking and Periodical Reexamination of Risks
    - Not only are new risks addressed on a quarterly basis, but all previously identified risks are reexamined at the quarterly Information Security Meeting to ensure their risk classification has stayed consistent and to ensure the safeguards put in place to control the risks are still sufficient.
    - A risk classification would be updated based on a change that impacts the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information.
    - Each Risk Category has its own Appendix within the Information Security Manual. All risk assessments are tracked in this location.
        - Employee Training, Management, and Access Control Review - Appendix A
        - Information Systems - Appendix B
        - Detection, Prevention, and Response to Attacks - Appendix C

C. Safeguard Development

Procedure Description

Utilizing the information identified in its risk assessments, the Information Security Council designs and implements safeguards to control risks. The different methodologies for executing this process are broken down in this procedure.

Procedure Details

On a quarterly basis, the Information Security Program's risk assessment is performed and updated to ensure safeguards are in place. The risk assessment and safeguards categories are broken down below, and the content covered in each section is identified. All updates made to these assessments are located in the Appendices A-C.

- Employee Training, Management, and Access Control Review
    - Authentication and Permission of Access Verification
        - When a new employee is hired at the organization, their supervising executive identifies the role they will play in the institution.
        - All roles within the institution have a security role associated with them.
        - The IT team member who grants access to the IT systems uses these security roles to ensure their access is appropriate.
        - Once access is granted, all employees are required to provide a password to access any company devices.
            - Individuals without access to the institution's network cannot access company devices.
            - Password Security Policy - Domain accounts have a minimum password length of 12 characters, a maximum password age of 42 days, 24 passwords remembered, and passwords are stored using encryption.
        - All employees who change status (i.e., department transfer, promotion, etc.) have an access verification performed on their account to ensure access is appropriate for their new role.
        - All employee access (whether they have a change in position or not) is audited, verified, and updated (when appropriate) on an annual basis.
    - Monitoring and Logging of Activity of Authorized Users
        - Weekly, two reports are generated to support the monitoring and logging of activity of authorized users.
            - Web Violations Report - This report identifies any users who attempted to access a website that does not comply with the institution's computer policy.
            - Data Loss Prevention Report - This report identifies any user behavior identified by our cybersecurity system as out of compliance with our data loss prevention policies.
            - If a user is identified on either of these reports, their supervising executive is responsible for assessing whether the user was performing the functions of their post.
                - If yes, they can disregard the notification.
                - If not, they address the situation with the user and retrain.

        - Automatic notifications are set up for the following types of events:
            - Sophos Cybersecurity software monitors and restricts high-volume data downloads from the network to avoid data loss.
            - Google for Education identifies an instance that may not align with our PII policy
        - Sophos Cybersecurity software restricts the utilization of USB/Peripheral Device for data transfer to avoid data loss.
    - Limiting Authorized User Access Levels
        - The Information Security Coordinator utilizes Security Groups within the campus's Active Directory to implement a Least Access Policy.
            - Least Access Policy for network-stored data – group employees so that access is granted to the areas of the student's file that are needed to perform the functions of their position.
            - This access is broken down by view-access, modify-access, and delete-access.
        - The Information Security Coordinator utilizes VLANs (virtual local area networks) to segment departments and prevent internal and external data breaches.
    - Change Management Policy and Procedure
        - All changes made to IT systems or processes must be approved in writing by the Information Security Coordinator.
        - Once the change has been approved, the IT system should be updated.
        - Once the update is completed, the IT team member performing the change must track the changes made in the Change Management Log.
            - Any relevant documentation must be linked to the Change Management Log for future reference.
        - Once the update is completed, the change should be monitored regularly to ensure that the change was effective and did not have any unforeseen negative impact.
        - This policy should be reviewed annually to ensure it complies with existing standards and industry best practices.
- Information Systems
    - Data Encryption Analysis
        - All institutional data must be encrypted at rest in transit or on external networks.
            - At Rest - all data is stored in our Google Share Drive infrastructure. This data is encrypted.
            - In Transit - Sophos Email Security provides email encryption for data that is being sent from any member of the NCC team.
        - The Information Security Coordinator has reviewed these encryption standards and verified their voracity.
    - In-House Developed Applications Practices
        - All in-house developed apps are created with cybersecurity protocols in mind.
        - Annually, these applications are reviewed to ensure no new/addititional risks exist.
        - These risks are reviewed via the Information Security Council Meeting.
    - Multi-Factor Authentication
        - All institutional data is stored in our Google Share Drive infrastructure.
        - All individuals accessing this data have multi-factor authentication enabled for their accounts.
    - Data Destruction and Secure Disposal Policy
        - Annually, any hard drives that have reached their "end of life" are appropriately destroyed to ensure data cannot be extracted once the hardware is no longer in use.

- NCC utilizes a nationally certified hard drive disposal company that specializes in properly destroying hard drives to avoid any data loss/extraction. Upon completion of the hard drive destruction process, a certified hard drive destruction log is generated to ensure process completion.

- Data Retention Policy
  - Annually, NCC “archives” any data that has not been utilized within the last seven years in an offline format that can be accessed only by campus leadership. By doing so, PII on the network is reduced, and network speeds are increased.
    - Since students often need the information from their student records to continue their education, NCC’s Information Security Council determined that seven years was an appropriate time to maintain their records on hand.
    - The types of requests that come through generally are transcripts and financial records.
  - This policy is reviewed annually at the Information Security Council Meeting.

- Detection, Prevention, and Response to Attacks
  - Please Refer to the next section, which addresses testing and monitoring of safeguards.

D. Testing and Monitoring the Safeguards

Procedure Description

As safeguards are developed, it is vital to test and monitor the effectiveness of the safeguards' key controls, systems, and procedures. Specifically, testing to detect actual and attempted attacks on or intrusions into information systems is a core tenant of our Information Security Program.

