**INFORMATION SECURITY**





USER HANDBOOK

January 1 2017

Foreword 3

Confidentiality 3

Integrity 3

Availability 3

Accountability 3

Information Security Prerequisites 4

Access to Information Systems 4

Password 4

PC / Laptop Security 6

Mobile Computing 6

Physical Access 6

Internet Usage 7

Email Usage 7

Clear Desk and Clear Screen 8

Computer Viruses and Worms 8

Software Use 8

Human Resource Security 9

Security Incidents 9

Security Violation and Disciplinary Action 9

# Foreword

JK Lakshmi Cement recognizes its dependency on Information Systems to enable effective operation of its businesses. It is, therefore, essential that this information (and the infrastructure that supports it) is protected from destruction, corruption, unauthorized access and breach of confidentiality, whether accidental or deliberate. The management is aware of the challenges and the risks posed by Information Systems and have formulated an Information Security Policy to set a framework for Information Security throughout the organization. The objectives of Information Security are to safeguard confidentiality, integrity and availability of information and ensuring accountability for information use.

## Confidentiality

Ensuring that information and processing capability are protected from unauthorized disclosure or use.

## Integrity

Ensuring that information held on Information Systems is not subject to malicious or accidental alteration and that processes function correctly and reliably.

## Availability

Ensuring that information systems (including stored information and processing capability) are always available to authorized users when needed.

## Accountability

Ensuring that users are held answerable for all actions carried out by them on Information Systems.

This Handbook on Information Security has been designed to provide employees with information on the use of information assets, the responsibilities that go with accessing the company’s Information Systems and the need for exercising caution when accessing these resources. This handbook is not a substitute for the Information Security Policy, the complete policy is available on Intranet under the section “Information Security” and these policies must be referred to by the users. It shall be the endeavor of every employee to ensure security of Information Systems, to help maintain the confidentiality, integrity and availability of these systems and to promptly report to the appropriate authority any actual or suspected security weakness or breach. Also, every employee will be accountable for his / her actions with respect to Information Systems.

# Information Security Prerequisites

The deployment and use of Information Systems in the company are governed by the Information Security Policy. Upon joining JK Lakshmi Cement, employees will be required to sign Information Systems Acceptable Use Agreement before they can access any of the company’s Information Systems.

As users of JK Lakshmi Cement Information Systems, all employees must:

1. Use Information Systems and data in a legal and ethical manner.
2. Use the Information Systems for legitimate business purposes only and not for personal benefit.
3. Promptly report any suspected breach of security policy to the IT Head. The name and details of the person reporting any security breach will be kept confidential, if so desired by the person. Additionally, information assets shall not be used to:
	1. Attempt to degrade system performance
	2. Deprive an authorized user access to a resource
	3. Obtain extra access or privileges, beyond those allocated
	4. Circumvent computer security
	5. Harass other users
4. Upon resignation, retirement or transfer, employees must hand over all company information, SAP Login ID, Email ID, Internet Access, VPN ID, computer peripheral, Mobile, IT devices, keys (keys of filing cabinets and storage shelves), identification badges and any files, documents, manuals, brochures, media, tokens and authentication codes to their respective IT Heads / Managers / Administration Department / HR Department as applicable.

# Access to Information Systems

Employees will be granted access to Information Systems based on business needs. The level of access granted and the activities that a user can perform on authorized systems would vary from user to user. Users will be assigned User ID and Password to enable them to gain access to Information Systems. The IT department regularly monitors and audits the usage of Information Systems. Users must remember that they are accountable for all actions committed on the Information Systems using their User ID and password. It is, therefore, essential that User ID and passwords are never shared with others and any suspected password compromise is reported promptly to Manager / IT Head.

# Password

Whilst User IDs identify users to the system, passwords are a mechanism for authenticating them to the system. It is, therefore, essential that password confidentiality be maintained at all times.

