The Orissa Minerals Development Company Limited

(A Govt. of India Enterprise)

Information Technology Policy
and
Procedures

Sourav Abasan
AG-104,2nd Floor, Sector-II
Salt Lake City, Kolkata-700091.
Ph:-03340169200, Website: **www.birdgroup.co.in**

1.0 Introduction and Policy Statement:

1.1 Policy Statement: The Orissa Minerals Development Co. Ltd. (OMDC) is committed to leverage Information Technology (IT) as the vital enabler in improving the customer-satisfaction, organizational efficiency, productivity, decision making, transparency and cost effectiveness and thus adding value to the business of Production & Marketing of Iron Ore & Manganese Ore and allied value added services. Towards this, OMDC shall.

- Follow best practices in Process Automation & Business Processes through IT by in house efforts / outsourcing and collaborative efforts with other organizations / expert groups / institutions of higher learning, etc, thus ensuring the quality of product and services at least cost;
- Follow scientific and structured methodology in the software development processes with total user-involvement and thus delivering integrated and quality products to the satisfaction of internal and external customers;
- Install, maintain and upgrade suitable cost-effective IT hardware, software and other IT infrastructure and ensure high levels of data and information security;
- Strive to spread IT-culture amongst employees based on organizational need, role and responsibilities of the personnel and facilitate the objective of becoming a world-class business organization;
- Enrich the skill-set and knowledge base of all related personnel at regular intervals to make employees knowledge-employees;
- Periodically monitor the IT investments made and achievements accrued to review their cost effectiveness.

1.2 This document sets out the Information Technology (IT) Policy and procedure for OMDC for the protection of its IT & ITES systems and defining baseline responsibilities for its IT & ITES security, equipment and file storage. "IT & ITES" refers to the IT network, hardware including portable media, system and application software, communication components including Local Area Network (LAN) and Wide Area Network (WAN) systems, documentation, physical environment and other information assets. It does not include IT systems those are not connected to the OMDC network and those properties which does not belongs to OMDC.

1.3 This Policy covers the IT & ITES systems/Networks for OMDC employees across all offices and the separate network provided for Evidence & Practice Information Management and Technology in order to manage OMDC websites and publishing systems.

1.4 The equipment covered by this policy includes:

a. Network Infrastructure – The equipment housed internally to provide the OMDC IT network, including servers, enclosures, racks, cabling, switches/hubs, Routers, wireless access points, firewalls, proxies, authentication systems and devices, NTEs, ATAs and remote access systems.

b. Desktops – Personal Computers (PCs) issued or provided to employees for carrying out their duties.

c. Laptops/Notebooks - Portable Personal Computers issued or provided to staff for carrying out their duties.

d. Mobile Phones/Blackberries - Digital communication devices issued or provided to staff for carrying out their duties.

e. Media/Portable Media – Electronic Storage Devices such as DVDs, CDs, memory sticks, Dongle and hard drives issued or provided to employees for carrying out their duties.

f. External Communications Infrastructure – Equipment used to connect OMDC to the external world including the Wide Area Network, analogue telephone lines, digital telephone lines, leased lines, LES/WES/Ethernet first mile circuits, ADSL circuits, SDSL circuits and all related equipment and services.

g. All related Facilities & Estates controlled IT media used in OMDC's meeting rooms.

1.5 The objective of this policy is to ensure: -

- **Confidentiality** of data and information assets are protected against unauthorized disclosure and incidents are promptly reported (see section 10.1.d).
- **Integrity** of data and information assets so that they are protected from unauthorized or accidental modification.
- **Availability** and accessibility of IT systems as and when required by employee.

1.6 This policy sets out the principles of IT security including the maintenance, storage and disposal of data and explains how they will be implemented at OMDC to ensure that there is a centralized and consistent approach to IT security.

1.7 One of the aims of the policy is to raise awareness of the importance of IT security in the day to day business of OMDC.