Procedure Details

On a quarterly basis, the Information Security Program's risk assessment and safeguards are reviewed and monitored for effectiveness. Specifically, the safeguards' key controls, systems, and procedures involving intrusion and actual/attempted attack detection are reviewed. Existing content from previous council meetings is validated, and new content is investigated and tested. The risk assessment and safeguards categories are broken down below, and the content covered in each section is identified. All updates made to these assessments are located in the Appendices A-C.

Employee Training, Management, and Access Control Review

- Please Refer to the previous section, which addresses Employee Training, Management, and Access Control.

Information Systems

- Please Refer to the previous section, which addresses Information Systems.

Detection, Prevention, and Response to Attacks

- All institutional information systems are monitored and tested.
- There are three categories of detection, prevention, and response to attacks.
- They are listed here below with details of the methodology currently used.
    - Continuous Monitoring and Testing
        - The IT Department has cybersecurity software that generates automated notifications for Web Threats and critical hardware performance failures.
        - The Information Security Coordinator responds to the notification of issues, assesses their viability, and takes the appropriate action to mitigate their impact and risk.
        - The Information Security Coordinator monitors daily end-user's security practices in-person and remotely, ie. Ensuring computers are locked, ensuring employees are using security best practices, and preventing unauthorized access.
        - A Weekly Report is generated to audit the ticketing system for potential reoccurring issues that might be indicative of potential insider threats.
        - The Information Security Coordinator utilizes Sophos EndPoint Management for all devices on campus from end-user PCs to servers. This cybersecurity solution uses AI to provide real time protection for all devices and quarantine potential threats, i.e., viruses, malware, phishing, and ransomware.
        - The Information Security Coordinator utilizes Sophos Managed Detection & Response (MDR), a managed security service that includes Instant Security Operations Center (SOC), 24/7 Threat Detection and Response, and expert network monitoring.
    - Detection Systems
        - Sophos Intercept X Technology – employs a comprehensive defense-in-depth approach to endpoint protection rather than simply relying on one primary security technique. It utilizes all of the following features to eliminate the risk of attacks/intrusions:

- Intrusion Detection System/ Intrusion Prevention System
- Deep Learning – Artificial Intelligence to review workstation/server performance and identify any security risks. If there is any unauthorized access and activity on the network, the Information Security Coordinator is notified.

- Sophos MDR
  - 24/7 Human monitoring SOC
  - Autonomous Response
- (Detection) NinjaRMM – Hardware Performance Monitoring Software installed on all Servers and Workstations.
  - Provides notifications via email when hardware:
    - Loses power
    - Excessive CPU Usage
    - Limited Disk Space
  - Allows Information Security Coordinator to:
    - Push critical Windows Updates
    - Push software applications
    - Provide remote desktop support for end-users
- Fortinet Firewall
  - Security Intrusion Detection System
    - The Fortinet Firewall performs real-time sweeps of the network environment to identify security risks and notifies the Information Security Coordinator if there is any unauthorized access and activity on the network.
  - Fortinet provides notifications via email in the case of:
    - Power Loss
    - Hardware Reboots
    - Connection issues
  - Application-aware firewall: Fortinet's firewall includes application-aware capabilities, allowing IT teams to control and monitor network traffic based on the applications being used.
  - Stateless Firewall: Velocloud’s firewall is stateless and allows or blocks network traffic based on firewall rules set in place
  - Intrusion detection and prevention: Fortinet's firewall includes intrusion detection and prevention capabilities that can detect and block attacks against enterprise networks.
  - Malware protection: Fortinet's firewall includes malware protection features that can detect and block malware infections.
  - Content filtering: Fortinet's firewall includes content filtering capabilities that allow IT teams to block access to websites or applications that may pose a security risk or violate corporate policies.
  - User authentication and access control: Fortinet's firewall includes user authentication and access control features that can restrict network access based on user credentials or other criteria.
- Google Workspace Context Aware Blacklisting
- Time of Click – all NCC emails are run through a process called “Time of Click”. Within this process, all websites included in email communications are assessed by Sophos and verified as “non malicious”. Each and every email URL is protected and secured, and

whenever a link within an email is clicked, regardless of the device used, our cloud-based Sophos SXL database verifies its credibility.
    - Sandstorm – all NCC emails are also run through the Sophos Sandstorm, which checks all emails to ensure that the latest zero-day and unknown threats are quarantined before entering the NCC network environment.
    - Quarantine - Sophos provides employees with quarantined emails daily for review to either review or release.
- Periodic Penetration Testing and Vulnerability Assessment
    - The Information Security Coordinator scans our network using Rapid7, a software designed to collect data from across your environment, making it easy for teams to manage vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate your operations.
        - This scan is performed at least 2x per year from an external perspective and identifies risks and vulnerability.
    - The Information Security Coordinator provides feedback and an assessment of our current environment.
    - The Information Security Coordinator provides recommended improvements/enhancements to the security layout of our network environment to eliminate the risk of future threats.
    - In the case of a significant shift in our Information Systems, there will be additional penetration and vulnerability testing performed.

E. Policies and Procedures to Ensure Personnel Can Enact Information Security Program

Procedure Description

It is critical for the institution to have policies and procedures that support the execution of the information security program. The purpose of this section is to detail the steps taken by the institution within the area of **Employee Training and Management**.

