BEHARI LAL ENGINEERING LIMITED (“**Company**”)

INFORMATION TECHNOLOGY
&
CYBER SECURITY POLICY

OBJECTIVES

The primary objective of this document to use IT resources in a cost-effective manner that safeguards Company's data and promotes accuracy, safety, Information, and efficiency. It also provides Policy to achieve efficient and effective use of Information Technology to improve business processes, to increase productivity while ensuring accuracy, accountability, confidentiality, availability, and integrity of the information.

This document aims to provide Policy on the aspect related with information technology such as Software usage Management, Network Management, Desktop Management, Internet usage, Usage and Access control of ERP Applications and Email usage etc. Proper use and control of computer resources is the responsibility of all employees.

SCOPE OF INFORMATION TECHNOLOGY (IT) CYBER SECURITY POLICY

This policy applies to all employees and contractors/third party of our Company who are using and managing IT resources includes hardware and software resources. The Policy aim to regulate and control, the access to the information through ERP system, Intranet and Internet, Users to manage the Computer Hardware / Peripherals for proper usage. The scope aims at safeguarding business interest of the Company by preventing occurrence of inappropriate, unethical, or unlawful behavior by any of the users and preventing external threats to IT system.

The scope can be reviewed time to time to incorporate changes in policy due to changes in technology, Company's policy, statutory requirement, business requirements, and operational requirement. Such changes, amendments, deletions are to be affected after proper approval of the Management.

ACCEPTABLE USE OF IT ASSETS

Objectives

The purpose of this policy is to outline the acceptable use of IT assets. These rules are in place to protect the authorized user and the Company. Inappropriate use exposes the Company to risks including Virus/Malware attacks, compromise of network systems and services.

Scope

This policy applies to all employees, users or third party who are using Desktop or IT resources/infrastructure issued by the Company. All are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the Company's policies.

Policy

All electronic files created, sent, received, or stored by the Company are the property of the Company.

Access requests must be authorized and submitted from departmental HoD for employees to gain access to IT systems.

Authorized users are accountable for all activity that takes place under their Username or User-id.

Authorized users should be aware that the data and files they create on the IT systems immediately become the property of the Company.

System level and user level passwords must comply with the Password Policy. Authorized users must not share their login ID(s).

ERP SYSTEM USAGE AND ACCESS CONTROL POLICY

Objective

ERP System are key Transaction processing systems. It is important to have policy connected to the usage and access control mechanism for ERP System in order to ensure that; the system provides the access to authorized users only to acquire information for business decisions on the need-to-know principals.

Policy

Users of the Company can access the ERP System through their user id's and password. They will maintain confidentiality of access through his/her password and will take all appropriate care not to leak out password to any unauthorized person.

For any access to ERP System, User will initiate the request through the concerned Head of the Department. IT Department will review/ revise/ reject/ approve this request application as per the requirement.

Access rights required by third party working for the Company will be given as per the approval of the HoD. HoD of that functional department which has hired services of third party will have to initiate request for access rights.

Request for new development or modification in the program, form, report, view etc will be initiated by the user of duly concurred by the concerned Head of the Department and will forward to IT Department. IT Department will review/ revise/ reject/ approve the request after assessing operational, technical feasibility.

In case of problems with the functioning of software application ERP System, users must intimate IT Department.

Even though the system or program development work is carried out with its proper procedure and with proper testing, it is users responsibility to verify the output time to time and inform IT Department in case anything wrong in that.

All accounts must be disabled immediately upon notification of any employee's termination.

INTERNET USAGE POLICY

Objective

The purpose of this Internet Usage policy is to define standards to ensure employees use the Internet to gather information, which are relevant to the Company's business activities in a safe and responsible manner.

Scope

This policy applied to all employees or third party who are using internet through the Company's network.

Policy

Users are provided access to the Internet to assist them in the performance of their jobs and used for business purpose. At any time, at the request of management, Internet access may be revoked.

IT Department will monitor misuse of Internet connectivity and will inform concerned user to desist from such use.