1.8 The policy supports the OMDC business objectives of ensuring that the security, integrity and availability of IT systems for the need of employee to access systems and services that are necessary for their job, within the limits imposed by this policy. It will also help to protect data from misuse and minimize the impact of service disruption by setting standards and procedures to manage and enforce appropriate IT security.

1.9 The policy supports the legal obligations of OMDC to maintain the security and confidentially of its information, notably under the IT Act 2000, the Copyright Patents and Designs Act and Indian Record Act, and also supports adherence to information governance standards set by the Government of India.

2.0 Scope:

2.1 This policy applies to all OMDC IT systems and those working at or for OMDC (Employees):

a. All OMDC employees (including staff/sub-staff of the organizations) in HO, Mines Office, regions and branches.

b. Contractors, agencies, vendors, customers and other outside agencies, where they are directly using OMDC's network.

c. Employees on deputation to OMDC from other organizations.

3. **Responsibilities**:

3.1 Defining responsibilities ensures that all users of OMDC IT systems are aware of their responsibilities to minimize the risks to IT security and operations. The HoD of IT Dept. is responsible for formulating and implementing the policy across the organization in consultation with MD/Director. He/She is *inter-alia* responsible for monitoring and reporting on the state of IT systems and security. HoDs/Business Heads are responsible for implementation of IT procedure, in their respective Dept. framed by IT Dept. MD/Director is vested full authority to implement the IT Policy across the organization.

3.2 Internal Procedure parts which are not covered in this policy and procedure will be framed in line with this policy with the approval of Managing Director for execution and administration.

3.3 Employees/Users who do not have administration rights over their issued equipment are responsible for ensuring that:

a. No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote log-in data secure (except where, it is necessary to disclose them to the IT department for administrative purposes) and to deny unauthorized third party access to OMDC systems. This is particularly important for home workers and when using wireless networks.

b. All reasonable care is taken to protect the security of IT equipment, when taken outside the offices. These are issued together with confidential data stored on it.

c. All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the OMDC IT department regardless of the working state of the equipment.

d. Sensitive data stored on portable IT equipment is kept to the minimum for business use and encrypted in order to minimize the risks and impacts, should a security breach or loss of that equipment occur.

e. Actual or suspected security breaches are reported as soon as they arise.

f. Only employees explicitly authorized by the OMDC ICT dismantle, repair or alter OMDC supplied IT equipments.

g. Further advice is contained in ***Annexure-A***.

3.4 Users who do have administration rights over their issued equipment are responsible for ensuring that:

a. No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote log-in data secure (except where necessary to disclose them to the OMDC IT or Technical Department for administrative purposes) and to deny unauthorized third party access to OMDC systems. This is particularly important for home workers and when using wireless networks.

b. All reasonable care is taken to protect the security of IT equipment, when taken outside the office, which are issued together with confidential data stored on it .

c. All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the OMDC IT department regardless of the working state of the equipment.

d. Contractors engaged by OMDC for providing IT services comply with this policy.

e. Sensitive data, stored on portable IT equipment, for business use, is kept to the minimum requirement and encrypted in order to minimize the risks and impacts, should a security breach or loss of that equipment occur.

f. Actual or suspected security breaches are reported as soon as they arise.

g. Only licensed or in house developed software, specifically required for their job within OMDC, is installed in the equipment for which they are responsible.

h. The equipment for which they are responsible, is used only for work purposes (no private use) and specifically their own job.

i. All due skill, care and attention is taken to ensure that no virus, Trojan spyware or other malware is introduced to their equipment or OMDC systems

j. All due skill, care and attention is taken to ensure that no configuration, miss-configuration or alteration to systems, software, equipment or infrastructure has any detrimental effect on the normal running, availability or stability of the OMDC IT Infrastructure as detailed in section 1.4.

k. Only employee/staff explicitly authorized by the IT/Technical Department's HoD for Operations dismantle, repair or alter OMDC supplied equipment subject to approval of Director (P & P)/MD. Further advice is contained in Appendix A.

