IT POLICY AND CYBER SECURITY POLICY

Coal India Limited and Subsidiaries

Table of Contents

Information Technology (IT) is the most important enabler of Business. The information technology 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 worldwide distribution of information and communication technology (ICT) devices and networks.
In the light of the growth of IT in our organisations, providing right kind of focus for creating 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 infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the need of the hour

The following policy aims to protect information and information infrastructure in
from cyber incidents through a combination of processes, guidelines, technology and cooperation.

All the Policies are laid down according to the guidelines Govt. of India

The following Policies and Guidelines covers Coal India and Subsidiaries:

1. **Policy and Guidelines on the Use of IT Resources(as per MeitY - F. No. 2(22)/2013-EG-II and amendments/ modification there off from time to time)**
2. This policy governs the usage of IT Resources from an end user's perspective**.** Guidelines 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.

3. **e-mail Policy (as per MeitY - F. No. 2(22)/2013-EG-II and amendments/ modification there off from time to time)**
   This governs the usage of email servies prodived to employees.

4. **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.

5. **Policy on Adoption of Open Source Software(as per MeitY - 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 Coal India and Subsidiaries.

6. **Backup Policy for Servers (as per extant policies at Coal India HQ Kolkata)**
   The purpose of this policy is to provide consistent rules for backup management to ensure backups are available when needed.

Additional Points Covered in the Policy

- **DC/ DRC (Data Center and Disaster Recovery Centre) Requirements**
  All data centers to be built/ upgraded are to adhere to the Guidelines of Government of India for Data Centers.
  Appropriate levels of Data Redundancy is to be built into all the systems with Active mode Disaster Recovery center for Business critical applications.

- **Document Digitization**
  All extant Digital Initiatives like e-office, e-mail, Document Digitisation are to be enforced. Document management system should be in place in CIL and all subsidiaries.

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

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

- **Bill Tracking**: All transparency related policies declared by CIL should be incorporated in the IT systems.

- **Suggestions from GM Coordination meeting on 07/11/19**

PART-A
Policy on the Use of IT Resources

1. Introduction

1.1.1. Coal India and Subsidiaries 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 in an efficient and effective manner.

1.1.2. For the purpose of 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 and scanners and the software associated therewith.

1.1.3. Misuse of these resources can result in unwanted risk and liabilities for the Coal India and Subsidiaries . It is, therefore, expected that these resources are used primarily for Coal India and Subsidiaries' 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 Coal India and employees of Subsidiaries

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 Coal India and Subsidiaries imply the user's agreement to be governed by this policy.

4. Roles

4.1. The following roles are required in each Subsidiary . 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. Implementing Authority - **GM System and GM E&T of CIL and respective subsidiaries**

4.1.2. Designated Nodal Officer – **Nominated by Implementing Authority**

4.1.3. Implementing Department – **System/E&T department**

5. Access to the Network

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

6. Access to Internet and Intranet

6.1. A user should register the client system and obtain one time approval /permission from the Implementing authority before connecting the client system to the Coal India and Subsidiaries 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 which may affect the network's performance or security

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

6.4. Users shall not connect any other devices to access Internet / any other network in the same client system configured for connecting to LAN/WAN of the company 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 softwares/pirated copy of softwares before connecting to company's network.

7. Access to Coal India and Subsidiaries Wireless Networks

7.1. For connecting to a Coal India and Subsidiaries wireless network, user should ensure the following:

7.2. A user should register the access device and obtain one time approval / permission from the Implementing authority before connecting the access device to the Coal India and Subsidiaries' wireless network.

7.3. Wireless client systems and wireless devices should not be allowed to connect to the Coal India and Subsidiaries' wireless access points without due authentication.

7.4. 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 softwares/pirated copy of softwares before connecting to company's Wi-Fi network.

8. Filtering and blocking of sites:

8.1. Implementing Department may block content over the Internet which 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.

8.2. 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 .

9. Monitoring and Privacy:

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

9.2. Coal India, 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.

10. e-mail Access from the Coal India and Subsidiaries Network

10.1. Users should refrain from using private e-mail servers from CIL/Subsidiary network.

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

More details in this regard are provided in the "e-mail Policy of CIL and Subsidiaries ".

