Regd. Off. : 1501, Vikram Tower, Rajendra Place, New Delhi - 110008
Ph. : +91-11-43661111 (30 lines) • Fax : +91-11-43661100, 41538600
E-mail : info@bharatgroup.co.in • Website : www.bharatgroup.co.in
CIN : L24119DL1989PLC036264

CYBER SECURITY POLICY & USER GUIDELINE

Overview

Cybercrimes are becoming more and more common across the world, making cyber security of the top priorities for everyone. Consequently, there has been a rapid increase in various cyber laws.

In order to protect our company from numerous cybercrimes, we should have a clear and organized cyber security company policy.

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This cyber security policy is for our employees, vendors and partners to refer to when they need advice and guidelines related to cyber law and cybercrime. Having this cyber security policy we are trying to protect Bharat Group's data and technology infrastructure.

This policy applies to all Bharat Group's employees, contractors, volunteers, vendors and anyone else who may **have** any type of access to Bharat Group's systems, software, network and hardware.

Examples of Confidential Data

Some of the common examples of confidential data include:

- Classified financial information
- Customer data
- Contracts & Regulatory Data
- Data about vendors
- Patents, formulas or new products

Device Security- Using personal devices

Logging in to any of the company's accounts for personal devices such as mobile phones, tablets or laptops, can put our company's data at risk. Bharat Group does not recommend accessing any company's data from personal devices. If so is inevitable, employees are obligated to keep their devices in a safe place, not exposed to anyone else.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

We recommend employees to follow these best practices:

- Keep all electronic devices' passwords secured and protected

Regd. Off. : 1501, Vikram Tower, Rajendra Place, New Delhi - 110008
Ph. : +91-11-43661111 (30 lines) • Fax : +91-11-43661100, 41538600
E-mail : info@bharatgroup.co.in • Website : www.bharatgroup.co.in
CIN : L24119DL1989PLC036264

- Logging into company's accounts should be done only through safe networks
- Install security updates on a regular basis
- Upgrade antivirus software on a regular basis
- Don't ever leave your devices unprotected and exposed
- Lock your computers when leaving the desk
- Don’t connect your device to any public Wi-Fi, which is open for all

Email Security

Emails can carry scams or malevolent software (for example worms, bugs etc.). In order to avoid virus infection or data theft, our policy is always to inform employees to:

- Avoid opening attachments or clicking any links in situations when the content of email is not properly explained
- Make sure to always check sender’s email address, name of senders and correct domain name
- Be careful with clickbait titles (for example offering prizes, advice, etc.)
- Always check the URL before clicking any link sent via email.
- Always report all suspicious activity and cyber incidents to concerned authority.
- Official E-mail account should be used for official purpose only.
- Official E-mail should not be forwarded to personal E-mail account.
- Never respond to emails received from strangers
- Don’t click on links from an unknown or untrusted source
- Don’t send any personal or sensitive information, such as credit card numbers, passwords or other private information, through email.

In case that an employee is not sure if the email received, or any type of data is safe, they can always contact the IT team respectively.

Managing Passwords

To ensure avoiding that your company account password gets hacked, use these best practices for setting up passwords:

- At least 8 characters (must contain capital and lower-case letters, numbers and symbols)
- Do not write down password and leave it unprotected.
- Do not make password by your name, surname and company name.
- Do not exchange credentials when not requested or approved by supervisor
- Change passwords every one month
- Do not share credentials over email

Regd. Off. : 1501, Vikram Tower, Rajendra Place, New Delhi - 110008
Ph. : +91-11-43661111 (30 lines) • Fax : +91-11-43661100, 41538600
E-mail : info@bharatgroup.co.in • Website : www.bharatgroup.co.in
CIN : L24119DL1989PLC036264

Computer / Laptop

- Do lock your computer and laptop when not in use
- Do keep all devices, such as laptops and computer physically secured
- If a device is lost or stolen, report it immediately to competent authority
- Antivirus software should be installed on computer, and it should be kept updated
- Don't install unauthorized programs on your work computer / laptop.
- Don't leave devices unattended

Transferring Data

Data transfer is one of the most common ways cybercrimes happen. Follow these best practices when transferring data:

- Avoid transferring personal data such as customer information and employee confidential data to the other device or accounts unless absolutely necessary. When mass transfer of such data is needed. We request employees to ask our security specialists for help
- Data can only be shared over the company's network
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Report Scams, privacy breaches and hacking attempts

Mobile

- Do lock your mobile phone when not in use
- Do keep mobile devices, IP phones etc. physically secured
- Personal information should be guarded properly
- Requests for personal or account information over the mobile should be avoided
- If a device is lost or stolen, report it immediately to competent authority
- Always check what permissions are asked by mobile app which you want to install
- Advisable to check the reputation of the application before installing it
- Be cautious about using geo-location services. Stalkers can easily access one's location
- Don't respond to phone calls requesting confidential data
- Don't leave mobile unattended
- Don't be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner

Portable Media

- Do lock portable media containing sensitive information in a drawer to reduce the risk of unauthorized disclosure

Regd. Off. : 1501, Vikram Tower, Rajendra Place, New Delhi - 110008
Ph. : +91-11-43661111 (30 lines) • Fax : +91-11-43661100, 41538600
E-mail : info@bharatgroup.co.in • Website : www.bharatgroup.co.in
CIN : L24119DL1989PLC036264

- Do destroy information properly when it is no longer needed
- Do use official portable storage media for official purpose and should not be handed over to unauthorized person
- In case of loss of official portable storage media, it should be reported to the competent authority at the earliest
- Don't leave portable media containing sensitive information on your desk
- Don't plug in portable devices without permission. It may contain virus or may be Corrupted

Wireless Connectivity

- Do remember that wireless is inherently insecure. Avoid using public Wi-Fi hotspots when you must to use Wi-Fi, use VPN to protect the data and the device
- Do ensure that the wireless interfaces are disabled by default
- Don't leave wireless or Bluetooth turned on when not in use
- Secure websites using public Wi-Fi should not be used

Internet Usage

- Do use latest version of Internet browser.
- Do log-out from web based services, like web mail, before closing the browser session.
- Do close the browser session, after completing the activity in the current web based application
- Cookies should be allowed from the trusted web sites only
- Don't enable "save password" and auto-complete features of the browser
- Don't download or distribute malicious software and tools
- Don't violate any copyright or license agreement by downloading and distributing protected material

Security from Virus & malicious Code

- Do ensure that client system is configured with authorized centrally managed anti-virus software
- Do ensure that anti-virus software and the virus pattern files are up-to-date
- In case a virus does not get cleaned, incident shall be reported to the competent authority

Web Browser Security

- In case a virus does not get cleaned, incident shall be reported to the competent authority
- Latest version of web browser should be used
- Don't forget to delete browsing history which deletes all the cookies, temp files, history and ActiveX filtering

Regd. Off. : 1501, Vikram Tower, Rajendra Place, New Delhi - 110008
Ph. : +91-11-43661111 (30 lines) • Fax : +91-11-43661100, 41538600
E-mail : info@bharatgroup.co.in • Website : www.bharatgroup.co.in
CIN : L24119DL1989PLC036264

- Don't forget to turn off all JavaScript or ActiveX support in your web browser before you visit any unknown websites
- Don't give any personal information in any untrusted links
- Don't allow pop-ups and plugins; disable them in the browser settings

Web Application

- Security patches and software updates should be installed as soon as they are available

Printouts / Faxes

- Do lock printouts containing sensitive information in a drawer to reduce the risk of unauthorized disclosure
- Do be aware of your surroundings when printing or faxing sensitive information
- Do pick up information from printers, copiers, or faxes in a timely manner
- Don't leave sensitive information lying around the office
- Don't leave printouts or portable media containing private information on your desk

Social Networking

- Do use privacy settings on social media sites to restrict access to your personal information

  Only add people you KNOW offline, If must add strangers, keep your guard up
- Convincing imitations of banks, card companies, charities and government agencies should be watched out carefully
- Privacy settings of profile should be checked and make sure they are set to the right level
- Even if social network is set to private, it doesn't guarantee that information is completely private. It should be remembered that friends' friends might be able to see posts and updates even if they are not friends with them. So be careful
- Don't tolerate being uncomfortable
- Don't post any private or sensitive information, such as credit card numbers, passwords or other private information, on public sites, including social media sites
- Don't over share the information. Sensitive information like birth date, mother's maiden name, pet's name or any other identifying information should not be shared on social-media platforms such as Facebook, LinkedIn or Twitter. Social media has made cyber stalking much easier. A stalker can easily locate and track their target's every move. Personal titbits collected over time can give them a whole picture of who you are, where you work, live and socialize

Working Remotely

- Even when working remotely, all the cybersecurity policies and procedures must be followed

Disciplinary Action

Regd. Off. : 1501, Vikram Tower, Rajendra Place, New Delhi - 110008
Ph. : +91-11-43661111 (30 lines) • Fax : +91-11-43661100, 41538600
E-mail : info@bharatgroup.co.in • Website : www.bharatgroup.co.in
CIN : L24119DL1989PLC036264

When best practices and company's policy are not followed, disciplinary actions take place. Some of the examples of disciplinary actions include:

- In case of breaches that are intentional or repeated, and are harmful to our company, Bharat Group will take serious actions including termination
- Depending on how serious the breach is, there will be given of warnings or termination
- Each incident will be evaluated
- Each case and incidence will be assessed on a case-by-case basis

Review of Cyber Security Policy (CSP)

The Cyber Security Policy may be reviewed at least annually or whenever significant changes occur in relevant ecosystem.

****