सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

NCVET
कौशल गुणवत्ता प्रगति

Guidelines for Information and Data Security

NATIONAL COUNCIL FOR VOCATIONAL EDUCATION AND TRAINING (NCVET)

Skill India
कौशल भारत - कुशल भारत
Phone : +91-11-25788001-12

सत्यमेव जयते

राष्ट्रीय व्यावसायिक शिक्षा और प्रशिक्षण परिषद
कौशल विकास और उद्यमशीलता मंत्रालय
भारत सरकार
कौशल भवन, बी-2, पूसा रोड, नई दिल्ली-110005
NATIONAL COUNCIL FOR VOCATIONAL EDUCATION AND TRAINING
Ministry of Skill Development and Entrepreneurship
Government of India
Kaushal Bhawan, B-2, Pusa Road, New Delhi - 110005

F. No.: 22001/02/2024/NCVET

Date: 27/05/2024

Subject: Guidelines for Information and Data Security

1. In today's digital age, where information is constantly flowing and data is the lifeblood of organizations, safeguarding sensitive information is paramount. Information and data security encompass a broad range of principles, practices, and technologies designed to protect data from unauthorized access, disclosure, alteration, and destruction. Whether it's financial records, customer information, intellectual property, or proprietary business data, every piece of information holds value and requires safeguarding.

2. Information and DATA Security is critically important for the NCVET due to its role in overseeing the development, qualitative improvement, and regulation of Vocational Education, Training and Skilling (VETS). It is vital to safeguard the integrity and confidentiality of the vast amount of sensitive data that NCVET handles.

3. Hence, NCVET has developed guidelines on Information & Data Security. This Guideline shall address the safety of personal information of employees, and individuals undergoing vocational training, assessment results, accreditation details, and various other confidential records. Furthermore, given the increasing digitization of educational and training processes, ensuring robust "Information & DATA Security" measures are essential to protect against data breaches, unauthorized access, and cyber threats that could compromise the trust and effectiveness of activities overseen by the NCVET.

4. This Guideline defines the mandatory minimum information security requirements for NCVET. Any entity (such as Awarding Bodies and Assessment Agencies) which may get associated with NCVET may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this guideline, but must, at a minimum, achieve the security levels defined by this Guidelines.

5. The Guidelines were presented in 10th Council meeting of the NCVET held on 21st February 2024 and are being notified herewith. These guidelines may be further amended/ updated from time to time with approval of the NCVET based on the feedback and requirements received during the implementation of these guidelines.

27/05/2024

(Dr. Suhas Deshmukh)
Director
NCVET

PREFACE

In the ever-evolving digital landscape, the paramount importance of safeguarding Information and Data Security is of the utmost priority. As we navigate through an era where data flows incessantly and forms the core operational foundation of organizations worldwide, it becomes imperative to shield such sensitive information from the myriad of vulnerabilities that the digital age presents.

The National Council for Vocational Education and Training (NCVET) plays a crucial role in regulating the Vocational Education, Training and Skilling (VETS) ecosystem and various skill initiatives across the nation. The data managed by NCVET is of paramount importance and sensitivity, encompassing personal information of employees, details of individuals undergoing vocational training, assessment outcomes, and recognition/accreditation records, among other critical data. Consequently, NCVET carries a significant responsibility in maintaining the accuracy, integrity, and security of this information.

With an acute awareness of these responsibilities, NCVET has embarked on formulating robust Guidelines for Information and Data Security. These guidelines are rigorously crafted to ensure compliance with ISO 27001 standards and the adoption of ISO 27002 processes, align with the NICNET security policy, and adhere to the stipulations of the National Cyber Security Policy, 2013, and the Digital Personal Data Protection Act 2023 (DPDPA). By proactively addressing information and data security, NCVET demonstrates its unwavering dedication to safeguarding the sensitive information entrusted to it. This strategic approach ensures that VETS initiatives can thrive in a secure and trustworthy environment, empowering individuals and organizations to achieve their full potential.

The development of these guidelines has been a meticulous process. NCVET has collaborated closely with the team from the National Informatics Centre (NIC) to tailor the requirements specific to the organizational needs while ensuring compliance with broader legal and federal norms. Inspired by the framework provided by Karmayogi Bharat and through continuous iterative consultations with various stakeholders, a draft was conceived and subsequently unveiled for public scrutiny. This consultative journey was vital in enriching the guidelines with diverse perspectives and insights, thereby enhancing their relevance and applicability.

