NORTHPOINT COLLEGE

GLBA Financial Information Security Program Policy

Updated May 2024

PURPOSE/POLICY:

The Federal Trade Commission's Safeguards Rule, which implements the security provisions of the Gramm-Leach-Bliley Act (GLBA), went into effect on May 23, 2003. This rule requires financial institutions, including colleges like Northpoint College that are significantly engaged in providing financial services, to protect the security, confidentiality, and integrity of customer financial records and non-public personally identifiable financial information. The GLBA Safeguards Rule mandates that all covered institutions establish appropriate administrative, technical, and physical safeguards.

Therefore, any office or department within Northpoint College that collects, stores, or processes Covered Data must implement data protection standards to ensure compliance. This is in addition to any other College policies and procedures that may be required pursuant to federal and state laws and regulations, including the Family Educational Rights and Privacy Act (FERPA).

SCOPE:

This Policy applies to Northpoint College as a whole. It encompasses all departments and personnel that may handle Covered Data.

REASON FOR POLICY:

To ensure that individuals and departments that access or utilize Covered Data understand their responsibility with respect to GLBA compliance at Northpoint College.

WHO SHOULD READ THE POLICY:

Any individual or department that has access to Covered Data, including but not limited to Admissions Director, Finance, Business Office, Registrar, Human Resources, Financial Aid Office, etc.

OBJECTIVE OF THE PROGRAM:

- Protect the security and confidentiality of Covered Data.
- Protect against anticipated threats or hazards to the security or integrity of Covered Data.
- Protect against unauthorized access to or use of Covered Data that could result in substantial harm or inconvenience to any customer.

DEFINITIONS:

“College” refers to Northpoint College, including all its departments and administrative units.

“Covered Data” means (i) non-public personal financial information about a Customer and (ii) any list, description, or other grouping of Customers (and publicly available information pertaining to them) that is derived using any non-public personal financial information. Examples of Covered Data include bank and credit card account numbers, income and credit histories, tax returns and social security numbers and lists of public information such as names, addresses and telephone numbers derived in whole or in part from personally identifiable financial information (e.g., names of students with outstanding loans). Covered Data is subject to the protections of GLBA, even if the Customer ultimately is not awarded any financial aid or provided with a credit extension.

Covered Data includes such information in any form, including paper and electronic records.

“Customer” means any individual (student, parent, faculty, staff, or other third party with whom the University interacts) who receives a Financial Service from the University for personal, family or household reasons that results in a continuing relationship with the University.

“Financial Service” includes offering or servicing student and employee loans, receiving income tax information from a student or a student’s parent when offering a financial aid package, engaging in debt collection activities, and leasing real or personal property to individuals for their benefit.

“Related Entities” means the following types of entities and their subsidiaries, if legally separate from the University and unless otherwise indicated: auxiliary enterprise corporations, college associations, student services corporations, childcare centers, performing arts centers, and art galleries.

“Service Provider” means any person or entity that receives, maintains, processes, or otherwise is permitted access to Covered Data information through its direct provision of services to the University.

RISK ASSESSMENT AND MANAGEMENT:

Northpoint College will conduct a risk assessment of its financial information systems to evaluate the effectiveness of the current safeguards for confidential information. This will involve identifying potential risks in each relevant area of the College's operations, including:

1. Employee training and management.

2. Information systems, including network and software design, as well as information processing, storage, transmission, and disposal.
3. Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

Northpoint College will regularly test and monitor the effectiveness of its safeguards.

EMPLOYEE TRAINING AND MANAGEMENT:

Northpoint College will train all staff to handle personal customer information securely. Employees will be informed of the importance of confidentiality and customer privacy, as well as the safety and security of customer information.

OVERSIGHT OF SERVICE PROVIDERS:

When engaging service providers that have access to or manage private customer information, Northpoint College will take steps to ensure that these providers handle customer information appropriately. This includes requiring service providers by contract to implement and maintain safeguards for customer information.

EVALUATION AND REVISION OF STANDARDS:

Northpoint College will periodically evaluate and, where appropriate, revise its information security program in light of relevant circumstances, including changes in technology and operations, or any material changes in its business arrangements.

INFORMATION SECURITY PROGRAM COORDINATOR:

Northpoint College will designate an Information Security Program Coordinator. This individual will be responsible for coordinating and overseeing the College's information security program. The Coordinator's duties will include:

1. Working with relevant departments to identify risks to customer information.
2. Developing, implementing, and updating security measures.
3. Ensuring employee training and compliance with security policies.
4. Managing service provider arrangements.
5. Evaluating the effectiveness of the College's security program.

IDENTIFICATION AND ASSESSMENT OF RISKS:

Northpoint College will identify and assess external and internal risks to the security, confidentiality, and integrity of customer financial information. The risk assessment will include considering the following areas:

1. How and where the College collects, stores, and transmits customer financial information.
2. Potential internal and external threats to information.
3. The sufficiency of current policies, procedures, information systems, and other safeguards in place to control risks.

DESIGN AND IMPLEMENTATION OF SAFEGUARDS:

The Information Security Program Coordinator at Northpoint College will design and implement safeguards to control the risks identified through risk assessments. These safeguards may include:

1. Improving existing controls and procedures.
2. Implementing new controls and procedures where necessary.
3. Regularly monitoring and testing the effectiveness of safeguards.

SERVICE PROVIDER ARRANGEMENTS:

Northpoint College will require, through written contracts, that its service providers implement and maintain appropriate safeguards for customer information. The College will select service providers capable of maintaining appropriate safeguards and will provide oversight to ensure that the service providers are upholding their obligations regarding the handling of customer information.

MONITORING AND TESTING:

Northpoint College will regularly monitor and test the effectiveness of its safeguards. This may include system-wide risk assessments, monitoring network security, and regular audits to ensure compliance with the GLBA and this policy.

RESPONSE TO SECURITY INCIDENTS:

In the event of a breach or other security incident, Northpoint College will take appropriate action to address the incident, mitigate harm to customers, and make necessary modifications to its safeguards and procedures.

Northpoint College's Policy on Acceptable Use of Computer Resources

I. INTRODUCTION

Northpoint College's computer resources are dedicated to the support of the College's mission of education, research, and public service. In furtherance of this mission, NC respects, upholds, and endeavors to safeguard the principles of academic freedom, freedom of expression, and freedom of inquiry.

NC recognizes that there is a concern among the College community that because information created, used, transmitted, or stored in electronic form is by its nature susceptible to disclosure, invasion, loss, and similar risks, electronic communications and transactions will be particularly vulnerable to infringements of academic freedom. NC's commitment to the principles of academic freedom and freedom of expression includes electronic information. Therefore, whenever possible, NC will resolve doubts about the need to access NC Computer Resources in favor of a User's privacy interest.

However, the use of NC Computer Resources, including for electronic transactions and communications, like the use of other College-provided resources and activities, is subject to the requirements of legal and ethical behavior. This policy is intended to support the free exchange of ideas among members of the NC community and between the NC community and other communities, while recognizing the responsibilities and limitations associated with such exchange.

II. APPLICABILITY

This policy applies to all Users of NC Computer Resources, as defined in Article III below. This policy supersedes any college policies that are inconsistent with this policy.

III. DEFINITIONS

1. "NC Computer Resources" refers to all computer and information technology hardware, software, data, access, and other resources owned, operated, or contracted by Northpoint College. This includes, but is not limited to, desktop and laptop computers, handheld devices that allow or are capable of storing and transmitting information (e.g., cell phones, tablets), mainframes, minicomputers, servers, network facilities, databases, memory, memory sticks, and associated peripherals and software, and the applications they support, such as e-mail, cloud computing applications, and access to the internet.

2. "E-mail" includes point-to-point messages, postings to newsgroups and listservs, and other electronic messages involving computers and computer networks.

3. “Faculty” includes full-time, part-time, and adjunct faculty.

4. “FOIA” is the Michigan Freedom of Information Act.