**Ideas for choosing a complex password**

1. Use passwords similar to car license plates utilizing letters and numbers to make up a phrase like
	* Too late again - 2L8again
	* Music is for me - MusikS4me
2. Mnemonics - Passwords formed by using the first letters of the words that make up any popular or personal phrases:
	* water, water everywhere and not a drop to drink - Wwe&nadtd
	* The grass is greener on the other side - Tgigotos123
3. Some applications have a password-saving feature that allows storage of user’s password, which may save time, as well as the trouble of remembering passwords. Users must not use these Password-Save-features in any application or software, as they defeat the purpose of using a password for improving security.
4. Users must not store passwords in files on their workstations, in readable format using Notepad, Word, Excel, etc. In addition, users must never write down passwords on paper. Users must memorize their passwords.
5. If any password has been compromised or suspected of being compromised, users must immediately change the password and report the same their Manager / IT Head.
6. Users will be assigned a password at the time of their User ID creation, which will be communicated to them. It will be the responsibility of the users to change this password at the time of their first login.
7. The passwords selected by the users must be at least 8 characters in length consisting of alphabets, numerals and special characters. The time and effort required to break a longer password is much more than that required for breaking a shorter password.
8. Users must change passwords at least every 90 days. Frequent password change prevents unauthorized users from gaining access to a user account.
9. Users should note that user accounts would be automatically disabled by the system if incorrect passwords are entered five times.
10. When receiving technical assistance from help desk, users must input all passwords themselves rather than letting the help desk personnel enter the password. To ensure that passwords are difficult to guess, users should note the following tips:
	* Passwords must NOT contain consecutive identical characters or all-numeric or all alphabetical groups (aaaa, 1234, abcdefgh, etc. are weak passwords)
	* Passwords must not be based on anything that somebody else could easily guess or obtain using collateral information like:
		+ Names, telephone numbers and date of birth
		+ Passwords relating to one's personal work life
		+ Common dictionary words
		+ Technical words relating to the company’s Information Systems environment
		+ Famous dates, people, company names
11. IT department will not keep any password of any person. End user has to write down the password in his diary / note book.

# PC / Laptop Security

1. Users are responsible for their PCs/ Laptops and must not install unauthorized software (shareware, games, etc.). Users must not share folders or disk drives on PCs or laptops unless shared folders are password protected.
2. Users must log out of their active sessions on completion of work to prevent unauthorized people from carrying out any activity in their absence. Users must switch off their computer at the end of the day. This reduces the risk of computers getting hacked or infected by viruses/worms when unattended. Switching off computer at the end of the day also saves precious energy.
3. Users must periodically delete confidential information from the local hard disk that is no longer needed or move it to a secure location on the server to reduce the chances of confidential information from falling into wrong hands.
4. User must not attempt to access any data or programs for which they do not have authorization or explicit consent, or inappropriately use any system utilities.
5. All Laptop should be insured from 1st day of receiving the laptop. Pl contact with IT department for taking the insurance in company’s account. This is applicable only for company’s property.
6. If Laptop is not insured and it is stolen concerned employees will be responsible for that. The books value will be debited to concerned employees

7. Life of Laptops is considered for 5 years. Laptop can be replaced after usage of 4 to 5 years considering the workload on laptop

8. If anyone is having laptop, he will not be entitled to keep desk top. One item either desktop or laptop will be provided at any level.

# Mobile Computing

1. Users must make sure that laptops are locked in a secure area, at the end of / working of the workday if left the working place.
2. Laptops / Mobiles must not be left, unattended in cars, public places like airports, restaurants, phone booths, etc.
3. While travelling by air, users must always carry laptops as hand-baggage in a laptop carrying case. Laptops must not be checked-in. When required to be left in hotel rooms, users must lock laptops inside their luggage or make sure that it is kept out of sight. Personal laptops must not be used within the organization premises. Doing so may unintentionally expose our organization’s network to security threats. In addition, users also must not use personal removable media. (USB drive, CDs).
4. Only company issued data cards / modems / Mobiles must be used to connect to Internet. Users must ensure that they are disconnected from the LAN while using data cards / modems.
5. Users must immediately report the loss / theft of a laptop/ handheld devices to their respective manager and if so advised by the manager, the user should file a Police complaint.
6. Users must not synchronize their PCs / laptops or emails with PDAs and Handheld device unless these devices have been authorized or issued by Corporate IT for such purpose.
7. Users must ensure the security of their company issued handheld device. In case of loss or theft of a handheld device, it must be immediately reported to the manager / IT Head and if advised must file a police complaint.
8. The physical security of mobiles / Laptop shall be ensured to protect the information residing in these systems.
9. Employees, trainees and contract personnel to whom mobiles / Laptops are issued will be responsible for keeping it in safe custody.
10. IT person will keep mobiles details containing name of the staff and details of mobile issued (like make, model, serial number of machine and accessories) and Issue & Return Date.
11. While traveling, mobiles must be carried in safe custody, Mobiles should not be left unattended in Cars, Public places like airports, restaurants, phone booths, public transport etc.
12. The concerned staff must file a police report in the event a mobile is stolen or lost. The staff must also notify his /her manager or IT Head, within one business day of the theft / loss for blocking the apps installed on Mobile.
13. Mobile will be replaced only after completion of three years and 15% of the amount of net purchase cost of old mobile set will be recovered from end user.
14. Mobile used more than 01 year and less than 2 years by the employee leaving the organization shall necessarily to pay 60% of the purchase cost
15. Mobile used more than 02 year and less than 3 years by the employee leaving the organization shall necessarily to pay 25% of the purchase cost
16. Mobile used for less than 01 year by the employees leaving the company shall be handed over to the IT department in good condition otherwise purchase price will be deducted for the component.
17. Repairs &Maintenance: After expiry of warranty period all necessary repairs/replacement of the part etc shall be responsibility of the users including loss or damage to the mobile. But company’s work should not be suffered.
18. if company has provided mobile to any one, it is compulsory to use the company’s mobile only. JKLC will load software only official mobile.