4.0 Security:

4.1 Technical security measures will be put in place to protect OMDC systems from viruses and other malicious software, and all IT systems will be monitored for potential security breaches.

4.2 Contact will be maintained with the appropriate national security organizations to ensure that OMDC IT systems comply with and National standards and best practices regarding IT security management, including network connectivity.

4.3 Allocation of accounts to temporary workers using a generic username that cannot be mapped back to the user will not be allowed.

4.4 All relevant contracts with third parties will include standard Office of Government Commerce clauses on information security. All central processing equipment, including file servers, will be covered by third party maintenance agreements.

4.5 All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the OMDC IT Department/Technical department.

4.6 All IT equipment, including virtual systems, will be uniquely identified and recorded.

4.7 Environmental controls will be maintained in the server/communications rooms of all premises to protect key equipment. Smoking, drinking and eating is not permitted in these areas.

4.8 Records of all faults and suspected faults will be maintained.

4.9 All OMDC laptops must be encrypted with access to OMDC IT networks via a strong authentication method.

4.10 Access to premise server/communications rooms will only be with the express permission of the OMDC IT Department and accompanied by the appropriate representative.

4.11 Memory sticks and other portable media must be encrypted or have password protection when sensitive data is being transported outside secure offices.

5.0 Software protections:

5.1 Only licensed copies of commercial software or in house developed software and network connectivity (is the connection between OMDC IT systems and the OMDC intranet) are used by OMDC. The OMDC IT Department will maintain a register of all commercial software, including all software licenses, to ensure that OMDC complies with license conditions and relevant laws. Users must not install ANY externally developed software on OMDC IT equipment without prior written approval of the IT Department or where delegated, the Technical department.

5.2 All users are reminded that it is a criminal offence to make or use unauthorized copies of commercial software and that offender may be liable to disciplinary action.

5.3 Software products required by any department should be approved by the OMDC IT Department or Technical Department, prior to purchase. Unless otherwise directed all software purchasing and licensing will be carried out by the OMDC IT department, and employees/users must follow any instructions issued with regard to specific software or applications.

5.4 OMDC will minimize the risks of computer viruses through education, good practice and procedures, and application of robust anti-virus software and ensuring firewall policies, which follow appropriate national guidelines. Users must report any detected or suspected viruses, Trojan, spyware or malware on their computers immediately to the OMDC IT Department or Technical Department as appropriate.

6.0 Physical access controls:

6.1 Physical access controls to secure areas will minimize the threat to the OMDC IT systems through damage or interference. The OMDC IT Department will be responsible for access to all IT systems located in secure areas, with access being restricted using the principle of least privilege. An entry restriction system to the server/communications rooms at all premises will be implemented.

6.2 The server/communications rooms and store rooms for IT equipment will be locked at all times and the keys/codes will be held securely by the OMDC IT department.

6.3 Authenticated representatives of third party support agencies or other parties will be given access through specific authorization from the Procurement and IT in-charge. Such access, if granted, and will be supervised by OMDC IT Department representatives while on site.

6.4 No remote access to OMDC IT systems will be given to third parties at any time unless specific authorization is received from the Procurement and IT in-charge or the HoD of Technical Department. Such access, if granted, must be supervised at all the time.

7.0 User access control to the IT network drives:

7.1 User access to the IT network will be granted where access is necessary to perform the person's job following the principle of least privilege. Access will be modified or removed as appropriate when a person changes job or leaves OMDC. It will be the responsibility of the HR department to notify the OMDC IT Department and the Technical Department immediately of any changes required to access controls, and procedures will be established between the three teams to ensure this happens.

7.2 For those with existing access to the IT network, requests to change access permissions should be made to IT. These will be authorized by the IT in-charge who will, if necessary, check the requirement with the relevant HoD or line manager.