5. “Non-Public College Information” is considered personally identifiable information (such as an individual’s Social Security Number; driver’s license number or non-driver identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account; personal electronic mail address; Internet identification name or password; and parent’s surname prior to marriage); information in student education records that is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA) and the related regulations set forth in 34 CFR Part 99; other information relating to the administrative, business, and academic activities and operations of the College (including employee evaluations, employee home addresses and telephone numbers, and other employee records that should be treated confidentially); and any other information available in College files and systems that by its nature should be treated confidentially.

6. “User” means a user of NC Computer Resources, including all current and former users, whether affiliated with NC or not, and whether accessing those resources on an NC campus or remotely.

IV. RULES FOR USE OF NC COMPUTER RESOURCES

1. Authorization.

a. Users may not access an NC Computer Resource without authorization or use it for purposes beyond the scope of authorization. This includes attempting to circumvent NC Computer Resource system protection facilities by hacking, cracking, or similar activities, accessing or using another person’s computer account, and allowing another person to access or use the User’s account.

b. Notwithstanding subsection 1.a. above, a User may authorize a colleague or clerical assistant to access information under the User’s account on the User’s behalf while away from an NC campus or when the User is unable to efficiently access the information on the User’s own behalf (including as a result of a disability), but delegated access will be subject to the rules of Section 10 – Security, below.

c. NC Computer Resources may not be used to gain unauthorized access to another computer system within or outside of NC. Users are responsible for all actions performed from their computer account that they permitted or failed to prevent by following ordinary security precautions.

2. Purpose.

a. Use of NC Computer Resources is generally limited to activities relating to the performance by NC employees of their duties and responsibilities, by students in connection with their college courses and activities, and by retired NC teaching faculty, librarians, and other retired employees approved by the college president or where the employee is a member of the Northpoint College Office staff then by the Academic Dean or his or her designee. For example, use of NC Computer Resources for private commercial or not-for-profit business purposes, for private advertising of products or services, or for any activity meant solely to foster personal gain, is prohibited. Similarly, use of NC Computer Resources for partisan political activity is also prohibited.

b. Except with respect to NC employees other than faculty, where a supervisor has prohibited it in writing, incidental personal use of NC Computer Resources is permitted so long as such use does not interfere with NC operations, does not compromise the functioning of NC Computer Resources, does not interfere with the User's employment or other obligations to NC, and is otherwise in compliance with this policy, including subsection 2.a. above. Users should be aware that personal messages, data, and other information sent or received through a User's NC account or otherwise residing in an NC Computer Resource are subject to NC review pursuant to Section 13 of this policy and may also be subject to public disclosure pursuant to FOIA.

3. Compliance with Law.

a. NC Computer Resources may not be used for any purpose or in any manner that violates NC rules, regulations, or policies, or federal, state, or local law. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those other states and countries, and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular use.

b. Examples of applicable federal and state laws include those addressing defamation, invasion of privacy, obscenity and child pornography, and online gambling, as well as the following:

Computer Fraud and Abuse Act

Copyright Act of 1976

Electronic Communications Privacy Act

Export control regulations issued by the U.S. Departments of Commerce, State, and Treasury

Family Educational Rights and Privacy Act

FOIA

4. Licenses and Intellectual Property.

a. Users may use only legally obtained licensed data or software and must comply with applicable licenses or other contracts, as well as copyright, trademark, and other intellectual property laws.

b. Much of what appears on the internet and/or is distributed via electronic communication is protected by copyright law, regardless of whether the copyright is expressly noted. Users should generally assume that material is copyrighted unless they know otherwise, and not copy, download, or distribute copyrighted material without permission unless the use does not exceed fair use as defined by the federal Copyright Act of 1976. Protected material may include, among other things, text, photographs, audio, video, graphic illustrations, and computer software. More information about copyright and file sharing is available in Northpoint College’s consumer information on the college’s website.

5. False Identity and Harassment. Users may not employ a false identity, mask the identity of an account or computer, or use NC Computer Resources to engage in abuse of others, such as sending harassing, obscene, threatening, abusive, deceptive, or anonymous messages within or outside NC.

6. Confidentiality.

a. Users may not invade the privacy of others by, among other things, viewing, copying, redistributing, posting such data to the Internet, modifying, or destroying data or programs belonging to or containing personal or confidential information about others, without explicit permission to do so.

b. NC employees must take precautions by following all IT Security Policies and Procedures to protect the confidentiality of Non-Public College Information encountered in the performance of their duties or otherwise.

7. Integrity of Computer Resources. Users may not install, use, or develop programs intended to infiltrate or damage an NC Computer Resource, or which could reasonably be expected to cause, directly or indirectly, excessive strain or theft of confidential data on any computing facility. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms. Users should consult with the IT director at their college before installing any programs on NC Computer Resources that they are not sure are safe or may cause excess strain.

8. Disruptive Activities.

a. NC Computer Resources must not be used in a manner that could reasonably be expected to cause or does cause, directly or indirectly, unwarranted or unsolicited interference with the activity of other users, including:

i. chain letters, virus hoaxes, or other e-mail transmissions that potentially disrupt normal e-mail service;

ii. spamming, junk mail, or other unsolicited mail that is not related to NC business and is sent without a reasonable expectation that the recipient would welcome receiving it;

iii. the inclusion on e-mail lists of individuals who have not requested membership on the lists, other than the inclusion of members of the NC community on lists related to NC business; and

iv. downloading of large videos, films, or similar media files for personal use.

b. NC has the right to require Users to limit or refrain from other specific uses if, in the opinion of the IT director at the User's college, such use interferes with efficient operations of the system, subject to appeal to the President or, in the case of Northpoint College office staff, to the IT Coordinator.

9. NC Names and Trademarks.

a. NC names, trademarks, and logos belong to the College and are protected by law. Users of NC Computer Resources may not state or imply that they speak on behalf of NC or use an NC name, trademark, or logo without authorization to do so. Affiliation with NC does not imply authorization to speak on behalf of NC.

b. Notwithstanding subsection 9.a. above, NC employees and students may indicate their NC affiliation on e-mail, other correspondence, and in academic or professionally related research, publications, or professional appearances, so long as they do not state or imply that they are speaking on behalf of the College.

10. Security.

a. NC employs various measures to protect the security of its computer resources and of Users' accounts. However, NC cannot guarantee such security. Users are responsible for engaging in safe computing practices such as guarding and not sharing their passwords, changing passwords regularly, logging out of systems at the end of use, and protecting Non-Public College Information, as well as for following NC's IT Security Policies and Procedures.

b. Users must report incidents of non-compliance with IT Security Policies and Procedures or other security incidents to the President of Northpoint College and the IT Coordinator.

11. Filtering. NC reserves the right to install spam, anti-malware, and spyware filters and similar devices if necessary in the judgment of Northpoint College's IT Director or his designee to protect the security and integrity of NC Computer Resources. NC will not install filters that restrict access to e-mail, instant messaging, chat rooms, or websites based solely on content, unless such content is illegal, such as child pornography sites.

12. Confidential Research Information. Principal investigators and others who use NC Computer Resources to collect, examine, analyze, transmit, or store research information that is required by law or regulation to be held confidential or for which a promise of confidentiality has been given are responsible for taking steps to protect such confidential research information from unauthorized access or modification. In general, this means storing the information on a computer or auxiliary hard drive that provides strong access controls (passwords) and encrypting files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. Robust encryption and passwords must be used to protect Non-Public College Information, and is strongly recommended for information stored electronically on all computers, especially portable devices such as notebook computers, Personal Digital Assistants (PDAs), and portable data storage (e.g., auxiliary hard drives, memory sticks) that are vulnerable to theft or loss, as well as for information transmitted over public networks. Software and protocols used should be reviewed and approved by NC's IT Coordinator. In addition, the steps taken to protect such confidential research information should be included in submissions to the NC Board reviewing the research protocol.

