IT POLICY AND CYBER SECURITY POLICY

Oil Industry Development Board

Table of Contents

Information Technology (IT) is the most important enabler of Business. IT provides new advantages to business operations and can be used as a tool for business process transformation that crosses several functional lines.

Cyberspace is a complex environment consisting of interactions between people, software and services supported by the worldwide distribution of information and communication technology (ICT) devices and networks.

In light of the growth of IT in the organization, providing the right kind of focus for creating a secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks has become one of the compelling priorities.

The protection of information, information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the need of the hour

Therefore, following IT policy (based on the government of India's guidelines) that aims to protect information and information infrastructure from cyber incidents through a combination of processes, guidelines, technology and cooperation, is hereby adopted in OIDB.

1. **Policy and Guidelines on the Use of IT Resources (as per MeitY** circular no- **F. No. 2(22)/2013-EG-II and amendments/ modification thereof from time to time)**-This policy governs the usage of IT Resources from an end user's perspective**.** Guidelines support the implementation of this policy by providing the best practices related to the use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners.

2. **E-mail Policy (as per MeitY** circular no **- F. No. 2(22)/2013-EG-II and amendments/ modification there off from time to time)-** This governs the usage of email services provided to employees.

3. **Password Policy (based on Meity White Paper and amendments/ modification there off from time to time)-** The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.
4. **Policy on Adoption of Open Source Software (as per MeitY circular no - F. No. 1(3)/2014 – EG II and amendments/ modification there off from time to time)-**This will encourage the formal adoption and use of Open Source Software (OSS) in OIDB.

Additional Points Covered in the Policy

- **Document Digitization**
  All extant Digital Initiatives like e-office, e-mail, Document Digitization are to be enforced. Document management system should be in place in OIDB.

- Preparation of Attendance from B**iometric Attendance** should be in place.

- **Centralized Inventory for IT Assets**: Centralized inventory of IT assets to be maintained.

1. Introduction

1.1.1. OIDB provide IT resources to its employees to enhance their efficiency and productivity. These resources are meant as tools to access and process information related to their areas of work. These resources help officials to remain well-informed and carry out their functions efficiently and effectively.

1.1.2. For this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers & scanners and the software associated therewith.

1.1.3. Misuse of these resources can result in unwanted risk and liabilities for the OIDB. It is, therefore, expected that these resources are used primarily for OIDB' related purposes and in a lawful and ethical way.

2. Scope

2.1. This policy governs the usage of IT Resources from an end user's perspective**.**

2.2. This policy is applicable to all employees of OIDB including channel partners in OIDB in connection with IT/System related work.

3. Objective

3.1. The objective of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users. Use of resources provided by OIDB implies the user's agreement to be governed by this policy.

4. Roles

4.1. The following roles are required in OIDB. The official identified for the task should be responsible for the management of the IT resources deployed for the use of entire user base under their respective domain

4.1.1. WIM/Implementing Authority – **DCF&AO (Admin), OIDB**

4.1.2. Designated Nodal Officer – **Manager (P&A)**

4.1.3. Implementing Division – **IT Division, OIDB**

5. Access to the Network

5.1 All devices on the network of OIDB should not be accessible without proper Authentication (Preferably Biometric Authentication for Physical access to Computer / Data Centre at Office Premises).

6. Access to the Internet and Intranet

6.1. A user should register the server system and obtain one-time approval /permission from the Implementing authority before connecting the client system to the OIDB network.

6.2. Users should not undertake any activity through any website or applications to bypass filtering / Policy / Firewall / UTM of the network or perform any other unlawful acts that may affect the network's performance or security

6.3. Users are not allowed to change the NIC configuration, IP address or any other parameters set for accessing the OIDB's LAN & WAN without permission of the implementing authority.

6.4. Users shall not connect any other devices to access the Internet / any other network in the same client system configured for connecting to LAN/WAN of the OIDB without permission.

6.5. It is the responsibility of the user to ensure that the client system is free from any Virus/Malware/Potential threat software's/pirated copy of software's before connecting to OIDB's works

6.6. For connecting to a OIDB wireless network, user should ensure the following:

6.7. A user should register the access device and obtain one-time approval / permission from the Nodal officer/Implementing authority before connecting the access device to the OIDB' wireless network.

