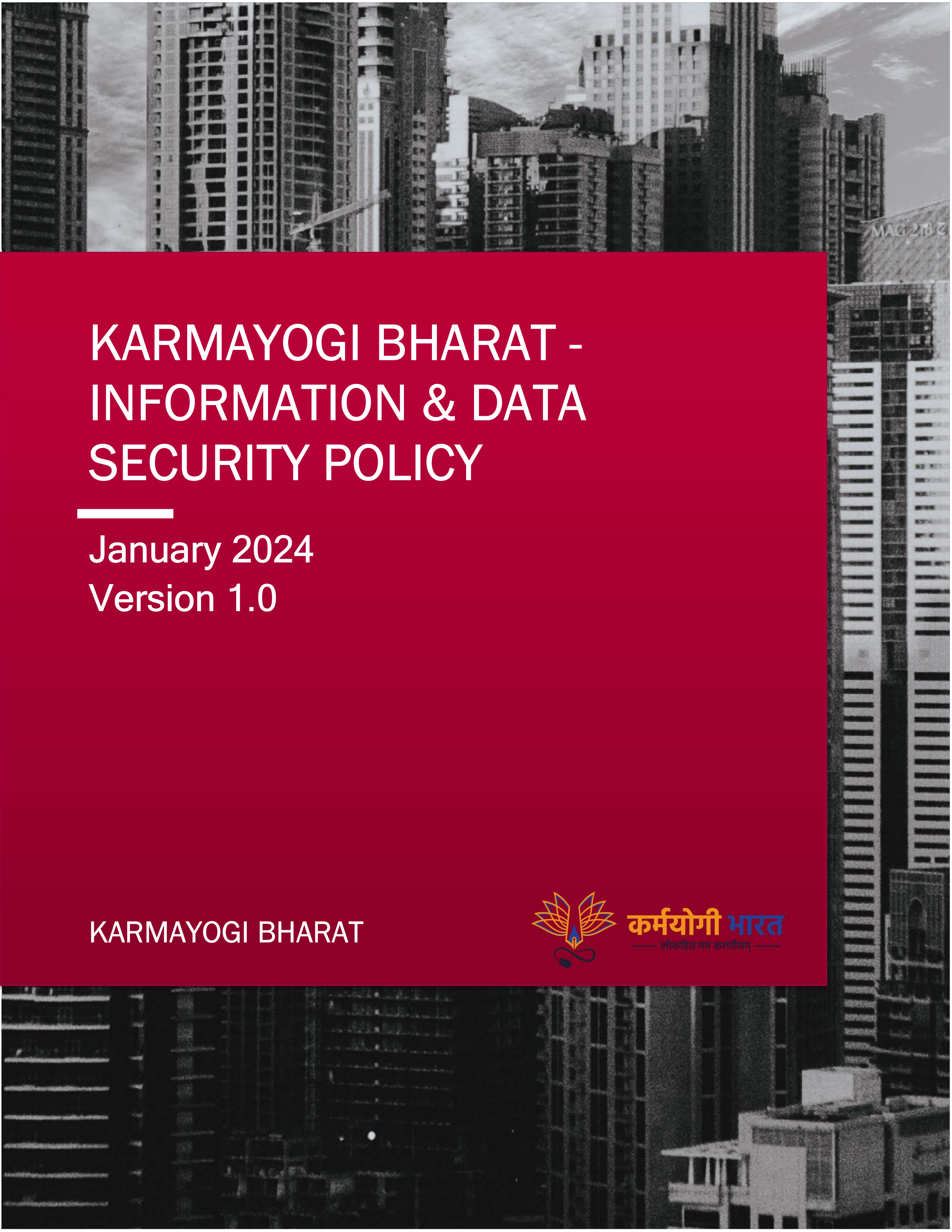

KARMAYOGI BHARAT - INFORMATION & DATA SECURITY POLICY

January 2024
Version 1.0

KARMAYOGI BHARAT

कर्मयोगी भारत
लोकहित मम करणीयम्

Contents

1. Purpose of the Policy

This policy defines the mandatory minimum information security requirements for Karmayogi Bharat *as defined below in in the* Scope *section*. Any entity which may get associated with Karmayogi Bharat may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy. The policy aims to maintain compliance with Digital Personal Data Protection Act, 2023 and adherence to the security guidelines of Ministry of Electronics and Information Technology, Government of India.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility 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 benefits Karmayogi Bharat by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure 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.