I extend my sincerest gratitude to all the stakeholders who actively participated in the consultations, contributing significantly to the development of this comprehensive policy document. This strategic guideline will empower the Vocational Education, Training and Skilling (VETS) community to fortify their information security posture, safeguarding the sensitive data entrusted to them. By adhering to these robust standards, organizations shall cultivate a trusted environment that enables individuals and enterprises to reach new heights of success.

I request all the stakeholders, including Government Agencies, Awarding Bodies, Assessment Agencies, and the broader VETS community, to refer to and implement the "Guideline for Information and Data Security". This way, we can secure the data of the stakeholders, future of the skilling ecosystem and empower the nation's workforce to thrive in this digital age.

I also acknowledge the work done at NCVET under the able guidance of Executive Members, Dr. Neena Pahuja and Dr. Vinita Aggarwal with the NCVET team comprising of Dr. Suhas Deshmukh, Director, Shri Pradeep Thota Deputy Director, Shri Amresh Kumar, Consultant and Ms. Ratna Priya Kanchan, Young Professional. NCVET also received valuable inputs from MSDE, National Informatics Centre (NIC), Karmayogi Bharat and other reputed organizations in the development of these guidelines which are very well appreciated. NCVET welcomes further suggestions for improvement on this guideline which is dynamic in nature and shall be updated periodically.

My best wishes for the Implementation of the "Guideline for Information and Data Security".

Dr. N.S. Kalsi, IAS Retd.
Chairperson
NCVET

Contents

1. Introduction

The National Council for Vocational Education and Training (NCVET) has been notified by the Government vide notification no. No. SD-17/113/2017-E&PW dated 5th December 2018, subsuming the erstwhile National Skill Development Agency (NSDA) and the National Council of Vocational Training (NCVT). The establishment of NCVET has also consolidated the fragmented regulatory framework in the Vocational Education and Training (VET) and skill ecosystem.

The National Council for Vocational Education and Training has been entrusted with the development, qualitative improvement and regulation of vocational education and training, for granting recognition to and monitoring the functioning of awarding bodies, assessment agencies, skill information providers, and training bodies, and to perform other incidental functions as specified in the notification.

Information & Data Security is critically important for the NCVET due to its role in overseeing the development, qualitative improvement, and regulation of Vocational Education, Training and Skill development (VET & SD). It is vital to safeguard the integrity and confidentiality of the vast amount of sensitive Data that NCVET handles. This includes personal information of employees, and individuals undergoing vocational training, assessment results, accreditation details, and various other confidential records. Furthermore, given the increasing digitization of educational and training processes, ensuring robust "Information & Data Security" measures are essential to protect against Data breaches, unauthorized access, and cyber threats that could compromise the trust and effectiveness of activities overseen by the NCVET. Hence, a strong "Information & Data Security framework" is imperative for NCVET to maintain the trust of stakeholders, protect sensitive Data, and ensure the smooth and secure functioning of the VET/S.

2. Purpose of the Policy

This policy defines the mandatory minimum information security best practices for NCVET *as defined below in in the* Scope *section*. It is essential for any entity associated with NCVET to adhere to the security levels required by the policy. While they have the flexibility to surpass these requirements based on their individual business needs and legal obligations, meeting the minimum-security levels outlined in the document is mandatory.

This policy acts as an umbrella document to all other security policies and associated standards. This policy caters processes to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions and vital government functions; compromise Data; and result in legal and regulatory non-compliance.

This policy helps in creating a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of Data. This also ensures that staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

3. Scope

This policy applies to all locations of NCVET, employees of the parent company, and correspondingly contractors/ vendors working for NCVET. It also applies to information received from users/learners, external service providers and/or guests, to whom non-disclosed information is communicated or made available by NCVET.