Existing Procedures

1. **Standard Employee Training**
    a. Daily Training – the Information Security Coordinator completes user-by-user training when closing out work tickets and executing projects with specific departments.
    b. Annual Training – the Information Security Coordinator facilitates in-person training in a classroom environment with a pre-planned curriculum that is adjusted according to trends in the industry and is updated before each presentation.
        i. Each in-personal training is also videotaped and delivered to all NCC employees to ensure that employees have access and are able to complete the training.
        ii. All in-person training concludes with a short assessment to verify competency.
    c. New Employee Training: All new employees at NCC are required to complete any quarterly/annual security training from the previous 12 months and to complete an in-person information security training with our Information Security Coordinator during their first week of employment.
    d. Remote Work Training – optimizing home network environment from a security standpoint (home internet, networking, best practices, data transfer restrictions, etc.)
        i. Mitigate risk of data loss based on employee's home network being compromised through increased enforcement of data storage policies
        ii. Eliminate the potential for the storage of data of any type on personal device – risk of having team members leave the organization and/or lose the personal device, another cohabitant in the domicile accesses the data when the personal device is not in use, which poses a data loss risk.
            1. Increase enforcement of personal device policies
    e. ThreatAdvice – Phishing Campaigns are being deployed bi-annually to identify high-risk employees. ThreatAdvice Courses are being deployed in each of the following areas:
        i. New Employees
            1. Everyone must complete during onboarding
        ii. Phishing Remediation
            1. Anyone who fails the phishing campaigns (that occur quarterly)
        iii. Bi-annual training via ThreatAdvice

2. **Qualified Information Security Personnel Oversight Tools**
    a. The IT Department has cybersecurity software that generates automated notifications for Web Threats and critical hardware performance failures.
        i. The Information Security Coordinator responds to the notification of issues, assesses their viability, and takes the appropriate action to mitigate their impact and risk.

b. The Information Security Coordinator monitors daily end-user's security practices in-person and remotely, ie. Ensuring computers are locked, ensuring employees are using security best practices, and preventing unauthorized access.
c. The CEO delivers any available Information Security policy and procedure updates via weekly department meetings to ensure employee understanding and compliance.
d. The Information Security Coordinator generates a Weekly Report of Policy Violations (ie. Attempting to access prohibited websites/content) and sends it to the Executive Board.
    i. The Executive Board reviews violations and notifies managing members to perform retraining and coaching for end-users as a result of the findings.
e. A Weekly Report is generated to audit the ticketing system for potential reoccurring issues that might be indicative of potential insider threats.

3. Training of Information Security Personnel

a. Annual Training – Information Security/Technology Online Training Certificates are completed by all members of the IT Department through a third-party professional development company.
b. Training by Cybersecurity Partners - information security personnel are encouraged to attend webinars and other training provided by our Cybersecurity Partners (i.e., Sophos, Google for Education, Canvas LMS, etc.).

4. Verification of Key Personnel's Maintenance of Current Knowledge

a. Quarterly Email-based Information Security Bulletins – for example:
    i. Phishing awareness
    ii. Spam awareness
    iii. Password strength/effectiveness awareness/standards
    iv. Best practices for data management/digital delivery
b. As Needed Information Security Bulletins - the Information Security Coordinator provides updates regarding current events and best practices for cyber security.
    i. Newly released content from CISA
    ii. News stories about existing cybersecurity incidents
    iii. Best practices from partner institutions

F. Third-Party Services – Oversight Procedures

Procedure Description

Northwest Career College (NCC) has third-party service providers that assist the designated individual(s) in coordinating the Information Security Program of the institution.

Procedure Details

NCC has selected and retained three service providers that assist in the storage and transmission of student information:

- Campus Management – provides the Student Information System of the institution
- LeadSquared - provides the Customer Relationship Management of the institution
- Google for Education - provides storage for the institution

The Information Security Council initially verified that these service providers maintain appropriate safeguards for student information and comply with the Federal Trade Commission's regulations for implementing the Gramm-Leach-Bliley Act.

- Each vendor has a contract in place that requires them to implement and maintain these safeguards.
- Annually, the Information Security Coordinator reaches out to these vendors and verifies that they are still in compliance with these standards.

G. Procedure for Adjusting Information Security Program

Procedure Description

NCC's Information Security Program includes testing, monitoring, material changes to your operations, results of risk assessments, and a review of any other circumstances that impact this program. Each quarter, the Information Security Council meets to evaluate these items and adjust their effectiveness.

Procedure Details

- The CEO schedules the four quarterly Information Security Council Meetings at the beginning of each calendar year.
- At the Information Security Council Meetings, a review of all of the following materials takes place:
    - Vulnerability and Penetration Testing
    - Relevant Security Notifications from Sophos, Google, and Fortinet Firewall
    - Updates from CISA and other industry leaders
- Based on the results of the review, an action plan for improvement is established when appropriate.
- Then, each action plan for improvement is managed and tracked within the Information Security Council Meeting.
- Until the action plan is fully implemented, the Information Security Coordinator will keep track of action items and hold all team members accountable.

H. Incident Response Plan

Procedure Description

Below is NCC's incident response plan that should be used to promptly respond to and recover from any security event materially affecting the confidentiality, integrity, or availability of customer information in your control.

Procedure Details

Goal:
The purpose of the incident response plan is to ensure that the institution can quickly and effectively respond to and recover from a network security event (i.e., data loss, cybercrime, internet outage, network outage).