2. Authority

Karmayogi Bharat is a Special Purpose Vehicle (SPV) set up under the Mission Karmayogi. Karmayogi Bharat is a company registered Section 8 of the Companies Act, 2013 and is fully owned by Department of Personnel and Training, Government of India. Karmayogi Bharat forms a key pillar of the National Capacity Building Program for Civil Servants (Mission Karmayogi) and has been entrusted with the responsibility to enable manage and operate a digital online platform for capacity development of civil servants called the iGOT Karmayogi platform. Karmayogi Bharat shall be the final authority to maintain, update and implement this policy and shall be applicable to Karmayogi Bharat including its subsidiaries.

3. Revisions

Revisions to this document will be made annually, or whenever deemed necessary.

4. Scope

This policy applies to all locations of Karmayogi Bharat, employees of the parent company, and correspondingly contractors working for Karmayogi Bharat. 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 Karmayogi Bharat.

This policy encompasses all systems, automated and manual, for which Karmayogi Bharat has administrative responsibility, including systems managed or hosted by third parties on behalf of Karmayogi Bharat. 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
15. Open Source Technology
16. Business Continuity Plan

5. Information Classification Guidelines

All information available with Karmayogi Bharat 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 and National Information Security Policy and Guidelines 2014 issued by Ministry of Home Affairs as updated from time to time))

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: Karmayogi Bharat 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

6. Organisational Security

a) Information security requires both an information risk management function and an information technology security function. Hence, the Risk Compliance and Data Security Committee shall be the apex authority for Karmayogi Bharat for assuring the below mentioned functions.
   i. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and
   ii. the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.

b) The chief information security officer (CISO) of Karmayogi Bharat 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, Karmayogi Bharat retains overall responsibility for the security of the information that it owns.

7. Functional Responsibilities

7.1. Risk Compliance and Data Security Committee

The Committee shall be chaired by an Independent Director who is an expert in data, risk, compliance and technology. One of the Government Directors conversant with this area shall be a member of this Committee. The Chief Information Security Officer shall be part of this committee. The Chief Technology Officer (CTO) of the Company shall be an invitee to the Committee meetings. The committee shall be responsible for :

i. evaluating and accepting risk on behalf of the Karmayogi Bharat;
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. Regular Security Patch updates, based on Vulnerability assessment/new vulnerabilities detected.

7.2. Chief Information Security Officer

The appointed Chief Information Security Officer shall be responsiable for :

i. maintaining familiarity with business functions and requirements;
ii. maintaining 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 how to appropriately manage those risks;
v. representing and assuring 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 considers Karmayogi Bharat’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;

xix. monitoring external sources for indications of data breaches, defacements, etc.

xx. maintaining ongoing contact with security groups/associations and relevant authorities;

xxi. providing timely notification of current threats and vulnerabilities; and

xxii. providing awareness materials and training resources

Ensuring

a) Regular security Audits

b) ISO 27001 compliance and adoption of ISO27002 processes.

c) Data encryption, as required of information stored for different stakeholders of IGOT as per Data Privacy Policy of Government of India.

7.3. Chief Technology Officer

The Chief Technology Officer of the company shall be responsiable for:

i. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;

ii. providing resources needed to maintain a level of information security control consistent with this policy;

iii. identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;

iv. implementing the proper controls for information owned based on the classification designations;

v. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);

vi. 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; and

vii. implementing business continuity and disaster recovery plans.

viii. Providing dashboards on system access including unknown/suspicious access/ information/threats

7.4. Workforce, Consultants and Third Parties

The workforce, consultants, sub-consultants and third parties who are providing their services to Karmayogi Bharat shall be responsiable 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.