This policy encompasses all systems, automated and manual, for which NCVET has administrative responsibility, including systems managed or hosted by third parties on behalf of NCVET. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

The following core domains have been covered as a part of this document. These are as listed below:

1. Networking and Infrastructure Security
2. Identity, access and privilege management
3. Physical Security
4. Data Security and Handling
5. Threat and vulnerability management
6. Personnel Security
7. Security and incident management
8. IT Asset Management
9. Mobility and Bring Your Own Device (BYOD)
10. Virtualization
11. Social Media
12. Security Testing
13. Security Auditing
14. Operations Security

4. Information Classification Guidelines

All information available with NCVET should be classified into one of the following categories (based on existing classification of Manual on paper records issued by Ministry of Home Affairs, 1994)

1. **Top Secret**: Information, unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for nation's closest secrets and is to be used with great reserve.

2. **Secret**: Information, unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

3. **Confidential**: Information, unauthorized disclosure of which could be expected to cause damage to the security of the organization or could be prejudicial to the interest of the organization, or could affect the organization in its functioning. Most information, on proper analysis, will be classified no higher than confidential.

4. **Restricted**: Information, which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose

5. **Unclassified**: Information that requires no protection against disclosure. e.g. Public releases

Information handling: NCVET shall share information with employees and related parties only on need to know basis and shall only share information through proper communication channels as defined in this policy document

5. Organisational Security

a) The **Risk Compliance and Data Security Committee of NCVET** is responsible for overseeing both information risk management and information technology security at NCVET. This includes looking at risk for information assets and individual information systems as part of the organization's overall strategic goals, and managing security risks in line with the organization's risk tolerance and other types of risks to ensure business success.
b) The Chief Information Security Officer (CISO) of NCVET will be responsible for evaluating and advising on information security risks.
c) Information security risk decisions shall be made through consultation with both function areas described in above points
d) Although the technical information security function may be outsourced or contracted, NCVET retains overall responsibility for the security of the information that it owns.
e) Standard procedure (SOP) for - Shifting of PC/Hardware within and outside office premise.
   i. Obsolete Software to be upgraded.
   ii. PC Hardware reached end of life (EOL) to be declared obsoleted.
   iii. PC/Desktops to be shut down on daily basis.
   iv. Standard procedure for onboarding and offboarding of NCVET team of consultants, so mechanism for proper onboarding and proper offboarding can avoid gaps in cybersecurity defences as, departing employees may still have access to sensitive data and systems.

6. Functional Responsibilities

6.1. Risk Compliance and Data Security Committee

The Committee shall be chaired by an Executive Member/ Director/ nominated officer of NCVET who is an expert in Data, risk, compliance and technology. A National Informatics Centre (NIC)'s officer conversant with this area may be a member of this Committee. The Chief Information Security Officer (CISO) shall be part of this committee. The committee shall be responsible for:

i. evaluating and accepting risk on behalf of the NCVET;
ii. identifying information security responsibilities and goals and integrating them into relevant processes;
iii. supporting the consistent implementation of information security policies and standards;
iv. supporting security through clear direction and demonstrated commitment of appropriate resources;
v. promoting awareness of information security best practices through the regular dissemination of materials provided by the CISO;
vi. implementing the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;
vii. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;
viii. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the Data;
ix. participating in the response to security incidents;
x. complying with notification requirements in the event of a breach of private information;
xi. adhering to specific legal and regulatory requirements related to information security;
xii. communicating legal and regulatory requirements to the CISO; and communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements
xiii. Review of regular Security Patch updates, based on Vulnerability assessment/new vulnerabilities detected.

6.2. Chief Information Security Officer

The appointed Chief Information Security Officer (CISO) shall be responsible for:

i. Understanding and maintaining familiarity with business functions and requirements.
ii. Ensuring an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security.
iii. Assessing compliance with information security policies and legal and regulatory information security requirements.
iv. Evaluating and understanding information security risks and appropriately managing those risks.
v. Representing and assuring that security architecture considerations are addressed.
vi. Advising on security issues related to procurement of products and services.
vii. Escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures.
viii. Disseminating threat information to appropriate parties.

