NORTHERN
NEW MEXICO COLLEGE

Your school, your future.

Removable Media Acceptable Use Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to connect portable removable media to any infrastructure within NNMC’s internal network(s) or related technology resources. This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.

- Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.

- USB card readers that allow connectivity to a PC.

- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function.

- PDAs, cell phone handsets, and smartphones with internal flash or hard drive-based memory that support a data storage function.

- Digital cameras with internal or external memory support.

- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.

- Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth, among others) or wired network access.

The policy applies to any hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity of the private and confidential client and business data that resides within NNMC’s technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently moved outside the enterprise network and/or the physical premises where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company’s public image. Therefore, all users employing removable media and/or USB-based technology to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

Applicability

This policy applies to all Northern New Mexico College employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-owned removable media and/or USB-based technology to store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust NNMC has built with its clients, supply chain partners and other constituents. Consequently, employment at Northern New Mexico College does not automatically guarantee the initial and ongoing ability to use these devices within the enterprise technology environment.

It addresses a range of threats to – or related to the use of – enterprise data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive corporate data is deliberately stolen and sold by an employee.
Copyright	Software copied onto portable memory device could violate licensing.
Spyware	Spyware or tracking code enters the network via memory media.
Malware	Viruses, Trojans, Worms, and other threats could be introduced via external media.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional USB-related connectivity within corporate facilities will be managed at the sole discretion of IT. Non-sanctioned use of USB-based hardware, software, and/or related components to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of portable memory devices to any element of the enterprise network.

Responsibilities

The VP of Finance of Northern New Mexico College has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

The VP of Finance, Northern New Mexico College has delegated the execution and maintenance of Information Technology and Information Systems to the Director of Information Technology.

Other IT, IS, and ICT staff under the direction of the Director of Information Technology are responsible for following the procedures and policies within Information Technology and Information Systems.

All Northern New Mexico College employees have the responsibility to act in accordance with company policies and procedures.

Affected Technology

All USB-based devices and the USB ports used to access workstations and other related connectivity points within the corporate firewall will be centrally managed by NNMC’s IT department and will utilize encryption and strong authentication measures. Although IT is not able to manage the external devices – such as home PCs – to which these memory resources will also be connected, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company’s infrastructure.

Policy and Appropriate Use

It is the responsibility of any employee of Northern New Mexico College who is connecting a USB-based memory device to the organizational network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any portable memory that is used to conduct Northern New Mexico College business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, and clients at risk.

2. Prior to initial use on the corporate network or related infrastructure, all USB-related hardware and related software must be registered with IT. A list of approved USB devices and related software is available for viewing at feature not available yet. If your preferred device does not appear on this list, contact the help desk at itservices@nnmc.edu or 505-747-2259. Although IT currently allows only listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in future.

3. End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet NNMC's established enterprise IT security standards.

4. NNMC will maintain a list of approved USB-based memory devices and related software applications and utilities, and it will be stored it.nnmc.edu/acceptableremovablemedia. Devices that are not on this list may not be connected to corporate infrastructure.

Security

5. Employees using removable media and USB-related devices and related software for data storage, back up, transfer, or any other action within NNMC's technology infrastructure will, without exception, use secure data management procedures. A simple password is insufficient. See the NNMC's password policy for additional background. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

6. All USB-based devices that are used for business interests must be pre-approved by IT, and must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed whatever anti-virus and anti-malware software deemed necessary by NNMC's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be used must be updated in accordance with existing company policy.

7. All removable media will be subject to quarantine upon return to the office before they can be fully utilized on enterprise infrastructure.

8. Passwords and other confidential data as defined by NNMC's IT department are not to be stored on portable storage devices.

9. End users must apply new passwords every business/personal trip where company data is being utilized on USB-based memory devices.

10. Any USB-based memory device that is being used to store NNMC data must adhere to the authentication requirements of NNMC's IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by NNMC's IT department before any enterprise data-carrying memory can be connected to it.

11. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. See sanitation policy for detailed data wipe procedures for flash memory.

Help & Support

12. NNMC's IT department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media. This applies even to devices already known to the IT department.

13. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of NNMC's IT department. This includes, but is not limited to, reconfiguration of USB ports.

14. IT may restrict the use of Universal Plug and Play on any client PCs that it deems to be particularly sensitive. IT also reserves the right to disable this feature on PCs used by employees in specific roles.

15. IT reserves the right to summarily ban the use of these devices at any time. IT need not provide a reason for doing so, as protection of confidential data is the highest and only priority.

16. IT reserves the right to physically disable USB ports to limit physical and virtual access.

17. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

Organizational Protocol

18. IT can and will establish audit trails in all situations it feels merited. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to NNMC's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains NNMC's highest priority.

19. The end user agrees to immediately report to his/her manager and NNMC's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

20. NNMC will not reimburse employees if they choose to purchase their own USB-based memory devices.

21. Any questions relating to this policy should be directed to Jorge C. Lucero in IT, at 505-747-2158 or jorgecolu@nnmc.edu.

Policy Non-Compliance

Failure to comply with the Removable Media and Acceptable Use Policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

The (i) Vice-President of Finance, (ii) Chief Operating Officer, and (iii) immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.

Employee Declaration

I, [_________________], have read and understand the above Removable Media and Acceptable Use Policy, and consent to adhere to the rules outlined therein.

Employee Signature	Date
Manager Signature	Date
IT Administrator Signature	Date