1. Objective

The objective of this SOP is to provide guidelines for acceptable use of IT assets and information systems, to protect the data from unauthorized or malicious use and to make users aware about their duties and responsibilities towards company's IT assets.

2. Scope

This SOP is applicable to all employees of Sula and its group companies.

3. Construct of the policy

This SOP has been categorized into following sections:

1. Eligibility for laptop/desktop
2. Acceptable use
3. Internet usage
4. Email usage
5. Personal use
6. Data protection
7. Loss/damage of IT assets

3.1 Eligibility for laptop/desktop:

An employee is issued laptop based on approval of the respective HOD. The eligibility limit for laptops will be as per the prevailing laptop policy.

Laptops older than 3 years will be upgraded. User is eligible to procure the previous laptop for personal use by paying Rs. 10,000/-. In case the User does not want to retain the old Laptop, it is swapped and used wherever required.

As per existing desktop policy, desktops older than 4 years will be upgraded and swapped as per the requirement and the older machines would be used wherever required/ donated to schools as CSR activity/made available to

interested employees as per the approved rate (presently Rs. 4000/- per desktop).

3.2 Acceptable use:

IT assets provided to users is a property of Sula Vineyards Pvt. Ltd., and users are expected to protect the IT assets and information in it. Users can use IT resources solely for their official work purposes.

Examples of misuse would include:

- Viewing inappropriate internet sites
- Allowing unauthorized persons to use the IT assets given to the user
- Sharing user ids and passwords with **any** person
- Circumvent, probe or test security measures
- Installing, attaching or downloading any hardware or software. For any specific work requirement, prior written approval of concerned HOD should be taken. IT representative should install the software only on the basis of written approval from the HOD
- Formatting the laptop/desktop. *In case of any issues with laptop/desktop, kindly contact your respective IT in-charge.*

3.3 Internet usage:

- Users are given access to internet on their respective laptops/desktops via network cables/wifi. As per the acceptable use clause, certain sites (for eg. Social networking sites, e-commerce sites, etc.) are blocked on Sula network. In case a user needs access to any of the blocked sites, it can be provided based on prior approval of his/her HOD. However following employees should have **unrestricted access** to internet:
  - All HODs
  - Special category employees specifically approved by the HOD
- According to work needs, temporary access to restricted sites can be given to employees based on prior approval of his/her reporting manager.
- However, all employees will have unrestricted access to internet during 2 P.M. to 3 P.M.

- Internet data cards can be provided to employees based on approval of his/her reporting manager. However; employees should not exceed the approved data usage limit of the data card.
- Usage of Sula wifi network on mobile phones is not allowed. However following employees can have temporary access to internet via wifi:
  - All HODs
  - Special category employees specifically approved by the HOD

  Employees will have to login into Sula wifi network to access internet via wifi. Temporary access will be given for one hour. After one hour, employee will have to re-login into Sula network to access wifi.

  IT department should maintain a log of employees using wifi on their mobiles.

3.4 Email usage:

- E-mails sent through Sula ids are visible representations of the entity. Receiving parties can forward e-mail messages to other unintended persons without the original sender's permission or knowledge. Accordingly, users are expected to use Sula ids in a responsible manner. *Kindly read the "Best Practices Handbook" for e-mail etiquettes*
- E-mails sent to outside recipients should always have proper signature as per Sula standards.
- Size of e-mail attachments can't exceed 10 MB. Employees are advised to use .zip files for bulky attachments. Also, sensitive documents should be password protected before sending the same through email.
- Size of primary inbox can not exceed 2 GB. IT department shall create archival folder for each user in outlook*. Users should move emails to archival folder on a regular basis and keep the primary inbox free. In case the size of primary inbox reaches 2 GB, no further emails can be sent or received through outlook

  *To be implemented in phased manner

- Users are not allowed to use Sula e-mail ids for personal communication. Also, use of commercial e-mail systems (eg. Yahoo, Gmail, etc.) for official purpose is prohibited.

3.5 Personal Usage:

Personal use of Sula IT assets to a reasonable extent is allowable. However; personal use is restricted to users and does not extend to the user's family members or acquaintances.

3.6 Data Protection

a. Passwords:

Under no circumstances are ID's and passwords to be shared (this includes the employee's supervisor and IT personnel) or written down and placed in a visible location. If password is compromised for any reason, then concerned employees will be held responsible for the same. Following are the guidelines regarding passwords:

- All passwords must be changed every 90 days
- Passwords must be at least 8 characters in length
- Passwords must contain at least one alphabet, one number and one special character

It should be noted that IT dept. doesn't have backup of passwords and thus will not be responsible for recovery of the passwords.

b. Data backup:

Data stored in "PC-Data" folder in "D" or "E" drive automatically gets backed up, if the user is connected to the company network. Users should store all official data in "PC-Data" folder to ensure smooth recovery of data in case of emergency.

c. Data confidentiality:

Users are not allowed to make unauthorized disclosure or copy confidential information from the IT assets belonging to the Company

3.7 Loss/damage of IT assets:

- In case of loss/damage of IT assets, the user should immediately inform the IT department.
- IT department shall take immediate steps to recover the data in the IT asset.
- IT department shall inform the Accounts department, and accounts department should take steps to lodge insurance claim if the asset is insured. For any reason if the insurance claim is rejected, then amount equivalent to WDV of lost/damaged asset will be recovered from the employee. For recurring instances of damage to IT assets, penal actions will be taken against the employee.

Breach of policy:

Employees are expected to adhere to this policy. Any breach of the above mentioned clauses may result into inquiry and penal actions against the employee. Company will not be responsible for any liability arising due to breach of any of the clauses mentioned in this policy.