Bombay Oxygen Investments Limited
(Formerly known as "Bombay Oxygen Corporation Limited")

Information Technology Policy

INTRODUCTION

Information Technology Framework for Non-Banking Financial Company (NBFC) Sector ('Master Directions') were issued by the Reserve Bank of India (RBI) on 8th June, 2017. The broad intention of Master Directions was to enhance safety, security, efficiency in information technology processes leading to benefits for NBFCs and their customers.

The Master Directions require the NBFCs with asset size below Rs.500 crore to formulate and adopt an Information Technology (IT) Policy which commensurate with the size, scale and nature of the business carried out by NBFC and which will act as a framework for usage of IT resources within the organization.

Keeping in mind, the directions issued by the RBI in this regard, the following internal policy ('IT Policy' or 'Policy') has been formulated and adopted by the board of directors of the 'Bombay Oxygen Investments Limited' ('the Company' or 'Bomoxy').

For the purpose of this Policy, the term "IT" would include but not be limited to the Company's IT network, hardware including portable media, system and application software, communication components including telephone and WAN systems, documentation, physical environment and other information assets.

PURCHASING POLICY

Objective and Scope

The objective of this policy is to outline the procedure by which the company acquires and disposes of systems for Partners, Executives, and Employees. The goal of the policy is to ensure that each user has a suitable system to perform his/her assigned responsibilities while also providing judicious services of company resources.

This Policy applies to all the employees and also consultant and to the purchase of all laptop and desktop computers and other peripherals. In the context of this policy, a "System" is defined as a complete working computer system with operating system and office applications and other system software.

Rules for System Purchase

IT Department will be solely responsible for purchase of all the systems and its peripherals. Company has a centralized purchasing system and the benefits of the process include the following.

- ✓ Ensuring the top officers, executives and the all the other employees have up-to-date

computer systems.

- ✓ Requiring that computer system or peripherals purchases are reviewed by IT Team.
- ✓ Consolidating purchasing into large orders to lower cost associated with acquisition and deployment.
- ✓ Maximizing value by working with preferred vendors.
- ✓ Reducing the total cost by purchasing standardized configurations.
- ✓ Centralizing record keeping to facilitate effective planning, maintenance, upgrades and disposal.

All systems and peripherals must be made with the company's preferred suppliers and online and conform to set of company's specified standards models with the following exceptions:

- ✓ Partners require an alternative to the standard configuration - Must be approved by the board of Managing Committee
- ✓ Executives and Trainees whose specific technical configuration – Must be approved by the HOD

Preferred Vendors and Service Providers

The company has negotiated purchasing contracts with selected vendors and service providers. Utilization preferred vendors help ensure that the company receives the maximum value for its purchasing. The relationship also includes special access to warranty and other services that assist IT Team in fixing problems and lower the cost of the equipment.

Standard Models

The IT Department maintains a standard desktop and a standard laptop configuration that will meet the general computing needs of most users.

Purchasing Schedule

The IT Department schedules the purchases of systems or peripherals after the request from the users. And also purchase new systems for replacing disposed system which is not capable up to the level of the user or technology ends.

Delivery of System

Once the system has been purchased and setup, the system will become the property of the respective department or vertical. The IT team will hand over to the user after completing the signing of IT policies and other relevant polices.

Retention/Return of System

The user who does not intent to retain the system after retirement or cessation of service during the life span of the system can return the same to the IT Department. The IT Department shall issue necessary clearance report to the vertical as well as HR Department.

Loss/Theft of System

The user shall be personally responsible for safe custody of the computer system or laptop. In case of theft or loss of system or peripherals, the user shall be responsible for the same and for any replacement, he has to remit the value of the system with the company.

Refresh Cycle

The systems are replaced once in a five years cycle or more or when the technology ends its life.

