

Insert company Logo



| Policy Name: | **Confidentiality & Company Asset Policy** |
| --- | --- |
| Policy Number: |  |
| Version: | Effective Date: |

|  | **Name** | **Designation** | **Signature** | **Date** |
| --- | --- | --- | --- | --- |
| Prepared By: |  |  |  |  |
| Reviewed By: |  |  |  |  |
| Approved By: |  |  |  |  |

| **Date** | **Version** | **Summary of Change** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

**Table of Contents**

[**1.**](#_heading=h.gjdgxs) **DEFINITION** 3

[**2.**](#_heading=h.1fob9te) **PURPOSE** 3

[**3.**](#_heading=h.3znysh7) **APPLICABILITY** 3

[**4.**](#_heading=h.2et92p0) **RESPONSIBILITY & ACCOUNTABILITY** 4

[**5.**](#_heading=h.tyjcwt) **POLICY-** 4

[**5.1**](#_heading=h.3dy6vkm) **Confidentiality** 4

[**A.**](#_heading=h.1t3h5sf) **Confidential Information** 4

[**B.**](#_heading=h.4d34og8) **Intellectual Property and Copyrights** 5

[**C.**](#_heading=h.2s8eyo1) **Company Assets/ Records/ Documents** 5

[**5.2**](#_heading=h.17dp8vu) **Company Asset & Usage** 6

[**6.**](#_heading=h.3rdcrjn) **RESTRICTIVE CLAUSE** 8

# **DEFINITION**

1. **Confidentiality** is an ethical principal that an Employee/ Member will hold secret all information pertaining to all the activities in the Organization.
2. **Company Asset** is an item of value owned by the Organization. Assets can be physical, tangible objects or intangible objects.
3. **Company/ Organization** means all the businesses which are under the umbrella of ***“Company Name”*** group.
4. **Member/ Employee** means a person employed with ***“Company Name”*** at all levels for wages or salary.
5. **Management** means the group of individuals that operate at the higher level at ***“Company Name”*** and have day-to-day responsibility for managing all individuals and maintaining responsibility for all the key business functions.

# **PURPOSE**

* To ensure personal information and confidential information is protected from unauthorized use and disclosure.
* To appropriately protect the confidentiality and integrity of information assets, thereby ensuring the appropriate protection of information assets
* To comply with applicable legal, regulatory, contractual and other requirements.

# **APPLICABILITY**

* This Policy applies to all the Members of the ***“Company Name”*** across all the locations and branches. Employee shall mean all individuals on full-time or part-time employment with the Company, with permanent, probationary, trainee, retainer, temporary or contractual appointment.
* The policy also applies to all contractors and anyone else who has permanent or temporary access to our software and hardware.

# **RESPONSIBILITY & ACCOUNTABILITY**

All stakeholders (internal and external) namely Employees, suppliers, investors, creditors, customers.

# **POLICY-**

***“Company Name”***  is committed to full, fair, accurate and timely disclosure in all reports and communications with all its stakeholders.

***“Company Name”*** is responsible for the integrity and accuracy of business documents, communications and financial reports and records. This information serves as a basis for managing our business and is important in meeting our obligations to employees. Suppliers, distributors, government regulators, investors, creditors and our customers.

All books and records of the company are subject to review and independent audit. If a member is asked to respond to requests by internal auditors, legal staff, independent accountants, or special counsel, his/ her response must be complete and truthful. Member should include all relevant information, even if the request is not specific as to what information is required. If a member knows something that could be relevant, it must also be disclosed.

This policy is divided into two parts:

## **5.1 Confidentiality**

### **A. Confidential Information**

Some of ***“Company’s Name”*** most valuable assets are intangible and include our trade secrets and company’s confidential information. Member must guard the intangible assets just as he/she would guard company's physical assets.

No Member is allowed to disclose confidential information to outsiders unless there is a clear business purpose or justification for the disclosure and a company-approved confidentiality agreement has been signed by the recipient. In addition, no member can discuss business matters within hearing distance of unauthorized personnel including co-workers, family and friends.

Some examples of confidential information include:

* Undisclosed financial information and earnings reports
* Confidential product performance information
* New product offerings
* Merger, acquisition, divestiture or business plans
* Proprietary or classified government information
* Procurement plans
* Capital requirements and plans
* Personnel information or organizational changes
* Confidential technical data
* Marketing, pricing or service strategies
* Business negotiation information
* Product costs and volumes
* Supplier and subcontractor information
* Proprietary computer software

### **B. Intellectual Property and Copyrights**

Intellectual property consists of ***“Company Name”*** ’stangible products such as abstract concepts, informational notes, symbols, and expressions that are protected by law. It also includes patents, copyrights, trademarks, and trade secrets as well as designs for products and software programs created by other companies that are copyrighted or otherwise restricted.

A member must vigorously protect companys own intellectual property rights as well as the rights of others. He/ she should fully document product development research and use appropriate company trademarks and copyright notices on all correspondence, articles, manuals or other papers. A Member should also avoid disclosing proprietary and confidential information outside of the Organization unless there is a clear business purpose and the recipient has signed a confidentiality agreement.

**Avoid infringing on the intellectual property rights of others.**

**Do *not*:**

* Make unauthorized copies of software
* Photocopy magazine/journal articles or other publications unless you have the authority or license to do so
* Hire a competitor's employee to obtain that competitor's trade secrets
* Affix the trademark of another company to goods without authorization
* Fail to remove another's trademark when the goods or parts are remanufactured
* Erroneously allege patent infringement or mark a product with an untrue patent notice

### **C. Company Assets/ Records/ Documents**

Business documents and records are important company assets. They contain data and information critical to the continuity of our business, preserve information necessary to protect our legal rights and support and document and other regulatory requirements.