13. NC Access to Computer Resources.

a. Copying. NC may copy a User's account and/or hard drive on an NC Computer Resource, without monitoring or inspecting the contents of such account and/or hard drive, at any time for preservation of data or evidence, without notice to the User.

b. General Monitoring Practices. NC does not routinely monitor, inspect, or disclose individual usage of NC Computer Resources without the User's consent. In most instances, if the College needs information located in an NC Computer Resource, it will simply request it from the author or custodian. However, NC IT professionals and staff do regularly monitor general usage patterns as part of normal system operations and maintenance and might, in connection with these duties, observe the contents of websites, e-mail, or other electronic communications. Except as provided in this policy or by law, these individuals are not permitted to seek out contents or transactional information or disclose or otherwise use what they have observed. Nevertheless, because of the inherent vulnerability of computer technology to unauthorized intrusions, Users have no guarantee of privacy during any use of NC computer resources or in any data in them, whether or not a password or other entry identification or encryption is used. Users may expect that the privacy of their electronic communications and of any materials stored in any NC Computer Resource dedicated to their use will not be intruded upon by NC except as outlined in this policy.

c. Monitoring without Notice.

i. Categories. NC may specifically monitor or inspect the activity and accounts of individual users of NC computer resources, including individual login sessions, e-mail, and other communications, without notice, in the following circumstances:

A. when the User has voluntarily made them accessible to the public, as by posting to Usenet or a web page;

B. when it is reasonably necessary to do so to protect the integrity, security, or functionality of NC or other computer resources, as determined by the IT Coordinator or his or her designee, after consultation with NC's President or his or her designee;

C. when it is reasonably necessary to diagnose and resolve technical problems involving system hardware, software, or communications, as determined by the college IT Coordinator or his or her designee, after consultation with NC's President or his or her designee;

D. when it is reasonably necessary to determine whether NC may be vulnerable to liability, or when failure to act might result in significant bodily harm, significant property loss or damage, or loss of evidence, as determined by the college president or a staff member designated by the president or, in the case of the Northpoint College Office by the Academic Dean or his or her designee, after consultation with the Board and the Campus Pastor (if a current NC faculty member's account or activity is involved);

E. when there is a reasonable basis to believe that NC policy or federal, state, or local law has been or is being violated, as determined by the college president or a staff member designated by the president or, in the case of the Northpoint College Office by the Academic Dean or his or her designee, after consultation with the Board and the Campus Pastor (if a current NC faculty member's account or activity is involved);

F. when an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns, as determined by the college president or a staff member designated by the president and the IT Coordinator or his or her designee or, in the case of the Northpoint College Office by the Academic Dean or his or her designee, after consultation with NC's IT Coordinator or his or her designee, the Board, and the Campus Pastor (if a current NC faculty member's account or activity is involved); or

G. as otherwise required by law.

ii. Procedures. In those situations, in which the Campus Pastor is to be consulted prior to monitoring or inspecting an account or activity, the following procedures shall apply:

A. if the monitoring or inspection of an account or activity requires physical entry into a faculty member's office, the faculty member shall be advised prior thereto and shall be permitted to be present to observe, except where specifically forbidden by law; and

B. the college president or the Academic Dean, as the case may be, shall report the completion of the monitoring or inspection to the Board and the NC employee affected, who shall also be told the reason for the monitoring or inspection, except where specifically forbidden by law.

iii. Other Disclosure.

A. NC, in its discretion, may disclose the results of any general or individual monitoring or inspection to appropriate NC personnel or agents, or law enforcement or other agencies. The results may be used in disciplinary proceedings, discovery proceedings in legal actions, or otherwise as is necessary to protect the interests of the College.

B. In addition, users should be aware that NC may be required to disclose to the public under FOIA communications made by means of NC Computer Resources whether in conjunction with College business or as incidental personal use.

C. Any disclosures of activity of accounts of individual Users to persons or entities outside of NC, whether discretionary or required by law, shall be approved by the Board and shall be conducted in accordance with any applicable law. Except where specifically forbidden by law, NC employees subject to such disclosures shall be informed promptly after the disclosure of the actions taken and the reasons for them.

iv. Annual Statement. Pending breach of this policy, the Board shall issue an annual statement of the instances of account monitoring or inspection that fall within categories D through G above. The statement shall indicate the number of such instances and the cause and result of each. No personally identifiable data should be included in this statement.

v. Privacy Policy. More information about Northpoint College's privacy practices can be found in the consumer information.

14. Waiver of Policy

a. An NC employee or student may apply to the Board for an exception or waiver from one or more of the provisions of this policy. Such an application may be for single use or for periodic or continuous uses, such as in connection with a course or program. Any application for a waiver should be made prior to using the NC Computer Resource for the purposes described in the application.

b. The written waiver application must state:

i. the policy provision or provisions for which the User is seeking a waiver;

ii. how the User plans to use NC Computer Resource to be covered by the waiver and the reasons why the User believes a waiver should be approved;

iii. If the waiver involves confidential research information, what steps will be taken to protect such information;

iv. the length of time for which the waiver is being requested; and

v. if a student, how and by whom the student will be supervised.

c. The Board shall consult with NC's IT Coordinator and the president of the applicant's college (or, if the applicant is a Northpoint College Office employee, the Academic Dean) or their designees, prior to making a determination regarding the application.

d. Users should be aware that NC cannot waive federal, state, or local law; for example, the contents of NC Computer Resources (including confidential research information) may be subject to a valid subpoena regardless of the terms of any waiver.

15. Enforcement.

a. Violation of this policy may result in suspension or termination of an individual's right of access to NC Computer Resources, disciplinary action by appropriate NC authorities, referral to law enforcement authorities for criminal prosecution, or other legal action, including action to recover civil damages and penalties.

b. Violations will normally be handled through the College disciplinary procedures applicable to the relevant User. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed by the Office of the President.

c. NC has the right to temporarily suspend computer use privileges and to remove from NC computer resources material it believes violates this policy, pending the outcome of an investigation of misuse or finding of violation. This power may be exercised only by the president of each college or the Academic Dean.

16. Additional Rules. Additional rules, policies, guidelines, and/or restrictions may be in effect for specific computers, systems, or networks, or at specific computer facilities at the discretion of the directors of those facilities. Any such rules which potentially limit the privacy or confidentiality of electronic communications or information contained in or delivered by or over NC Computer Resources will be subject to the substantive and procedural safeguards provided by this policy.

17. Disclaimer.

a. NC shall not be responsible for any damages, costs, or other liabilities of any nature whatsoever regarding the use of NC Computer Resources. This includes, but is not limited to, damages caused by unauthorized access to NC Computer Resources, data loss, or other damages resulting from delays, non-deliveries, or service interruptions, whether or not resulting from circumstances under the NC's control.

b. Users receive and use information obtained through NC Computer Resources at their own risk. NC makes no warranties (expressed or implied) with respect to the use of NC Computer Resources. NC accepts no responsibility for the content of web pages or graphics that are linked from NC web pages, for any advice or information received by a user through the use of NC Computer Resources, or for any costs or charges incurred by a user as a result of seeking or accepting such advice or information.

c. NC reserves the right to change this policy and other related policies at any time. NC reserves any rights and remedies that it may have under any applicable law, rule, or regulation. Nothing in this policy will act as a waiver of such rights and remedies.

Northpoint College Information Security Policy

I. General

1. Introduction – Each College entity (i.e., a college or a Northpoint College Office department) and all users with access to college information available in college files and systems, whether in computerized or printed form, are continually responsible for maintaining the integrity, accuracy, and privacy of this information. Loss of data integrity, theft of data, and unauthorized or inadvertent disclosure could lead to significant exposure of the College and its constituents and those directly responsible for the loss, theft, or disclosure. Non-compliance with state or federal laws could lead to direct financial loss to the College. Users are directed by these Information Technology Security Procedures ("IT Security Procedures"), which cover all College networks and systems.

Any proposed exception to these IT Security Procedures must be communicated in writing and approved by the IT Coordinator or his designee prior to any action introducing a non-compliance situation.

2. Non-Public College Information – For the purpose of these IT Security Procedures, the term "Non-Public College Information" means personally identifiable information (such as an individual's Social Security Number; driver's license number or non-driver identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; personal electronic mail address; Internet identification name or password; and parent's surname prior to marriage); information in student education records that is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA) and the related regulations set forth in 34 CFR Part 99; other information relating to the administrative, business, and academic activities and operations of the College (including employee evaluations, employee home addresses and telephone numbers, and other employee records that should be treated confidentially); and any other information available in College files and systems that by its nature should be treated confidentially.

II. Access Issues

3. Access to College Information

(a) General. Access to College information available in college files and systems, whether in electronic or hard copy form, must be limited to individuals with a strict need to know, consistent with the individual's job responsibilities.

(b) Employees Permitted Access to Non-Public College Information. Except as provided elsewhere in this section 3, access to Non-Public College Information must be restricted to full-time and regular part-time employees of the College and its related entities, the College's adjunct faculty, and employees of the College's contractors who have been permitted such access under a written agreement with the College. All employees permitted access to Non-Public College Information must be specifically reviewed by the Northpoint College Office department involved in accordance with section 4 below.

(c) Employees Requiring Waiver. Employees of the College or its related entities who are not full-time and regular part-time employees (e.g., individuals hired as part of a temporary staff augmentation or in connection with an individual project), College adjunct faculty, or employees of the College's contractors who have been permitted access to Non-Public College Information under a written agreement with the College may not be permitted any such access, except pursuant to the waiver procedure set forth in section 3(e) below.

(d) NC Students. NC Students may not be permitted any access to Non-Public College Information, except pursuant to the waiver procedure set forth in section 3(e) below. For these IT Security Procedures, "NC Students" means all students enrolled in any academic program, or taking any course or courses, at the College, except the following:

(i) students who are also College adjunct faculty,

(ii) employees of the College or its related entities or contractors who are auditing a course at the College,

(iii) employees of the College or its related entities or contractors who are taking a credit-bearing course at a College other than where they are employed, and

(iv) employees of the College or its related entities who are taking a credit-bearing course at the College where they are employed, provided they are taking the course pursuant to a tuition waiver program under a collective bargaining agreement, or are excluded from collective bargaining and are taking the course under a College tuition waiver policy.

(e) Waiver Procedure. An individual who is not permitted access to Non-Public College Information under sections 3(c) and (d) above may be permitted such access on a strict need to know basis, consistent with the individual's job responsibilities, but only if a waiver is granted by the IT Coordinator or his designee following a written, electronic request by the Northpoint College Office department involved. Any waiver granted will be limited to a specific period of time, which may not exceed one year. In order to extend the waiver after expiration, this waiver procedure must be repeated. The written waiver request must state:

- the specific status of the individual as an employee of the College or one of its related entities or contractors and/or as an NC Student,
- the type and form of access that is being requested,
- the length of time for which access is being requested,
- the reasons for permitting such access, and
- how and by whom the individual will be supervised.

The IT Coordinator or equivalent at the College or in the Northpoint College Office department will be responsible for maintaining all documentation of any waiver request and disposition.

(f) Acknowledgment of College Policy. All employees described in section 3(b) above and all employees and NC Students granted a waiver under section 3(e) above must acknowledge, by signature, receiving a copy of the College's Policy on Acceptable Use of Computer Resources and these IT Security Procedures.

4. Review of Access to College Files and Systems – Each College entity must review, at least once during each of the fall and spring semesters, individuals having any type of access to College files and systems and must remove user IDs and access capabilities that are no longer current. This review includes, but is not limited to, access to College networks, applications, sensitive transactions, databases, and specialized data access utilities.

An attestation letter of such review must be completed by the IT Coordinator or the equivalent at the College or in the Northpoint College Office department and submitted to the College IT Coordinator or college Registrar no later than the date specified in the instructions for completing the attestation letter. Documentation showing the review steps taken in arriving at the attestation must be retained in the office of the Registrar or the equivalent at the College or in the Northpoint College Office department and be made available for further review by the IT Coordinator and internal/external audit entities as appropriate.

5. Severance of Access upon Termination or Transfer of Employment – Access to College files and systems must be removed no later than an individual's last date of employment. User IDs must not be re-used or re-assigned to another individual.

For job transfers, access to College files and systems must be removed no later than the individual's last date in the old position and established no sooner than his or her first date in the new position.

In special circumstances where underlying information attributed to a user ID must be retained and made accessible from another user ID, approval must be obtained from both the IT Coordinator or the equivalent at the College or in the Northpoint College Office department. Such arrangements, if approved, will be for a fixed duration of time, determined on a case-by-case basis.

6. Authentication – Users of College files and systems must use an individually assigned user ID to gain access to any College network or application.

7. User IDs – Users of College files and systems other than technical employees within Information Technology departments at the College or in the Northpoint College Office must have no more than one individually assigned user ID per system. The user ID must be in a format consistent with the College naming standards, clearly identifiable to a user, and not shared.

Generic-named user IDs used in background/batch processes or peer-to-peer processes and multiple user IDs required to maintain, support, and operate systems by technical employees within Information Technology departments at a College or in the Northpoint College Office may be allowed under limited circumstances, provided that use of such identities is auditable, individual user accountability is assigned to each of these identities, oversight is administered by line management of the user assigned to the account, and use of these accounts is specifically approved by the IT Coordinator or the equivalent at the College or in the Northpoint College Office department.

8. Passwords – Passwords and private encryption keys must be treated as Non-Public College Information and, as such, are not to be shared with anyone. A password must be entered by the user each time he or she authenticates to a college system. Use of auto-complete features to expedite or script user logins (e.g., "Windows Remember My Passwords?") is prohibited. All passwords must be changed at least every 180 days. Passwords should not be based on personal information (e.g., family names, pets, hobbies, and friends) and should be difficult to guess. Passwords should be at least eight characters in length. Each College entity may adopt more stringent password controls.

III. Disclosure Issues

10. Disclosure of Non-Public College Information

(a) General Rule. Unless otherwise required by law, users of College files and systems must not disclose any Non-Public College Information (as defined in section 2 above) to the public or any unauthorized users.

(b) Definition of Social Security Numbers. For the purpose of these IT Security Procedures, the term "Social Security Number" means the nine-digit account number issued by the U.S. Social Security Administration and any number derived therefrom. It does not include any number that has been encrypted.

(c) Special Rules for Social Security Numbers. Unless required by law, users of college files and systems must not:

- Intentionally communicate to the public or otherwise make available to the public in any manner an individual's Social Security Number.
- Publicly post or display an individual's Social Security Number or place a Social Security Number in files with unrestricted access.
- Print an individual's Social Security Number on any card or tag required for the individual to access products, services, or benefits provided by the College.

- Print an individual’s Social Security Number on any identification badge or card, including any timecard.
- Require an individual to transmit his or her Social Security Number over the Internet unless the connection is secure or the Social Security Number is encrypted.
- Require an individual to use his or her Social Security Number to access an Internet website unless a password or unique personal identification number or other authentication device is also required to access the Internet website.
- Include an individual’s Social Security Number, except the last four digits thereof, on any materials that are mailed to the individual, or in any electronic mail that is copied to third parties, unless state or federal law requires the Social Security Number to be on the document to be mailed. Notwithstanding this paragraph (vii), Social Security Numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the Social Security Number. A Social Security Number that is permitted to be mailed under this paragraph (vii) may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.
- Encode or embed a Social Security Number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the Social Security Number as required by this section 10.
- Transmit an individual’s Social Security Number onto portable devices without encryption as specified in section 13 below.

These special rules do not prevent the collection, use, or release of a Social Security Number as required by state or federal law, or the use of a Social Security Number for internal verification, fraud investigation, or administrative purposes.

11. Web Accessible Data – Because Non-Public College Information must not be made accessible to the public, all College web pages must be programmed with a parameter to prevent the caching of Non-Public College Information by Internet search engines. Directory/folder listings of files through a web page must be disabled. Secure and encrypted data transfer protocols must be used when uploading data to a web site.