7.3 No individual will be given access to the IT network unless properly trained and made aware of his or her security responsibilities.

7.4 Each member of employee/staff will be provided with a USB drive. This storage space is free for the individual to use (subject to sections 7.5 & 7.6 below). If this storage limit is exceeded then the USB drive will be unable to save any additional data – it is individual's responsibility to manage this allocation.

7.5 'USB drives' remain part of the OMDC IT systems and OMDC has full rights of access to all data stored on its IT network. The content of USB drives is not routinely monitored but OMDC reserves the right to view content if there are reasonable grounds for doing so; for example to prevent fraud or suspected breach of OMDC policies. Further information is contained in the Email and Internet policy.

7.6 Users are not permitted to store entertainment files (including but not limited to music, pictures, video, electronic games) upon the OMDC systems. Files which have the same nature but are for work purposes must be notified to and approved via the OMDC IT department.

8.0 Disposal/reallocation of equipment:

8.1 Equipment allocated to an individual user (including memory sticks) must not under any circumstances be reallocated to any other user and must always be returned to OMDC IT for reallocation to ensure correct management of sensitive data.

8.2 Where equipment is obsolete for OMDC's business purposes but is still in working order and is deemed to be of use to private individuals, that equipment will be offered for sale. The Finance Department will be notified of any sums due from the buyer of the equipment.

8.3 Where the equipment is deemed to be of no use to private individuals, it will be either disposed of by the Disposal Committee (or successor organization) or returned to the manufacturer in accordance with the applicable law. Alternatively, it may be passed on to a properly registered charity who will seek to reuse the equipment. As a last resort the equipment will be passed to a properly registered waste carrier for certified recycling.

9.0 Email Communication and usage of Internet & Social Media:

9.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) should be avoided. Any form of harassment via email, whether through language, frequency, or size of message would be considered as offence and is subject to disciplinary action.

9.2 Official communications through e-mail, to be done using official e-mail ID unless there is any operational issue.

9.2 Use of Social Media (like Twitter, Facebook, LinkedIn etc.) should be done wherever possible to communicate with the stakeholders to inform them about various developments and activities of the company. However, contents published on the social media should have proper authorization and to be handled only by designated persons for this purpose.

9.3 No objectionable, frivolous or illegal activity should be carried out on internet that shall damage the company's business or its image.

9.4 Policy on usage of Internet:

9.4.1 Purpose

The purpose of the policy on usage of internet is to provide a guideline so that the bandwidth is not overburdened and security is not compromised. Such protocol/guidelines will also be applicable for use of company intranet.

9.4.2 Policy

Users will not misuse the internet by downloading contents which will not benefit the company or go to such sites which are not related to official work. Normal users will have access to OMDC's web sites only. If other sites are required by the user then that is to be approved by the HoD and communicated to the head of IT Deptt. /System in-charge to get the site accessible to user. Usage is monitored and HoD of IT Deptt./System in-charge may report to Competent Authority for any unethical downloading like music, movies etc through his/her Controlling Authority.

10.0 Security incident investigations and reporting:

10.1 The objective of security incident investigation is to identify detect, investigate and resolve any suspected or actual computer security breach. All security or any concerns or suspicions about security breaches should be reported, as soon as they arise.

IT systems are always subject to high degree of risks and therefore continue to be given top priority, and for this purpose:

a. Licensed anti-virus should be installed and should be updated on regular basis.
b. Firewall should be installed to protect the OMDC network from external attack.
c. Back-up of critical data and system configurations on a regular basis and storage of data in a safe place. Backup procedure is placed at **10.2**.
d. All security threats/incidents will be formally recorded and categorized by severity and actions taken thereon should also be recorded in accordance with prescribed procedure. Provision for safeguarding / protection of confidentiality of data / information is put in place especially with regard to sensitive information including Aadhaar, etc. in line with Government guidelines.
e. Users of IT system be imparted training on usage of related guidelines and procedures

10.2 Backup Policy

10.2.1 **Purpose**

The purpose of the policy is to provide a guideline to follow for backing up data on external media. Back up is taken to protect data from corruption of media or to use elsewhere if necessary.