Process for Responding to Security Event:
In the case of a security event, the following steps must be taken:

- Upon identification of the security event, the following individuals must immediately be notified via phone, chat, and email. These individuals each hold vital roles within the response plan.
    - CEO - Incident Manager
        - This individual is the leader of the response, focusing on communication, internal stakeholder coordination, and task delegation.
    - Information Security Coordinator - Technology Manager
        - This is the subject matter expert who will identify whether this event can be handled internally by our institution's staff or whether additional support is needed.
    - CIO - Communications Manager
        - This is the point of contact for the press, our social media platform communications, and external stakeholders.
- The Information Security Coordinator will perform an initial assessment and move through the following phases:
    - Scope - Identify the scope of the incident.
    - Containment - Verify at what level the threat can be isolated/contained and proceed with isolating the threat.
    - Investigation - Once the initial threat has been contained, an investigation must occur to determine the priority, risk, and root cause of the incident.
        - Sophos Cybersecurity Software Remediation Settings allow the Information Security Coordinator to:
            - Enable Threat Case creation
            - Provides reports and events to Sophos Central
            - Root Cause Analysis – provide detailed analysis to determine the cause of any intrusion attempt so that the institution can make adjustments and prevent further intrusion attempts.
    - Remediation - Establish a plan to repair or replace affected systems and ensure there are no residual problems within the network that could lead to additional network incidents.
        - Sophos Cybersecurity Software Remediation Settings allow the Information Security Coordinator to:
            - Establish automated equipment isolation in the case of infection (i.e., Ransomware, Malware, etc.)

- Clean impacted equipment to allow it to be safely reintroduced into the environment
- Utilize MDR - an active network response by Sophos SOC (Human 24/7 monitoring/mitigation/reporting) to use the collective knowledge of industry professionals for remediation efforts.

  - Recovery - Assess the impact of the incident, review the effectiveness of our existing policies/procedures, and establish recommendations to mitigate risk in the future.

- The CEO will provide support to the Information Security Coordinator and will be responsible for communicating with the campus at large regarding the impact of the incident. The CEO will also be responsible for providing the Information Security Coordinator with whatever resources are needed to quickly move through the phases of the Incident Response Plan.
- The CIO will coordinate with the press regarding any communication that should occur as a result of the network event. The CIO will also be directly responsible for any social media-based messaging that is appropriate to the situation.

<u>Roles, Responsibilities, and Levels of Decision-Making Authority:</u>

- CEO - Incident Manager
  - This individual is the leader of the response, focusing on communication, internal stakeholder coordination, and task delegation.
  - Is empowered with the highest level of decision-making authority.
- Information Security Coordinator - Technology Manager
  - This is the subject matter expert who will identify whether this event can be handled internally by our institution's staff or whether additional support is needed. This individual will also identify the scope of the incident and what data may have been compromised. This individual is also responsible for securing any compromised equipment and leading our team through the recovery process.
  - Is empowered with the decision-making authority regarding all technology-related topics.
- CIO - Communications Manager
  - This is the point of contact for the press, our social media platform communications, and external stakeholders.
  - Is empowered with the decision-making authority regarding all communications-related items.

<u>External and Internal Communication and Information Sharing Plan:</u>

- Communication when an incident or potential incident occurs
  - Anyone suspecting an exposure of institutional data or systems should immediately contact:
    - IT Department - 702 - 254 - 7577
    - IT Department - itdept@northwestcareercollege.edu
    - IT Department - via NCC App form
  - Employees of the institution can also feel free to report the issue directly to the Information Security Coordinator via an instant message in the case of a time-sensitive emergency.
- Communication once an incident is confirmed
  - Once the Information Security Coordinator confirms an incident, they are responsible for immediately notifying all members of the Information Security Council with the details of the incident. This communication should occur via instant message to ensure prompt delivery and receipt.
  - It is the responsibility of the CIO to determine from this moment forward which group of external and internal stakeholders must be notified and in which order.

- The CIO will utilize CISA guidance to make this determination.
- The CEO will provide consultative support to the CIO and be a conduit for facilitating support from outside vendors (i.e., attorneys, IT specialty firms, etc.).
- The CEO will determine if and when to contact the Office of the Attorney General (through the AG's Privacy and Data Security Department), the Governor's Office, and/or any other appropriate State Officials to inform them about the data exposure.

Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls:

- If the Information Security Coordinator identifies areas of weakness in our infrastructure, they must outline these details and provide them to the Information Security Council at the post-incident special session.
  - This breakdown must identify whether the issue can or cannot be remediated internally or whether it will require additional expertise or experience.
  - This breakdown should include the projected costs/time investment to implement additional software/technology recommendations.
- The Information Security Council will review these recommended improvements and either implement them immediately or establish a more appropriate alternative plan that resolves the issue.
  - The final conclusions of this process must be communicated to the board in writing directly following the special session.

Documentation and reporting regarding security events and related incident response activities:

- NCC's cybersecurity software, Sophos, creates automated incident response documentation that is distributed to all members of the IT Department at the time of the incident. This document identifies the scope of the issue, the technical details available about the incident cause, and recommendations on the next steps.
- NCC's Information Security Coordinator must outline the events leading up to the network incident, the response to the incident, and the conclusion of the incident.
- All documentation is filed in the IT Department Storage location.

Evaluation and Revision of the Incident Response Plan Following a Security Event:

- Following a security event, within 90 days, the Information Security Council must hold a special session to evaluate and revise the incident response plan (if needed) based on its real-world effectiveness.
- Any conclusions or recommended changes must be provided to the board in writing within 72 hours of this meeting to allow prompt action to be taken.
- The board will assess recommendations, make the appropriate changes to policies/procedures, and take responsibility for appropriately communicating findings to the institution's staff, faculty, and students. The board will also contact the Office of the Attorney

I. Reporting of Information Security Program Status and Material Matters

Procedure Description

NCC’s Information Security Program Coordinator reports on a quarterly basis to the board with the status of the information security program, our compliance with the standards, and any material matters that are identified. These matters include risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

Procedure Details

Upon completing the quarterly review of the Information Security Manual, the institution's Information Security Program Coordinator ensures that a written update with all required components is provided via email to the board.

Appendix A: Risk Assessment & Safeguards (Employee Training and Management)

Procedure Description

Performing risk assessments and establishing safeguards to control each of the risks identified is a critical component of the institution's Information Security Program. The purpose of this section is to detail the steps taken by the institution within the area of **Employee Training and Management**.