6.8. Wireless client systems and wireless devices should not be allowed to connect to the OIDB' wireless access points without due authentication.

6.9. To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks. It is the responsibility of the user to ensure that the device is free from any Virus/Malware/Potential threat software's/pirated copy of software's before connecting to company's Wi-Fi network.

7. Filtering and blocking of sites:

7.1. The Implementing Department may block content over the Internet if it is in contravention of the relevant provisions of the Government Laws and other applicable laws, or which may pose a security threat to the network.

7.2. Implementing Department may also block content, which, in the opinion of the organization concerned, is inappropriate or may adversely affect the network security and productivity of the users/organization.

7.3. The following site category shall be applied subject to such changes as may approved by the competent authority(ies):

	Group I		Group II		Group III	
	DCFAO and above-level officers		Other Regular Officers/ officials of OIDB only.		Contractual Employee/ Consultant/ Auditors/Visitors of OIDB.	
Site Category	**Monitor**	**Block**	**Monitor**	**Block**	**Monitor**	**Block**
Abortion		B		B		B
Adult Content		B		B		B
Lingerie and Swimsuit		B		B		B
Nudity		B		B		B
Sex		B		B		B
Sex Education		B		B		B
Internet Radio and TV	M			B		B
Internet Telephony	M			B		B
Peer to Peer File Sharing	M		M		M	
Personal Network Storage and Backup	M		M			B
Streaming Media (Netflix, Amezon prime, Hotstar Etc.)	M			B		B
Financial data and Services	M		M		M	
Abused Drugs		B		B		B
Prescribed Medications	M		M			B
Supplements and Unregulated Compounds	M		M			B
Cultural Institutions	M		M		M	
Educational Institutions	M		M		M	
Reference Materials	M		M		M	
Entertainment	M			B		B
MP3 and Audio Download Services		B		B		B

Elevated Exposure	M		M			B
Emerging Exploits	M		M		M	
Potentially Damaging Content		B		B		B
Gambling		B		B		B
Games Application and Online		B		B		B
Military	M		M		M	
Political Organizations	M			B		B
Health	M		M		M	
Illegal or Questionable		B		B		B
Computer Security	M		M			B
Hacking		B		B		B
Proxy Avoidance		B		B		B
Search Engines and Portals	M		M		M	
URL translation Sites	M		M		M	
Web hosting	M		M			B
General Email	M		M		M	
Organizational Email	M		M			B
Text and Media Messaging	M		M			B
Web / Whatsaap Chat	M		M			B
Job Search	M		M		M	
Social Media (Facebook, Instagram, Twitter, Snapchat , etc)		B		B		B
Military and Extremist		B		B		B
File Download Servers	M		M		M	
Images (Media)	M		M		M	
Images Servers	M		M		M	
Private IP Address	M			B		B
News and Media	M		M		M	
Alternative Journals	M		M		M	

Advertisements		B		B		B
Freeware and Software Downloads		B		B		B
Online Brokerage and Trading		B		B		B
Pay- to- Surf		B		B		B
Racism and Hate		B		B		B
Non- Traditional Religions and Occult and Folklore		B		B		B
Traditional Religions	M		M			B
Malicious Web Sites		B		B		B
Phishing and other Frauds		B		B		B
Potentially unwanted Software		B		B		B
Spyware		B		B		B
Internet Auctions	M		M			B
Real State	M		M		M	
Professional and Worker Organization	M		M		M	
Government Organization	M		M		M	
Alcohol and Tobacco		B		B		B
Gay or Lesbian or Bisexual interest		B		B		B
Hobbies	M		M		M	
Personals and Dating websites	M		M		M	
Restaurants and Dining	M		M		M	
Sports	M		M		M	
Violence		B		B		B
Weapons		B		B		B

8. Monitoring and Privacy:

8.1. OIDB should have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

8.2. OIDB, for security-related reasons or for compliance with applicable laws, may access, review, copy, or delete any kind of electronic communication or files stored on devices under intimation to the user. This includes items such as files, e-mails and Internet history etc.

9. E-mail Access from the OIDB Network

9.1. Users should refrain from using private e-mail servers from the OIDB network.

9.2. e-mail service authorized by the OIDB and implemented by the Implementing Department should only be used for all official correspondence. For personal correspondence, users may use the name-based/designation e-mail ID assigned to them on the OIDB- authorized e-mail service.

More details in this regard are provided in the "e-mail Policy of Miety".

10. Access to Social Media Sites from OIDB Network.

11.1 Use of social networking sites by Employees is governed by "Framework and Guidelines for the use of Social Media for Government of India Organizations" available at http://meity.gov.in.

11.2 User should comply with all the applicable provisions under the Government Laws, while posting any data pertaining to the OIDB on social networking sites.

11.3 User should adhere to the "Terms of Use" of the relevant social media Platform/website, as well as copyright, privacy, defamation, discrimination, harassment and other applicable laws.

11.4 User should report any suspicious incident as soon as possible to the Implementing authority.

11.5 User should always use high security settings on social networking sites.\User should not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

11.6 User should not disclose or use any confidential information obtained in their capacity as an employee/contractor of the organization.

11.7 User should not make any comment or post any material that might otherwise cause damage to the organization's reputation.

11. Use of IT Devices Issued by OIDB.

11.1.1. IT devices (Desktops, Printers, Scanners, Standalone PCs) issued by the OIDB to a user should be primarily used for Official purposes and in a lawful and ethical way and should be governed by the practices defined in the document **"Guidelines for Use of IT Devices on OIDB Network"** Under the caption "Policy on Use of IT Resources".

12. Responsibility of OIDB.

13.1 Policy Compliance

12.1.1. OIDB should implement appropriate controls to ensure compliance with this policy by their users. Implementing Departments should provide necessary support in this regard.

13.1.1. A periodic reporting mechanism to ensure the compliance of this policy should be established by the Implementing authority of the organization.

13.1.2. Nodal Officer of the OIDB should ensure resolution of all incidents related to the security aspects of this policy by their users. Implementing Departments should provide the requisite support in this regard.

13.1.3. Implementing Authority of the user organization spread awareness of the proper use of IT resources at regular intervals.

13.1.4. Users should not install any network/security device on the network without consulting the Implementing Division.

13.2 Policy Dissemination

13.2.1 Implementing Authority of the user organization should ensure proper dissemination of this policy.

13.2.2 Implementing Authority may use newsletters, banners, bulletin boards, corporate Websites and Intranet or any other channel of communication etc. to increase awareness about this policy amongst their users.

13. Security Incident Management Process

13.1. A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of data owned by OIDB.

13.2. Implementing Division reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the Implementing authority.

13.3. Any security incident noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the Implementing Division.

14. Scrutiny/Release of logs

14.1. Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the Implementing Department should be done as per the Government Laws and other applicable laws.

15. Intellectual Property

15.1. Material accessible through the network and resources of OIDB may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information.

15.2. Users should not use the network and resources of OIDB in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

16. Enforcement

16.1. This policy is applicable to all employees of OIDB and such other users directly or indirectly engaged in the officers of OIDB as specified in clause 2 of this document. All users must adhere to the provisions of this policy.

17. Deactivation

17.1. In case of any threat to the security of the systems or network from the resources being used by a user, may be deactivated immediately by the Implementing Division.

17.2. Subsequent to such deactivation, the concerned user and the Implementing authority of that organization be informed.

Part-B

E-mail Policy

1. Introduction

1.1 OIDB uses email as a prevalent mode of communication. Communications include OIDB (data that travel as part of mail transactions between users located both within the country and outside.

1.2 This policy of OIDB lays down the guidelines with respect to the use of email services. The Implementing Agency (Implementing Department) for the OIDB e- mail service should be National Informatics Centre (NIC), under the Department of Electronics and Information Technology (DeitY), Ministry of Communications and Information Technology.

2. Scope

2.1. Only the e-mail services provided by NIC, the Implementing Agency of the OIDB should be used for official communications by all organizations. The e-mail services provided by other service providers should not be used for any official communication.