POLICY FOR SAFETY AND SECURITY OF IT ASSETS

Introduction

Information and information systems are important assets to every organization and it is essential to take all the necessary steps to ensure that they are comprehensively protected, available and accurate to support the operation and continued success of the company all times. The Information Security and Equipment Policy is a key component of the company's overall information security management framework and is designed to:

- Provide a corporate framework in which security threats to our Information Systems can be identified and managed;
- Illustrate the CCGs commitment to the security of information and information systems;
- Provide accepted formal procedures to ensure a uniform implementation of security measures;
- Introduce and formalize procedures to minimize the risk of unauthorized modification, destruction or disclosure of information; and

  Note: these objectives can only be achieved if every staff member observes the highest standards of personal, ethical and professional conduct in relation to the handling and management of information.

For Physical Damage, Loss, Theft etc.

1. All the Users whosoever is allotted with Desktop, Laptop, Printers, Hard drives, CDs or any other materials (referred as IT Assets of Bomoxy), whether dedicatedly or temporary for specific assignment, shall use and deal with these assets with utmost care and precaution so as to prevent them from any physical damage, loss, theft or other effect hampering its proper functioning.
   (Refer Annexure for General Laptop or Desktop Acceptable Use Rules & How to Avoid Laptop / Desktop Theft)

2. No IT Assets especially Desktop, Laptops, Pen Drive and Datacard shall be given to other person without consent from the partner in-charge and IT Department.

3. In case of any damage or loss or improper functioning being noticed / observed for any of the IT Assets, the same shall be reported to the IT department immediately for necessary action. IT department shall take required action to make repair / rectification / correction or replacement for smooth functioning of such IT Assets.

4. All users are personally responsible for the security and safety of their assigned IT Assets and will be fully liable if stolen, lost, destroyed or not returned. All users will be required to reimburse for the full replacement cost of the laptop/ desktop if it is stolen, lost or destroyed in full. The replacement cost will be determined by the IT department at the time of loss.

5. The costs of partial damages of IT assets, in case the same need to be replaced or repaired, shall be recovered in full from the user allotted with such assets or person causing the damages due to negligence and / or careless handling of the assets.

6. IT department shall maintain a register recording all such incidents and reasons for damages / non-functioning of the assets.

For Regular Maintenance & Backup

1. All the users are required to give their dedicated laptops/ desktops, at least once in two months to IT department at office for regular maintenance, back up of data, virus definitions update and other updates. IT department in consultation with the respective Vertical Heads will define a schedule for submitting the Laptops. In case, the user is not able to give the laptop on a particular date, he will intimate to the IT department and concerned vertical partner.

2. For the Laptops/ Desktops allotted from the Pool Account, the same be returned back to IT department once the assignment is over and all the data be saved in the office server. In specific cases / longer duration assignment (more than 2 months) or in case pool laptop/ desktop given dedicatedly for regular client, they need to be given back as per schedule of regular maintenance of dedicated laptops/ desktops.

Prohibited Practices with IT Assets

Any activity, action or lack of action on the part of a user that damages the image of Bomoxy or compromises security or confidentiality is prohibited. Examples of prohibited practices include:-

1. Installing new desktops/equipment or upgrading equipment or adding peripheral equipment without prior approval by the IT Department.
2. Downloading and/or installing programs that are not specifically approved by the IT Department.
3. Using unlicensed software. Users may not copy and share software that is installed on their desktops or laptops with other users.
4. Using programs or Internet web sites that compromise the privacy of customers or employees.
5. Removing or compromising desktop virus protection programs.
6. Opening email attachments that are inappropriate or from someone you do not know.
7. Using Firms provided IT equipment for non-business reasons or for personal gain.

8. Unauthorized attempts to break into any workstation.
9. Unauthorized access to Firms files, programs, databases or confidential information.
10. Sending or posting confidential files to unauthorized persons.
11. Failing to fully cooperate with IT security investigations.
12. Allowing co-workers or other users to use your desktop without approval of your manager or by the IT Department.
13. Sharing password information or displaying it in plain view on or around your desktop. Users must secure their passwords and not reveal them to others.
14. Do not move Desktops Machine or any of its components like monitor, keyboard and mouse without notification and approval of IT Dept.

Annexure to Policy for Safety & Security of IT Assets

Users shall use Bomoxy provided IT Assets responsibly and for company business purposes only.