Existing Procedures

1. **Employee Training**
    a. Daily Training – the Information Security Coordinator completes user-by-user training when closing out work tickets and executing projects with specific departments.
    b. Annual Training – the Information Security Coordinator facilitates in-person training in a classroom environment with a pre-planned curriculum that is adjusted according to trends in the industry and is updated before each presentation.
        i. Each in-personal training is also videotaped and delivered to all NCC employees to ensure that employees have access and are able to complete the training.
        ii. All in-person training concludes with a short assessment to verify competency.
    c. Annual Training – Information Security/Technology Online Training Certificates are completed by all members of the IT Department through a third-party professional development company.
    d. New Employee Training: All new employees at NCC are required to complete any quarterly/annual security training from the previous 12 months and to complete an in-person information security training with our Information Security Coordinator during their first week of employment.
    e. Quarterly Email-based Information Security Bulletins – for example:
        i. Phishing awareness
        ii. Spam awareness
        iii. Password strength/effectiveness awareness/standards
        iv. Best practices for data management/digital delivery
    f. Remote Work Training – optimizing home network environment from a security standpoint (home internet, networking, best practices, data transfer restrictions, etc.)
        i. Mitigate risk of data loss based on employee's home network being compromised through increased enforcement of data storage policies
        ii. Eliminate the potential for the storage of data of any type on personal device – risk of having team members leave the organization and/or lose the personal device, another cohabitant in the domicile accesses the data when the personal device is not in use, which poses a data loss risk.
            1. Increase enforcement of personal device policies
    g. ThreatAdvice – Phishing Campaigns are being deployed bi-annually to identify high-risk employees. ThreatAdvice Courses are being deployed in each of the following areas:
        i. New Employees
            1. Everyone must complete during onboarding
        ii. Phishing Remediation
            1. Anyone who fails the phishing campaigns (that occur quarterly)
        iii. Bi-annual training via ThreatAdvice

2. **Employee Management**
    a. The IT Department has cybersecurity software that generates automated notifications for Web Threats and critical hardware performance failures.
        i. The Information Security Coordinator responds to the notification of issues, assesses their viability, and takes the appropriate action to mitigate their impact and risk.
    b. The Information Security Coordinator monitors daily end-user's security practices in-person and remotely, ie. Ensuring computers are locked, ensuring employees are using security best practices, and preventing unauthorized access.
    c. The CEO delivers any available Information Security policy and procedure updates via weekly department meetings to ensure employee understanding and compliance.
    d. The Information Security Coordinator generates a Weekly Report of Policy Violations (ie. Attempting to access prohibited websites/content) and sends it to the Executive Board.
        i. The Executive Board reviews violations and notifies managing members to perform retraining and coaching for end-users as a result of the findings.
    e. A Weekly Report is generated to audit the ticketing system for potential reoccurring issues that might be indicative of potential insider threats.

Risk Assessment and Safeguards

1. **Identify Risks**
    a. Based on the initial assessment of the current process, the Information Security Coordinator finds that the level of training provided via the daily, quarterly, and annual training meets industry standards and reduces end-user risk substantially and meets the standards provided.
    b. The risks identified during this assessment were as follows:
        i. Based on the delivery method of the quarterly campus-wide training, there is a risk that individuals may not attend the training and do not complete it remotely.
2. **Qualify Risks (Low-Risk Tolerance)**
    a. Campus-wide Completion of annual Trainings
        i. Impact – Medium
        ii. Probability – Low
    b. New Employee On-boarding Training
        i. Impact – Medium
        ii. Probability – Low
3. **Plans for Mitigating Risks**
    a. Campus-wide Completion of annual training – Generating a system for ensuring that ALL employees complete the training in one format or another, ie. Ensuring that individuals who miss the in-person training watch the recorded version of the training and complete the post-training assessment.
4. **Monitoring or Managing Risks – Generating *Safeguards***
    a. Using Quarterly Information Security Council Meetings, the Information Security Coordinator will provide data regarding the progress of our plans for eliminating risks in the form of:
        i. Employee Training Attendance records for all bi-annual campus-wide trainings
    b. Using the data provided, the Information Security Council will ensure the safeguards are controlling the identified risks.

Appendix B: Risk Assessment & Safeguards (Information Systems)

Procedure Description

Performing risk assessments and establishing safeguards to control each of the risks identified is a critical component of the institution's Information Security Program. The purpose of this section is to detail the steps taken by the institution within the area of **Information Systems, including network and software design, as well as information processing, storage, transmission, and disposal**.

Existing Procedures

i. Network and Software Design

1. Network
    - i. The Information Security Coordinator utilizes Security Groups within the campus's Active Directory to implement a Least Access Policy.
        1. Least Access Policy for network-stored data – group employees so that access is granted to the areas of the student's file that are needed to perform the functions of their position.
        2. This access is broken down by view-access, modify-access, and delete-access.
    - ii. The Information Security Coordinator utilizes VLANs (virtual local area networks) to segment departments and prevent internal and external data breaches.
    - iii. The Information Security Coordinator utilizes firewalls to ensure that all NCC locations are protected.
        1. Fortinet Firewall are available at each location protecting the network from external/internal threats.
        2. Windows Defender/Firewall is on every Microsoft workstation.
        3. Macintosh systems include built-in application firewalls
    - iv. The Information Security Coordinator utilizes Sophos EndPoint Management for all devices on campus from end-user PCs to servers. This cybersecurity solution uses AI to provide real time protection for all devices and quarantine potential threats, i.e., viruses, malware, phishing, and ransomware.
    - v. The Information Security Coordinator utilizes Sophos Managed Detection & Response (MDR), a managed security service that includes Instant Security Operations Center (SOC), 24/7 Threat Detection and Response, and expert network monitoring.
    - vi. Server Lockdowns – locking down server configuration modifications during non-business hours
    - vii. Password Security Policy - Domain accounts have a minimum password length of 12 characters, a maximum password age of 42 days, 24 passwords remembered, and passwords are stored using encryption
2. Software as a Service (SAAS)
    - i. ADP software is the institution's HRIS (human resources information system) that manages all employee information from the point of enrollment until graduation. The following safeguards are in place to ensure limited visibility of the SAAS.
        1. PII (Personal Identifiable Information) Restriction – ADP has restricted access to PII (Personal Identifiable Information) via the ADP software based on each employee's department, function, and position.