ix. Participating in the response to potential security incidents.
x. Participating in the development of enterprise policies and standards that consider the organization's needs.
xi. Promoting information security awareness.
xii. Providing in-house expertise as security consultants as needed.
xiii. Developing the security program and strategy, including measures of effectiveness.
xiv. Establishing and maintaining enterprise information security policy and standards.
xv. Assessing compliance with security policies and standards.
xvi. Advising on secure system engineering.
xvii. Providing incident response coordination and expertise.
xviii. Monitoring networks for anomalies and external sources for indications of Data breaches, defacements, etc.
xix. Maintaining ongoing contact with security groups/associations and relevant authorities.
xx. Providing timely notification of current threats and vulnerabilities.
xxi. Providing awareness materials and training resources.
xxii. Ensuring regular security audits.
xxiii. Ensuring ISO 27001 compliance and adoption of ISO 27002 processes.
xxiv. Implementing Data encryption, as required, for information stored for different stakeholders of NCVET as per the Data Privacy Policy of the Government of India.
xxv. Providing clear direction and consideration of security controls in the Data processing infrastructure and computing networks that support the information owners.
xxvi. Supplying resources needed to maintain a level of information security control consistent with the organizational policy.
xxvii. Identifying and implementing all processes, policies, and controls relative to security requirements defined by the business.
xxviii. Implementing proper controls for information owned based on the classification designations.
xxix. Providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration).
xxx. Fostering the participation of information security and technical staff in protecting information assets and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures.
xxxi. Implementing business continuity and disaster recovery plans from damaged systems.
xxxii. Providing dashboards on system access, including unknown/suspicious access/information/threats.

6.3. Workforce, Consultants and Third Parties

The workforce, consultants, sub-consultants and third parties who are providing their services to NCVET shall be responsible for:

i. Understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
ii. Protecting information and resources from unauthorized use or disclosure;
iii. Protecting personal, private, sensitive information from unauthorized use or disclosure;
iv. Abiding by Acceptable Use of **Information Technology Resources Policy**

v. Reporting suspected information security incidents or weaknesses to the appropriate manager and CISO /designated security representative.

7. Separation of Duties

a) To reduce the risk of accidental or deliberate system misuse, NCVET shall clearly demark separation of duties and areas of responsibility where appropriate.
b) Whenever separation of duties is not technically feasible, other compensatory controls shall be implemented, such as monitoring of activities, audit trails and management supervision.
c) The audit and approval of security controls shall always remain independent and segregated from the implementation of security controls.

8. Policy Applicability on Core Domains

8.1. Networking and Infrastructure Security

This shall include but are not limited to servers, platforms, networks, communications databases and software applications *(In reference with "National Informatics Centre (NIC) through its Information and Communication Technology (ICT) Network – NICNET" security policy)*

i. The CISO of the NCVET or a designated individual/group appointed by him/ her shall assume the responsibility for maintenance and administration of any system deployed on behalf of NCVET. A list of assigned individuals or groups shall be centrally maintained.
ii. Security shall be considered at system inception and documented as part of the decision to create or modify a system.
iii. Each system shall have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
iv. All system clocks shall synchronize to a centralized reference time source set to NTC (Universal Time) which is itself synchronized to at least three synchronized time sources.

8.2. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):

(In reference with NICNET security policy)

a) Access to sensitive information or Data related to NCVET or its related parties shall be only done through secured connections such as VPN
b) All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
c) Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.
d) Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:

- All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
- sensitive data is masked or overwritten with fictional information.

e) Where technically feasible, development software and tools must not be maintained on production systems.
f) Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
g) Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
h) Privileged access to production systems by development staff must be restricted.
i) Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.
j) Separation of environments (e.g., development, test, quality assurance, production) shall be provisioned, either logically or physically, including separate environmental identifications.
k) Validation environments and test plans should be devised to ensure the system functions correctly before deployment in production.
l) Formal change control procedures for all systems, including any change potentially impacting the production environment or data, should be developed, implemented, and enforced for any NCVET commissioned system

8.3.Network Systems

(In reference with NICNET security policy)

a) Connections between systems must be authorized by the CISO of the NCVET of all relevant entities and protected by the implementation of appropriate controls.
b) All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the CISO/designated security representative annually, at a minimum, to assure:
    - the business case for the connection is still valid and the connection is still required; and
    - the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
c) A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
    - Internet accessible systems and internal systems;
    - systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and
    - user and server segments.
d) Network management must be performed from a secure, dedicated network.
e) Authentication is required for all users connecting to internal systems.
f) Network authentication is required for all devices connecting to internal networks.
g) Only authorized individuals or business units may capture or monitor network traffic.

h) A risk assessment must be performed in consultation with the CISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.
i) Provide network/ resource usage dashboard including usage from unknown IPs/Locations supporting risk analysis.

