Information Security Policy

Version: 1.6
Updated as on: June 2022

PREFACE

To all Employees and Contractors

We are rolling out the Information Security Policy to comply with our mandate to protect customer information that we get access to and also the intellectual property of the organisation.

We request everyone to review this document in detail and understand the same. If anyone is unsure about what constituted Information Security Policy, then he/she should ask his/her supervisor for further guidance and clarification or can contact the IT Department.

All terms and conditions as stated in this document are applicable to all employees and contractors within the organisation's network. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned herein. Any user violating these policies is subject to disciplinary actions deemed appropriate by the organisation.

This Information Security Policy will be modified/updated at the discretion of the management and the updated version will be shared with everyone.

It is mandatory that everyone fill in details in the last page (User Compliance), sign and provide the document to IT Department.

1. USER RIGHTS

1) All Users' systems will be given sufficient rights to perform their job function.

2) Where possible no one person will have full rights to any system. The IT Department will control network/server passwords and system passwords will be assigned by the system administrator to the users.

3) The system administrator will be responsible for the maintaining the data integrity of the users' data and for determining end-user access rights.

4) Access to the systems/Internet will be by individual username and password.

5) Usernames and passwords must not be shared with others nor be written down.

6) Usernames will be mapped to email addresses that will be assigned to each user.

7) All users will have an alphanumeric password of at least 8 characters and passwords will expire every 90 days and must be unique.

8) CMD and System Admin have read and write access to USB and DVD writer. Except CMD and System Admin, all employees' workstations and laptops will have no access to USB and DVD.

9) Employees cannot carry any DVD/CD and Pen Drives inside the organisation.

10) Printer should be used judiciously for business purpose only. All print out given by the user should be collected from the printer and used accordingly. No print outs should be left on the printer. IT Department will be responsible to track these and alert the respective stakeholders in case of any misuse or defaults.

11) Access to the network/servers will be restricted to normal working days. Users requiring access during weekends or holidays, requisition to the IT Department to be made in advance via email with brief details through their Project Managers.

12) The HR Department will notify the IT Department of all employees leaving the organisation's employment on the date acknowledgement of resignation is issued. The IT Department will then remove the employees' rights to all systems.

13) All users can submit their requisition to the IT Department via Email. In extreme situation, personal requests will be addressed by the IT Department.

14) Employees can escalate if the request was not solved in defined SLA in the following order:

    1. LSIT Support
    2. IT Manager

2. Internet Access Policy

1) The internet service should be used primarily for official purposes.

2) Users should not access any non- business-related internet sites. Doing so can lead to disciplinary action (up to and including) termination of employment.

3) User should not download any software including freeware without prior permission from the IT Department. Doing so can lead to disciplinary action (up to and including) termination of employment.

4) User should not involve Hacking into unauthorised websites.

5) Internet access is limited to job-related activities only and personal use is not permitted.

6) Personal Chatting services such as Skype and other chat applications are restricted to only customer interfacing people. The list of employees having this privilege is mentioned later on in this document and it will be updated at the discretion of the management.

9) The IT Department will have complete control on the Username and Password of the Skype and MSN chat services and will be configured and maintained by them. This is applicable to everyone.

3. Email Access Policy

1) The email service must be used primarily for official purposes. Non-business related emails are restricted.

2) Sending attachments will be provided for all users. The list of employees having this privilege is mentioned later on in this document and it will be updated at the discretion of the management.

3) Since email accumulates over time, the storage in email servers can overflow. Users must, therefore, regularly clean out their mail-boxes, failing which system administrator may delete excess emails.

4) User should not share the company's confidential information outside of the company, without authorisation, at any time. Users are also not to conduct personal business using the company computer or email.

5) Viewing pornography or sending pornographic jokes or stories via email, is considered sexual harassment and will be addressed according normal legislative laws.

6) Keep in mind that the company owns any communication sent via email or that is stored on company's equipment.

7) Management and other authorized staff have the right to access any material in your email or on your computer at any time.

8) Please do not consider your electronic communication, storage or access to be private if it is created or stored at work.

9) User should not send or post information that is defamatory to the company, its products/services, colleagues and/or customers.

10) Users should not send or post chain letters, solicitations, fraudulent, threatening, anonymous, harassing emails or advertisements not related to business purposes or activities.

4. Use of only Licensed Software

1) Software programs are covered by copyrights and a license is required for their use. IT Department will ensure that they have either a commercial or public license (as in the case of 'free' software) for any software they install on the systems that they are responsible for.

2) User should not use any pirated software over the network.

3) The downloading and use of software that is not characterized as public domain or 'free' is prohibited. Also, installation of these software's without prior approval from the IT Department is prohibited.

5. Backup and Physical security

1) All contractors working within the organization environment are to be supervised at all times by the respective Project Managers and IT Department should be notified of their presence and provided with details of all work to be carried out, at least 48 hours in advance of its commencement.

2) Project Managers should ensure the IT Department is informed at least 24 hours before any resources working on weekends.

3) Users must logout of their workstations when they leave their workstation for any length of time. Alternatively, Windows workstations may be locked.

4) All unused workstations must be switched off at the close of work every day.

5) All servers will be kept securely under lock and key. Any attempt for unauthorized entry to the server room will be dealt severely.