11. Access to Social Media Sites from Coal India and Subsidiaries 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://deity.gov.in.

11.2 User should comply with all the applicable provisions under the Government Laws, while posting any data pertaining to the Coal India and Subsidiaries 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.

12. Use of IT Devices Issued by Coal India and Subsidiaries

12.1. IT devices(Desktops, Printers, Scanners, iPads, Standalone PCs) issued by the Coal India and Subsidiaries 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 Coal India and Subsidiaries Network”** Under the caption “Policy on Use of IT Resources”.

13. Responsibility of Coal India and its Subsidiaries

13.1 Policy Compliance

13.1.1. Coal India and its Subsidiaries should implement appropriate controls to ensure compliance with this policy by their users. Implementing Departments should provide necessary support in this regard.

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

13.1.3. Nodal Officer of the Subsidiaries 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.

13.1.4. Implementing Authority of the user organization should ensure that training and awareness programs on use of IT resources are organized at regular intervals. Implementing Agency should provide the required support in this regard.

13.1.5. Users should not install any network/security device on the network without consultation with the Implementing Department.

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 etc. to increase awareness about this policy amongst their users.

13.2.3 Orientation programs for new recruits should include a session on this policy.

14. Security Incident Management Process

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

14.2. Implementing Department 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.

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

15. Scrutiny/Release of logs

15.1. 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.

16. Intellectual Property

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

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

17. Enforcement

17.1. This policy is applicable to all employees of Coal India and Subsidiaries of Coal India as specified in clause 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.

17.2. Each Subsidiary should be responsible for ensuring compliance with the provisions of this policy. The Implementing Departments would provide necessary technical assistance to the organizations in this regard.

18. Deactivation

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

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

Part-B

E-mail Policy

1. Introduction

1.1 Coal India and Subsidiaries use email as a major mode of communication. Communications include Coal India and Subsidiaries (data that travel as part of mail transactions between users located both within the country and outside.

1.2 This policy of Coal India and Subsidiaries lays down the guidelines with respect to the use of email services. The Implementing Agency (Implementing Department) for the Coal India 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 Coal India and Subsidiaries (Coal India) 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 employees of Coal India and employees of those Subsidiaries that use the e-mail services of Coal India. The directives contained in this policy must be followed by all of them with no exceptions.

2.3. e-mail can be used as part of the electronic file processing in Coal India and Subsidiaries (Coal India).

3. Objective

3.1. The objective of this policy is to ensure secure access and usage of Coal India and Subsidiaries (Coal India) 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 Coal India and Subsidiaries (Coal India) 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 Coal India.

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

4. Basic requirements of Coal India 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, there would not be any other e-mail service under Coal India.

4.3. Updation of current mobile numbers under the personal profile of users is mandatory for security reasons. The number would be used only for alerts and information regarding security sent by the Implementing Department. Updation of personal e-mail id , in addition to the mobile number, should also be mandatory in order to reach the user through an alternate means for sending alerts.

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

4.5. 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 Coal India and Subsidiaries (Coal India)and hence no e-mails should be redirected.

4.6. 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.

4.7. In case a compromise of an e-mail id is detected by the Implementing Department, an SMS alert should 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 should be sent. Both the e-mail and the SMS should 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 compromise), the Implementing Department reserves the right to reset the password of that particular e-mail id under intimation to the nodal officer of that respective subsidiary.

4.8. In case of a situation when a compromise of a user id impacts a large user base or the data security of the deployment, the Implementing Department should reset the password of that user id. This action should be taken on an immediate basis, and the information should be provided to the user and the nodal officer subsequently. SMS should be one of the prime channels to contact a user; hence all users should ensure that their mobile numbers are updated.

4.9. Forwarding of e-mail from the e-mail id provided by Coal India to the Coal India and Subsidiaries (Coal India)official's personal id outside the Coal India e-mail service should not be allowed due to security reasons. Official e-mail id provided by the Implementing Department can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.