2.2. This policy is applicable to all users who use the e-mail services provided by OIDB.

2.3. e-mail can be used as part of the electronic file processing in OIDB (Oil Industry development board).

3. Objective

3.1. The objective of this policy is to ensure secure access and usage of OIDB e-mail services by its users. Users have the responsibility to use this resource in an efficient, effective, lawful, and ethical manner. Use of the OIDB e-mail service amounts to the user's agreement to be governed by this policy.

3.2. All services under e-mail are offered free of cost to all officials of OIDB as well as other user.

3.3. **A**ny other policies, guidelines or instructions on e-mail previously issued should be superseded by this policy.

4. Basic requirements of OIDB e-mail Service

4.1. e-mail account should be either name based, or designation based.

4.2. Considering the security concerns with regard to a sensitive deployment like e-mail, apart from the service provided by the Implementing Department(i.e NIC/GOV), there would not be any other e-mail service under OIDB.

4.3. Users should not download e-mails from their official e-mail account, configured on the OIDB mail server, by configuring POP [9] or IMAP [10] on any other e-mail service provider. This implies that users should not provide their OIDB e-mail account details (id and password) to private e-mail service providers.

4.4. Any e-mail addressed to a user, whose account has been deactivated /deleted, should not be redirected to another e-mail address. Such e-mails may contain contents that belong to the OIDB and hence no e-mails shall be redirected.

4.5. The concerned nodal officer of the organization should ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User.

4.6. In case a compromised e-mail id is detected by the Implementing Department, an SMS alert will be sent to the user on the registered mobile number. In case an "attempt" to compromise the password of an account is detected, an e-mail alert will also be sent. Both the e-mail and the SMS will contain details of the action to be taken by the user. In case a user does not take the required action even after five such alerts (indicating a compromised threat), the Implementing Department reserves the right to reset the password of that particular e-mail id under intimation to the user .

4.7. Auto-save password in the OIDB e-mail service is not permitted due to security reasons.

5. E-mail Account Management

5.1. Use of alphanumeric characters as part of the e-mail id is recommended for sensitive users as deemed appropriate by the Implementing authority.

5.2. OIDB officers and other such users who resign, superannuate, or leave the OIDB on any other ground , their email services account shall be deactivated within a month of .

5.3. **Use of Secure Passwords**

5.3.1. All users accessing the e-mail services must use strong passwords for security of their e-mail accounts. More details about the password policy are available in "Password Policy of OIDB"

6. Privacy

6.1. Users should ensure that e-mails are kept confidential. Implementing Department should take all possible precautions on maintaining privacy. Users must ensure that information regarding their password or any other personal information is not shared or disclosed with anyone.

7. Responsibilities of User Organization.

7.1 Policy Compliance

7.1.1. OIDB should implement appropriate controls to ensure compliance with the e-mail policy by their users. Implementing Department has to give the requisite support in this regard.

7.1.2. OIDB should ensure that official e-mail accounts of all its users are created only on the NIC e-mail server of the Implementing Department.

7.1.3. Nodal officer should try resolution of all incidents related to the security aspects of

the e-mail policy. Implementing Department should give the requisite support in this regard.

7.1.4. All users/user organization to follow the instruction issued by Gov of India from time to time, OIDB shall make necessary changes as required in compliance of such guidelines of Govt of India.

8. Responsibilities of Users

8.1 Appropriate Use of e-mail Service

8.1.1. e-mail is provided as a professional resource to assist users in fulfilling their official duties. Id's of type designation/office/ division/ section and personal name basis but these can be used only for official communication and shall not be used for any personal purpose.

8.1.2. While sending an official email it is obligated to indicate the designation and details of the sender to give information regarding the identity of the sender.

8.2 **Examples of inappropriate use of the e-mail service:**

8.2.1 Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening is prohibited.

8.2.2 Unauthorized exchange of proprietary information or any other privileged, confidential, or sensitive information is prohibited.

8.2.3 Unauthorized access to the services. This includes the distribution of e-mails anonymously, use of other officers' user ids or using a false identity is prohibited.

8.2.4 Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail is prohibited.