8.4.Identity, access and privilege management

a. Offline IT Infrastructure:

i. Based on security features of the devices such as Access Control, Audit & Accountability, Identification & Authentication, the following list of devices are allowed for operations in NICNET of MSDE Laptops:
    1. Mobiles
    2. Tablet
    3. Network Printer
    4. VC system
    5. Smart TV
    6. External Storage Device ex. Pen drive; only identified External storage devices will be allowed.
    7. Mandatory UEM/EDR Agent configuration recommended by NIC for each PC/endpoint.
    8. Restricted access for entry into network Server room.

ii. In case of Desktops, Administrative and User Access Separation is mandatory. If the Users are provided with Administrator rights, they can install any software available on internet and hence expose the system and network to threats. A normal user has to be created on each desktop for daily operations of the officials. MAC binding is mandatory for desktops and Smart TVs.

iii. Unauthorized access, physical damage, and tampering to IT systems should be prevented by implementing physical security. Important / sensitive zones should be monitored through CCTV cameras and footage should be stored for at least 180 days.

iv. The organisation must ensure that default credentials of network devices and information systems such as usernames, passwords, and tokens are changed prior to their deployment or first use. All devices at User level should use USER account and use of Administrator account should be restricted to Network/System Administrators only.

b. Online IT Infrastructure:

i. Only Government email id. Shall be used for official work

ii. All accounts being created on Government system and managed by the core IT team of NCVET/ third party vendor led by the CISO.
iii. Except as described in the, Account Management/Access Control Standard, access to systems shall be provided through the use of individually assigned unique identifiers, known as user-IDs.
iv. With each user-ID an authentication token (e.g., password, key fob, biometric) must be used to authenticate the identity of the person or system requesting access. The password must meet the below criteria:
    a) Should be at least 8 characters' long
    b) Should at least have an upper case and a lower-case letter
    c) Should at least have a special character
    d) Should be alpha numeric
v. Password should be changed every 6 months and should be linked to mobile number. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. While accessing Data related to company, users should ensure that information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock. In case of inactivity or when these devices are attended users should ensure that these devices are properly locked.
vi. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.
vii. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).
viii. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with NCVET missions and business functions (i.e., least privilege).
ix. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).
x. Advance approval for any remote access connection must be provided by NCVET. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.
xi. All remote connections must be made through managed points-of-entry reviewed by the CISO /designated security representative.
xii. Working from a remote location must be authorized by management and practices which assure the appropriate protection of Data in remote environments must be shared with the individual prior to the individual being granted remote access.

8.5. Secure Cloud Services *(In reference with NICNET security policy)*

i. Thoroughly examine the shared responsibility model for security and compliance in cloud services.

ii. Implement appropriate security policies and measures for testing, staging, and backup environments hosted on cloud services.
iii. Verify the public accessibility of all cloud instances in use.
iv. Ensure that no server/storage is inadvertently leaking data due to inappropriate configurations.
v. Implement the least privilege principle for access control with granular permission to cloud resources.
vi. Enable cloud native security controls and logging for critical cloud resources.
vii. Ensure continuous monitoring of these resources for enhanced security.
viii. Ensure User Accounts have Multi-Factor Authentication (MFA) along with a strong password policy.
ix. Implement a procedure/standard for disabling accounts when an administrator/user leaves an organization.

8.6. Physical and Environment Security

i. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.
ii. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks.
iii. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.
iv. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.
v. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

8.7. Data Security and Handling

i. Any system or process that supports business Data must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.
ii. Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
iii. Risk assessment results, and the decisions made based on these results, must be documented.
iv. All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.
v. All information assets must have an information owner established within the lines of business. They should also be trained on Data privacy guidelines.
vi. Information must be meticulously managed from creation through authorized use to disposal, consistently classified according to its confidentiality, integrity, and availability, with each asset classified at the highest level required by its individual data elements.

vii. If NCVET is unable to determine the confidentiality classification of information or the information is personal identifying information (PII) the information must have a confidentiality classification and, therefore, is subject to confidentiality controls.

viii. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged Data is warranted.

ix. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.

x. Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.