8. Separation of Duties

a) To reduce the risk of accidental or deliberate system misuse, Karmayogi Bharat 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.

9. Policy Applicability on Core Domains

9.1. Networking and Infrastructure Security

This shall include but are not limited to servers, platforms, networks, communications databases and software applications

i. The CTO of the company or a designated individual/group appointed by him shall assume the responsibility for maintenance and administration of any system deployed on behalf of Karmayogi Bharat. 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. All systems shall be developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC).
iv. Each system shall have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
v. All system clocks shall synchronized to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
vi. Environments and test plans shall be established to validate the system works as intended prior to deployment in production.
vii. Separation of environments (e.g., development, test, quality assurance, production) shall be provisioned, either logically or physically, including separate environmental identifications.
viii. Formal change control procedures for all systems shall be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data will be included for any commissioned system by Karmayogi Bharat.

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

a) 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.
b) 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.
c) 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.

d) Where technically feasible, development software and tools must not be maintained on production systems.
e) 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.
f) Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
g) Privileged access to production systems by development staff must be restricted.
h) Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

9.1.2. Network Systems

a) Connections between systems must be authorized by the CTO in consultation with CISO 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.

9.2. Identity, access and privilege managementAll accounts being created on Karmayogi Bharat systems or platforms being managed by the company shall be managed by the core IT team of Karmayogi Bharat led by the CTO.

i. 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.
ii. Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access. A password set by the user must meet the below criteria:

a. Should be at least 8 characters long
b. Should at least have a upper case and a lower case letter
c. Should at least have a special character
d. Should be alpha numeric

iii. Should be changed every 6 months- 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.

iv. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

v. Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the CISO/designated security representative.

vi. 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.).

vii. 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 Karmayogi Bharat missions and business functions (i.e., least privilege).

viii. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

ix. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that user activities may be monitored and the user should have no expectation of privacy.

x. Advance approval for any remote access connection must be provided by Karmayogi Bharat. 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.

xiii. Access to sensitive information or data related to Karmayogi Bharat or its related parties shall be only done through secured connections such as VPN.

9.3. 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.

9.4. 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. Karmayogi Bharat shall follow international standard of ISO/IEC 27001:2013 (ISO 27001) as a standard risk management approach in accordance to the rules and laws for cyber security laid down by the Government of India

iv. Risk assessment results, and the decisions made based on these results, must be documented.

v. All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.

vi. All information assets must have an information owner established within the lines of business. They should also be trained on data privacy guidelines.

vii. Information must be properly managed from its creation, through authorized use, to proper disposal.

viii. All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.

ix. An information asset must be classified based on the highest level necessitated by its individual data elements.

x. If Karmayogi Bharat 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.

xi. 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.

xii. 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.

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

xiv. Karmayogi Bharat must communicate the requirements for secure handling of information to its workforce.

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

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

xvii. The data of behaviour patterns of users on the platform shall only be available on need-to-know basis to selected individuals governed by the NDA and authorised by the CISO and shall be anonymised. The data shall only be used for analysis of generic user behaviour on the platform.

xviii. Behaviour pattern data for users on the platform shall be archived every year and shall be stored only for a maximum of 3 years duration after which it shall be completed destroyed.

xix. PII must not be made available without appropriate safeguards approved by Karmayogi Bharat.

xx. For non-public information to be released outside Karmayogi Bharat 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.

9.5. 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 Karmayogi Bharat 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 CTO. 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.

9.6. 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 Karmayogi Bharat sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by Karmayogi Bharat.

ii. Karmayogi Bharat 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, Karmayogi Bharat 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 Karmayogi Bharat to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to Karmayogi Bharat.

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

vi. Karmayogi Bharat 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.

9.7. Security and Incident Management

i. Karmayogi Bharat 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 CEO or the Board directly to report the threat.

iii. The Security Operations Center 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.