10.2.2 Policy

Periodic back up is to be taken by each user every Friday and is properly labeled. However, every sensitive data like in-house computer applications or records will be backed up whenever changes are affected. Users will keep all data in a partition other than in the partition where system (OS) is loaded i.e. users should keep data in partition other than C:/drive. Files of incremental type will be kept in a pen drive. For users whose USB/DVD/Mobile HDD are blocked and are unable to use pen drive or DVD will temporarily copy the files in the file server and then use a machine where the port/DVD is open to import the files from the file server to the pen drive/DVD. After copying the file to a backup media such files will be removed from the file server. However, for files which are complete in nature (i.e. no future appending on the file) will be backed up in a CD/DVD using multi-session or Mobile HDD. Data backups taken on external media should be tested at least once a month. Proper record of backup and testing of media will be kept by the user. A copy of the backup will also be with HOD. CD/DVD/Pen media/Mobile HDD are required to be the items available from the IT Deptt./Stores/Material Deptt. so that for backing up, users can get the desired media from the IT Deptt./Stores/Material Deptt.

10.3 Incidents should be notified to the Head of Technical and/or in-charge of IT as appropriate, who will report incidents to the Business Head and Managing Director, in accordance with Incident Reporting Procedure. All security incidents that may have an impact on network connectivity will be reported immediately to in-charge IT.

10.4 All employees/users must report actual security breaches, or any concerns or suspicions about security breaches, as soon as they arise.

10.5 All actual security incidents will be formally logged, categorized by severity and actions recorded by the OMDC IT department, and reported to the Business Head/MD in accordance with Incident Reporting Procedures.

11.0 Disaster recovery and business continuity:

11.1 All business critical data will be replicated between servers at relevant locations so that if the servers in one location become unavailable, access is automatically switched to the servers in another location.

11.2 All data will be backed up onto tape libraries/USB Drive/Mobile Hard Drive/CDs/DVDs at each site so that data exist in four places (server and tape library at each site). Critical computer equipment must be fitted with battery back-ups (UPS) to ensure that it does not fail during switchovers or emergency shutdowns.

11.3 To minimize the risk to OMDC IT systems, robust disaster recovery plans will be put in place to ensure:

i) Identification of critical computer systems.

ii) Identification of areas of greatest vulnerability and prioritization of key users and user areas.

iii) Agreement with users to identify disaster scenarios and what levels of disaster recovery are required.

iv) development, documentation and testing of disaster recovery plans, including identifying tasks, agreeing responsibilities and defining priorities

v) recovery plans cater for different levels of incident, including loss of key user area within a building, loss of building(s), loss of a key part of the IT network, and loss of processing power

vi) the existence of emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel) and actions to be taken to return to full normal service

12.0 Maintenance of Official Website of the Company:

a. Contents uploaded on the website shall be regularly updated and archived as per relevant archival policy.

b. All content on the website should have proper approval or authorization before it is published and should be reviewed on regular basis.

c. Guidelines issued by Government/Government agencies regarding security, contents, design, style, etc. of the website from time to time should be followed.

d. All information published on the website should meet prescribed statutory requirements to bring more transparency about the working of the company.

13.0 Risk management:

13.1 The objective of risk management is to identify, counter and report on actual and possible threats to IT systems. The risk management will be periodically reviewed following the procedures of audit as per IFC (see cl.14).

13.2 Significant IT risks will be included in the OMDC risk register and will be made available to the Audit Committee.

14.0 Media Handling

14.1 Policy Statement

All electronic media and documents shall be securely handled to protect them from physical damage and/or unauthorized access.