xi. NCVET must communicate the requirements for secure handling of information to its workforce.

xii. A written or electronic inventory of all information assets must be maintained.

xiii. Content made available to the general public must be reviewed according to a process that will be defined and approved by NCVET. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.

xiv. Personal Identifiable Information (PII) must not be made available without appropriate safeguards approved by NCVET.

xv. For non-public information to be released outside NCVET or shared between other entities, a process must be established that, at a minimum:

a. evaluates and documents the sensitivity of the information to be released or shared;
b. identifies the responsibilities of each party for protecting the information;
c. defines the minimum controls required to transmit and use the information;
d. records the measures that each party has in place to protect the information;
e. defines a method for compliance measurement;
f. provides a signoff procedure for each party to accept responsibilities; and
g. establishes a schedule and procedure for reviewing the controls.

8.8. Threat and Vulnerability Management

i. All systems shall be scanned for vulnerabilities before being installed in production and periodically thereafter.

ii. All systems are subject to periodic penetration testing.

iii. Penetration tests are required periodically for all critical environments/systems.

iv. Where NCVET has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing shall be coordinated and documented.

v. Scanning/testing and mitigation must be included in third party agreements.

vi. The output of the scans/penetration tests will be reviewed in a timely manner by the CISO. Copies of the scan report/penetration test must be shared with the CISO /designated security representative for evaluation of risk.

vii. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

viii. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the CISO /designated security representative. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

ix. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption and should be recognised/empanelled with CERT-IN of Government of India.

x. Accessibility test to be done for all software by bodies authorized by STQC - Standardisation Testing and Quality Certification (STQC), Ministry of Electronics and Information Technology (MeitY).

8.9. Personnel Security

i. The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to NCVET sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by NCVET.

ii. NCVET must require its workforce to abide by the Acceptable Use of Information Technology Resources Policy, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

iii. All job positions must be evaluated by CISO determine whether they require access to sensitive information and/or sensitive information technology assets.

iv. For those job positions requiring access to sensitive information and sensitive information technology assets, NCVET shall conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for NCVET to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to NCVET.

v. A process shall be established within NCVET to repeat or review suitability determinations periodically and upon change of job duties or position.

vi. NCVET shall be responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

8.10. Security and Incident Management

i. NCVET shall create an incident response plan, consistent standards, to effectively respond to security incidents.

ii. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the CISO /designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the Chairperson, NCVET directly to report the threat.

iii. The Security Operations Center/ CERT-In must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

8.11. IT Asset Management

i. All IT hardware and software assets must be assigned to a designated organisational unit or individual.
ii. NCVET shall maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory may be automated where technically feasible.
iii. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

8.12. Mobility and Bring Your Own Device (BYOD)

i. Individuals may access data and systems of NCVET as their access rights and privileges provided to them end point computing devices owned/managed by them or their respective organisations
ii. These devices shall comply with the standards of various software and tools as described in the NICNET's SOP.
iii. Users should configure devices with secure passwords as per NCVET password policy or biometric.
iv. NCVET shall audit Mobile and user owned devices from time to time to ensure compliance to the policy.
v. Access of NICNET for Guest:

Guests will be provided NICNET access through WiFi SWAGAT. SWAGAT team sends daily OTP with Kaushal Bhawan coordinator which will be shared with the IT support team. IYT support team in turn can share the OTP with the guests and get them registered. *(Refer: SOP for Network Security, MSDE)*

8.13. Security Measures for Official Social Media Accounts

i. Access to official social media platform accounts will be limited to only designated officials and systems.
ii. Each official social media platform account will be operated using a dedicated and separate email account.
iii. The official email account and social media platform account will have different sets of credentials.
iv. All social media platform account credentials must follow the organization's password policy.
v. Personal email accounts must not be used for operating official social media accounts.
vi. Multi-Factor Authentication (MFA) must be enabled for all social media accounts wherever possible.
vii. All content to be posted on social media handles requires approval by an appropriate authority within the organization.
viii. Official social media platform accounts will be operated only by designated officials and on trusted devices.