4.10. Auto-save of password in the Coal India and Subsidiaries (Coal India)e-mail service should not be 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. Coal India and Subsidiaries (Coal India)officers who resign or superannuate the email services account should be deactivated on the date of superannuation.

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 Coal India"

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 with anyone.

7. Responsibilities of Subsidiaries

7.1 Policy Compliance

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

7.1.2. CIL and Subsidiaries should ensure that official e-mail accounts of all its users are created only on the e-mail server of the Implementing Department**.**

7.1.3. Nodal officer of CIL and Subsidiaries 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.Implementing Authority should ensure that training and awareness programs on e-mail security are organized at regular intervals. Implementing Agency should provide the required support.

7.2 Policy Dissemination

7.2.1 Implementing Authority of the concerned organization should ensure dissemination of the e-mail policy.

7.2.2 Implementing Authority should use Newsletters, banners, bulletin boards,website,intranet etc, of Coal India and Subsidiaries to increased awareness on the e-mail policy.

7.2.3 Orientation programs for new recruits should include a session on the e-mail policy.

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

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. Designation based ids should be used for official communication and name based ids can be used for both official and personal communication.

8.1.2 Departmental Emails must not be used for internal communication

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

8.2.7 Misrepresentation of the identity of the sender of an 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.

9 User’s Role

9.1 The User is responsible for any data/e-mail that is transmitted using the Coal India 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 wrong people.

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

9.7 Logs generated by System should be retained for atleast three months and those generated and programmed by application development should be retained as per existing guidelines of document retention policy.

10 Scrutiny of e-mails/Release of logs

10.1 Notwithstanding anything 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 Coal India and Subsidiaries (Coal India)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 immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the Implementing Department.

12 Intellectual Property

12.1 Material accessible through the Implementing Department's e-mail service and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users should not use the Coal India and Subsidiaries (Coal India)service and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

13 Enforcement

13.1 This "e-mail policy" is applicable to all employees of Coal India and Subsidiaries.

13.2 Each subsidiary shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Department would provide necessary technical assistance to the subsidiaries in this regard.

14 Deactivation

14.1 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.

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

15 Review

15.1 Future changes in this Policy, as deemed necessary, should be made by Systems Division,Coal India with approval of the Director(T),Coal India after due consultations with E&T division.

Part-C

Password Policy of Coal India

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 Coal India Network. 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(6) and comprising of mix of alphabets, numbers and special characters.

3.5. Passwords should not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.

3.6. All access codes including user ID passwords, network passwords, PINs etc. should not be shared with anyone, including personal assistants or secretaries. These should be treated as sensitive, confidential information.

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

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

3.9. Passwords should not be revealed on questionnaires or security forms.

3.10. 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.

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

3.12. 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.

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

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

3.15. 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. The backend database should store hash of the individual passwords and never passwords in readable form.

4.3. 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 Coal India Network,and system/network administrators of Coal India 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 Coal India and Subsidiaries to adopt Open Source Software. The “Policy on Adoption of Open Source Software for Coal India and Subsidiaries” (hereinafter referred to as “Policy”) will encourage the formal adoption and use of Open Source Software (OSS) in Coal India and Subsidiaries.

1.4. Coal India and Subsidiaries 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 Coal India and all its subsidiaries.

2. How to comply

2.1. All Subsidiaries and CIL, 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. Coal India and Subsidiaries 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. Coal India and Subsidiaries 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 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. All data stored on the Servers i.e., Coal Net Database and the webservers will be backed up.

3. Complete Automated Backup Frequency and retention

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

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 Data Centre.

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 restores must be tested when any change is made that may affect 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 may be considered :

6.2.1.: You must have at least three copies of your data: the original production data and two backups.

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

6.2.3.: You must keep at least one backup offsite (in the cloud or in a remote site).

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 the backups are performed successfully and logs are to be maintained if they are successful/failed.

Part-F

Guidelines for Use of IT Resources

1. Introduction:

1.1. Coal India and Subsidiaries 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 User should take prior approval from the Implementing authority of their respective subsidiaries to connect any access device to the network.

2.2.2 User 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 eMail attachments received from unknown senders as they may contain malicious software.