8.2.5 Creation and exchange of information in violation of any laws, including copyright laws is prohibited.

8.2.6 Willful transmission of an e-mail containing a computer virus is prohibited.

8.2.7 Misrepresentation of the identity of the sender in e-mail is prohibited.

8.2.8 Use or attempt to use the accounts of others without their permission is prohibited.

8.2.9 Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing anti-national messages, sending e-mails with obscene material, etc. is prohibited

8.2.10 Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc. Any case of inappropriate use of e-mail accounts should be considered a violation of the policy and may result in deactivation of the account. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation. However shall official email with Govt organization related to newsletter modules, study material etc., which are benefits to employees in a way to enhance their knowledge skill.

9 User's Role

9.1 The User is responsible for any data/e-mail that is transmitted using the NIC- OIDB e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

9.2 Sharing of passwords is prohibited.

9.3 The user's responsibility should extend to the following:

9.4 Users should be responsible for the activities carried out on their client systems, using the accounts assigned to them.

9.5 The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to the undefined email account.

9.6 All digital documents are to be treated as regular documents and retained as per existing guidelines of document retention policy.

10 Scrutiny of e-mails/Release of logs

10.1 Notwithstanding anything contained in the clauses above, the disclosure of logs/e-mails to law enforcement agencies and other organizations by the Implementing Department would be done only as per the Government Laws and other applicable laws.

11 Security Incident Management Process

11.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of OIDB data. Security incidents can be due to factors like malware, phishing, loss of a device, compromise of an e- mail id etc.

11.2 It should be within the right of the Implementing Department to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.

11.3 Any security incident noticed or identified by a user must be brought immediately to the notice of the Indian Computer Emergency Response Team (ICERT) and the Implementing Department.

12 Deactivation

12.1 In case of threat to the security , the e-mail id involved to impact the service may be suspended or deactivated immediately by the Implementing Department.

12.2 Subsequent to deactivation, the concerned user and the Implementing authority of that respective organization should be informed.

Part-C

Password Policy of OIDB

1. Purpose

1.1. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

2. Scope

2.1. The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the OIDB. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

3. Policy Statements

3.1. For users having accounts for accessing systems/services

3.2. Users should be responsible for all activities performed with their personal user IDs. Users should not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.

3.3. All user-level passwords (e.g., email, web, desktop computer, etc.) should be changed periodically (at least once every three months). Users should not be able to reuse previous passwords.

3.4. Password should be enforced to be of a minimum length (8) and comprising of mix of alphabets, numbers and special characters.

3.5. All access codes including user ID passwords, network passwords, PINs etc. should as far as possible not be shared with anyone, including personal assistants or secretaries. These should be treated as sensitive, confidential information. However, nodal officer may share their designation/organization office wise.

3.6. All PINs (Personal Identification Numbers) should be constructed with the same rules that apply to fixed passwords.

3.7. Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.

3.8. Passwords should not be revealed on questionnaires on security forms.

3.9. Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.

3.10. The "Remember Password" feature of applications should not be used.

3.11. Users should refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

3.12. First time login to systems/services with administrator created passwords, should force changing of password by the user.

3.13. If the password is shared with support personnel for resolving problems relating to any service, it should be changed immediately after the support session.

3.14. The password should be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

4. For designers/developers of applications/sites

4.1. No password should be traveling in clear text; the hashed form of the password should be used.

4.2. For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

5. Responsibilities:

5.1. All individual users having accounts for accessing systems/services in the OIDB Network,and system/network administrators of OIDB servers/ network equipment should ensure the implementation of this policy.

5.2. All designers/developers responsible for site/application development should ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

Part-D

Policy on adoption of Open Source Software

1. Introduction:

1.1. Organizations worldwide have adopted innovative alternative solutions in order to optimise costs by exploring avenues of “Open Source Software”. GoI has also been promoting the use of open source technologies in the e- Governance domain within the country in order to leverage economic and strategic benefits.

1.2. Further, the National Policy on Information Technology, 2012 has mentioned, as one of its objectives, to “Adopt open standards and promote open source and open technologies".