12. Security Incident Response and Reporting

(a) Acknowledgment and Reporting of Security Incidents. The appropriate faculty member or Northpoint College Office department must, within 24 hours of receipt by his or her department, acknowledge or respond in writing to any initial security incident report issued by the IT Coordinator. The faculty member or the Northpoint College Office department must make a full written report of such incident to the IT Coordinator, including root cause identification, explanation of the remediation plan, and extent of data loss, within 72 hours of the College's or department's receipt of the initial security incident report.

(b) NC Breach Reporting Procedure. The NC Breach Reporting Procedure must be followed whenever a security incident occurs involving the unauthorized disclosure of any of the following Non-Public College Information without encryption:

(i) Social Security Number;

(ii) driver's license number or non-driver identification card number; or

(iii) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(c) Limiting Disclosure. When any Non-Public College Information has been disclosed without valid authorization and encryption, all reasonable efforts must be taken to eliminate further disclosure, including immediate disconnection of any computer device involved from the College network.

13. Portable Devices/Encryption – The Non-Public College Information listed in section 12(b) above must not be stored, transported, or taken home on portable devices (e.g., laptops, flash drives) of any type without specific approval of both the IT Coordinator or the equivalent at the College or in the Northpoint College Office department. Where approval is granted, additional password protection and encryption of data are required. In addition, the Non-Public College Information listed in section 12(b) above stored on non-portable devices or transmitted between devices (e.g., servers, workstations) must be encrypted.

14. Safeguarding and Disposal of Devices and Records Containing Non-Public College Information – Whenever records containing Non-Public College Information are subject to destruction under the NC Records Retention and Disposition Schedule, the storage devices such as hard disk drives and other media (e.g., tape, diskette, CDs, DVDs, cell phones, digital copiers, or other devices) and hard copy documents that contain such information must be securely overwritten or physically destroyed in a manner that prevents unauthorized disclosure. While in use, such devices and documents must not be left open or unattended on desks or elsewhere for extended periods of time.

IV. Maintenance of Data and Systems

15. Change of Data in Records

(a) Authorization of Changes. When updates are not part of normal business processing, individuals within Information Technology departments at the college or in a Northpoint College Office department who have access to college information to support ongoing operations of administrative files and systems must not alter any such information unless given specific approval by the appropriate Northpoint College Office department. A record of any data change, including evidence of approval, must be retained in the office of the Registrar or the equivalent at the College or in the appropriate Northpoint College Office department.

(b) No Changes from Non-compliant Endpoints. Change to official College data of record by NC employees (i.e., faculty and staff) must only be performed from endpoints that are in compliance with section 20, "Device Management." Due to the increased risk of the presence of insidious malware that captures and/or interferes with the integrity of entered data, such changes may not be made from publicly accessible computers, Internet "cafés" and similar uncontrolled environments.

16. Centralized Data Management – Data that is acquired or managed by Northpoint College Office departments (e.g., CPE, skill scores) must be loaded into college files and systems and may not be modified by departments. Departments will be able to view such data and through an exception process be able to request changes. Each department is responsible for reviewing a data edit report for accuracy and completeness whenever data is uploaded to its respective student or human resources systems.

17. Grade Changes – Any college system that allows for grade changes must have multiple security levels enabled, including the maintenance of a separate password that is administered and changed regularly for the purpose of authenticating individual users to the grade change function. Grade change functions must be able to create an audit trail from which edit reports will be regularly prepared for review by a management designee other than the person who has responsibility for the area making grade changes. The number of individuals allowed to make grade changes must be strictly limited to employees of the College and its related entities, subject to the additional criteria set forth in section 3 above. Current College student information systems support this requirement.

18. Changes in Information Files and Systems – Existing and new information files and systems must comply with these IT Security Procedures. Modifications to existing information files and systems will be required to maintain compliance. Ghost files and systems and development/test files and systems holding copies of data from master files and systems must also comply with these procedures. Ghost files and systems should be eliminated to minimize the number of copies and access points to Non-Public College Information. Where files and systems cannot be modified to comply with these procedures, the College entity must notify the IT Coordinator, providing a written business case justifying the decision.

19. Device Management – All devices that are allowed to connect to college networks and systems that support administrative, business, and academic activities and operations must be maintained at current anti-virus/malicious code protection at all times. In addition, security updates to operating systems must be applied on a timely basis after appropriate testing. Although the College does not manage student computers, procedures should be implemented to minimize the risk to college files and systems.

20. Management Responsibility – The Northpoint College Office and its management are responsible for maintaining and overseeing compliance with these IT Security Procedures within their line responsibilities.

21. Information Technology Security Procedure Governance – The College will organize working groups and work through existing councils to identify and establish procedures and other areas of change that may be instituted to further protect the integrity of college files and systems. Additional and/or revised procedural statements may be adopted and introduced for college compliance. Further procedural documents may be developed to elaborate in detail on these IT Security Procedures, but they will in no way detract or suggest a different level of compliance that is expected or required. Non-compliance with these IT Security Procedures may result in termination of access to college network and applications until compliance is re-established. Non-compliance may also result in disciplinary action.

Northpoint College Data Center Security and Environment Support Policy

1. Policy Statement

Northpoint College is committed to maintaining a secure and resilient data center to protect the institution's critical information assets and infrastructure. This policy outlines the minimum protections required for the data center and mandates an annual risk assessment to ensure these protections are adequate and effective.

2. Scope

This policy applies to all Northpoint College employees, contractors, and third-party service providers with access to the data center, including the physical premises and the information systems housed within.

3. Minimum Protections

- Physical Security: Access to the data center must be restricted to authorized personnel only. Physical access controls such as key cards and security personnel will be implemented to enforce this requirement.
- Environmental Controls: The data center must be equipped with appropriate environmental controls to protect against fire, flooding, and other natural or man-made disasters. This includes, but is not limited to, fire suppression systems, water leak detection, and temperature and humidity controls.
- Power Supply and Backup: Uninterruptible power supplies (UPS) and backup generators must be in place to ensure continuous power in the event of an outage. Regular testing of these systems will be conducted to ensure their reliability.
- Network Security: Network access to and within the data center must be secured using firewalls, intrusion detection/prevention systems (IDS/IPS), and other appropriate security measures. Network segmentation will be used to isolate sensitive systems and data.
- Surveillance: Continuous video surveillance of the data center's (Northpoint College’s offices) exterior and interior will be maintained. Recorded footage will be stored securely for a minimum period as defined by institutional policies.
- Maintenance and Operations: Regular maintenance of data center infrastructure, including hardware, software, and security systems, must be performed to ensure operational reliability and security. All maintenance activities will be logged and reviewed.

4. Annual Risk Assessment

- Assessment Process: Each year, Northpoint College will conduct a comprehensive risk assessment of the data keeping centers to evaluate the adequacy of existing protections and identify any vulnerabilities or threats. This assessment will cover physical security, environmental controls, network security, and any other relevant areas.
- Documentation: The findings of the risk assessment, including any identified risks and recommended mitigations, will be documented in a formal report. This report will be

reviewed by the data center security team, the College's IT Coordinator (ITC), and other relevant stakeholders.

- Action Plan: Based on the risk assessment findings, an action plan will be developed to address identified risks and vulnerabilities. This plan will prioritize actions based on the level of risk and available resources.
- Review and Approval: The risk assessment report and action plan will be submitted to the College's senior management for review and approval. Once approved, the action plan will be implemented within a defined timeframe.

5. Compliance and Enforcement

- Responsibility: All individuals with access to the data center are responsible for complying with this policy. The ITC is responsible for enforcing policy compliance.
- Violations: Violations of this policy may result in disciplinary action, up to and including termination of employment, revocation of data center access privileges, and legal action.

6. Policy Review and Update

This policy will be reviewed annually or as needed to reflect changes in technology, risks, and regulatory requirements. The ITC, in coordination with the appropriate departments in Northpoint College’s office, and other relevant stakeholders, will lead the review process.