Internet user is prohibited to download video files, music files, game and other free software that are detrimental to the performance of desktop machines.

IT Department will block the websites that fall under objectionable category and also those which are being used for purposes other than business activity.

Internet user discipline is of prime importance to the overall IT networks security of the organization.

User will not use any medium to access Internet connectivity which are not approved by the management.

Users shall not launch any social media handle, page using Company's name and logo without written permission of the authorized Corporate Communication Department / HR Department.

HARDWARE (DESKTOP / LAPTOP) AND PERIPHERAL MANAGEMENT AND SECURITY POLICY

Objective

The policy is aimed to provide enhance security and quality operating status for Computer Hardware / Peripherals (Desktop/Laptop/Printers/Scanners etc.) and to ensure proper, efficient, optimum use of machines and peripherals so that overall performance and life of Hardware is maintained.

Scope

This policy applied to all employees or third party who are using Computer Hardware and other IT related resources of the Company.

Policy

Desktop/Laptop users are required to take regular backup of their files, data and e-mails.

User will be careful in using external devices such as pen drive or external hard disks etc. to avoid virus or malware etc. into IT infrastructure.

All Desktops/Laptop's issued by the Company are loaded with anti-virus, malware software's and user will ensure that anti-virus function is active on their desktops/Laptops. IT will obtain alerts of infected workstations and perform certain remediation tasks.

All peripherals such as printers, scanners etc. attached to desktop shall be optimally used so as to conserve stationery items.

Desktop users have to ensure that their local files and folders are not shared on the Company's network.

Users should ensure their Desktops/Laptops are fully shut down and turned off at end of day.

Users should get in the habit of logging off when their work is done. This is not only to protect their personal account data but also to protect others using the system.

Computers should be locked or shut down when left unattended for any significant period of time

Individual user shall reasonably protect and take care of the desktops and peripherals from dust, spillages and physical damages.

Requirements for new hardware should be discussed in advance with the IT department to assess the detailed specification.

The user of a particular department will initiate request form for new hardware requirement duly concurred by concerned Head of the Department. IT Department will review the requirement based on the technical feasibility and shall issue the required hardware based on the availability of hardware and budget.

The deployment of new hardware or re-deployment of existing hardware will be undertaken by the IT Department after consultation with concerned Departmental Heads.

The relocation of hardware within or outside Company's premises should not carried out without prior intimation/approval from IT department in advance to ensure good reason for relocation, determine the most appropriate means of relocation and to ensure equipment registers are updated.

Problems with hardware and software installed at user's desktop should be reported to the IT Department in accordance with established IT Help Desk procedures.

IT department may resort to disabling all communication ports on the desktop if the same is required in the interest of the security of data and information. Such activity shall be duly approved by Management, in case if required.

To monitor, regulate and control use of unauthorized software of files and objectionable data storage for different desktops is under the purview of IT department.

The Laptop Policy in force will be integral part of this policy.

EMAIL SECURITY AND USAGE POLICY

Objective

The purpose of this policy is to ensure the proper use of e-mail system by its employees. Users have the responsibility to use this resource in an efficient, effective and ethical manner.

Scope

This policy applied to all employees who are using email account on the Company's domain.

Policy

E-mail accounts are created by the IT department. (Approval by concerned HOD)

Users shall not use third party email systems (e.g. Google, Yahoo, Hotmail etc.) to store, transmit and/or process official information. Additionally, users shall be prohibited from copying/ forwarding official emails and information to such unauthorized third-party email systems.

Employees are responsible for safeguarding their identification (ID) codes and passwords, and for using them only as authorized

Access to the Company's e-mail services is a privilege that may be wholly or partially restricted by the company without prior notice and without the consent of the e- mail user.

Employees who have retired, terminated or resigned from the Company will have email privileges removed/ blocked effective on their last worked day.

NETWORK ACCESS AND USAGE POLICY

Objective

The purpose of this policy is to ensure secured and reliable network access and usage by the users. This policy is intended to protect the integrity of the Company's network and to mitigate the risks and losses associated with security threats to the Company's network and information systems.

