IT Policy

For

Employees on Payroll, Contract and Consultants

Issued On – July 14, 2015
Version – 1.0

Policy Nomenclature

Policy Title: IT Policy

Policy Authorizer: COO

Decision

☑ □

Cognizant Officer (Person handling queries relating to the policy):

Name: Kishore Karmakar

Department: IT

Email Id: Kishore.Karmakar@ibc24.in

Extension:125

Table of Contents

1.0 Introduction

This document describes general requirements and responsibilities for computer use, network access, user administrative rights and prohibited activities.

2.0 Scope

It applies to all permanent & temporary employees of IBC24 and PAN India .

General Guidelines

a) Responsibilities of IT

The Information Technology Department has overall control and responsibility for computer systems, software, and network components. The Information Technology Department shall provide support for business computer systems and related network systems. Business computers are those systems that have supported hardware, standard load set and are properly joined to the IT Department Windows Active Directory domains. The Information Technology Department shall provide computers for normal business activities to designated users.

b) Responsibilities of User

Users shall use computer resources for business purposes. Computers are assigned to users to perform normal business activities, email and office applications. Other business uses are not specifically prohibited; however such uses should be presented to the Information Technology for review and approval.

c) Prohibited Activities

i. Users shall not use computer resources for non-business activities.
ii. All files on IT Department network components and computers are company property. File contents and network activities may be reviewed.
iii. Inappropriate use of computer resources shall call for disciplinary action.
iv. All software that is loaded on a computer or the network file systems shall be properly licensed. No unlicensed or pirated software shall be loaded or used.

v. Users shall not operate Web sites on their computers or with Network resources. Users shall not run experimental servers, workstations, or other devices on the Network without *explicit* permission from the IT Manager.

d) **User Administrative Rights**

i. Administrative rights by individuals on assigned computers shall be limited. Usually, individuals shall NOT be granted administrative rights on an assigned computer.

ii. User privileges are limited to prevent users from loading non-business related software, unlicensed software or otherwise modify the computer and decrease its capability to perform normal business functions or prevent required administrative activities by the IT Group.

Internet and Intranet Policy

1.0 Purpose

To establish consistent guidelines on the appropriate use of Internet / Intranet access throughout the Organization.

2.0 The Policy

The access provided to the Internet / Intranet and other networks are only provided for business purposes. The use of the Internet resource is only authorized when that use is in conjunction with valid work or project-related requirements. The use by any employee for any other purpose may subject the employee to disciplinary action up to and including termination.

Examples of improper uses of the Company-granted Internet access are using the access for:

a) Viewing or transferring obscene, pornographic, abusive, and slanderous, defamatory, harassing, vulgar, threatening and/or offensive material.

b) Downloading or uploading (including posting) material containing any comments that would violate the business ethics and conduct, or any content prohibited by law or regulation.

c) Unauthorized viewing or transferring of material that is confidential or proprietary to the Company.

d) Communicating, disseminating, or printing of any copyrighted materials in Violation of copyright laws.

e) Using, copying or downloading proprietary software when not authorized to do so.

f) Using a computer system as a conduct for unauthorized access attempts on other computer systems.

g) Using a corporation owned system for private purposes or for purposes not in the direct interest of the corporation.

h) Uploading, downloading, modification, or removal of files on any node in the Network for which such action is not authorized.

i) Any other activity deemed by the Company to be in conflict with the intent of this policy. (This list is not intended to be all-inclusive.)

Company owned computers and associated computing components are property of the organization. The Organization will track usage of these resources through a variety of reporting techniques. The Company reserves the right to conduct this monitoring as well as accessing and viewing any data on any company-owned computer or systems. As a result of this monitoring, an employee's use of the Internet and any Internet material is not private. Even when Internet materials are erased, it is still possible to recreate the information. Therefore, the privacy of Internet materials cannot be ensured to anyone.