General Laptop or Desktop Acceptable Use Rules

1. Every employee working from office will be entitled for a laptop or desktop or other peripheral devices like Pen Drive / Data Card / Webcam / Flash Drives etc. only after the approval of head of the department.
2. Data Card should only be used while the employee is travelling. In office premises one should use LAN Network for internet access.
3. Active desktops and laptops may not be left unattended for prolonged periods of time. Users should secure their workstation whenever he or she leaves the desk by applying the OS based auto lock feature.
4. Bomoxy's information displayed on screens or on reports shall be treated as confidential and private. Users must guard such information from unauthorized access or use. Any employee-signed confidentiality agreement shall fully apply to information accessed with Bomoxy's IT Assets.
5. Managers are responsible to ensure that their employees are adequately trained on appropriate use of IT equipment and that they adhere to this policy.
6. Users should regularly back up the data on the laptop/ desktop on the network folder on the Server as a safety precaution against hard drive failure.
7. All laptops & Desktops should have Bomoxy's Licensed Antivirus Software Installed. If you don't have one installed, please contact the IT Team.
8. All system should be installed with Bomoxy Screen Saver & Desktop Background.
9. Since the laptop's keyboard and touch pad are permanently attached to the rest of the system, make sure that your hands are clean before using them. Because hand lotion is a major contributing factor to dirt and dust, please make sure your hands are free from lotion before using the computer. It is costly to change a laptop keyboard and/or touch pad that has been damaged by excessive dirt.
10. Do not place drinks or food in close proximity to your laptop.

11. Extreme temperatures or sudden changes in temperature can damage a laptop. You should NOT leave a laptop in an unattended vehicle.

12. When using the laptop, keep it on a flat, solid surface so that air can circulate through it. For example, using the laptop while it is directly on a bed can cause damage due to overheating.

13. IT Assets provided by the firm shall be kept in secure manner so that the user's household members and others do not have access to them.

How to Prevent Laptop/Desktop Theft

Laptops, desktops, tablets and cell phones are necessary tools your employees use to get their everyday job duties completed. However, laptops and other small personal electronic devices are desirable items for thieves. Since laptops can easily be resalable, thieves often target them to make a quick profit.

If an employee's personal laptop/ desktop is stolen, it'll probably only affect them. But if their stolen laptop/ desktop contains work information, or is owned by the company, that employee's job and the security of the company could all be affected in minutes.

To minimize the risk of theft, below are the few suggestions to the employees and aim to keep their laptop/ desktop (and all the data it contains) safe.

1. Use strong passwords, change passwords frequently and avoid setting up automatic sign-ins. This will make it more difficult for thieves to log on to your computer and access your personal information.
2. Don't write down your passwords. If you must write your passwords down, don't keep the list close to your laptop (for example, on a sticky note kept in your laptop bag).
3. Never leave your laptop in an unlocked car.
4. Never leave your laptop in plain sight in your locked car. Lock it in the trunk and make sure no one sees you put it there.
5. Carry your laptop in something other than a laptop bag. This may seem unusual, but using a laptop bag makes it very obvious to thieves that you are carrying a laptop. Use something more inconspicuous, such as a backpack or messenger bag.
6. Lock up your laptop with a security cable. Attach it to a desk or other heavy stationary object. This visual deterrent will make your laptop less appealing to a thief.
7. Always keep your laptop in your sight. Don't leave a meeting or a conference room without your laptop—always bring it with you. You never know who could have access to that room, even if you're only gone for a few minutes.
8. Be especially diligent when traveling—airports are a common place for laptop theft. Also be careful in taxis, hotel rooms, restaurants and coffee shops.
9. Encrypt and back up data and information. The loss of important data and information would probably be more devastating than the physical loss of the laptop/ desktop.
10. If your laptop/ desktop is stolen, report it right away. Tell police the make, model and serial number so a complete report can be filed and the chances of getting your laptop/ desktop back are greater.

If a theft does occur, immediately notify IT Department.