1.3. In view of the above, there is a need to formulate a policy for OIDB to adopt Open Source Software. The “Policy on Adoption of Open Source Software for OIDB” (hereinafter referred to as “Policy”) will encourage the formal adoption and use of Open Source Software (OSS) in OIDB.

1.4. OIDB should endeavour to adopt Open Source Software in all technologies, as a preferred option in comparison to Closed Source Software (CSS).

1.5. The policy should be applicable to OIDB.

2. How to comply

2.1. OIDB, while implementing applications and systems should include a specific requirement in Request for Proposal (RFP) for all suppliers to consider OSS along with CSS. Suppliers should provide justification for exclusion of OSS in their response, as the case may be.

2.2. OIDB should ensure compliance with this requirement and decide by comparing both OSS and CSS options with respect to capability, strategic control, scalability, security, life-time costs and support requirements.

3. Exception

3.1. OIDB should endeavour to adopt Open Source Software in all applications and systems implemented. However, in certain specialised domains where OSS solutions meeting essential functional requirements may not be available or in case of urgent / strategic need to deploy CSS based solutions or lack of expertise (skill set) in identified technologies, may consider exceptions, with sufficient justification.

Part-E

Data Backup Policy (For OIDB-NAS Server Data)

1. Purpose:

1.1. **T**he purpose of this policy is to provide consistent rules for backup management to ensure backups are available when needed.

2. Data to be Backed Up:

2.1.1. All data stored on the OIDB NAS Servers i.e., OIDB Database and the webservers will be backed up.

3. Complete Automated Backup Frequency and retention

3.1. Backups are to be taken in the OIDB NAS automatically with variable retention periods from (1 Week for daily backups and 4 weeks for weekly and 6 months for monthly backups)

3.2. The NAS administrator creates a user account and user folders and grants permission to access data backups.

3.3. If the user has forgotten their username and password, contact the NAS administrator. Only the NAS administrator can provide the username and password.

4. Manual Backup Frequency and Retention

4.1. Backups may also to be taken in an **encrypted (preferably)** hard drive to prevent data leakage, clearly labelled daily, which is to be stored in a physically remote location and fire/water proof cabinet on premises away from the OIDB Server.

4.2. This will ensure that the backups are physically isolated and the encryption will protect the data against theft

5. Restoration Testing

5.1. Full Backup restoration must be tested when any change is made affecting the backup system.

5.2. Full Backup restores must also be tested half yearly in test environment to ensure the integrity of the backups in case of a crisis.

6. Backup Plan

6.1. A backup plan should be prepared keeping in mind the daily, weekly and monthly backup schedule depending on the criticality of data.

6.2. The 3-2-1 rule of backup detailed below to be followed :

6.2.1. : Users may have at least three copies of data: the original production data and two backups.

6.2.2. : Users may use at least two different types of media to store the copies of data (e.g. local disk, tape and external hard disk).

6.2.3. User can reset NAS server password and backup selected files from his computer.

6.2.4. Users must keep at least one backup offsite (in the cloud or in a remote site).

6.2.5. User shall be responsible for any user owned data backup, if data backup is not working then inform IT department.

6.2.6. The IT division is only responsible for data backup in NAS server.

7. Data restoration

7.1. Onsite data would be restored from backups within 3 working days provided the equipment for the same is available.

8. Authorized Persons

8.1. Two officials are to be nominated with the approval of Implementing Authority to ensure the working of the Backup Policy.

8.2. They should be responsible for checking that backups are performed successfully and logs are to be maintained if they are successful/failed.

Part-F

1. Introduction:

Guidelines for Use of IT Resources

OIDB has formulated the **"Policy on Use of IT Resources"**. This document supports the implementation of this policy by providing the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners.

2. Desktop Devices

2.1. Use and Ownership

2.1.1. Desktops should normally be used only for transacting official work. Users should exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

2.2 Security and Proprietary Information

2.2.1 Users should take prior approval from the Implementing authority of their respective devices to connect to the network.

2.2.2 Users should keep their passwords secure and not share their account details.

2.2.3 All active desktop computers should be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.

2.2.4 Users should ensure that updated virus-scanning software is running in all systems. Users should exercise due caution when opening e-mail attachments received from unknown senders as they may contain malicious software.