2. Least Access Policy – The information security Coordinator groups employees so that access granted to each employee's information is limited only to the information required to perform job roles.
3. Multi-factor authentication (MFA) is required for anyone who has Admin access to ADP.

ii. Canvas software is the LMS (Learning Management System) of the institution that manages the entire student educational experience from the point of enrollment until graduation. The following safeguards are in place to ensure the viability of the SAAS.
1. Dual Authentication – All administrators are required to use MFA through SMS.
2. PII (Personal Identifiable Information) Restriction – Canvas software has restricted access to PII (Personal Identifiable Information) via the Canvas software based on department and function.
3. Least Access Policy – All students only have access to their own personal grades and educational experience.

i. LeadSquared software is the CRM (customer relationship management) of the institution that manages the prospective student experience.
1. PII (Personal Identifiable Information) Restriction – this software has restricted access to PII (personally identifiable information) via the LeadSquared software based on department and function.
2. Least Access Policy (Staff Groups) – the Information Security Coordinator groups employees so that access is granted to the areas of the student's file that are needed to perform the functions of their position. This access is broken down by view-access, modify-access, and delete-access.
3. Dual Authentication – All administrators are required to use MFA through Google their Google SSO (single sign on).

ii. Campus Nexus software is the SIS (student information system) of the institution that manages the entire student experience from the point of enrollment until graduation. The following safeguards are in place to ensure the viability of the SAAS.
1. PII (Personal Identifiable Information) Restriction – this software has restricted access to PII (personally identifiable information) via the Campus Nexus software based on department and function.
2. Least Access Policy (Staff Groups) – the Information Security Coordinator groups employees so that access is granted to the areas of the student's file that are needed to perform the functions of their position. This access is broken down by view-access, modify-access, and delete-access.
3. Microsoft Azure - this platform is used for authentication and authorization for NCC employees to have access and permission-based roles for Campus Nexus. This syncs with our Active Directory/Microsoft Accounts.

2. Information Processing, Storage, Transmission and Disposal

1. Processing

i. NCC requires all employees to use network-based secure storage for all information processing. All network-based secure requires NCC-issued network credentials to access.
1. NCC expects all NCC employees to avoid locally saving any data on physical hardware.

2. Storage
    i. NCC utilizes Network Access Storage to store data on its network. The following components ensure the security of the storage:
        1. Least Access Policy (Staff Groups) – group employees so that access is granted to the areas of the student's file that are needed to perform the functions of their position. This access is broken down by view-access, modify-access, and delete-access.
        2. Firewall-based protections are utilized to ensure that data is not being removed from our network environment.
        3. Port-level security ensures that only computers from the NCC domain can connect to the network environment.
        4. Anti-virus: Malware Remover from QNAP is utilized on our network storage and scans and protects daily for malware
        5. Advanced Anti-virus: McAfee ensures that the Network Access Storage is being scanned for viruses daily and protected from internal/external threats.
        6. Malware Detection Program: Malware Remover ensures that the Network Access Storage is being scanned for malware daily and protected from internal/external threats.
        7. Security Counselor: Vulnerability Detection Program ensures that the Network Access Storage is being scanned for vulnerabilities daily and protected from internal/external threats.
    ii. NCC utilizes **Google Drive** to store data in the cloud. The following components ensure the security of the storage:
        1. Least Access Policy (Departments) – group employees so that access is granted only to the department that they are assigned and permissions suitable for their position. Additional access is only given when an ESign has been submitted by the appropriate authority figure.
        2. Encryption (at rest and on the move)
        3. Limited Access – Only those with northwestcareercollege.edu emails are allowed to view files that are stored in our shared drives
        4. Automated Backups – backups of data are stored in the cloud daily from Syscloud.
        5. Multi-factor authentication – All employees and faculty are forced to have two factor authentication to be able to log into their Google Account, making it harder for unauthorized users to enter accounts.
        6. Password expirations & complexity requirements – Passwords now expire every 90 days, passwords cannot be repeated, they are required to be strong passwords by Google's standards, and **must have a minimum length of 8 characters** and must include at least one uppercase and one lowercase letter along with one symbol. Password history in Google does not allow passwords to be reused
        7. Google Education Plus allows the IT department to have alerts on Data Loss Prevention and PII/CC information.
    iii. Secure Data Backups
        1. On Network – all data is backed up monthly for Servers & Networking Equipment.
        2. Off Network – all data is backed up monthly on password protected external hard drives that are securely stored in fire-proof/flood-proof safes.
        3. Cloud-based – all data is backed up daily via SysCloud for Google Workspace and Amazon Web Services (AWS) for our Network Access Storage (NAS).