Controls

14.2 Management of Removable Media

Usage of removable media which includes but not limited to USB devices, CD ROMs, magnetic tapes shall be restricted and based on prior approval. Inventory of all removable media (storage devices) shall be maintained and the media shall be physically secured and maintained, which not in use.

(A) Requirements:

i. Media containing classified information shall be labeled appropriately.
ii. Approvals from the authorized persons shall be taken for management of any removable media which includes USB devices, CD ROMs, DVDs, magnetic tapes, disks, flash disks.
iii. The following controls shall be implemented for the management of removable computer media.
   a. Computer media shall be stored in safe and secure environment both offsite and within the premises in accordance with the manufacturer's specifications.
   b. Data on re-usable computer media to be removed from OMDC premises shall be erased if it is not required.
   c. Classified information shall be stored on Desktop or workstation hard disk drives with appropriate protected by a password or encryption.
   d. When the storage media such as CD-ROMs, Hard disks and Tapes containing classified information become defective, they shall be physically shredded/destroyed so that they cannot be reused.

15.0 <u>Audit and Internal Financial Control(IFC)</u>:

15.1 The implementation of OMDC's IT policy and procedures will be subject to periodic review by both internal and external auditors and the subsequent recommendations will be agreed and action plans put in place and monitored.

15.2 Internal Financial Control (IFC) is implemented in the company. IFC is covering all transactions and controls are achievable through implementation of several control measures which are preventive in nature and automated. Detective controls and monitoring control are technology enabled which are achievable through efficient and effective IT Policy.

15.3 Breach of this policy would invite disciplinary action, wherever necessary.

16.0 <u>Compliance</u>:

16.1 Breach of this policy may result in disciplinary action in accordance with the OMDC Disciplinary Policy and Procedure (CD&A)/Standing Orders. Any breach of the law will be reported to the appropriate authorities.

17.0 **<u>Related Policies</u>:**

17.1 This policy should be read in conjunction with but not limited to the following policy and procedure documents:

- E Mail and Internet Policy of Govt. of India

- Disciplinary Policy and Procedure Incorporating Suspension Guidelines(CD&A Rule of OMDC)
- Risk Management Policy
- National Cyber Security Policy of Govt. of India
- Password Policy of Govt. of India
- Security Policy For User of Govt. of India
- Policy on Preservation of Document of OMDC
- Code of Conduct for Board and Senior Management.

18.0 Review:

18.1 This policy will be monitored by the IT Department to ensure it is fit for purpose and reviewed every 3 years or whenever necessity arises subject to approval of the Managing Director/ Board of OMDC.

19.0 Signatories:

On behalf of The Orissa Minerals Development Company Limited (Head Office)

Signed: ________________________________ Date: ______________________

On behalf of OMDC Mines

Signed: ________________________________ Date: ______________________

Appendix A

Good Practice Guide

Below is a summary of recommended Do’s and Don’ts for all users of OMDC IT systems. It is intended to complement approved OMDC IT policies and support new information governance standards set by the Government of India.

- **Do** ensure **that** you keep security in mind when working – If you have been sent a file or a web link, are you sure you can trust the person it came from, is this the type of thing they would normally send, does it ‘feel right’? Remember, lots of spam and viruses sent impersonate the e-mail address of a real person, so the e-mail may not have been sent by the person you think. Lots of viruses move from machine to machine as hidden files on storage devices. Remember, only IT equipment issued, or approved, by the OMDC IT Department should be used, except where personal PCs and laptops are used in accordance with the Home Working policy.

- **Do** report any errors or problems promptly – If you have an error or an issue, especially if it may be security related, please report it to the IT helpdesk quickly and with as much detail as possible. Reporting that you had a problem 3 days ago and you can’t remember the error message makes it almost impossible to track and correct the problem. Reporting promptly with details of which system (e.g. terminal server, e-mail) was affected, the date and time the problem occurred and the specific error message or event makes it much easier to find and fix the problem, and get you working again.

