INTRODUCTION

This Information Security Policy outlines the guidelines, practices, and procedures for safeguarding the information assets of NATCCO MBAI. The policy aims to ensure the confidentiality, integrity, and availability of sensitive information, while also promoting a culture of security awareness among all employees, partners, and stakeholders.

1. POLICY STATEMENT

It is hereby the declared policy of NATCCO MBAI to be proactive in ensuring that the association's information assets are well documented and protected and are accessed only by identified individual or group.

2. APPLICABILITY

This policy applies to all employees, contractors, partners, and third parties who have access to NATCCO MBAI's information assets. It covers all forms of information, including digital and physical records, regardless of the medium or location.

3. PROCEDURES

4.1 Information Classification

All information assets shall be classified into appropriate categories based on their sensitivity and criticality. Classification levels shall include:

4.1.1 **HIGHLY RESTRICTED**: Very sensitive; of highest value to the MBA and intended for use by authorized individual only; if disclosed, could cause severe impact to the MBA if compromised.

4.1.2 **Confidential**: Information regarding MBA's members, employees, and partners MBA internal operations, that is available only to a specific group of employees in conducting MBA operation.

4.1.3 **Internal Use**: Information intended for internal use and not meant for public disclosure. Intended for use by MBA employees in conducting MBA operation, or third-party entities under a non-disclosure agreement.

4.1.4 **Public**: Information that can be shared openly without any restrictions.

4.2 Responsibilities

4.2.1 Management: MBA Management shall take ownership of information security and provide necessary resources for its implementation.
4.2.2 Employees: All personnel are responsible for adhering to the security practices and reporting any security incidents promptly.
4.2.3 MIS: The IT team shall manage and maintain the technical aspects of information security, including access controls, network security, and software updates.

4.3 Access Control
4.3.1 Access to information assets shall be granted on a need-to-know basis, using role-based access controls.
4.3.2 Strong and unique passwords shall be used for authentication. Passwords must be changed regularly and not shared with others.
4.3.3 User accounts of employees no longer associated with the organization shall be promptly deactivated.

4.4 Data Protection
4.4.1 Personal and sensitive data shall be collected, processed, and stored in accordance with relevant data protection laws and regulations.
4.4.2 Encryption shall be used for sensitive data transmission and storage.
4.4.3 Regular backups of critical data shall be performed and tested to ensure data availability and recoverability.

4.5 Security Awareness
4.5.1 Regular training and awareness programs shall be conducted for all employees to educate them about information security best practices.
4.5.2 Employees shall be informed about the potential risks of phishing, social engineering, and other security threats.

4.6 Incidence Response
4.6.1 A clear incident response plan shall be in place to address security breaches, data leaks, and other incidents promptly and effectively.
4.6.2 All employees must report any security incidents they come across to MIS personnel.

4.7 Physical security
4.7.1 Access to physical facilities shall be controlled and monitored.
4.7.2 Sensitive documents and storage media shall be securely stored and protected against unauthorized access.

4.8 Compliance
4.8.1 This policy shall adhere to relevant legal, regulatory, and industry-specific requirements.

4.9 Enforcement
4.9.1 Non-compliance with this policy may result in disciplinary action, up to and including termination of employment and/or legal action.

4. SEPARABILITY CLAUSE

If any provision or part of this policy is declared invalid, the remaining parts or provisions not affected must remain in full force and effect.

5. AMENDMENTS

This Policy may be amended or modified only by a written instrument, executed by the Committee and approved by the Board of Trustees.

6. DATE OF EFFECTIVITY

This policy must take effect on the date of the approval of the Board of Trustees.

Prepared by:	Reviewed and endorsed by:	Approved by:
MINERVA G. TEJADA President Date: 01/10/2025	**LEONARDO S. BANGA** MIS Committee Chairperson Date: 01/10/2025	**EVELIA BARDOS-TIZON** BOT Chairperson Date: 02/01/2025

Attachment 1: Information Asset Storage Security Guidelines

1. Data Classification
   Classify information assets based on their sensitivity and criticality. Assign appropriate labels such as:
   - Highly Restricted,
   - Confidential,
   - Internal Use, and
   - Public

2. Access Control
   - Need-to-Know Basis: Limit access to information assets to only those employees who require it for their roles. Apply role-based access controls.
   - Authentication and Authorization: Enforce strong authentication mechanisms, including strong passwords and two-factor authentication (2FA) where possible.

3. Encryption
   - Data in Transit: Utilize encryption (SSL/TLS) for data transmitted between systems, such as when accessing information through web applications.
   - Data at Rest: Employ encryption techniques for data stored in databases, files, and storage devices to prevent unauthorized access.

4. Physical Security
   - Access Control: Restrict physical access to data storage areas. Install locks, access cards, or biometric controls as needed.
   - Secure Facilities: Ensure that servers, storage devices, and backup tapes are stored in secure environments with controlled temperature and humidity.

5. Backups
   - Regular Backups: Perform regular backups of critical information assets. Store backup copies in secure, off-site locations.
   - Test Restoration: Periodically test the restoration process to ensure backups are functioning properly and data can be recovered in case of emergencies.

6. Disaster Recovery
   - Plan Development: Create a comprehensive disaster recovery plan outlining steps to take in case of data loss, hardware failures, or other emergencies.
   - Off-site Replication: Replicate critical data to off-site locations to ensure redundancy and data availability in the event of a disaster.

7. Patch Management
   - Regular Updates: Keep server operating systems, database management systems, and storage solutions updated with the latest security patches.