9.8. IT Asset Management

i. All IT hardware and software assets must be assigned to a designated business unit or individual.

ii. Karmayogi Bharat 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.

9.9. Mobility and Bring Your Own Device (BYOD)

i. Individuals may access data and systems of Karmayogi Bharat as their access rights and privileges provided to them end point computing devices owned/managed by them or their respective organisations

ii. These devices will however need to comply to the below mentioned standards

   a. **Operating Systems**: Windows 10 or higher, Android 11 or higher, Chrome OS, Ubuntu 18.10 or higher, Macintosh OS or iOS

   b. **End-Point Security**: Users should have licenced end point security software updated and installed on the respective devices which should at the minimum provide for anti-virus, anti-malware, anti-spyware and firewall protection and should allow to detect threats on system files, data and network

   c. **Software**: Users should only use licenced or cloud hosted free softwares to access files and data related to Karmayogi Bharat to perform their necessary tasks and actions

   d. **Data Sharing**: Users should only use secured channels to secure data. Such as Bluetooth 3.0 or higher, USB 2.0 or higher, Wifi 802.11, TCP/IP, IPv4 or IPv6. Data sharing in peer to peer networks should be avoided.

iii. Users should configure devices with secure passwords as per Karmayogi Bharat password policy or biometric.

iv. Karmayogi Bharat shall audit Mobile and user owned devices from time to time to ensure compliance to the policy

9.10. Virtualization

i. Karmayogi Bharat shall carry out risk assessment of virtual environments owned or managed by the company from time to time. These shall include environments managed by third party vendors on behalf of Karmayogi Bharat.

ii. All types of access to these virtual environments weather physical or virtual shall need to be authorized by Karmayogi Bharat

iii. Karmayogi Bharat shall implement appropriate capabilities to segregate, track and monitor traffic originating from virtual assets

iv. Any virtualization management console must be thoroughly tested prior to deployment

v. The administrative access to the virtualization environments should not have the ability to modify, delete, or disable audit logs

vi. Adequate malware protection capabilities should be enabled on virtual assets

vii. Karmayogi Bharat shall ensure deployment of patches and other mitigating measures as and when new security vulnerabilities are discovered

viii. Karmayogi Bharat shall ensure appropriate mechanism for integrating virtual environments with the company’s log management and monitoring processes

ix. Any virtualization management console deployed by Karmayogi Bharat or associated parties shall at the minimum confer to the below requirements

   a. Use directory services for user and group authentication

   b. Restrict root access via ssh

c. Prevent MAC address spoofing in virtualized environments
d. Configure NTP for time synchronization for logs
e. Maintain file system integrity for incident response and regulatory compliance by monitoring critical files that should be monitored for changes and accidental deletion or corruption
f. Disable copy/paste to remote console/location
g. Disable unnecessary devices within virtual machines
h. Prevent connection and removal of devices from virtual machines
i. Prevent use of any default self-signed certificates for SSL communication
j. Use vulnerability management tools to regularly scan the host OS and VMs for vulnerabilities

9.11. Social Media

i. Access to social media should be avoided on devices with official information which includes official as well as personal devices
ii. Employees, contractual staff, consultants, partners, third party staff etc., who manage, operate or support information systems, facilities, communications networks and information created, accessed, stored and processed by or on behalf of Karmayogi Bharat should be contractually bound against disclosure of official information on social media or social networking portals or applications
iii. Karmayogi Bharat shall conduct training programs for all individuals and associated entities to educate them on perils and threats in the virtual world such as phishing emails, suspicious code in page etc. and for following best practices for practicing safe online behaviour
iv. Only designated and authorized personnel of Karmayogi Bharat may be authorised to communicate unclassified information on public forums and may use social media or social networking portal and applications on devices with official data. These devices should however be configured with adequate security protocols and controls before they are used to access such sites or applications.