Northpoint College Policy on Email Auto-Forwarding

Purpose and Background:

Auto-forwarding of Northpoint College emails is the automated re-sending of email from an NC email service to a non-NC email service. Auto-forwarding is typically requested to avoid separately accessing multiple email accounts (e.g., personal and college-related). Auto-forwarding raises concerns, however, regarding security, privacy, and reliability and risks potential legal and public institution governance implications. Auto-forwarding can also be technically problematic. Potential issues posed by auto-forwarding include:

- Inappropriate disclosure of Non-Public College Information (NPCI), including personally identifiable information such as social security numbers. (Additional examples of NPUI are included below.) Although email is not generally appropriate for the transmission of unencrypted NPUI, risks increase when NPUI in any form leaves NC’s systems

- Significantly increases the complexity of complying with Michigan’s Freedom of Information Act (FOIA) and e-discovery
- External (non-NC) email providers can block NC email or mail servers when too much spam is auto forwarded. If a major email provider blocks email from NC, it can result in a broad and extended impact to NC
- Non-NC email providers can impose terms of service that reserve them the right to collect, read, use, distribute or even claim ownership of email that is sent to their system
- Senders may not receive a non-delivery receipt (“bounce back”) even when delivery to an auto-forwarded address does not occur
- Important email from NC may be delayed or fail to be delivered
- NC IT may take longer or be unable to diagnose or resolve delivery problems with a non-NC email provider
- Interferes and introduces complexity with anti-spam measures such as Sender Policy Framework (SPF)

Northpoint College Information Security Procedure

Email Auto-Forwarding

Scope:

This procedure applies to Northpoint College and the Northpoint College Office email systems that facilitate NC academic and administrative communication by faculty, staff, and students.

Statement:

Email sent to an NC email address mailbox shall not be forwarded through an automated means to a non-NC destination email address. Selected email may be manually forwarded by an NC user to a non-NC destination when such forwarding:

a. will not result in an inappropriate disclosure of NPCI
b. does not also automatically delete the email from the NC mail server
c. complies with the requirements of the NC Policy on Acceptable Use of Computer Resources

Full consideration of the use of POP, IMAP, ActiveSync, and similar protocols used to retrieve or synchronize mail with mobile devices and non-NC email accounts is not within the scope of this procedure, nevertheless, any such use must comply with a, b, and c above.

Procedure(s):

A northpointcollege.edu (i.e., Northpoint College provided) email account should be used to issue and receive NC-related email communications. College email systems must be configured to prevent or disallow auto-forwarding where technically feasible. NC email can be accessed using mobile devices with no use of auto-forwarding required. Mobile devices, desktop email applications, etc., support concurrent access to multiple email accounts by combining email from separate accounts into a consolidated view. In this way, the need to auto-forward email from one account to another is conveniently avoided. For email setup and support information, contact the IT Coordinator.

Responsibility:

NC faculty, staff, and students and affiliates of Northpoint College

Northpoint College Acceptable Use of College Data in the Cloud Policy

1. Purpose:

This Acceptable Use of College Data in the Cloud Policy is established to ensure the responsible and secure use of cloud computing services at Northpoint College in compliance with Title IV regulations and the Gramm-Leach-Bliley Act (GLBA). The purpose of this policy is to safeguard sensitive data, uphold the privacy and confidentiality of student information, and maintain the integrity of Northpoint College's cloud-based systems.

2. Scope:

This policy applies to all faculty, staff, students, contractors, and any other individuals or entities granted access to Northpoint College's cloud services.

3. Data Classification:

All data stored, processed, or transmitted through cloud services must be classified based on sensitivity, with special attention to Personally Identifiable Information (PII), financial information, and any data covered by Title IV regulations or the GLBA.

4. Authorized Cloud Services:
Only approved cloud service providers, vetted by the college's IT department, shall be used for storing, processing, or transmitting college data. Faculty, staff, and students must seek approval before engaging with any new cloud service.

5. User Responsibilities:

- Users must adhere to the terms of service and acceptable use policies of the selected cloud service providers.
- Access credentials (usernames, passwords, etc.) must be kept confidential and not shared.
- Users are responsible for classifying data correctly before uploading it to cloud services.

6. Data Encryption:
All sensitive data must be encrypted during transmission and storage in the cloud. Encryption keys must be managed securely.

7. GLBA Compliance:
In accordance with the GLBA, the college will implement measures to protect nonpublic personal information (NPI) related to financial aid and student accounts. Access to such information will be restricted to authorized personnel only.

8. Title IV Compliance:
All data related to Title IV financial aid programs must be handled in compliance with applicable regulations. This includes protecting the confidentiality and integrity of student records and financial information.

9. Incident Reporting:
Any unauthorized access, disclosure, loss, or other security incidents related to cloud data must be reported promptly to the college's IT department.

10. Training and Awareness:

Regular training sessions will be conducted to educate users on the proper use of cloud services, data protection, and compliance with relevant regulations.

11. Enforcement:
Violations of this policy may result in disciplinary action, including but not limited to account suspension, termination, or legal action, depending on the severity of the violation.

12. Review and Revision:
This policy will be reviewed annually and updated as necessary to address changes in technology, regulations, or the college's operational environment.

13. Contact Information:
For questions or concerns regarding this policy, please contact the Northpoint College IT Department at mfusaro@northpointcollege.edu.

By agreeing to use Northpoint College's cloud services, users acknowledge their understanding and acceptance of this Acceptable Use of College Data in the Cloud Policy.

Northpoint College Data Classification Standard

Purpose and Background:

This standard defines a framework for categorizing the college's institutional data assets by establishing a data classification standard. It is the intention of this standard to promote the widest possible use of College Data in support of college academic, research, and administrative objectives by providing the uniform basis to define appropriate levels of protection and to comply with applicable laws and regulations. This standard is derived from a variety of sources, including FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, the State of Michigan Department of Technology, Management and Budget (DTMB) IT Technical Policies, Standards and Procedures, NIST SP800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), as well as the data classification standards of other institutions of higher education.

Scope:

This standard applies to all College Entities and governs all College Data, electronic or non-electronic, which is processed, created, collected, stored, or archived by the college. Any individual who uses, stores, or transmits College Data shares the responsibility to appropriately safeguard such data.

Statement:

This Data Classification Standard categorizes types of data for determining security measures that correspond to its sensitivity and the level of risk should the data be inappropriately exposed, altered, purged, or unavailable. The Data Owner is the primary party responsible for using this standard to evaluate and classify College Data within its purview according to the classification categories outlined below. It is appropriate for the Data Owner to confer with Subject Matter Experts who possess in-depth knowledge regarding its information assets.

A dataset or system must be classified to reflect the highest classification required of any data element that can be present. For example, if a dataset contains a student's name and optional social security number, the dataset should be classified as Confidential Data even though a student's name may, by itself, be classified at a less restrictive classification level. Equally important, data must be classified according to the lowest (least restrictive) category appropriate to that data in its context.

Three data classification categories are defined below:

- **Confidential Data:** Data shall be classified as *Confidential* when the unauthorized disclosure, alteration, or destruction of that data could result in a *significant level of risk* to the college. Significant risk includes but is not limited to substantial financial, reputational and/or personal privacy loss; impairing the functions of the college; or presenting legal or financial liability. Confidential Data requires the highest level of protection and control. See Appendix A for a list of predefined types of Confidential Data.
- **Sensitive Data:** Data shall be classified as *Sensitive* when the unauthorized disclosure, alteration, or destruction of that data could result in a *moderate to low level of risk* to the college. All data not classified as Confidential Data or Public Data should be considered Sensitive Data. Sensitive Data requires moderate protection. See Appendix B for examples of Sensitive Data.
- **Public Data:** Data shall be classified as *Public* when the unauthorized disclosure, alteration, or destruction of that data could result in *little or no risk* to the college. Examples of Public Data include data published on public websites, press releases, course catalog information, job postings, etc. While access control measures may or may

not be required for particular Public Data, protections to ensure the integrity and/or availability of certain Public Data may be appropriate.