3. Transmission (Email Security)
    i. NCC has an Advanced Email Security software through **Sophos Central** that has a series of features that ensure the safe transmission of information via email. Here are the critical features that ensure the safe transmission of information within our network environment:
        1. **Email Encryption** – all NCC email addresses have the capability to encrypt messages to ensure that any sensitive information can be delivered securely.
        2. **Time of Click** – all NCC emails are run through a process called "Time of Click". Within this process, all websites included in email communications are assessed by Sophos and verified as "non malicious". Each and every email URL is protected and secured, and whenever a link within an email is clicked, regardless of the device used, our cloud-based Sophos SXL database verifies its credibility.
        3. **Sandstorm** – all NCC emails are also run through the Sophos Sandstorm, which checks all emails to ensure that the latest zero-day and unknown threats are quarantined before entering the NCC network environment.
        4. **Quarantine** - Sophos provides employees with quarantined emails daily for review to either review or release.
    ii. NCC has Email Security through Google that has many features to help ensure the security of inbound and outbound emails within our email domain
        1. **Email Encryption** – Encrypts and delivers mail securely through the use of Transport Layer Security for both inbound and outbound mail traffic.
        2. **Spam Filtering** – Incoming emails are scanned for potential phishing attempts as well as for malware.
            1. Pre-delivery, messages with attachments confirmed to be malware before delivery are placed in the user's spam folder with the attachments disabled.
            2. Post-delivery, messages with attachments that pass initial malware checks are placed in the user's inbox, but may be identified as malware after the fact by longer-running malware scans. Attachments are disabled once they are classified as malware.
    iii. Data Loss Prevention Policies
        1. Sophos Cybersecurity software monitors and restricts high volume data downloads from the network to avoid data loss.
        2. Sophos Cybersecurity software restricts the utilization of USB/Peripheral Device for data transfer to avoid data loss.
        3. Google Workspace scans applications including Sheets, Docs, Slides, and Forms File Upload to avoid data loss.
4. Disposal
    i. Annually any hard drives that have reached their "end of life" are appropriately destroyed to ensure data cannot be extracted once the hardware is no longer in use.
    ii. NCC utilizes a nationally certified hard drive disposal company that specializes in properly destroying hard drives to avoid any data loss/extraction. Upon completion of the hard drive destruction process, a certified hard drive destruction log is generated to ensure process completion.
    iii. Annually, NCC "archives" any data that has not been utilized within the last 7 years to an offline format that can be accessed only by department leadership. By doing so, PII on the network is reduced, and network speeds are increased.

Risk Assessment and Safeguards

1. **Identify Risks**
   a. Based on the initial assessment of the current process, we find that the processes in place for information processing, storage, transmission, and disposal meet industry standards and mitigate risks at each step in the process.
   b. The risks that were identified during this assessment were as follows:
      i. End-user computer locking consistency – it has been identified that a percentage of the end-users in the institution are not diligent when locking their computers when exiting their work area. This poses a risk because it allows anyone in the vicinity to access their computer and the data available based on their security.
2. **Qualify Risks (Low-Risk Tolerance)**
   a. End-user computer locking consistency
      i. Impact – Medium
      ii. Probability – Low

3. **Plans for Mitigating Risks**
   a. Implement monthly campus walk-throughs to identify any end-users that are away from their workstations and not using the appropriate security protocol (locking their computer).

4. **Monitoring or Managing Risks – Generating *Safeguards***
   a. Using Quarterly Information Security Council Meetings, the Information Security Coordinator will provide data regarding the progress of our plans for eliminating risks in the form of:
      i. Monthly Campus Walk-Through Results
      ii. Monthly Sophos Performance Reports

Appendix C: Risk Assessment & Safeguards (Detection, Prevention and Response to Attacks)

Procedure Description

Performing risk assessments and establishing safeguards to control each of the risks identified is a critical component of the institution's Information Security Program. The purpose of this section is to detail the steps taken by the institution within the area of **Detection, Prevention, and Response to attacks, intrusions, or other system failures.**

Existing Procedures

1. **Detecting, Preventing, and Responding to:**
    a. Attacks/Intrusions
        i. (Detection) Sophos Intercept X Technology – employs a comprehensive defense-in-depth approach to endpoint protection rather than simply relying on one primary security technique. It utilizes all of the following features to eliminate the risk of attacks/intrusions:
            1. Intrusion Detection System/ Intrusion Prevention System
            2. Deep Learning – Artificial Intelligence to review workstation/server performance and identify any security risks. If there is any unauthorized access and activity on the network, the Information Security Coordinator is notified.
        ii. (Detection) **Fortinet Firewall** – Security Intrusion Detection System
            1. The Fortinet Firewall performs real-time sweeps of the network environment to identify security risks and notifies the Information Security Coordinator if there is any unauthorized access and activity on the network.
        iii. (Detection) Vulnerability and Penetration Testing
            1. IT scans our network from an external perspective and identifies risks and vulnerability.
            2. IT provides feedback and an assessment of our current environment to enhance our security program.
            3. IT provides recommended improvements/enhancements to the security layout of our network environment to eliminate the risk of future threats.
        iv. (Prevention) Sophos Intercept X Technology
            1. Live Protection – Scheduled Daily Workstation/Server Scans
            2. Real-time scanning of internet content and downloaded content to avoid malicious content being transferred into our network environment.
            3. Sandstorm – blocks malware/malicious content before it executes and quarantines/deletes affected files to ensure the security of our network environment.
            4. CryptoGuard Anti-Ransomware – prevents Ransomware from being deployed in our network environment.
            5. Automatic Isolation Setting – automatically isolates and shuts down any workstation/server that is compromised.
        v. (Detection/Prevention) Sophos MDR
            1. 24/7 Human monitoring SOC
            2. Autonomous Response
        vi. (Responding) Sophos Intercept X Technology

1. Remediation Settings allow the Information Security Coordinator to:
    1. Automatically clean up malware if identified and isolated
    2. Enable Threat Case creation
    3. Provides reports and events to Sophos Central
2. Root Cause Analysis – provide detailed analysis to determine the cause of any intrusion attempt so that the institution can make adjustments and prevent further intrusion attempts.
3. MDR - Active network response by Sophos SOC (Human 24/7 monitoring/mitigation/reporting.)

vii. (Responding) Historical Knowledge Database (Kiwi Server)