EMAIL & INTERNET POLICY

The Bomoxy has clear standards relating to the use of e-mail, Internet and intranet and the deliberate or accidental misuse of electronic systems. The procedures cover use of any systems used to store, retrieve, manipulate and communicate information (e.g. telephone, e-mail, Skype, IT systems and the Internet). All employees and third parties are required to familiarize and adhere to them.

Acceptable email use policy

Use of email by employees of Bomoxy is permitted and encouraged where such use supports the goals and objectives of the business.

However, Bomoxy has a policy for the use of email whereby the employee must ensure that they:

- comply with current legislation;
- use email in an acceptable way;
- do not create unnecessary business risk to the company by their misuse of the internet.

Unacceptable behavior

The following behaviour by an employee is considered unacceptable:

- use of company communications systems to set up personal businesses or send chain letters;
- forwarding of company confidential messages to external locations;
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal;
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment;
- accessing copyrighted information in a way that violates the copyright;
- breaking into the company's or another organisation's system or unauthorised use of a password/mailbox;
- broadcasting unsolicited personal views on social, political, religious or other non-business related matters;
- transmitting unsolicited commercial or advertising material;
- undertaking deliberate activities that waste staff effort or networked resources;
- introducing any form of computer virus or malware into the corporate network.

Monitoring

Bomoxy accepts that the use of email is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's email resources are provided for business purposes. Therefore, the company maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the company also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees.

Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record. [These procedures will be specific to your business. They should reflect your normal operational and disciplinary processes. You should establish them from the outset and include them in your acceptable use policy.]

Agreement

All company employees, contractors or temporary staff who have been granted the right to use the company's email services are required to sign this agreement confirming their understanding and acceptance of this policy.

Email Best Practices

- Writing emails:
  - Write well-structured emails and use short, descriptive subjects.
  - Use bullet points were possible.
  - Sentences used in the Email can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations such as OMG, LOL etc. and characters such as smileys however, is not encouraged.
  - Signatures must include your name, job title and company name. A disclaimer will be added underneath your signature (see Disclaimer below).
  - Users must spell check all mails prior to transmission.
  - Don't click Send before re-reading your entire email. Many mistakes can be avoided in this way.
  - Do not send unnecessary attachments. Compress attachments larger than 5 MB before sending.
  - Do not write emails in capitals.

- Beware of viruses:
  - Do not click on any links or open any attachments of unsolicited or suspicious looking emails. These messages could infect your computer with a virus.

- Beware of phishing:
  - If you receive an email from a bank or any other institution, asking you to click on a link and update your details, DO NOT CLICK on the link. Do not be fooled if the sender appears to have some of your private details. This information can be obtained through Facebook, Linked-in and other social media websites. Instead, go to the company website by typing in the URL in a web browser, or call the company.

Confidential Information

Do not send credit card details, social security numbers, or other confidential information via email. If you need to send confidential information, check with your IT Head for safe methods.

Passwords

Use a combination of words, numbers and special characters for passwords. All passwords must be made known to the Firm. The use of passwords to gain access to the computer system or to secure specific files does not provide users with an expectation of privacy in the respective system or document.

Email Accounts

All email accounts maintained on our email systems are property of the firm. Passwords should not be given to other people and should be changed once a month. Email accounts not used for 60 days will be deactivated and possibly deleted.

Disclaimer

The following disclaimer will be added to each outgoing email:
DISCLAIMER:- This e-mail message may contain confidential, proprietary or legally privileged information. It should not be used by anyone who is not the original intended recipient. If you have erroneously received this message, please delete it immediately and notify the sender. The recipient acknowledges that Bombay Oxygen Investments Limited are unable to exercise control or ensure or guarantee the integrity of/over the contents of the information contained in e-mail transmissions and further acknowledges that any views expressed in this message are those of the individual sender and no binding nature of the message shall be implied or assumed unless the sender does so expressly with due authority of Bombay Oxygen Investments Limited.

Before opening any attachments please check them for viruses and defects.

Please do not print this email unless it is absolutely necessary.

BUSINESS CONTINUITY PLANNING (BCP)

A Business Continuity Plan (BCP) is a document that outlines how a business will continue operating during an unplanned disruption in service. It's more comprehensive than a disaster recovery plan and contains contingencies for business processes, assets, human resources and business partners – every aspect of the business that might be affected.

