Information Technology

Acceptable Use Agreement for

Microsoft 365 Services

Purpose

The purpose of this agreement is to establish clear guidance on the appropriate use of Microsoft 365 (M365) services by Northern Virginia Community College (NOVA) staff, faculty, and other users.

Acknowledgement of this agreement is required and by accessing any NOVA / VCCS IT resources hosted, owned, or leased by the College including Microsoft 365 services, users are agreeing to adhere to NOVA/VCCS IT security and acceptable use and security policies including:

NOVA – Policy 502 – Acceptable Computer Use
NOVA – Policy 503 – IT Security Awareness Policy
NOVA – Policy 504 – Storage of Sensitive Data and Portable Storage Devices
NOVA – Policy 505 – Email Policy
NOVA – Policy 519 – Disciplinary Actions for Violations of IT Security

Application

This agreement applies to all NOVA faculty, staff, contractors, and all other persons having access to the College's technology and information systems.

Definitions

Microsoft 365 (M365) – is a suite of cloud-based productivity solutions including Office 365 Apps (Word, Excel, PowerPoint, Access), Exchange/Outlook email, SharePoint Online, OneDrive for Business, Teams, and security tools.

Exchange Online – is cloud-based enterprise-class email which is accessible via an Outlook client, Outlook on the Web from up-to-date web browsers, or mobile devices using the Outlook app.

SharePoint Online – is a cloud-based collaborative platform that integrates with M365 and allows organizations to share and manage content and applications.

OneDrive for Business – is a cloud-based enterprise storage solution which provides users up to 1TB of secure data storage.

Teams – is a cloud-based collaboration app which integrates presence (availability), individual/group chat, video/audio conferencing, document and calendar sharing in a central workspace.

M365 Cloud Storage – is the collection of storage repositories used in M365 for Exchange email, SharePoint Online, OneDrive for Business, and Teams.

Confidential data – is sensitive or protected data including: Personal Identifiable Information (PII); data covered by Federal Educational Rights and Privacy Act (FERPA); Protected Health Information (PHI); financial data covered under the Payment Card Industry Data Security Standard (PCI DSS), or passwords and access codes. Examples of confidential data in these categories are listed below for reference.

- **Personal Identifiable Information (PII)** including but not limited to social security number, date of birth, mother's maiden name, passport number, driver's license number, taxpayer identification number, bank account and credit/debit card numbers.

- Data, such as student educational records, are covered by the **Federal Educational Rights and Privacy Act (FERPA)**. This includes class rosters, test scores, grades and financial aid information that can be associated with an individual.

- **Protected Health Information (PHI**), including medical records, health status, and records covered by health privacy laws.

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

Scope

All Users have the responsibility to make use of Microsoft 365 resources in an efficient, ethical, and legal manner. These resources are to be used in a manner consistent with the instructional and administrative objectives of the College in general, and for the purposes such resources were provided. Access to these resources is a privilege and imposes upon users' certain responsibilities and obligations, as further described in this agreement.

Background

M365 allows users to work anywhere, anytime using the latest communication, collaboration, and productivity tools. M365 is accessible from your college-issued device or personal computer/device. The ubiquitous nature of M365 presents unique security challenges which requires the deployment and configuration of integrated security tools for data loss protection and compliance. In addition to these advanced security tools, users must adhere to security

best practices to ensure the M365 services are used in a manner that best protects the security of the College's confidential and sensitive data.

This document provides guidelines regarding the acceptable use of M365 by all NOVA employees for academic, research and administrative purposes. These guidelines are applicable only to M365 and are a supplement to NOVA's Employee Acceptable Use Policy. Any questions can be directed to the College CIO and/or VP of IET and Campus Computing.

Securely Accessing M365 Services

College-Issued Devices

If you have a college-issued device, you must regularly connect it to the College network through a direct connection or VPN. College-issued Windows and Mac devices are managed by enterprise tools which help ensure that software updates, antivirus updates, and security settings are properly configured and updated.

Personal Devices

As an employee of the College and a user of M365 services, you are also responsible for securing personal computers and any devices you are using to access M365 services.

- Ensure virus/malware detection software is installed with the latest definitions.
- Keep your operating system and software up-to-date.
- Password-protect your workstation or device and use idle-time screen saver passwords where possible.
- Only use your workstation or device with the privileges of a regular user—not as a system administrator.

Data Storage and Security

M365 Cloud Storage is the collection of storage repositories used in M365 for Exchange email, SharePoint Online, OneDrive for Business, and Teams. Users should adhere to the following data storage and security guidelines:

- Only use M365 Cloud Storage for College documents.
- Do not store personal files or data in M365.

  - Files stored on your NVCC M365 Cloud can be considered College records and could be subject to open records requests (under FOIA).
- MS Teams and SharePoint Online provide a time limited repository and should not be used as a substitute for personal storage solutions such as OneDrive for Business, staff home drives (H: drive) or department common drives (G: drive).
- Do not store College data locally on College or personal devices. These devices do not get backed up and allow for the possibility of data to be lost or stolen.
- Users should refer to Appendix A - Standards for Data Storage and Collaboration for a reference matrix of data types and appropriate storage repositories.