6. Usage of Finger Print

1) All employees register finger print every day without fail. Employee should not enter the office without swipe card.

2) All employees should show the access card on every IN/OUT from the office premise.

3) In case the employee have lost the Swipe card, it should be informed to IT Department and HR, and the new card will provided by IT Department as per the HR Policy of the company.

4) In case the Swipe Card entries not recorded on any day for IN/OUT, then it will be considered as loss of pay by the HR.

7. Laptop Policy

1) Ownership of the Laptop will reside with the company and the same shall be returned to the company upon completion of the time for which laptop is handed over, resignation by\termination of the employee.

2) It is the employee's responsibility to take appropriate precautions to prevent damage to or loss/theft of the Laptop.

3) It is recommended that laptops, even when protected by password, should not be left in the care of any person who is not trusted to protect the information it contains.

4) Sensitive data stored on a laptop should be kept to the minimum required for its effective business use in order to minimise the risks and impacts should a breach occur.

5) Laptops should be secured to a desk or other appropriate point using an appropriate locking mechanism.

6) Do not leave laptops unattended in insecure areas. For example, meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available.

7) Do not use laptops with removable media in places where that media could easily leave behind or misplaced.

8) When travelling, avoid placing laptops in locations where they could be easily forgotten or left behind. Example, overhead racks and taxi boots.

9) Be aware that the use of laptops in public places will likely draw the attention of those in the vicinity. It is possible that information viewed on a laptop screen could lead to the unauthorised disclosure of that information being processed.

10) The laptop will be configured with all suitable software & handed over to employee when he/she receives it for the first time. They should not install any other software than the ones installed without IT Department's prior approval.

11) The laptop would be submitted to the IT Dept. during any long-term absence (1 months or more), unless the employee gets an approval from the management.

12) The Employee is responsible for maintaining monthly backup files of their Laptop as an added precaution against data loss.

13) As virus causes high damage to laptop, employees are requested to upload antivirus package & update it once a month.

14) In case of any damage to the laptop due to employee's negligence/misuse, the cost of the damage would be recovered from the employee. If the damage is irreparable then the cost of the Laptop would be recovered.

15) The Company reserves the sole right to cancel the eligibility of employee to have a company Laptop at any time without giving any prior notice

16) While returning the Laptop the employee will get it checked and certified OK by the System Administrator, in order to ensure that the Laptop is in working condition with all applications working properly. In case there is any damage from the condition it was given to the employee, then the cost for the same will be recovered from the employee.

8. Auditing and Monitoring for IT Department

1) All network wiring along with drawings will be fully documented.

2) The IT Department will keep a full inventory of all computer equipment and software in use throughout the company.

3) Computer hardware and software audits will be carried out periodically. These audits will be used to track unauthorized copies of software and unauthorized changes to hardware and software configurations.

4) The operating system will be kept up to date and patched on a regular basis and the evidence should be documented for audit.

5) Servers will be checked daily for viruses and Symantec Antivirus report should be documented for audit.

6) Network/server supervisor passwords and system supervisor Passwords will be stored in a secure location in case of an emergency or disaster. For example, a fire safe in the IT Department.

7) IT Department should attend all the request raise by user Via internal Ticket tool/ Email within the defined SLA. The report for the same should be generated for audit.

8) Data stored laptops/Desktops should be securely erased before the laptop/desktop is reassigned for another purpose or disposed of when redundant. Failure to securely erase data may result in that data being available to the new owner/user of the laptop/desktop.

9) Users of laptops will be given appropriate training and instruction in the use of the laptop and its security functionality. This should include their responsibility for safeguarding the laptop and their obligation to comply with relevant information governance security procedures of the organization.

10) The use of any equipment outside the organization’s business premises for processing company information must be authorized by the management. The NDA form should be signed by employee and it will be authorized by the management.

11) For all the external resources working for us, the Project Manager should take an undertaking from these resources of having deleted the entire project related data.

12) An acceptable form of encryption should be provided at file or directory level to enable sensitive data to be encrypted whilst at rest.

13) Laptop BIOS passwords will be used to prevent BIOS settings from being changed.

14) IT Department should sweep unwanted data in all the desktop/laptop every month.

15) All connections made to the organization's network from outside the organization environment by the IT Department should be logged. The preferred method of connection should be using:

    a. Secure VPN connection, using IPSEC or SSL or Remote terminal.

16) Documents for the following will be maintained and should be available at any time to the authorized personnel:

    1. Software license details
    2. Hardware details
    3. Data Backup report
    4. Purchase Order copies
    5. Vendor details
    6. Inventory details
    7. Password Registry
    8. Bio-Metric report

17) A Business Continuity Plan will be developed and tested on a regular basis.

User Compliance

I confirm that I have read and understood the Information Security Policy of the organisation. I will abide by this Information Security Policy I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action will be taken.

At the time of my exit , I will abide by the rules and regulations of the organization. I will not be taking any data / documents with me from the company provided IT Asset and if the organization finds me violating the above they can proceed with legal action against me.

I would be solely responsible incase of any data transfers of the clients and will not use the knowledge gained in LanceSoft with the other competitors and can be prosecuted if found guilty.

Employee Name:

Employee No:

SIN/SSN/PAN:

Permanent Address:

.....

.....

.....

Employee Signature: ..... **Photo**

Date: