Asset Management Policy, version 1.0.0

Status: ☐ Working Draft ☒ Approved ☒ Adopted
Document Owner: Information Technology Committee
Last Review Date: May 2024

Asset Management Policy

Purpose

The purpose of the NICC Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by NICC.

Audience

The NICC Asset Management Policy applies to individuals who are responsible for the use, purchase, implementation, and/or maintenance of NICC Information Resources

Contents

Policy

Hardware, Software, Applications, and Data

- All hardware, software and applications must be approved and purchased by NICC IT.
- Installation of new hardware or software, or modifications made to existing hardware or software must follow approved NICC procedures and change control processes.
- All purchases must follow the defined NICC Technology Purchasing Standard.
- Software used by NICC employees, contractors, and/or other approved third parties working on behalf of NICC, must be properly licensed.
- Software installed on NICC computing equipment, outside of that noted in the NICC Standard Software List, must be approved by IT Management and installed by NICC IT personnel.
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**.
- The use of **cloud computing applications** must be done in compliance with all laws and regulations concerning the information involved, e.g. **personally identifiable information (PII)**, **protected health information (PHI)**, corporate financial data, etc.
- **Two-factor authentication** is required for external **cloud computing applications** with access to any **confidential information** for which NICC has a custodial responsibility.
- Contracts with **cloud computing applications** providers must address data retention, destruction, data ownership and data custodian rights.
- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- A general inventory of information (data) must be mapped and maintained on an ongoing basis.
- All NICC assets must be formally classified with ownership assigned.
- Maintenance and repair of organizational assets must be performed and logged in a timely manner and managed by NICC IT Management.

- NICC assets exceeding a set value, as determined by management, are not permitted to be removed from NICC's physical premises without management approval.
- All NICC physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by NICC.
- If a NICC asset is being taken to a High-Risk location, as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by IT before being taken offsite and before reconnecting to the NICC network.
- Confidential information must be transported either by an NICC employee or a courier approved by IT Management.
- Upon termination of employment, contract, or agreement, all NICC assets must be returned to NICC IT Management.

System Procurement

- Procurement of new hardware and software must be authorized by Information Technology and requested through the company procurement process.
- Information Technology must perform a review of all new hardware or software prior to final purchase commitment to ensure that necessary security controls can be configured.
- All newly procured hardware and software must be fully tested and accepted prior to deployment to the production environment.
- Deployment of new hardware and software to the production environment must be in accordance with the Change Control Policy.

System Acceptance

- Acceptance criteria must be provided by the **application\resource owner** and should specify:
- operational and functional requirements of the application,
- performance and capacity requirements,
- data classification,
- hardware specifications, if applicable.
- All acceptance criteria must be satisfied before any system or application can move into a production environment.

Mobile Devices

- The use of a **personally owned mobile devices to** connect to the NICC network is a privilege granted to employees only upon formal approval of IT Management.
- **Mobile devices** used to connect to the NICC network are required to use the approved **Mobile Device Management (MDM)** solution.
- **Mobile devices** that access NICC email must have a PIN or other authentication mechanism enabled.
- **Confidential data** should only be stored on devices that are encrypted in compliance with the NICC Encryption Standard.
- All **mobile devices** should maintain up-to-date versions of all software and applications.

Media Destruction & Re-Use

- Media that may contain **confidential** or **internal information** must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.

- Media reuse and destruction practices must be conducted in compliance with NICC's Media Reuse and Destruction Standards.
- All decommissioned media must be stored in a secure area prior to destruction.
- Media reuse and destruction practices must be tracked and documented.
- All information must be destroyed when no longer needed, included encrypted media.

Backup

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
- The NICC backup and recovery process for each system must be documented and periodically reviewed according to the defined review schedule.
- The vendor(s) providing offsite backup storage for NICC must be formally approved to handle the highest classification level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest NICC sensitivity level of information stored.
- A process must be implemented to verify the success of the NICC electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable in accordance with the backup standard.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Procedures between NICC and the offsite backup storage vendor(s) must be reviewed at least annually.
- Backups containing **confidential information** must be encrypted in accordance with the Encryption Standard
- **Signature cards** held by the offsite backup storage vendor(s) for access to NICC backup media must be reviewed annually or when an authorized individual leaves NICC.
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
    - System name
    - Creation Date
    - NICC Contact Information

Removable Media

- The use of **removable media** for storage of NICC Information must be supported by a reasonable business case.
- All **removable media** use must be approved by NICC IT prior to use.
- **Personally owned removable media** use is not permitted for storage of NICC information.
- Users are not permitted to connect **removable media** from an unknown origin, without prior approval from NICC IT.
- **Confidential and internal** NICC **information** should not be stored on **removable media** without the use of encryption.
- The loss or theft of a **removable media** device that may have contained any NICC information must be reported to the NICC IT.
- NICC will maintain inventory logs of all media and conduct media inventories at least annually.
- The transfer of information to removable media will be monitored.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 6, 8, 11, 12, 16, 18
- NIST CSF: ID.AM, PR.IP, PR.DS, PR.PT, DE.CM
- Change Control Policy
- Encryption Policy
- Encryption Standard
- Information Classification and Management Policy
- Media Reuse and Destruction Standard
- Technology Purchasing Standard

Waivers

Waivers from certain policy provisions may be sought following the NICC Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	August 2023		FRSecure	Document Origination
		2-27-2024	IT committee	Reviewed and Approved
		3-8-2024	Academic Council	Reviewed and Approved
		3-20-2024	Administrative Council	Reviewed and Approved
		4-3-2024	Executive Council	Reviewed and Approved
		5-17-2024	Board of Directors	Reviewed and Approved