Sharing confidential information

- Confidential, personal and/or sensitive information should only be shared, via M365 services, when required by business need.
- When the sharing of confidential information is required, users should exercise the following best practices:
  - Identify the data as confidential using file naming conventions, watermarks, and integrated security options including Outlook's built-in encryption, do not forward, confidential, and confidential – view only designations.
  - Seek appropriate permissions from the data owner prior to sharing.
  - Ensure the purpose of sharing the data is transparent.
  - Establish a clear timeframe to ensure that this data is removed as soon as it is no longer needed.
- To the best of your ability, limit the amount of confidential information shared as it increases the risk of a data breach.
- Ensure that information is only shared with intended audiences. When restricting information access always consider the principles of Need to Know and Least Privilege.

Email Security

Encryption of Emails Containing Sensitive Data

- Emails containing sensitive data must be encrypted by approved email encryption procedures before being sent over the network.
- All emails containing sensitive information must be limited to minimum necessary information.
- All emails containing sensitive information must be sent only to those individuals with a need to know.

Prohibited Forwarding of Email
Automatic forwarding of NVCC email to an outside third-party mail system is prohibited. Policies have been implemented to block all auto forwarding of NVCC email.

Abuse of Email Privileges
Use of email is a privilege, not a right. This privilege can be revoked. Unacceptable behavior includes, but is not limited to:

- Sending unsolicited and unauthorized mass email (spam)
- Use of offensive language
- Distribution of obscene material
- Threats
- Infringement on others' privacy
- Interference with others' work
- Copyright infringement
- Illegal activity

OneDrive for Business

- OneDrive for Business can only be synchronized to NVCC domain-joined devices. Synching to personal devices is prohibited.

Teams

- Teams creation is centrally administered by ITSS.
- Teams is an internal collaboration tool and external users can only be added with authorization by ITSS.
- Team owners are responsible for auditing and managing Teams activity and membership.
- Communication initiated on Teams channels, emails, posts, calls, chats, and meetings are subject to security data loss protection policies, audit, FOIA and/or legal subpoenas.

<u>Acceptable Use Requirements</u>

NOVA has granted access to you as a necessary privilege in order to perform authorized job functions at the College.

- You will not knowingly permit use of your entrusted access control mechanism for any purposes other than those required to perform authorized employment functions.

These include logon identification, password, workstation identification, user identification, file protection keys or production read or write keys.

- You will not disclose information concerning any access control mechanism unless properly authorized to do so by your supervisor or College authority.

- You will not use any access mechanism that the College has not expressly assigned to you.

- You will treat all information maintained on the VCCS or NOVA computer systems as strictly confidential and will not release information to any unauthorized person.

- You agree to abide by all applicable state, federal, VCCS, and College policies, procedures and standards that relate to the **Information Technology Employee Ethics Agreement** and the **Information Technology Employee Acceptable Use Agreement.** You will follow all the security procedures of the VCCS and NOVA computer systems and protect the data contained therein.

- If you observe any incidents of non-compliance with the terms of this agreement, you are responsible for reporting them to the College Information Security Officer and/or management.

- You understand that the NOVA Information Security Office, or other designated college officials, reserve the right without notice to limit or restrict any individual's access and to inspect, remove or otherwise alter any data, file, or system resource that may undermine the authorized use of any VCCS or NOVA IT resources.

- You understand the preceding terms and provisions and that you accept the responsibility of adhering to the same. You further understand that should you violate this agreement, you will be subject to disciplinary action.

Monitoring

Per the IT Employee Acceptable Use Agreement, NOVA and the VCCS reserve the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on NOVA or VCCS systems to ensure compliance with NOVA and VCCS policies, and federal, state, or local regulations.

Enforcement

Any person found to be in violation of this agreement will be subject to appropriate disciplinary action as defined in Policy 519, Disciplinary Actions for Violations of IT Security and Acceptable Use.

NOVA
Northern Virginia Community College

Information Technology
Acceptable Use Agreement for
Microsoft 365 Services

Standards for Data Storage and Collaboration - Appendix A

Types of Data and Collaboration Activity	NOVA Managed Services					VCCS Managed Services
	Network Storage Group (G: Drive)	Network Storage Home (H: Drive)	OneDrive for Business (@nvcc.edu)	SharePoint Online (@nvcc.edu)	Teams (@nvcc.edu)	Canvas
Highly Sensitive Data (PII, FERPA, HIPAA, CJIS)	✓	✓				
Restricted Data	✓	✓	✓			
Public Data	✓	✓	✓	✓	✓	✓
Individual file storage		✓	✓			
Departmental Group File Share	✓			✓	✓	
Internal document collaboration with other @nvcc.edu users	✓		✓	✓	✓	
External document collaboration with individuals outside the College			✓		✓	
Document collaboration with students						✓