9.12. Security Testing

i. Karmayogi Bharat 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. Karmayogi Bharat shall perform security evaluation by constructing scenarios combining internal and external threat agents
iii. In the event of an adversary Karmayogi Bharat shall perform both white hat and black hat testing to examine damage or estimate the impact by the adversary. Black hat testing should be done without the knowledge of the CTO or IT staff but with full knowledge of the CISO. White hat testing shall be carried with approval and consent of the CTO.

9.13. Security Audit

i. Karmayogi Bharat 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

ii. Karmayogi Bharat shall conduct periodic audits of all information systems, infrastructure facilities, third parties etc. which handle classified data at any instance in its lifecycle

iii. 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

iv. Karmayogi Bharat shall ensure that all audit observations, issues and recommendations by the audit team are reported to designated personnel and are resolved and recitified in a necessary time bound manner.

9.14. 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 Karmayogi Bharat 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.

xvi. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

xvii. 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.

xviii. Backup copies of Karmayogi Bharat information, software, and system images must be taken regularly in accordance with Karmayogi Bharat's defined requirements.

xix. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.

xx. 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.

9.15. Open Source Technology

i. Karmayogi Bharat must ensure suitable selections of open source technology which can be easily integrated with existing infrastructure and systems

ii. Karmayogi Bharat must ensure that selected open source technology has minimum licencing and binding requirements

iii. Karmayogi Bharat shall ensure that the selected open source technology has a robust community and support is readily available from the community

iv. Karmayogi Bharat must conduct independent security review of open source technology in addition to gathering information of such technology from subject matter experts etc.

v. Karmayogi Bharat must make sure that open source technology to be procured contains clearly defined and easy to understand installation procedures

vi. Karmayogi Bharat must ensure that additional system components required procurement of open source technology are adequately handled

vii. Karmayogi Bharat must ensure that there are multiple vendors providing the open source technology. Vendors should be contractually bound to provide lifetime support towards patching and up-gradation of the technology

9.16. Business Continuity Plan

i. Karmayogi Bharat shall maintain a disaster recovery plan and shall maintain an identical copy of all the applications as well as databases in data centre that is ideally in a different seismic zone or at least 100 Kilometres apart from the primary data centre.

ii. The copy of the data and application should always be maintained in an active-active mode so that in an event of a shutdown of the primary data centre the disaster recovery centre can service all users of the application immediately and the switchover may be seamless for all users without any impact on the business processes.

iii. The RPO and RTO between the primary and the disaster recovery data centres should be at least 15 mins and 1 hour.

10.Compliance Statement

This policy shall take effect upon publication. 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 Chief Information Security Officer (CISO) exception process.

11.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
CTO	Chief Technology Officer
ISO	International Organisation for Standardization
VPN	Virtual Private Network

.

12.Contact Information

Submit all requests for future enhancements to the policy owner at:
cto-karmayogi@gov.in

13.Revision History

The policy document shall be subject to periodic review to ensure relevancy

Date	Description of Change	Reviewer
17-February-2023	Creation of the policy document	Risk Compliance and Security Committee

14.References

1. National Information Security Policy and Guidelines, Ministry of Home Affairs, Government of India Version 5.0
2. ISO/IEC 27001:2013 (ISO 27001) Standards
    - i. Information Security Risk Management Standard
    - ii. Secure System Development Lifecycle (SSDLC) Standard
    - iii. Information Classification Standard; Sanitization/Secure Disposal Standard
    - iv. Secure Configuration Standard
    - v. Account Management/Access Control Standard
    - vi. Cyber Incident Response Standard
    - vii. Information Security Risk Management Standard
    - viii. Account Management/Access Control Standard; Authentication Tokens Standard
    - ix. Remote Access Standard; Security Logging Standard
    - x. Secure System Development Lifecycle 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

Further Suggestions

1. Restrictions on login password sharing & maintaining integrity.
2. Restrictions on storage of cognitive behaviours patterns of candidate.
3. It should be aligned with data privacy rules as instructed by GOI.
4. Security guidelines as updated by MEITY to be followed
6. DR Planning section to be included (DR to have real time data replication?)
5. Active- Active DR or Active- Passive DR