# Physical Access

1. It is mandatory for all employees, visitors and personnel on a contract basis to wear their identification badges within the office premises.
2. Any employee, who has lost an identification badge, must immediately report the same to the administration department. The server rooms, network rooms, electrical rooms and AC plants are restricted areas. Unauthorized entry to these areas is strictly prohibited and will be viewed as a serious security breach.
3. Users must escort their visitors in all critical areas throughout the duration of the visit.

# Internet Usage

1. To facilitate carrying out their job functions, users may be provided with access to the Internet either through Wi-Fi, corporate network or through data cards as appropriate. All users have a responsibility to use the Internet access in a professional, lawful and ethical manner.
2. Users should be aware of the following risks posed by the Internet: Confidentiality of information is not assured. The information transmitted over the Internet can be accessed by anyone. Users must take due precautions such as password protecting documents while transmitting them over the Internet.
3. Privacy is not assured: Many web sites employ technologies (e.g. cookies, Java applets, ActiveX components) designed to enable interactivity, track user preferences and gather personal information without the user’s knowledge.
4. Reliability of information is not assured: There is no guarantee that information sent over the Internet will be received by the recipient.
5. Internet must be used only for business purposes. Use of company resources and Internet connectivity for personal use, including but not limited to personal entertainment, personal business or profit, and publishing personal opinions is strictly prohibited.
6. To ensure security and to avoid the spread of viruses, users must access the Internet only through the company provided facility. Bypassing the corporate network security by accessing the Internet directly by modem, mobile phones and data cards or other means is strictly prohibited. When authorized, access to Internet can be made through data card / modem however, only after disconnecting from LAN.
7. Users will not perform acts that waste information resources or unfairly utilize resources by spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, or otherwise creating unnecessary loads on network traffic associated with non-business-related activities as this would deny the legitimate users that necessary network bandwidth.
8. The company has the right to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace. Also, the organization may monitor the activities of the users in order to track unethical and unauthorized use of Internet.
9. Users must be aware that any activities performed on Internet can be traced.
10. User is not allowed to use his personal email like ( Gmail, Rediff mail, Yahoo..etc) in office and upload any document from PC / Laptop/ Mobile. If any person found to upload the official data on personnel email it will be offence.

# Email Usage

1. The company maintains its e-mail system solely for conducting its businesses. While incidental and occasional personal use of the company's e-mail system is permitted, users should remember that information and messages stored in these systems would be treated in the same manner as business related information and messages; hence, users must not assume privacy of the mails being sent/received.
2. The company reserves the right to review any emails on the official email system.
3. E-mail messages must be considered to be the same as formal, written company memoranda.
4. Contents of e-mail may be disclosed by the company either internally or where necessary to external parties without the permission of the users.
5. Users are not permitted to read another individual's e-mail without that individual's permission.

**Users shall NOT:**

1. Transmit or store offensive material.
2. Conduct or solicit for political, personal, religious or charitable causes or other commercial ventures outside the scope of their employment.
3. Use the e-mail system to create, send, receive, or store any materials that infringe the copyright or other intellectual property right of either the company or any third party.
4. Send fraudulent, harassing or obscene messages/attachments and/or materials.
5. Use the email for purposes that could reasonably be expected to directly or indirectly cause strain on any information facility, or interference with others' use of the e-mail system (e.g. attaching or sending large files to multiple recipients, sending or forwarding chain mails, etc).
6. If any spam, unknown or hoax mail is received, user must inform to IT Department. Such types of email should not be opened.