Plans typically contain a checklist that includes supplies and equipment, data backups and backup site locations. Plans can also identify plan administrators and include contact information for emergency responders, key personnel and backup site providers. Plans may provide detailed strategies on how business operations can be maintained for both short-term and long-term outages.

A key component of a Business Continuity Plan (BCP) is a disaster recovery plan that contains strategies for handling IT disruptions to networks, servers, personal computers and mobile devices. The plan should cover how to re-establish office productivity and enterprise software so that key business needs can be met. Manual workarounds should be outlined in the plan, so operations can continue until computer systems can be restored.

There are three primary aspects to a Business Continuity Plan for key applications and processes:

- High availability: Provide for the capability and processes so that a business has access to applications regardless of local failures. These failures might be in the business processes, in the physical facilities or in the IT hardware or software.

- Continuous operations: Safeguard the ability to keep things running during a disruption, as well as during planned outages such as scheduled backups or planned maintenance.

- Disaster recovery: Establish a way to recover a data center at a different site if a disaster destroys the primary site or otherwise renders it inoperable.

BCP shall be designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster. Bomoxy should follow the above mentioned BCP which may be reviewed every year. The process will envisage the impact of any unforeseen natural or man-made disasters on the Company's business.

- ✓ Following Measures we adopt for BCP :

    1) Auto backup at prescribed time every day.
    2) Weekly Backup to Hard drive and sent to outside.
    3) Proper Power backup.

- ✓ IT Team of the company shall ensure adherence to business continuity and Disaster Recovery Plans (DRP), provide training to the staff for proper implementation of plans and conduct regular testing and upgrading of these plans, whenever required.

- ✓ Senior management will assess the greatest risks, the techniques to mitigate, control, or limit the risks, the actions are required to address the greatest exposures including activation of a DRP, and an estimate of costs.

SYSTEM GENERATED REPORTS

The IT Team having various logs like system logs, Security Monitoring Log of user activity, System behavior, virus alerts, phishing, malware attack, installing of software, hardware change, copy and deletion of files, etc. The logs record communications about programs and system functions.

System Logs

System Log provide a commercial solution for log collection, analysis, and reporting. Log management systems provide a configuration interface to manage log collection, as well as options for the storage of logs - often allowing the administrator to configure log retention parameters by individual log source. At the time of collection, log management systems also provide the necessary nonrepudiation features to ensure the integrity of the log files, such as “signing” logs with a calculated hash that can be later compared to the files as a checksum. Once collected, the logs can then also be analyzed and searched, with the ability to produce prefiltered reports in order to present log data relevant to a specific purpose or function, such as compliance reports, which produce log details specific to one or more regulatory compliance controls.

Security Monitoring Log

Monitoring an information technology system is a recognized method of providing situational awareness to a cyber-security team, and monitoring tools, such as SIEM and Log Management systems, are heavily utilized by enterprise IT departments for this reason. Improved situational awareness can also benefit industrial networks, although special care needs to be taken in determining what to monitor, how to monitor it, and what the information gathered means in the context of cyber security.

Policy Review

The implementation of the Policy shall be subject to periodic review at least once in a Quarter or any update or adoption of new policy as may be decided by the Board of Directors. The adopted policy or summary will be circulating to the users on timely basis.

Disclaimer

This policy are intended solely for the use of the individual or entity to whom they are addressed and may contain information which is privileged, confidential or prohibited from disclosure or unauthorized use. Any unauthorised review, use, disclosure, dissemination, forwarding, modification, distribution, publication, printing or copying of policy or any action taken in reliance on this is strictly prohibited and may be unlawful.

Use any other contents or alternation of this policy contents is not allowed, If there is evidence that you are not adhering to the guidelines set out in this policy, the company reserves the right to take disciplinary action, including termination and/or legal action.

Questions

If you have any questions or comments about this Policy, please contact Ms. Hema Renganathan (hema@bomoxy.com). If you do not have any questions Bomoxy presumes that you understand and are aware of the rules and guidelines in this Policy and will adhere to them.