LUCID COLLOIDS LIMITED

Information Security Policy

Overview

This Policy is divided into Four Parts viz. Information Security, Data Back Up, Data Restore and IT Procurements.

Every employee would generally be contractually bound to comply with this policy and would have to have sight of it prior to operating the IT Products provided by the Company to them for the day-to-day business activities of the Company.

This Policy provides the policies and procedures for selection and use of IT within the business which must be followed by all the employees to protect its digital assets and intellectual rights in efforts to prevent theft of industrial secrets and information that could benefit competitors.

Purpose

This policy is designed to protect IT Data in the organization, be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Scope

This policy applies to all the employees and to all equipment and data owned and operated by Lucid Colloids Limited.

A. Information Security

- Physical Security

For all servers and other network assets, the area must be secured with adequate ventilation and appropriate access.

It will be the responsibility of IT Dept. to ensure that this requirement is always followed. Any employee becoming aware of a breach to this security requirement is obliged to notify to their respective HOD or IT Department directly immediately.

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes in their Desktop, Laptop and mobile devices.
- Employees should ensure that technologies should be used and setup in acceptable network locations.

- The list of IT Products should include make, model and location of the device
- The list of IT Products should have the serial number or a unique identifier of the device and should be updated when devices are added, removed or relocated
- The IT devices should be periodically inspected to detect tampering or substitution.
- Employees using the IT devices should be trained and aware of handling the IT devices
- Employees using the devices should verify the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Employees using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised.
- All computer that stores sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

- **Information/Online Security**

- All machines must be configured to run the latest anti-virus software as approved by the Company The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans
- End users must not be able to modify and any settings or alter the antivirus software
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.
- Firewalls must be implemented at each internet connection and any demilitarized zone and the internal company network.

- **Technology Access**

Employees are only authorized to use computers for official use.

Every employee will be issued with a unique user id to access the business technology and will be required to set a password.
Each password is not to be shared with any employee within the business.

IT Department is responsible for the issuing of the identification code and initial password for all employees.

Where an employee forgets the password then only IT department is authorized to reset password that will be required to be changed when the employee logs in using the new initial password.

The following table provides the authorization of access:

Technology – Hardware/ Software	**Primary Persons authorized for access**				**Secondary Person**	**tertiary Person**
Location wise	**Mumbai**	**Jodhpur**	**Meglasiya**	**Jhagadia**	**All locations**	**All location**
Desktop/ Laptops	Salamon Disosa	Dilip Singh	Dilip Singh	Ashok Patil	Sudesh Dandekar	-
Mailbox	Salamon Disosa	Dilip Singh	Dilip Singh	Ashok Patil	Sudesh Dandekar	-
ERP SERVER - RDP	Salamon Disosa	Dilip Singh	Dilip Singh	Ashok Patil	Sudesh Dandekar	-
Tally ERP	Sushant Gurav	Sushant Gurav	Sushant Gurav	Sushant Gurav	-	-
Nas Server	Sushant Gurav	-	-	-	Sushant Gurav	-

B. **Data Backup**

All backups must conform to the following best practice procedures:

- All data and utility files must be adequately and systematically backed up
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at sufficient distance away to escape any damage from a disaster at the Lucid site
- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency

User Responsibilities

- All users must store their all-important data/files in the Documents & LCL Data folder of a computer. (None of other folder's backup will perform unless requested & approved by concerns.)
- All users will get automated email notification of backup status of their systems.
- All users should ensure data is backed up before updating or upgrading software on their computer.

IT Department should ensure following methods:

- Backups should be performed regularly as per backup is scheduled.
- Backed up critical data on a regular basis in the backup systems.

Backup Schedules

The users work must not be impacted by the running of back-up jobs. Back-ups are scheduled as daily, weekly or monthly depending upon the requirements

Further, according to standard definitions of terms, back-ups are determined as full, differential and Incremental.