- **Do** think about what you are saving and copying onto the network and in e-mail. Does the file need to be there? How big is it? If you are saving an attachment out of an e-mail, remember to delete the copy in the e-mail to save using up double the space. If you are copying data from a DVD, think if it is necessary? If it is only for your use, can it stay on the DVD?

- **Do** take care of the equipment you are issued with, either permanently or on loan. Most of it is expensive and it may contain sensitive or confidential data.

- **Do** remember to return the equipment before leaving OMDC. All data will be securely erased by the OMDC IT Department. Please note that any personal data that has not been erased from returned equipment may be viewed by the IT department.

- **Do** keep passwords secure and never disclose them to anyone else. Passwords should ideally contain at least 9 characters with a mix of letters and symbols in upper and lower case.
- **Do** keep portable media, especially laptops, taken outside OMDC offices secure at all times. For example, do not leave them in boots of cars overnight, in overhead luggage racks or unattended in

other insecure areas. Where possible carry IT equipment in anonymous cases without a manufacturer's logo and avoid using laptops in public places where possible if confidential information may be visible to other people.

- **Don't** connect any equipment (Laptops, USB devices including storage devices, networking equipment, 3G/4G or upper version cards etc.) to OMDC IT systems unless it has been supplied or specifically authorized by the OMDC IT department. If in any doubt, confirm with the helpdesk before connecting anything.
- **Don't** download any Software, Software updates, Installation Packages, or Executable files from the Internet or external storage devices (USB sticks, external hard drives, CD-ROM, DVD etc.) onto OMDC IT systems unless specifically authorized by the OMDC IT Department.
- **Don't** install any software on any IT systems unless specifically authorized by the OMDC IT department. All software installs are normally carried out by the OMDC IT department and user installation of software is only authorized in special circumstances.
- **Don't** download, upload, store, copy or distribute any materials, data or software of a pornographic, obscene, indecent, racist, defamatory, libelous, sexist, offensive or otherwise unlawful nature (other than for properly authorized and lawful research, for which written notification must be given to the relevant Director).
- **Don't** attempt to circumvent the security and restrictions in place on the OMDC IT systems. These are in place to ensure a safe working environment for all employees and maintain the security and resilience of the OMDC network.
- **Don't** leave portable media unattended in public places where there is a potential for opportunist theft or compromise (i.e. installation of a virus/worm etc.).
- **Don't** connect any third party issued equipment or storage devices into another computer or network unless you are sure that the network is correctly maintained and up to date Anti-Virus protection is in place. Viruses and malwares can be transferred using machines and storage devices connected to compromised computers or networks.
- **Don't** use the OMDC network, including USB drives, for the storage of music files, as these may breach copyright permissions. Private photographic and or video files should not be stored on USB drives as they use up large amounts of space.

For further information and advice please contact the OMDC IT department or log a call on email/ IT Helpdesk.

-x-

Appendix B

Version Control Sheet

Version	Date	Author	Replaces	Comment
Information Technology Policy V.1	24-01-2018	IT Deptt.		

Abbreviations:

SL	Acronyms	Description
1.	IT	Information Technology
2.	ITES	Information Technology Enabled Services
3.	WAN	Wide Area Network
4.	NTE	Network Termination Equipment
5.	ATA	Analog Telephone Adaptor
6.	PC	Personal Computer
7.	DVD	Digital Video Disc
8.	CD	Compact Disc
9.	LES	LAN Extension Service
10.	WES	Wholesale Extension Service
11.	ADSL	Asymmetric Digital Subscriber Line
12.	SDSL	Symmetric Digital Subscriber Line
13.	USB	Universal Serial Bus
14.	HDD	Hard Drive
15.	IFC	Internal Financial Control
16.	VLAN	Virtual Local Area Network
17.	VPN	Virtual Private Network
18.	MPLS	Multi-Protocol Label Switching
19.	OS	Operating System
20.	NTE	Network Terminal Equipment.

-x-