8. Monitoring and Auditing
   - Real-Time Monitoring: Implement intrusion detection systems and security information and event management (SIEM) solutions to monitor for any unauthorized access attempts.
   - Regular Audits: Conduct regular audits of access logs and permissions to identify and rectify any unauthorized access.

9. Employee Training
   - Security Awareness: Train employees on the importance of secure information storage, access control, and reporting suspicious activities.
   - Incident Reporting: Educate employees about the process of reporting security incidents to MIS.

10. Compliance
    - Legal and Regulatory Requirements: Ensure that the storage and protection of information assets adhere to relevant industry regulations and legal requirements.

Prepared by:	Reviewed and endorsed by:	Approved by:
MINERVA G. TEJADA President Date: 01/10/2025	**LEONARDO S. BANGA** MIS Committee Chairperson Date: 01/10/2025	**EVELIA BARDOS-TIZON** BOT Chairperson Date: 02/01/2025

Attachment 2: Information Asset Disposal Guidelines

Proper disposal of information assets is a critical aspect of maintaining information security and preventing unauthorized access to sensitive data.

1. Data Classification
   - Identify Sensitive Data: Classify information assets based on their sensitivity and categorize them as “Highly Restricted,” "Confidential," "Internal Use," or "Public."

2. Inventory and Review
   - Regular Assessment: Periodically review stored information assets to determine which ones are no longer needed or relevant.
   - Data Mapping: Maintain an inventory of all information assets, including their storage locations and classification levels.

3. Secure Deletion
   - Digital Data: Use approved data sanitization methods (e.g., shredding, wiping, degaussing) to ensure the complete and irreversible removal of data from digital storage devices like hard drives, solid-state drives, and USB drives.
   - Physical Records: For paper documents, shred them using a cross-cut shredder before disposal. Ensure all hardcopies are destroyed beyond reconstruction.

4. Secure Disposal Methods
   - Authorized Vendors: When outsourcing disposal, work only with reputable vendors who follow industry best practices for secure data destruction.
   - On-site Destruction: Whenever possible, consider on-site destruction of assets under proper supervision to ensure data security.

5. Digital Media Methods:
   - Mobile Devices: Factory reset or wipe mobile devices before disposal. Follow manufacturer guidelines to ensure data erasure.
   - Computers and Servers: Format or wipe storage media using recognized data erasure software before decommissioning systems.

6. Destructions and Documentation
   - Records: Maintain detailed records of the disposal process, including asset descriptions, disposal dates, methods used, and responsible individuals.
   - Verification: After disposal, verify that the data destruction process was successful and document the verification steps.

7. Compliance
   - Legal and Regulatory Requirements: Ensure that the disposal of information assets complies with relevant laws, regulations, and industry standards

8. Incident Reporting
   - Missteps: If any accidental or unauthorized disposal of sensitive information occurs, promptly report the incident to MIS personnel for appropriate action.

9. Audit and Review
   - Periodic Audits: Conduct regular audits to ensure compliance with these disposal guidelines and identify areas for improvement

10. Destruction of Hardware
    - Obsolete Hardware: Dispose of obsolete hardware, such as printers and fax machines, in a manner that ensures any data stored on them is irretrievable.

By adhering to these Information Asset Disposal Guidelines, we uphold the security and integrity of our organization's information, minimizing the risks associated with unauthorized access and data breaches

Attachment 3: Password Management

As employee of NATCCO MBAI, we are committed to ensure the security of our organization's information assets. To maintain a strong defense against unauthorized access and potential data breaches, please adhere to the following password management guidelines:

1. Creating Strong Passwords
   - Use Complexity: Create passwords that are at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters (e.g., !, @, #, $).
   - Avoid Personal Information: Do not use easily guessable information such as names, birthdates, or common words.
   - Randomness is Key: Generate random combinations of characters to increase password strength.

2. Password Usage
   - Unique Passwords: Use a unique password for each of your accounts, whether they are work-related or personal.
   - Avoid Sharing: Never share your passwords with anyone, including colleagues or family members
   - No Sticky Notes: Avoid writing down passwords on sticky notes or leaving them in easily accessible places.

3. Regular Updates
   - Change Regularly: Change your passwords regularly, at least every three months.
   - Avoid Reuse: Do not reuse old passwords. Create entirely new ones each time you update.

4. Two-Factor Authentication
   - Enable 2FA: Whenever possible, enable two-factor authentication for your accounts. This adds an extra layer of security by requiring a second verification step

5. Safe Storage
   - Use a Password Manager: Consider using a reputable password manager to securely store and manage your passwords.
   - Physical Security: If you must write down passwords, store them in a secure, locked place.

6. Avoid Phishing
   - Be Cautious: Do not click on suspicious links or provide your password via email or on unknown websites.
   - Verify Requests: If you receive an email or message requesting your password, verify its authenticity with the IT department.

7. Reporting Security Concerns
    - Incident Reporting: If you suspect any unauthorized access to your account or any security breaches, report it immediately to the IT department.

Remember, strong password management is a crucial aspect of maintaining the security of our organization's data. By following these guidelines, you play a vital role in ensuring the confidentiality and integrity of our information assets.

Prepared by:	Reviewed and endorsed by:	Approved by:
MINERVA G. TEJADA President Date: 01/10/2025	**LEONARDO S. BANGA** MIS Committee Chairperson Date: 01/10/2025	**EVELIA BARDOS-TIZON** BOT Chairperson Date: 02/01/2025