The detail Critical information and applications details:

Sr. No.	Applications	Key User/Responsible	System Details	Location
1	Tally ERP	Sushant Gurav	Server @ RB5518	DC Rabale
2	Relyon Saral Paypack	Salamon Disosa	AIO @ LCL/HO/IT/DT/01	HO - Mumbai
3	Matrix Cosec	Salamon Disosa	AIO @ LCL/HO/IT/DT/01	HO - Mumbai
4	CA Office (TDS)	Alpesh	AIO @ LCL/HO/IT/AIO/16 AIO @ LCL/HO/IT/AIO/01	HO - Mumbai
5	Sequrite Endpoint Security	Salamon Disosa	AIO @ LCL/HO/IT/DT/06	HO - Mumbai
6	Sequrite UTM	Salamon Disosa	UTM @ LCL/HO/IT/DVC/030	HO - Mumbai
7	User's systems folders & Files Documents & LCL Data & Mailbox .PST .OST	Salamon Disosa All Users	All Users Systems	HO - Mumbai

Backup schedules details:

Systems	Backup	Frequency of Backup	Location	Backup system	Backup Process	Backup location
DC Server (Tally	Primary	Daily	DC Rabale	Server Image @ Fission	AUTO	DC Pune
DC Server (Tally	Secondary	Weekly	DC Rabale	Latest database @ External	Manual	Y Vaza
DC Server (Tally ERP)	tertiary	Monthly	DC Rabale	Appended backup @ External HDD	Manual	A. Hargile
User Systems	Primary	Daily	HO - Mumbai	NAS	AUTO	HO - Mumbai
NAS SERVER	Primary	Weekly	HO - Mumbai	External HDD	Manual	SUM

C. Data Restores

Data restoration is a service performed by the IT Department to provide data recovery capability that may result from system failures, catastrophic occurrences or human error.

All Users must request data (files) to be restored by contacting to IT Department, preferably by raising mail with the HOD's approval. Only files which the user is authorized to access will be provided from the restore.

Users requesting a restore/s are required to provide as much information about the data (file/s) as necessary – this will include:

- The reason for the restore
- The name of file/s and/or folder/s to be restored
- Original location of file/s and/or folder/s

Backup and restore routines in place. Data (file) restores are normally carried out by the IT Support Team who will identify to restore files from a date specified by the user or from the nearest backed up date.

It is the responsibility of IT Department to ensure that the recovery procedures must be tested at least quarterly and Disaster Recovery procedures must be tested at least yearly.

Recovery tests must be documented by the IT Departments.

D. IT Procurements

IT procurement is the series of activities and procedures necessary to acquire IT products and services. IT procurement involves both strategic and administrative responsibilities.

The purpose of this policy is to provide a framework for the procurement of IT hardware and software within the Company.

IT Department should keep a "standard technology" list of preferred servers, desktops, mobile devices, etc., to provide a consistent environment and reduce complexity. The procurement of "nonstandard technology" should be avoided where possible.

The IT Department is the sole authority for submitting requisitions for IT equipment on behalf of any Department that has had approval for obtaining such equipment.

All IT-related hardware and software will be specified by IT Department. Hardware and software cannot be purchased without approval by IT Department. All equipment or software purchase requests, whether as individual items or as part of a larger project, must be sent to IT Department which will process the request pursuant to this policy.

- The IT Department will determine whether to approve, decline or amend the requirements for the purchase of the equipment.
- If an equipment or software purchase request is declined or changed, the IT Department will provide a brief explanation to the requesting Department/employee. The IT Department will keep the requesting manager informed of the decision and the outcomes if ordered.
- If the equipment purchase request is approved, with or without changes, IT will order the equipment directly from Company's suppliers. Where an equipment purchase is authorized and ordered, an installation window will be proposed; however, this may change according to IT priorities.
- The IT Department has a standard set-up procedure for new hardware, software and systems. This procedure ensures the equipment is configured correctly and that all IT security measures are addressed. This procedure includes the setup of passwords, anti-virus software, security marking the equipment and adding it to the Company asset management database;
- The IT Department will not install software or hardware unless it has been involved in the specification of both. Hardware and software may not be installed by non-IT staff.
- Installation of replacement equipment will be given priority over new equipment in order to maintain continuity of the existing service.

Training and awareness

The requirement of this policy will be brought to the attention of employees via the Company's induction training programme.

This policy will be brought to the attention of all Employee responsible for purchasing and procuring IT equipment.

Amendment

This policy may be amended/updated from time to time with the approvals of the Management.

Adopted by the Company as of March 28, 2018.

Uday Merchant
Managing Director