ix. Users must log out from the official social media platform account immediately after usage.
x. Official social media platform accounts must not be used on public or unauthorized devices.
xi. Geolocation (GPS) access feature will be disabled for official social media platforms.
xii. Social media platform software/application must be updated to the latest version and devices operating official social media accounts will be updated with the latest available security patches.
xiii. Always stay informed about the latest updates by social media companies about security and privacy settings, and implement them appropriately.
xiv. Role-based accounts will be enabled with appropriate privileges for social media management platform and official social accounts.
xv. Access to official social media accounts will be revoked when an employee's role changes or when an employee leaves the organization.
xvi. Account security logs will be enabled and periodically monitored to identify login attempts from untrusted devices or regions other than usual.
xvii. Alerts for unrecognized login attempts must be enabled under login and security settings of the social media platform.
xviii. Caution should be exercised when using third-party applications for managing social media platform accounts.
xix. The email account associated with the official social media accounts must be regularly monitored for any account activity alerts.

8.14. Security Testing/ Audit

i. NCVET shall conduct security testing to evaluate all systems, applications, networks, policies, procedures and technology platforms such as cloud computing, mobility platforms, virtual environments etc. to identify vulnerabilities as per CERT-IN guidelines
ii. NCVET shall perform security evaluation by constructing scenarios combining internal and external threat agents

iii. NCVET shall determine and define the security audit requirements on its deployed/owned systems including systems managed by third parties basis the parameters listed below
    a. Nature of operations, risk appetite of organization, criticality of processes and operational transactions
    b. Exposure of organizations information to security threats
    c. Enterprise security policy, strategy and standards
    d. Legal and compliance requirements
    e. Historical information: previous audit reports, security incidents
iv. NCVET shall conduct periodic audits of all information systems, infrastructure facilities, third parties etc. which handle classified Data at any instance in its lifecycle

ii. The security audit shall be carried out by an independent third party with a dedicated team with needful skillset to carry out the security audit
iii. NCVET shall ensure that all audit observations, issues and recommendations by the audit team are reported to designated personnel and are resolved and rectified in a necessary time bound manner.

8.15. Operations Security

i. All systems and the physical facilities in which they are stored must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.
ii. System configurations must follow approved configuration standards.
iii. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.
iv. Where NCVET provides a server, application or network service to another entity, operational and management responsibilities must be coordinated by all impacted entities.
v. Host based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed
vi. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.
vii. Controls must be implemented to disable automatic execution of content from removable media.
viii. Controls must be implemented to limit storage of information to authorized locations.
ix. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.
x. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.
xi. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.
xii. Systems which can no longer be supported or patched to current versions must be removed.
xiii. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and record events to provide evidence and to reconstruct lost or damaged Data.
xiv. Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with record retention schedules and requirements.
xv. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic on the business criteria applied.
xvi. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
xvii. Backup copies of NCVET information, software, and system images must be taken regularly in accordance with NCVET ’s defined requirements.
xviii. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.
xix. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

8.16. Contingency Plan

Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly.

a. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

b. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

9. Compliance Statement

This guideline shall take effect upon notification. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Technology Information Security Officer (CISO) exception process.

Any other advisory from NIC/CERT-In, even though not part of this document, needs to be immediately acted on and adhered to.

10.Definitions of Key Terms

Term	Definition
CISO	Chief Information Security Officer
CEO	Chief Executive Officer
PPI	Prepaid Payment Instruments
CERT-In	Indian Computer Emergency Response Team
OS	Operating System
PII	Personally Identifiable Information
ISO	International Organisation for Standardization
VPN	Virtual Private Network

.

11.References

1. National Information Security Policy and Guidelines, Ministry of Home Affairs, Government of India Version 5.0
2. ISO/IEC 27001:2022 (ISO 27001) Standards
    i. Enhanced Risk Management Framework
    ii. Information Security Policies and Documentation
    iii. Technology and Threat Landscape Adaptation
    iv. Secure System Development Lifecycle (SSDLC) Standard
    v. Information Classification Standard; Sanitization/Secure Disposal Standard
    vi. Secure Configuration Standard
    vii. Account Management/Access Control Standard
    viii. Cyber Incident Response Standard
    ix. Authentication Tokens Standard
    x. Remote Access Standard; Security Logging Standard
    xi. Security Logging Standard
    xii. Secure Coding Standard
    xiii. Secure Configuration Management Standard
3. National Institute of Standards and Technology (NIST) - National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.