Non-Public College Information

The definition of Non-Public College Information (NPCI), as defined in the NC IT Security Procedures – General, is superseded by this standard. The combined Confidential and Sensitive data classifications are substantially comparable to the less-detailed NPCI definition and may be used to guide compliance with the Procedures until they are revised.

Reclassification

On an ongoing basis, Data Owners should evaluate the classification of their College Data to ensure the assigned classification remains appropriate based on any changes to legal and contractual obligations as well as changes in the use of the dataset and its value to the college. If a Data Owner determines that the classification of a certain data set has changed, an analysis of security protections should be performed to determine if modifications are necessary to align with the new classification. Any required changes to the protection profile should be implemented in a timely manner.

Definitions and Terms

Affiliate or Affiliated Organization: Any organization associated with the College that uses College resources to create, access, store, or manage College Data to carry out its business functions. This applies to all third-party vendors under a contractual agreement.

Data Element: A unit of data that refers to one separate item of information, such as name, address, date of birth, etc.

Data Owner: The College Entity (typically a function or department) that can authorize or deny access to certain data, can delegate custody of that data, and is accountable for its accuracy, integrity, and timeliness. The Data Owner is responsible for classifying its data so that appropriate safeguards are applied to protect its data resources. Common examples of Data Owners:

Description	Common Data Owner(s)
Student Records	Registrar, Enrollment Management, Bursar, Student Finance, Student Affairs
Employee Records	Human Resources

Research Data	Researcher, Principal Investigator
Financial Data	Finance, Business Office, Procurement
Academic	Faculty, Department Chair, Dean, Provost, Academic Affairs

Data User: Creates, accesses, and alters data, uses data resources, and is responsible for complying with data use requirements.

Dataset: A collection of Data Elements, such as data contained in a file, document or database, or as aggregated in any form.

Personally Identifiable Information (PII): Any information that permits the identity of an individual to be directly or indirectly inferred.

Subject Matter Expert: A subject matter expert (SME) is an individual with an in-depth, authoritative understanding of a particular functional area such as registration, enrollment, finance, etc.

College Data: Any NC institutional data related to NC's academic, research, and administrative functions either stored on NC information technology systems or maintained by, or on behalf of, NC faculty, staff, students, and affiliates in any format or location.

College Entities: All colleges, academic and administrative departments, and affiliates.

Appendix – A

Predefined Types of Confidential Data

1. Personally Identifiable Information (PII)

PII is any information about an individual that can be used to distinguish or trace a natural individual’s identity.

The following list contains examples of information that may be considered PII.

- Name, such as full name, preferred name, maiden name, mother ‘s maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, state-issued driver’s license number, state-issued non-driver identification card number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as home street address or personal email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address and other persistent static identifier that consistently links to a particular person or a small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information

- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Contextual Considerations

The context, nature and combinations of PII data elements present are factors relevant to the level of confidentiality for a particular use. For example, a list of names contained within a file can be classified differently depending upon the nature of the list:

Example Context	Classification
Individuals with a criminal record	Confidential
Students requiring behavior intervention	Confidential
Immigration status	Confidential
Employees with poor performance ratings	Confidential
Compliance training participants	Sensitive
Attendees at a public meeting	Public

It is therefore relevant for Data Owners to consider context when determining an appropriate data classification for instances of PII. PII containing personal identification numbers shall be classified Confidential Data regardless of context.

2. State of Michigan Private Information

New York State data breach notification law defines “private information” as any information that permits the identity of an individual to be inferred (e.g., name) in combination with one or more of the following data elements:

- Social Security Number
- State-issued driver's license number
- State personal identification card number
- Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident’s financial accounts.

Data containing State of Michigan private information is classified Confidential Data regardless of context.

3. Personally Identifiable Education Records

Student educational records that require protection under the Federal Educational Rights and Privacy Act (FERPA). Examples include class rosters, test scores, grades and financial aid information that can be associated with an individual.

FERPA permits certain PII defined as “directory information” to be disclosed to outside organizations and/or inquirers without prior student consent, unless a student request such information be withheld. Directory information is information that is generally not considered harmful or an invasion of privacy if released. Such directory information should be classified as Sensitive.

Student ID

A student’s unique ID number and user ID can be considered directory information as above so long as it cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user’s identity, such as a password, personal identification number (PIN), or other factors known or possessed only by the authorized user.

4. Protected Health Information (PHI)

Health information about an individual including medical records, health status, and records covered by health privacy laws.

5. Citizenship

Information about an individual’s US citizenship status, immigration information, etc.

6. Personnel Records

Personnel records of a confidential nature including disciplinary and behavioral matters, evaluations, background checks, criminal records, police, court and investigation records, etc.

7. Payment Card Information

Payment cardholder information requiring protection under the Payment Card Industry Data Security Standard (PCI DSS), such as credit and debit card numbers, card expiration dates, etc.

This includes the credit/debit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a card's magnetic stripe

8. Covered Financial Information

Regulated financial information, such as student financial aid records requiring protection under the Gramm-Leach-Bliley Act (GLBA), and other relevant regulations.

9. Restricted Procurement Information

Procurement information that must remain confidential as defined by the State of Michigan Department of Technology, Management and Budget, including RFP bid responses during the "restricted period."

10. Federal Tax Information ("FTI")

FTI is defined as any return, return information or taxpayer return information entrusted to the college by a taxpayer or the Internal Revenue Services. See Internal Revenue Service Publication 1075 Exhibit 2 for more information.

11. Intellectual Property

Trade secrets, technology, designs, models and other information that may be relevant for the creation of a college, faculty or student owned patent.

12. Personally Identifiable and Restricted Research Data

Human subject and other research data containing PII (i.e., not de-identified) and/or licensed under a restricted data use agreement or other applicable restriction.

13. Passwords and Access Codes

Any information held in confidence by an individual that is used to verify the identity of the person, such as passwords and access codes. Such verifiers can also be used to prove the identity of a system or service. Examples include:

- Passwords
- PINs
- Access codes
- Tokens
- Shared secrets
- Cryptographic private keys

14. Export Controlled Materials

Export Controlled Materials is defined as any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations ("EAR") published by the U.S. Department of Commerce and the International Traffic in Arms Regulations ("ITAR") published by the U.S. Department of State. See the Information and Guidelines on Federal Export Control Laws and Regulations, published by the Office of Sponsored Programs, for more information.

15. Other Confidential Information

Any data that by its nature requires confidentiality or that the college is required to maintain confidentially, such as data subject to a confidentiality agreement executed by the college.

Appendix – B

Examples of Sensitive Data

- Email and other communications regarding internal matters which have not been specifically approved for public release
- Proprietary financial, budgetary or personnel information not explicitly approved by authorized parties for public release
- Identities of donors or other third-party partner information maintained by the college not specifically designated for public release
- Information designated as “Directory Information” under FERPA. Directory information withheld by a student's request should be classified as Confidential Data. (See “Appendix A Personally Identifiable Education Records”)
- Examinations (questions and answers)
- IT system configurations and logs not containing Confidential Data
- Business recovery and emergency response plans
- Any other non-Confidential Data that should not be distributed publicly

Appendix – C

Examples of Public Data

- The content of public websites, like www.northpointcollege.edu
- Course curriculums
- Class schedules (not student specific)
- Course catalogs
- Information about campus activities, clubs and organizations
- College policies
- Academic calendars
- Academic programs
- Information on how to access educational resources
- Publicly accessible services
- Press releases
- Public communications and advisories
- Information that by law or regulation is required to be publicly disclosed
- Scholarly publications, research data and findings not otherwise classified as Confidential or Sensitive Data.

Note: Though, by definition, disclosure of Public Data must present little or no risk to the college (irrespective of whether such disclosure is intended or desired), it is nevertheless appropriate for Data Users and Data Owners to apply access restrictions for certain Public Data. Examples include draft or provisional documents; scholarly publications during development, collaboration and peer review; targeted communications and other Public Data documents prior to approval for general release or publication.