2.2.5 Users should report any loss of data or accessories to the Implementing authority of OIDB

2.2.6 Users should obtain authorization from the Implementing authority before taking any issued desktop outside the premises of ODB.

2.2.7 Users should properly shut down the system before leaving the office.

2.2.8 Users will not be given administrator privileges.

2.2.9 Users should not be allowed to set static IP addresses in any of the devices and use DHCP only.

2.2.10 Users should abide by instructions or procedures as directed by the Implementing Department from time to time.

2.2.11 Any Annual Maintenance Contract with service providers should include a clause that Hard Disk should be retained by the OIDB, even if it is faulty. While disposing the Hard disk it should be destroyed so that data cannot be retrieved.

3. Use of software on Desktop systems

3.1. Users should not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the Implementing authority.

4. Sharing of data

4.1 Users should not share their account(s), passwords, security tokens (i.e. smartcard), Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

5. Use of Portable devices

5.1. Devices covered under this section include issued laptops, Printers, USB etc. by the Government organization. Use of the devices should be governed by the following:

5.2. User should be held responsible for any unauthorized usage of access devices issued by OIDB, by a third party.

5.3. Users should keep the devices issued by OIDB, with them or store them in a secure location when not in use. User should not leave the devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).

5.4. User should ensure that the portable devices are password protected and auto lockout enabled.

5.5. Users should be given an account with privileges on the server systems. User should not be given administrator privilege unless required on a temporary basis for any official uses.

5.6. User should ensure that remote wipe feature is enabled on the issued device, wherever technically feasible. Users should not circumvent security features on

their devices.

5.7. The concerned nodal officer of OIDB should ensure that the latest operating system, centralized anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls should be enabled.

5.8. Users should wipe or securely delete data from the device before returning/ disposing it off.

5.9. Lost, stolen, or misplaced devices should be immediately reported to the Implementing Department and the Implementing authority beside reporting to concerned public authority.

5.10. Data transmissions from devices to the services on the OIDB network should be over an encrypted channel.

6. External Storage Media:

6.1. Devices covered under this section include issued CD/DVD's, USB storage devices etc. Use of these devices should be governed by the following:

6.2. Users should use only the media issued by the organization for all official work. The user should be responsible for the safe custody of devices and content stored in the devices which are in their possession.

6.3. Classified data should be encrypted before transferring to the designated USB device. The decrypting key should not exist on the same device where encryption data exists

6.4. Classified/ sensitive information should be stored on separate portable media. User should exercise extreme caution while handling such media.

6.5. Unused data on USB devices should be cleaned through multiple pass process (like wipe/eraser software)

6.6. Users should not allow USB device belonging to outsiders to be mounted on OIDB systems.

7. Use of External storage media by a visitor

7.1. Visitors should not be allowed to carry any portable media without permission.

7.2. If it is necessary to allow the visitor to use a USB memory device for any reason, it should be used only on designated systems meant for specific purposes. The USB device belonging to visitors should be mounted on systems that are connected and belong to the network of OIDB.

8. Authority issuing External storage

8.1. Implementing Authority of the organization should ensure that process is in place to maintain records for procurement, issue, return, movement and destruction of the storage devices.

8.2. All obsolete USB devices should be physically destroyed to avoid misuse.

Part-G

Introduction:

Guidelines for Accessibility Standards (WCAG 2.1 AA, RPwD Act 2016)

In compliance with the Rights of Persons with Disabilities (RPwD) Act, 2016 and international best practices under Web Content Accessibility Guidelines (WCAG) 2.1, Level AA, the following standards shall be adopted in all IT systems, applications, and digital platforms of the OIDB:

1. Legal Compliance

1.1. All OIDB IT resources shall adhere to the accessibility provisions of the RPwD Act, 2016 and subsequent guidelines issued by the Government of India.

1.2. Accessibility features will be mandatory for all digital products, ensuring inclusivity for persons with disabilities.

2. WCAG 2.1 AA Standards

OIDB Websites and applications shall comply with WCAG 2.1 AA criteria, covering principles of:

2.1 **Perceivable:** Provide text alternatives, captions for multimedia, adaptable content, and sufficient color contrast.