Company Assets/ Records include paper documents, e-mail, electronic files stored on disk, tape or any other medium (CD, DVD, USB data storage devices, etc.) that contains information about the organization or its business activities.

Member must understand and follow ***“Company Name”s*** Confidentiality policy. It is a violation of company’s Code of Conduct to alter or falsify information on any record or document or to intentionally make a false or exaggerated statement to anyone.

Member cannot tamper with company records or remove or destroy them prior to the dates specified in our records retention schedules. In addition, records that have been put on “hold” by any department are not to be destroyed regardless of the retention schedule.

## **5.2 Company Asset & Usage**

1. **Cell Phone**

The policy applies to the user of any device that can make or receive phone calls, leave messages, send text messages, surf the internet, download information and view and respond to emails whether the device is personal or company owned. Cell phones given by the company need to be kept switched on at all times during working hours, during work related travel and other times specifically mentioned by the company.

**Use of cell phones are discouraged**

* While driving
* While operating equipment
* During office hours for gaming and entertainment
* For indulging in long personal calls during office hours
* During meetings
* From recording sensitive information pertaining to the company
* Employees can use cell phones for
* Making business calls
* Using productivity applications
* Checking important messages
* Scheduling and keeping track of appointments
* Making brief personal calls out of earshot of other employees

***“Company Name”*** retains the right to monitor employees for inappropriate and excessive cell phone usage

**Employee may face disciplinary action if it is proven that**

* He/ She has caused a security breach
* He/ She has violated confidentiality policy
* He/ She has caused an accident due to reckless use of their cell phone
1. **Internet**

The electronic communication system must be utilized exclusively to facilitate the business of the Company. Employees are cautioned against using the internet for matters of personal gain and entertainment. Employees should further expect that all content created, transmitted, downloaded, received or stored in the hardware belonging to the Company is subject to perusal by the Company and that no element of privacy holds good here. This information may be accessed without prior notice to the employee. This applies for password protected documents and any deleted content too.

**What constitutes appropriate internet usage**

* To complete jobs assigned
* To seek information on that, which can improve the work quality of the employee

**Inappropriate internet usage**

* Download or upload obscene, offensive and/or illegal material
* Send confidential information to unauthorized recipients
* Invade another person’s privacy
* Upload any kind of pirated software
* Visit potentially dangerous websites which can compromise the safety of the Company network
* Performing unauthorized/illegal actions hacking or purchasing prohibited items
* Forwarding any content which is discriminatory and obscene/inappropriate

The company advises using strong passwords and logging into accounts only from safe devices and to maintain their work devices locked at all times. Failure to adhere to the guidelines may result in disciplinary action and/or lead to employment termination.

1. **Use of Personal Devices**

***“Company Name”***does not encourage logging into Company accounts from any personal devices since it would put Company information at severe risk. In case it becomes inevitable to do so, employees are advised to keep such devices in a safe place. It must at all times be borne in mind that all devices whether personal or company owned need to be password protected, appropriate antivirus installed, regularly installed with security updates and logged in through safe networks.

1. **Email Security**

Email is a routine communication method within the company as well as with investors, business partners and our customers.

Many times emails can carry malicious content which might compromise the security of the Company. Employees are advised to maintain discretion at all times with respect to

* Opening mail with attachments wherein the content is not clearly explained
* Unknown senders and email addresses
* Inconsistent emails
* Mails with clickbait titles (offering prize money or advice)
1. **Managing Passwords**

To prevent company email accounts from being hacked, every employee is required to follow these safety practices

* Ensure password is at least 8 characters long with a mix of alphabets, numerals and special characters
* Do not write down passwords and leave them easily accessible
* Do not share or exchange credentials
* Change password every ***“number”*** of days/month ***“period of time”.***
1. **Transferring Data**

The data transfer stage is an easy mode for cybercrime to occur. Keeping in mind some best practices will bring down the risk considerably.

* Avoid transferring employee and customer confidential data to other devices
* Share confidential data over Company network and not over public WiFi systems or private networks
* Ensure that the recipients of the data are authorized people or organizations with adequate security policies in place
* Report scams, privacy breaches or hacking attempts
1. **Working Remotely/ WFH**

Even when working remotely, the employee must follow the cybersecurity policies and procedures

Employees observed to disregard the cybersecurity policy and procedures will face progressive discipline.

# **RESTRICTIVE CLAUSE**

* Any exceptions to the above would be at the sole discretion of the Management.
* Management reserves the right to change and or modify the policy without stating any reason.
* The organization reserves its right to withdraw this policy without assigning any reason by using its sole discretion which will be binding on all members. The Employees hereby unconditionally agree to all such changes / amendments / additions / deletions / modifications
* The Company's reputation and credibility are based upon its total commitment to ethical business practices and also on ethical conduct of its Employees. To safeguard the Company's reputation, Employees must conduct themselves in accordance with the highest ethical standards and also be perceived to be acting ethically at all times. Compliance with all policies of the Company, relevant applicable laws and regulations is the minimum standard which should be adhered to by all the Employees all the times.



www.gspuconsulting.com

***\_\_\_\_\_\_Disclaimer\_\_\_\_\_\_***

*Please note this is a draft Policy prepared by GSPU Group for your reference. You may amend it suiting to your requirement. GSPU Group expressly disclaims any liability arising out of the reliance on this draft.*