3.0 Procedure

a) Copyright material may not be duplicated or used in any manner that infringes on the copyright.
b) Software shall be obtained from "trusted" source sites only and always scanned for viruses.
c) IT Department shall be contacted if there is any query about file download sites or virus-scanning software.
d) Using, downloading or uploading of software protected by a license agreement shall only be done in strict compliance with the license agreement.
e) In all electronic communications, proper etiquette shall be followed to avoid claims of Defamation, sexual harassment, and the generation of offensive & Communication.
f) It shall be assumed that any message or information sent using the Internet /Intranet is available to the public.
g) The Internet / Intranet system shall not be used to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job-Related

solicitations.

h) All employees with access to the Internet or Intranet shall Understand and agree to comply with the provisions of the policy.

i) Employees aware of the improper use of Internet or Intranet shall notify their immediate supervisor or the Personnel Department.

Electronic Mail System Guidelines

1.0 Introduction

a) The guidelines have been designed to help employees understand the role of electronic mail & to make them aware of the risks inherent in using the system.

b) It is also required to distinguish between the appropriate & inappropriate uses.

c) The goal is to enable employees to use the system in a way that is most effective for them, their recipient & the Organization.

2.0 The Purpose of Electronic Mail

The electronic mail system has been put in place in order to help you obtain and share information more quickly and effectively with those with whom you do business. Electronic mail has the capability to do this due to three factors:

a) **Reduced message transfer time.** Through the use of electronic mail, files, documents, spreadsheets, reports, and databases can be quickly passed from one party to another. The delivery delay is typically far shorter than that of conventional mail.

b) **High reliability of delivery.** This pertains especially to the routine text messages that are sent through the electronic mail system. The probability of delivery failure for electronic messages is much lower than through conventional telephone and paper message systems.

3.0 The role of electronic mail.

Electronic mail is to be used for business purposes only. An E-mail message should be written only if it has a legitimate business reason. E-mail is **not** to be used as a substitute for direct, face-to-face dialogue. It is the belief of management that timely, in-person communications are an important element of Company name's culture and success.

4.0 Security and Privacy

a) *Security*

i. *Mailbox invasion*

Upon receiving access to E-mail, each person will be assigned his or her own unique identification and password. If used properly, this will generally secure their electronic mail from viewing by unauthorized parties. To reduce the risk of unauthorized access, the user should change his or her password frequently. Some suggestions to follow when choosing a password:
The password should be at least 6 characters long.

It should not be a word or name that might easily be guessed; for instance, the first name of the user's spouse or child is a bad password. It should not be based on a letter pattern, such as "AAAAA," or "ABCDE" or "QWERT".

Your e-mail password is synchronized with the network. Only you have the right to give others access to your mailbox. Please use discretion when granting this access.

The password should not be written down, or if it is, it should be kept away from the computer. If written, there should be no writing on the paper to identify it as a password.

Users should sign off the electronic mail system if they intend to be away from their desk for an extended period of time. When leaving for the day, the system should be logged off the electronic mail system, as well as the network.

ii. Message Interception

Although the Company name E-mail system is secure, it is **not** recommended for highly confidential communications. A good rule of thumb to follow: If information is sensitive enough that you would not leave it on top of a desk in an unlocked office for fear of the wrong person seeing it, it should probably not be sent via electronic mail.

Internet Mail - **No confidential information should be sent to destinations via Internet mail.** The Internet is generally unregulated and open to access by virtually anyone with a minimal investment. Any messages sent to destinations on the Internet are especially vulnerable to interception, and should **not** contain material or attachments of a confidential nature.

Third party private messaging systems - Caution should be exercised, on sharing of information while interacting with any business partner or vendor.

Internal/Corporate e-mail - Avoid the risk for the messages that are sent to the wrong person through errors in addressing the electronic mail, or that they are printed by the recipient and then seen by others.