Northpoint College Open Access Technology Facility Policy

Purpose and Background:

Open Access Technology Facility is a general term for a facility or lab that provides shared technology and related resources supporting the campus community, typically, but not necessarily, on a “drop in” basis. This policy defines supplementary information security requirements specific to NC Open Access Technology Facilities intended to promote a safe, secure and welcoming environment.

Scope:

This policy applies to all College Open Access Technology Facilities.

Statement:

I. Each user of the technology facility is required to use a unique login credential or equivalent unique access code to access services, where implementation of such is technically achievable.

a. Such sign-ons and sign-offs must be securely logged with a timestamp, username (or other unique identifier) unique system name and IP address that, in response to an incident, would help facilitate the attribution of activity to a particular account holder.
b. Users are permitted to request to view this sign-in/off log (i.e., when they have logged in or out) in a read-only manner, if feasible, but a user's log must not be accessible to, nor alterable by, other users.
c. The logs must be retained for three years so that the logged information can be retrieved to support an investigation within three business days.

Where the above is not technically achievable, other means to log usage, such as a supervised sign-in/out procedure, should be used where practical.

II. Periodically present a logon banner or equivalent conveyance to each user in which the user agrees that use must comply with the College Acceptable Use of Computer Resources policy and other relevant College policies, and highlighting that:

a. All use must be legal and in accordance with the Acceptable Use of Computer Resources policy.
b. Activity may be monitored in accordance with the Acceptable Use of Computer Resources policy.
c. The display or play of visual or audible material that is disruptive to other facility users, or that could violate the Policy on Sexual Misconduct, is not permitted. Where such is in support of a faculty-endorsed, academic purpose, appropriate care must be taken to avoid offending or disrupting other facility users.

III. Users should be automatically signed-off from their session after a period of inactivity, where implementation of such is technically achievable. The maximum period of inactivity before sign-off should be 30 minutes.

IV. Facility computers, loaner equipment (laptops, tablets, etc.) and other devices that access College networks or the Internet must conform to all NC IT Security policy requirements, including the following that may reinforce or supplement such requirements:

a. Real-time, anti-malware protection must be active with scheduled full scans of accessible memory and files performed at least weekly.

b. Anti-malware software and related signatures and configurations must be kept up-to-date.
c. Malware-infected computers or devices must be promptly removed from the network until verified as malware-free.
d. Facility Admins/Facility Managers are responsible for creating procedures that ensure the requirements are implemented on an ongoing basis.

V. Use of non-persistent desktops (e.g., virtual desktops) or automated system restore (e.g., “Deep Freeze”) upon sign-out or at regular intra-daily intervals is encouraged to ensure that facility users are presented with a clean, known-good environment. Non-persistent desktops help to avoid breaches of security or privacy that could occur from remnant temporary files, etc., persisting between user sessions, and to reduce cross-session, malware-related risks.

VI. Facility device software and operating systems, including system images used for non-persistent desktops, etc., must be updated as needed or required (at least monthly or promptly when there is a critical vulnerability, whichever is sooner) to include vendor-released security and anti-malware software updates.

Northpoint College Insider Threat to Technology Resources

Purpose and Background:

Insider Threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

This procedure enumerates controls that can deter, detect, prevent, mitigate or resolve Insider Threats against NC technology resources and assets.

Types of Insider Threats

Unintentional Threat

- Negligent: An insider of this type exposes an organization to a threat through carelessness. Examples include ignoring messages to install software updates and security patches, not properly safeguarding passwords and private keys, or failing to implement appropriate access control measures.
- Accidental: An insider of this type mistakenly causes an unintended risk to an organization. Examples include inadvertent disclosure of confidential information to unauthorized personnel, unknowingly or inadvertently clicking on a malicious hyperlink, opening an attachment that contains a virus within a phishing email, or improperly disposing of confidential documents.

Intentional Threats

Intentional threats are actions that harm or abuse an organization for personal benefit or to act on a personal grievance. Examples are individuals that retaliate due to a perceived lack of recognition (e.g., compensation, promotion) or involuntary termination. Retaliatory actions can include misappropriating College resources for personal gain, leaking or stealing sensitive or confidential information, deleting data, creating a denial-of-service condition, sabotaging equipment and services, harassing associates, and perpetrating violence.

Scope:

This procedure pertains to information technology insider threats relevant to technology resources and assets at all NC Colleges and the Northpoint College Office. This procedure does not address all forms of institutional insider threats.

Procedure:

Departments should implement a variety of controls to help reduce risks associated with IT insider threat. Each department should conduct a risk assessment and select and implement controls applicable to its respective technological and personnel environments. Controls are distinguished in two categories, organizational and technical.

Organizational Controls

- Separation of duties: The responsibility for approving and monitoring access to data centers, technology labs, server hardware, and the network should be segregated between multiple individuals with discrete roles to mitigate the risk of a lone insider threat actor and to support organizational checks and balances.

- Oversight: A Data Center Manager or equivalent function tracks and controls inactive/surplus hardware to prevent undetected misappropriation, unauthorized use, and theft.
- Know Your People: IT organizations must know and engage their staff to achieve a level of trust and personnel assurance.
- Train Your People: Provide training that helps staff recognize suspicious activity and misuse and explains how to report misconduct (anonymously, if desired).

Technical Controls

- Only permit network connections to authorized servers.
- Block unauthorized remote access protocols and remote desktop applications.
- Monitor the network for unauthorized use of network ports.
- Monitor wireless networks for rogue network access points.
- Explicitly authorize active subnets and address blocks to avoid rogue use of unallocated and unused address space.
- Conduct network scans to discover new systems to correlate with inventory of known and authorized servers.
- Use centralized system administration tools to provide visibility on all applications and activity on the network.
- Enable audit trails and utilize auditing tools as needed to record transactional activity associated with a user to support investigations.

Responsibility:

IT Coordinator and other IT leadership

Related Information:

DHS CISA Insider Threat Definitions - https://www.cisa.gov/defining-insider-threats

DHS CISA Insider Threat Assessment and Mitigation - https://www.cisa.gov/insider-threat-mitigation

Carnegie Mellon Software Engineering Institute Insider Threat Definition and Information - https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

Northpoint College IT Disaster Recovery and Business Continuity Policy

1. Governance

Coordinator Designation: Northpoint College’s IT Coordinator has also been designated as the Disaster Recovery (DR) and Business Continuity (BC) Coordinator(s) and is responsible for overseeing IT BC/DR efforts. This individual(s) is tasked with the development, implementation, and maintenance of the college's IT disaster recovery and business continuity plans.

2. Disaster Recovery Planning

Formal Written IT DR Plan: The college maintains a formal, written IT Disaster Recovery (DR) Plan outlining the systems and functions to be recovered in a disaster. This plan includes:

- A comprehensive list of critical systems and functions.
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each system.
- Detailed recovery procedures.

Activation Procedure: A procedure is in place to "activate" the DR Plan on short notice, ensuring rapid response to any incident. This includes:

- A communication plan for notifying relevant stakeholders.
- Steps for assessing the extent of the disaster.
- Specific instructions for initiating recovery efforts.

3. Periodic Data Backup

Back-up schedules and data sets are backed up within a suitable time period.

4. Proactive Loss Prevention

The unit has implemented "Proactive Loss Prevention" capabilities for its critical systems. This includes:

- Regular software updates and patch management.
- Advanced threat detection systems.
- Employee training on security best practices.

Policy Review and Updates

This policy and its procedures are reviewed annually or following significant changes to IT infrastructure or business operations. Amendments may be made to ensure continued effectiveness of the disaster recovery and business continuity strategy.

Responsibility

The DR and BC Coordinator(s), in collaboration with IT department heads and unit managers, is responsible for the implementation, periodic testing, and update of this policy. All employees are responsible for familiarizing themselves with and following the procedures outlined in this policy.