Scope

This policy applied to all employees or third party who are using our Company's network.

Policy

Technological changes and other factors may require a reconfiguration of the network resulting in a change to the network addresses assigned to computers. IT department will give prior notice to affected users before making any changes.

The users can access ERP system once they are connected using Internet to the Company's network/ Internet.

Departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the Company must get prior approval from IT Department.

Physical access to the Company's networking equipment (routers, switches, hubs, etc.) is not permitted without the prior approval of IT Department.

If security problems are observed, it is the responsibility of all network users to report problems to IT Department for investigation.

Establishing unauthorized network devices, including router, computer set up to act like such a device is not permitted.

Prior approval of IT Department is required for guest users for accessing Company's networks.

PASSWORD POLICY

Objective

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Company's entire corporate security. As such, all employees (including contractors and vendors with access to the systems) are responsible for taking the appropriate steps to secure their passwords.

Scope

This policy applied to all employees who have account or id to access the Company's IT Systems and applications.

Policy

It is recommended to change the password time to time to maintain confidentiality.

Users will be fully accountable for their passwords and any access related to these passwords

Do not share your passwords with anyone, including assistants, supervisors or co- workers.

Do not reveal a password over the phone line, in email messages, in any questionnaires or in any security forms.

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system without encryption.

Passwords should be at least of 8 alpha-numeric characters

PCs must not be left unattended without enabling a password-protected screensaver or logging off the device

The same password must not be used for multiple accounts.

DISPOSAL OF OLD HARDWARE/EXTERNAL MEDIA/ SCRAP OF E-WASTE

Objective

All hardware has a useful life. Once the useful life of the hardware if over, the hardware can be disposed off in form of a scrap or e-waste. It has to be ensured that no sensitive information is passed on while scrapping of IT assets.

Scrap or E-Waste is generated in the form of consumables like Printer Cartridges, Old Magnetic Media and Obsolete Computer Hardware viz. Desktops, Laptops, Printers, Scanners etc.

Scope

The scope of hardware disposal is applicable to all employees using Company's hardware.

Policy

The old desktops and laptops which are not working and are unusable are replaced with the new ones as per the need. Useful parts of the old machines are used and the old machines are stores in a specified location for disposal as scrap or e- waste.

All the equipment's such desktop, laptops or external media which is to be disposed off will be wiped of all data before disposal.

It is the responsibility of the users to take proper backup of the data before asking for a new machine. IT Department can help transfer the data from the old machine to the new machine but will not be responsible for the loss of data.

E-Waste of empty consumables are being sent to designated bins in the Scrap Yard of Stores Department under intimation to Stores Department and further disposal activities of the consumable Waste is being taken care by Stores Department.

E-Waste of Obsolete Computer Hardware viz. Desktop, Laptop, Printers, Scanners etc. are scrapped through Stores in line with the Scrap Procedure defined as per Purchase Policy.

DATA BACKUP

Objective

Data is important asset of the organization. Hence it is imperative that it has to be secure and backed up in case of any adversity.

Scope

This policy applied to all employees or third party who is using Company's data.

Policy

Users shall take regular backups of the business data residing in their Desktop's, Laptop's and any other devices. Additionally, users must prioritize the backup of critical and sensitive data, and if deemed necessary, ensure a more frequent backup interval. The backup shall be taken only on assets which are owned by the organization.

Users shall not share/store any business information on their personal devices such as pen drive, external hard disks etc.

The HoD of the respective department has to ensure that the data is backed up of the employees of their department and all necessary data is taken from the employee, when employee is leaving the company.

TRAINING & COMMUNICATION

The policy will be communicated to all the existing employees through an appropriate channel. New joiners and third-party users will be communicated at the time of on- boarding.

Annual training sessions on the policy will be organized for the employees and third- party users. All the records related to the training imparted will be duly maintained.

This policy is approved by the Board on 17th April 2025 with immediate effect.