1. The IT Department logs all troubleshooting efforts/network changes in its historical knowledge database. This allows the IT Department to more effectively respond to any potential attack/intrusion attempts.
2. Kiwi Servers is also utilized for investigative services in the event there is a breach or systems are compromised.

viii. (Responding) Disaster Recovery Plan

1. The IT Department has generated a Disaster Recovery Plan that should be used when responding to any disaster that could occur in the network environment.
2. The IT Department has updated the Disaster Recovery Plan to include a previously unaddressed topic – planning for a pandemic.

b. Systems Failures

i. (Detection) NinjaRMM – Hardware Performance Monitoring Software installed on all:

1. Servers
2. Workstations
3. Provides notifications via email when hardware:
    1. Loses power
    2. Excessive CPU Usage
    3. Limited Disk Space
4. Allows Information Security Coordinator to:
    1. Push critical Windows Updates
    2. Push software applications
    3. Provide remote desktop support for end-users

ii. (Detection & Prevention) Firewall

1. Fortinet provides notifications via email in the case of:
    1. Power Loss
    2. Hardware Reboots
    3. Connection issues
2. Application-aware firewall: Fortinet's firewall includes application-aware capabilities, allowing IT teams to control and monitor network traffic based on the applications being used.
3. Stateless Firewall: Velocloud’s firewall is stateless and allows or blocks network traffic based on firewall rules set in place
4. Intrusion detection and prevention: Fortinet's firewall includes intrusion *detection and prevention* capabilities that can detect and block attacks against enterprise networks.
5. Malware protection: Fortinet's firewall includes malware protection features that can *detect* and block malware infections.

6. Content filtering: Fortinet's firewall includes content filtering capabilities that allow IT teams to block access to websites or applications that may pose a security risk or violate corporate policies.
7. User authentication and access control: Fortinet's firewall includes user authentication and access control features that can restrict network access based on user credentials or other criteria.
8. Google Workspace Context Aware Blacklisting

iii. (Prevention) Continual Infrastructure Maintenance is performed by the Information Security Coordinator and includes:
1. Updating firmware
2. Update software patches
3. Rebooting core equipment to ensure optimal performance
4. Researching security vulnerabilities through security websites/blogs
5. Morning/Evening Daily Infrastructure Health Checks

iv. (Prevention) Continual End-User Workstation Maintenance is performed by the Information Security Coordinator and includes:
1. Updating firmware
2. Updating software patches
3. Disk cleanups
4. Disk defragmentation
5. Verify security settings
6. Remove old, unused software

v. (Prevention) Hardware cycling (Nevada State Recycle)
1. Assessing existing hardware performance (life cycle)
2. Purchasing replacement units
3. Retiring outdated equipment

vi. (Prevention) Network Infrastructure Physical Security
1. Server Cage locks – the IT Department has updated all locks on the server cages to ensure that all network infrastructure is locked physically on multiple levels.
2. Updated Locking Mechanism for Server Closets – access has been restricted to select personnel only.
3. Computer Locks – the IT Department has added locks to each computer on campus to ensure that computers cannot be moved around or off campus by anyone outside of the IT Department.

vii. (Response) Backups are in place in the case of a system failure. The Information Security Coordinator ensures the following backups are available for the institution:
1. Server Redundancy
2. Server Backups
3. Network Configuration Details
4. Network Access Storage On-Site and Cloud-Based Backups
5. Critical Workstation Backups

viii. (Response) Redundant Hardware Replacement Stock is maintained by the Information Security Coordinator to ensure that replacement hardware is always available in the case of hardware failure. This Hardware Replacement Stock includes:

1. Base Workstations
2. Specialized Workstations
3. Switches/Routers
4. Servers

Risk Assessment and Safeguards

1. **Identify Risks**
   a. System failure notifications are available for many of the core infrastructure units in place; however, these notifications are not expanded into every single unit of hardware.
   b. The hardware/firewall currently in place restricts access from external threats; however, there is no current method to identify potential attackers and proactively restrict their ability to attempt further attacks.
2. **Qualify Risks**
   a. System Failure Notifications for all Hardware
      i. Impact – Medium
      ii. Probability – Low
   b. External Threat Monitoring and Reporting
      i. Impact – High
      ii. Probability – Medium
3. **Plans for Mitigating Risks**
   a. Fine-tune and create viable notification sequences as we more deeply utilize the capability of the hardware/software currently in place on the network.
      i. Expand our existing network monitoring software to allow for these types of notifications to be centralized and configured consistently within our network environment.
         1. Provide system failure notifications for routers, switches, and Network Access Storage.
   b. Purchase and configure of a stateful firewall to add an additional layer of threat prevention and monitoring.
      i. Development of the DMZ (demilitarized zone) to buffer external threats and observe potential attackers/attack methods to adapt our environment to avoid future threats.
      ii. Development of a “honeypot”, which allows us to observe attack ideology and adapt our environment to avoid future threats.
4. **Monitoring or Managing Risks – Generating *Safeguards***
   a. During the Quarterly Information Security Council Meetings, the Information Security Coordinator will review the notifications/alerts from the last quarter to determine viability and assess whether or not any alerts were missed based on the day-to-day operational impact that was observed over the last quarter.
      i. Positive, Effective Alerts
      ii. Missing Alerts
      iii. False Positive Alerts
   b. During the Quarterly Information Security Council Meetings, the Information Security Coordinator will review
      i. Weekly Reports generated by the Stateful firewall and action plans implemented as a result of findings on reports.
         1. Blacklisting Threats
         2. Whitelisting Potential Customer/Client Access Points
         3. Notify the Internet Support Provider of malicious activity in their environment
         4. Notify the FBI of malicious activity (when appropriate)
         5. Review any information available via the DMZ/”honeypot” observation to establish plans for future defenses and enhanced protection efforts.