# Clear Desk and Clear Screen

1. Users must ensure that their desk and screen are clear during and outside normal working hours. This reduces the risk of unauthorized access, loss of and damage to information.
2. Users must store all paper documents and files in suitable locked cabinets, when they are not being used, especially after working hours.
3. Printouts must be collected immediately from the printer tray.
4. Documents which are no longer required must be shred (or torn into small pieces by hand) prior to disposal.
5. Password protected screen savers must be enabled to protect PC and laptop terminals that are left unattended. The automatic lock out time for screen saver must be set to five minutes.

# Computer Viruses and Worms

1. Software and information processing facilities are vulnerable to viruses and worms. These may affect the stability of the Information System and may cause damage or loss of valuable business data and information. All users, in order to ensure that viruses are kept out of the company’s Information Systems must follow the standards prescribed here :

**Users must:**

1. Ensure that their PCs / Laptops are installed with virus scanning programs. The virus-scanning program must never be bypassed or skipped.
2. Scan all removable disks (floppies, USB drive, and CDs) before use.
3. Not use disks containing unauthorized data and programs e.g. disks containing games, software utilities, etc.
4. In the event of an actual or suspected virus attack:
* Isolate the suspected diskettes, USB drives.
* Not use the virus-infected PCs. Inform IT helpdesk immediately.
* Await clearance from IT helpdesk before the PC can be used again.

5. User will not open any email or attachment which comes from unknown person to secure network / Pc's / Laptop from Spamming, Virus, Ransomware..etc

# Software Use

1. The company follows a strict policy of using only authorized and licensed software on its systems. As a general rule, all software procurement and installation will be done by the organization. This ensures that the software is procured from approved suppliers, meets quality standards and functional requirements, is adequately tested prior to use and is installed according to prescribed configurations. Users are strictly prohibited from installing any other software on their PC/Laptops unless explicit approval has been obtained from the IT Head. Shareware / freeware and open source software can be installed on PCs only if authorized by IT Department.
2. Users must not use unlicensed software, shareware, public domain software or pirated software.
3. Users must not make copies of software.
4. Unless authorized, users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system.
5. Machines access will be provided through Domain Server.
6. Important data must be kept in DMS and should approved from HOD
7. It is the duty of all end users to upload latest version / new documents of important documents on Document Management Server on timely basis and it should be duly approved by HOD. If any help is required he may contact with IT head. These types of documents may be : Drawing of Plants, Licenses, Manual, Protocols of Plants, Maps etc.

# Human Resource Security

1. Any employee / trainee / contract personnel, who becomes aware of any loss, compromise, or possible compromise of the Information Systems, or any other incident which has security implications on the Information Systems, will immediately report the incident to his respective manager/ IT Head.
2. When taking leave, employees should necessarily intimate manager/HR, in advance.
3. During transfer, resignation or termination, all employees shall complete a Clearance Certificate Form before being formally relieved from the company.
4. All employees shall attend security awareness training sessions.

# Security Incidents

1. An unwanted or unexpected incident that can cause damage to the security of the company information is referred to as security incident. Incidents can include but are not limited to unauthorized access, malicious code, network probes and denial of service attacks.
2. User must promptly report any suspected breach of security policy (loss, compromise or possible compromise of information or any incident with security implications) to the IT Head.
3. User must assist in the investigation of the security incidents.
4. Users must not, under any circumstances, attempt to prove a suspected weakness. This shall be interpreted as a potential misuse of the system.
5. User should not change IP Address of Pc's / Laptops at his end. If any user is found to use the IP Address of any other PC/Laptop, he will be punished.
6. User is not allowed to connect his personal Mobiles on Company’s Wi-Fi/LAN

# Security Violation and Disciplinary Action

1. Acts constituting security violations include, but are not limited, to the following:
2. Non-compliance with the requirements of the Information Security Policy.
3. Exposing the company to actual or potential monetary loss through the compromise of Information Security.
4. Unauthorized use of company information or disclosure of confidential information.
5. Usage of hardware, software or information for unauthorized or illicit purposes which may include violation of any law, regulation or reporting requirements of any law enforcement or government body in any country.
6. Users must promptly bring to the notice of their IT Head, any violation or suspected violation of the company’s Information Security.
7. Users will be subject to investigation and disciplinary action for violation of company’s Information Security Policies. Such disciplinary actions may include Warning & Reprimanding, Fines and Penalties, Suspension, Termination or Termination of Contractual Agreements, Civil or Criminal Prosecution, any or all of the above.