2.2 **Operable:** Ensure full keyboard navigation, adequate time for interaction, and no content that may trigger seizures.

2.3 **Understandable:** Use readable language, predictable navigation, and assistive error identification.

2.4 **Robust:** Ensure compatibility with assistive technologies (e.g., screen readers).

3. Testing & Compliance

3.1. Accessibility audits shall be conducted periodically using both automated tools and

manual testing with assistive technologies.

3.2. Vendors and developers must provide an Accessibility Conformance Report (ACR) before acceptance of deliverables.

4. Capacity Building & Awareness

4.1. Training programs shall be organized for IT Division, content creators, and administrators on accessibility best practices.

4.2. Guidelines for creating accessible digital documents (Word, PDF, PPT, Excel, etc.) shall be circulated to all OIDB employees.

5. Monitoring & Review

5.1. A designated Web Information Manager / Implementing Officer shall ensure continuous monitoring of compliance with WCAG 2.1 AA and RPwD Act requirements.

5.2. Non-compliance will be reported and corrective measures shall be undertaken promptly.

Part-H

Introduction:

Guidelines for Cyber-Security Certification

1. CERT-In Compliance

1.1. All OIDB IT infrastructure and applications shall comply with guidelines, advisories, and best practices issued by the Indian Computer Emergency Response Team (CERT-In).

1.2. Any security incident, breach, or cyber threat shall be reported to CERT-In as per statutory requirements.

1.3. Security audit of OIDB websites and applications shall be carried out by CERT-In empanelled auditors before deployment and at regular intervals thereafter.

2. STQC Certification

2.1 OIDB Websites and applications shall undergo Security & Quality Certification through the Standardization Testing and Quality Certification (STQC) Directorate.

2.2 STQC certification shall be obtained prior to hosting government

websites/applications on the production environment.

2.3 Applications handling sensitive or personal data must be validated against OWASP Top 10 and other security standards during STQC audit.

3. Periodic Security Audits

3.1 All OIDB IT systems will be subjected to Vulnerability Assessment & Penetration Testing (VAPT) at least once a year.

3.2 Third-party vendors must ensure their deliverables are CERT-In/STQC certified prior to acceptance.

4. Data Protection & Hardening

4.1 Systems shall implement encryption, secure configurations, and patch management as per CERT-In advisories.

4.2 Logs of security incidents shall be maintained for audit and compliance purposes.

5. Monitoring & Governance

5.1 A designated Cyber Security Nodal Officer will oversee compliance with CERT-In and STQC requirements.

5.2 Continuous monitoring mechanisms (IDS/IPS, SIEM, firewalls, endpoint security) shall be maintained.

Part-I

Introduction:

Guidelines for Periodic STQC Audit for CQW Certification

1. Mandatory Certification

1.1 All official websites and web applications of the OIDB shall undergo STQC audit and certification in line with the Continuous Quality Website (CQW) certification scheme of the Government of India.

2. Frequency of Audit

2.1 A periodic security and quality audit shall be conducted at least once every year or whenever major changes/enhancements are made to the website/application.

2.2 Certification shall be renewed regularly to maintain compliance.

3. Audit Scope

3.1 The STQC audit will cover security, functionality, accessibility, usability, and performance parameters.

3.2 Website and Application must comply with GIGW (Guidelines for Indian Government Websites), WCAG 2.1 AA accessibility standards, and CERT-In security guidelines.

4. Compliance Responsibility

4.1 The Web Information Manager (WIM) / Nodal Officer shall ensure timely scheduling of STQC audits.

4.2 Audit findings shall be documented, and corrective actions shall be implemented within the prescribed timelines.

5. Vendor/Developer Obligation

5.1 Vendors/Service Providers shall ensure that applications developed for the organization are STQC certifiable before deployment.

5.2 Acceptance of deliverables shall be subject to successful STQC audit clearance.

6. Monitoring & Renewal

6.1 A register of certification validity periods shall be maintained for proactive renewal.

6.2 Non-compliance or lapse of certification shall be treated as a serious violation of IT Policy.