





## IT POLICY – for Employees (Ver 2.0)

(w.e.f 1<sup>st</sup> April,2021)

	Prepared & Reviewed by	Approved By
Name	Mr. Kunal Mukherjee	Mr. Anurag Choudhary
Designation	AVP - HR	MD & CEO
Signature		
Date	26.03.2021	

Purpose: The aim of this policy is to provide a comprehensive guideline on our Information Technology system and create safe and secure cyber space to protect our data privacy and confidentiality and as well as Employees' cyber safety.

### **About the Information Technology Policy**

HSCL provides and maintains technological products, services and facilities like Personal Computers (PCs/Laptop), peripheral equipment, servers, telephones, Internet and application software to its Employees for official use. The Information Technology (IT) Policy of the organization defines rules, Regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them. It also provides guidelines for issues like purchase, compliance, IT support and grievance redressal of the employees pertaining to technological assets and services used for office work only.

### **1. Compliance**

- A. Employees are advised to comply as per IT Policy guideline for using Systems, Infrastructure, Software, Internet, and Data, provided by the organization for official use.
- B. Employees are not allowed to download any unlicensed product, software in their systems.
- C. Any improper use should be stopped or intimated to IT department on immediate basis.
- D. Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the HR Department.

### **2. Employee Training**

- A. Basic IT training and guidance are provided to all new employees about using and maintaining their Computer/Laptop, peripheral devices and equipment in the organization, accessing the organization network and using application software.

### **3. IT Support**

- A. HSCL uses an online Ticket System to provide IT Support to its employees.
- B. May need hardware/software installations or may face technological issues which cannot be resolved on their own. Employees are expected to get help from the IT
- C. Employees /Individuals/Departments to contact IT through Ticketing System or the IT Support Email ID only.
- D. Any IT Support work informed or assigned via emails sent on employee email IDs, chats or any other media except the Ticket System or the IT Support Email ID would be not entertained.
- E. For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all employees to inform the IT Dept. For any damage to Personal Computers, approval from HR Department would be required for PC replacements post incident investigation by the local IT team.
- F. After raising a ticket in the Ticket System, employees should expect a reply from the IT Dept. within 1 working day. The IT Dept. may ask the employee to deposit the problematic equipment to the IT Dept. for checking and will inform the timeline for repair/maintenance/troubleshooting/installations or the required work. If there is no response in 1 working day, then the IT Dept. Designated Staff should be asked for an explanation for the delay. If no response is obtained in 3 working days, a complaint can be raised through an email to the HR and IT Dept.
- G. Tickets will be resolved on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the designated team in IT Dept.

#### **4. Equipment Usage Policy**

##### Equipment Purchase

The following equipment is purchased by the organization and provided to individual.

- Employees/Departments for their official use. The list can be modified as and when required.
  - **Computing Devices (Desktop, Laptop)**
  - **Computer Peripherals (Printer, Scanner, Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker, Internet Dongle etc.)**
  - **Networking Equipment & Supplies (Router, Switch, Antenna, Wiring, etc.)**
  - **CCTV and Walky Talky**

### Equipment Allocation, De-allocation & Relocation

#### Allocation of Assets:

- New Employees may be allocated a Desktop or Laptop for office work on the Day of Joining, as per approval received from HR department.
- Allocation of additional assets to an employee is at the sole discretion of the HR Department.

#### De-allocation of Assets:

a. Employees who have already submitted resignation, must be returned all the received Asset to IT Department at the time of Full & Final Settlement from HR Department.

### Equipment Usage, Maintenance and Security

- 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 IT Dept. 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 IT Dept.
- 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.

### **Intercom Phone Usage Policy**

- Landline phone systems are installed in the organization's offices to communicate internally with other employees for Official Purpose.
- Long distance calls should be made after careful consideration since they incur significant costs to the organization. The IT Dept. is responsible for maintaining telephone connections in offices. For any problems related to telephones; they should be contacted.

## **Network Access**

1) Employees are expected to undertake appropriate security measures as guided by IT Department.

### Data Backup Procedure

- Data Backup is setup during installation of Operating System in a PC. As an additional
- security measure, it is advised that employees keep important official data in-
- A>For Laptop User
- Users are requested not to store anything in Local System. All Data Should be Stored in D drive only.
- B>For Desktop User
- Users are Requested not to store anything in Local System All Data should be Stored in User\_Data Drive.
- 3.2 Antivirus Software
- Employees are expected to make sure their Antivirus is updated regularly. The IT Dept.
- Should be informed if the Antivirus expires.

## **Internet Usage Policy**

### General Guidelines

- Internet is a paid resource and therefore shall be used only for office work.
- The organization reserves the right to monitor, examine, block or delete any/all incoming or
- Outgoing internet connections on the organization's network.

### Password Guidelines



The following password guidelines can be followed to ensure maximum password safety.

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 8 or more characters.
- Use at least one numeric and one special character apart from letters.
- Combine multiple unrelated words to make a password.

**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 not display it in a publicly visible area.
- Change your password periodically (every 3 months is recommended).
- Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.

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.

**Online Content Usage Guidelines**

- Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. They must not access any website content which prohibited by the organization; they should disconnect from that site immediately. (Movie, Trading of shares, Explicit contents, OTT platforms)
- During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless exclusively required for office work.
- Employees are not allowed to use Internet for unofficial purposes using the Internet facility in office.

- Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for all the times.

## **5. Inappropriate Use**

The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the IT Department as deemed fit.

Any disciplinary action considered appropriate by the IT Department 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.
- Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material.
- Accessing pirated software, tools or data using the official network or systems
- Uploading or distributing software, documents or any other material owned by the Organization online without the explicit permission of the IT Department.
- Invading privacy of coworkers
- Using the Internet for personal financial gain or for conducting personal business or usage.
- 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 organization's reputation

## **6. Email & Chat Policy**

### General Guidelines

- The organization reserves the right to approve or disapprove which electronic messaging systems would be used for official purposes. It is strictly advised to use the pre-approved platforms for office use only.

- An employee who, upon joining the organization, is provided with an official email address should use it for official purposes only. (Jr Engineer & above) for (Sr Supervisor to Support Staff to access all IT related information through KIOSK.
- Any email security breach must be notified to the IT Dept. immediately.
- Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned/provided by the organization.
- All messages composed and/or sent using the pre-approved messaging systems and platforms need to comply with the company policies of acceptable communication.
- Electronic mails and messages should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.
- All email signatures must have appropriate designations, Department along with contact no of employees with HSCL Logo.

### **Ownership**

- The official electronic messaging system used by the organization is the property of the organization and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic. messaging systems are the property of the organization.
- The organization reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems.
- The organization reserves the right to alter, modify, re-route or block messages as deemed appropriate.
- IT Administrator can change the email system password and monitor email usage of any employee for security purposes.
- Proprietary, confidential and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems.
- Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.



- Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.
- Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

### **Safe Email Usage:**

Following precautions must be taken to maintain email security:

- Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you.
- In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.
- Use Email spam filters to filter out spam emails.

## **7. Software Usage Policy**

### General Guidelines

- No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Dept.
- To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Ticket System or IT Support Email.
- Any software developed & copyrighted by the organization belongs to the organization.
- Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

## **8. USB Usage Policy**

### General Guidelines

- Any External storage device like Pen Drive or Hard Disk is not supported in Organization Desktop and Laptop.

### **Explanation of the policy:**

HR department will be the sole authority to interpret the content of this policy.

NB: Management reserves the right to exercise its discretion in special cases based on organizational values

X-----X