The most common cause of message interception is carelessness on the part of the sender or recipient. Messages are printed, then later thrown in the trash where they are found by others. Or, mistakes are made in addressing messages, causing the mail to be sent to the wrong party.

b) Privacy

ELECTRONIC MAIL SYSTEM IS THE PROPERTY OF COMPANY AND IS TO BE USED SOLELY FOR COMPANY'S BUSINESS PURPOSES. All communications are company records. IBC24 reserves the right to monitor the electronic mail system and communications to ensure the company's legitimate business interests in the proper utilization of its property. **IBC24** reserves the right to access and use, at any time and without notice, all communications sent over its electronic mail system for any purpose. As with other forms of company communications, employees do not have any personal privacy rights in any matter created, received, or sent from the **IBC24** E-mail system.

For privacy reasons, employees should not attempt to gain access to another employee's personal file of E-mail messages without the latter's expressed permission.

iii. Legal and Other Considerations

Just as the electronic files of the Corporation are considered part of the company records for legal purposes, so too are the messages in the electronic mail system. Numerous court cases have determined that documents and messages stored electronically can and will be recognized as equivalent to paper documents. Even informal communications via electronic mail can be subpoenaed, and are potentially as damaging as any other company records. For that reason, the following rules should be observed when using Electronic mail:

D**o not retain messages any longer than they are needed.** Delete messages from your inbox, message log, and any folders frequently, subject to compliance with Company's Records Retention Policy.

Electronic mail messages are an inappropriate vehicle for formal documentation. Communications, issues, and concepts that are to be retained per the guidelines for records retention should be placed in an alternative, more appropriate form, such as a memorandum, specification, or report. The electronic mail system is to be used as a **transit mechanism** only, and not a records repository.

There should be no display or transmission of sexually explicit images, messages, or cartoons, or any transmission or use of e-mail communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs. Any employee who violates this prohibition will be subject to disciplinary action, up to and including termination.

iv. Resource Conservation

Ineffective use of Electronic mail can have a costly impact on the resources of the company. This includes the tangible costs of the hardware and software required to operate the system, as well as the increased cost in "people time" that misuse of Electronic mail can cause. The following guidelines have been established to help you optimize your time and system performance:

Delete messages from your mailbox as soon as possible.

Be selective in attaching files to your messages. Embedded Word, Excel, and PowerPoint files take up a lot more space than the simple text messages. When it is necessary to include large attached files, **compress the files before sending them.** This will reduce the amount of space taken up by the attachments, sometimes dramatically.

When replying to messages, **include at least a thread of the original message** you are replying to, in order to remind the recipient of the original topic of discussion. If the message is short, you may choose to attach the entire original message.

Do not request a receipt or confirmation of message delivery unless you really need it. Set it off as a default.

Do not send or forward chain letters. They are a waste of time and company resources, and in some cases can be illegal.

Review and if necessary **revise your private mailing lists** at least once a month to keep them current. These will not be updated by the system administrator, as will the public directory.

Avoid "saturation mailing" by being selective in whom you send mail to.
This not only wastes the time of the recipient by forcing them to read unnecessary messages, but also multiplies the space needed to store all the duplicate copies of the message.

v. Interpersonal Aspects

Some guidelines to follow in order to avoid hard feelings or miscommunications:

Be careful of what you say, and the words you choose to say it. Electronic mail messages are free of context, so you cannot be sure how people will interpret them. You cannot convey the subtler shades of meaning that you do with facial expressions in spoken conversation. **Stay as factual as possible.**

Inclusion of any content in messages which might be considered vulgar, obscene, discriminatory, or otherwise offensive, or damaging to employee morale is strictly prohibited.

Electronic mail should be used exclusively for matters of concern to company operations. The use of electronic mail to solicit or recruit others for commercial ventures, religious or political causes, outside organizations or other non-job-related activities is strictly prohibited.

IT department has the right to amend, modify, and change the clauses of this policy without any prior intimation.