"ನೀರನ್ನು ಮಿತವಾಗಿ ಬಳಸಿ"
"ಕನ್ನಡದಲ್ಲೇ ವ್ಯವಹರಿಸಿ"

Phone : 080-22945253
E-mail: cedesign@bwssb.gov.in

ಬೆಂಗಳೂರು ನೀರು ಸರಬರಾಜು ಮತ್ತು ಒಳಚರಂಡಿ ಮಂಡಳಿ

BANGALORE WATER SUPPLY & SEWERAGE BOARD

ಮುಖ್ಯ ಅಭಿಯಂತರರು(ವಿನ್ಯಾಸ) ರವರ ಕಛೇರಿ, ೯ನೇ ಮಹಡಿ, ಕಾವೇರಿ ಭವನ, ಬೆಂಗಳೂರು-೫೬೦೦೦೯.

No.BWSSB/CEDQATE/ACE(MIS-IT)/TA(D&QA/ JE/ 1891 /2022-23 Date: 28/02/2023

Circular

Sub: Guidelines for usage of IT hardware and software in Board under the Purview of RB-IT Division

****

The following general guidelines are prescribed in managing the IT activities at the various BWSSB Offices;

Compliance

- All employees are expected to comply with the IT Guidelines while using and maintaining any equipment or software purchased or provided by the organization.
- Any employee who notices misuse or improper use of equipment or software within the organization must inform his/her Divisional/Sub divisional Officer(s) immediately.
- Inappropriate use of equipment and/or software by an employee will be subjected to disciplinary action as deemed fit by the Competent Authority.

Password Guidelines

The Board has commissioned many software applications which are required for Day –to –Day activities, secured with username and passwords.

The following password guideline requires to be followed to ensure maximum password safety.

1) Select a Strong Password:

- Choose a password which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.).
- Use minimum of 8 or more characters.
- Use at least one numeric and one special character apart from letters.
- Combine multiple unrelated words to make a password.

2) Keep your Password Safe:

- Do not share your password with anyone.
- Make sure no one is observing you while you enter your password.
- As far as possible, do not write down your password. If you want to write it down, do no display it in a publicly visible area.
- Change your password periodically (every 1 month is recommended).

- Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.
- Do not save passwords in any of the browsers.

3) Other Security Measures:

- Ensure your computer is reasonably secure in your absence.
- Lock your monitor screen, log out or turn off your computer when not at desk.
- **In case of employee being transferred to other office, concerned employee should inform RB-IT division to disable his/her login with immediate effect**

IT Asset Usage Guidelines:

Desktop:

- In Personal Computers, data shall be stored other than C drive.
- System should be shut down properly before leaving the office.
- No download and installation of any unauthorized software's to be taken up.
- Regular maintenance to be taken up regarding clearing the temporary files, check disk, defragmentation, scanning the system to check viruses/malwares and removing unwanted data.
- Ensuring proper functioning of UPS system to avoid power fluctuation for the safety of IT assets and related data thereof.
- It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.
- Proper guidelines or safety information must be obtained from designated staff in the RB-IT Division, before operating any equipment for the first time.
- Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the designated staff in RB-IT Division.
- Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action as deemed fit by the Competent Authority.

Antivirus Software

- Approved licensed antivirus software is installed on all PCs owned by the organization.
- Employees are expected to make sure their Antivirus is updated regularly. The RB-IT Division, should be informed if the Antivirus expires.
- Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.

Internet Usage Guidelines

Objective

The Internet Usage guidelines are provided for acceptable use of the Board's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network and the employees.

General Guidelines

- Internet is a paid resource and shall be used only for office work.
- The Board reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the Board's network.
- The Board at Central Offices has installed an Internet Firewall to assure safety and security of the Board network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action as deemed fit by the Competent Authority.

Online Content Usage Guidelines

- Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the Board, they should disconnect from that site immediately.
- During office hours, employees are expected to limit themselves from accessing news, social media and other websites online, unless explicitly required for office work.
- Employees are allowed to use Internet for official purposes using the Internet facility in office.
- Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads etc. for off-peak times.

- **Inappropriate Use**

The following activities are prohibited on Board's Internet network. This list can be modified/updated anytime by the RB-IT as deemed fit. Any disciplinary action considered appropriate by the Board can be taken against an employee involved in the activities mentioned below:

- Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth
- Downloading images, videos and documents unless required for official work
- Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work
- Accessing pirated software, tools or data using the official network or systems
- Uploading or distributing software, documents or any other material owned by the Board online without the explicit permission of the Management
- Engaging in any criminal or illegal activity or violating law Invading privacy of co-workers using the Internet for personal financial gain or for conducting personal business

- Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
- Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the Board's reputation

Chief Engineer
(Design & QA)

Copy submitted to Hon'ble chairman for kind information.
Copy submitted to CAO-S and FA & CAO for kind information.
Copy to all CE's for information
Copy to all ACE's for information and necessary action & to circulate to all concerned division/subdivision offices.
Copy to EE(MIS) to upload the circular on board official website and circulate to all officers through E-mail.