2.2.5 User should report any loss of data or accessories to the Implementing authority of their respective organization.

2.2.6 User should obtain authorization from the Implementing authority before taking any Company issued desktop outside the premises of their organization.

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

2.2.8 Users should encrypt all sensitive information while the desktop.

2.2.9 By default all interfaces on the client system should be disabled and those interfaces that are required are enabled.

2.2.10 Booting from removable media should be disabled.

2.2.11 Users should be given an account with privileges on the client systems. User should not be given administrator privileges.

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

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

2.2.14 If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be immediately reported to the Implementing Department/Nodal Agency for corrective action.

2.2.15 Any Annual Maintenance Contract with service providers should include a clause that Hard Disk should be retained by the Coal India and Subsidiaries, 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.

3.2. A list of allowed software should be made available by the Implementing Department. Apart from the Software mentioned in the list, no other software will be installed on the client systems. Any addition to the list by the respective subsidiaries should be done under intimation to Implementing Department.

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 network printers and scanners

5.1. User should use a strong administrator password on the device to help defend against attacks and to prevent re-configuration by an unauthorized user.

5.2. Where the device supports Access Control Lists (ACLs), the devices should be configured to block all traffic from outside the Network IP range.

5.3. FTP and telnet server on the printer should be disabled.

5.4. User should disable any protocol or service not required.

6. Use of Portable devices

6.1. Devices covered under this section include Coal India issued laptops, mobiles, iPads, tablets, PDAs etc. Use of the devices should be governed by the following:

6.2. User should be held responsible for any unauthorized usage of access device issued by CIL/Subsidiary by a third party

6.3. Users should keep the devices issued by CIL/Subsidiary with them at all times 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.).

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

6.5. Users should be given an account with privileges on the client systems. User should not be given administrator privilege excepting where required on a temporary basis.

6.6. User should ensure that remote wipe feature is enabled on the Coal India issued device, wherever technically feasible. Users should not circumvent security features on their devices.

6.7. The concerned nodal officer of Coal India and Subsidiaries 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.

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

6.9. Lost, stolen, or misplaced devices should be immediately reported to the Implementing Department and the Implementing authority.

6.10. Data transmissions from devices to the services on the Coal India network should be over an encrypted channel.

6.11. When installing software, user should review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

7. External Storage Media:

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

7.2. Use of external storage media, by default should not be allowed in the Coal India network. If the use of external storage is necessary, due approval from the Implementing authority should be taken.

7.3. 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.

7.4. 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

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

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

7.7. Users should not allow USB device belonging to outsiders to be mounted on Coal India systems.

8. Use of External storage media by a visitor

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

8.2. 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 Coal India and Subsidiaries .

9. Authority issuing External storage

9.1. 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.

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

Enabling IT for Coal India and Subsidiaries and Subsidiaries (Points raised in the Meeting between HOD(systems) at Coal India,HQ Kolkata on 07/11/19.

- Data Center: All the existing Computer centers are to adhere to the Guidelines of Government of India for Data Centers. The link https://meity.gov.in/writereaddata/files/Annexure-1_sdc.pdf provides the basic recommendations of Meity. CIL and Subsidiaries should try to comply with most basic requirements as suggested in the document.
- Disaster Recovery: Appropriate levels of Data Redundancy is to be built into all the systems with Active mode Disaster Recovery center for Business critical applications. The DR site specifications should be similar to DC. The objective of maintaining DR site should be 100% recovery and business continuity without losing invaluable time.
- Digitisation: All extant Digital Initiatives like e-office, e-mail, Document Digitisation are to be enforced. Document management system should be in place in CIL and all subsidiaries.
- IT Assets: Centralised inventory of IT assets to be maintained.
- Biometric Attendance based on suitable technology should be in place.
- All transparency related policies declared by CIL should be incorporated in the IT systems.
- Data Connectivity with redundancy should be provisioned up to mine level for implementing IT enabled services.
- Corporate Websites of Coal India Limited should be STQC Audited as per Govt Guidelines.
- **Cloud Technology:**
  1. Cloud options are to be explored to optimise resources and put to use wherever possible.
  2. NIC Cloud or MEITY Approved Cloud Service Providers should be preferred.