INFORMATION TECHNOLOGY POLICY

IIPRD and Khurana and Khurana, Advocates & IP Attorneys

Last Updated: June 2020

About the Policy

Khurana and Khurana (K&K) and IIPRD (collectively referred to as Khurana & Khurana or K&K or "the firms" or "the firm" hereinafter) provide and maintain several technological products, services and facilities like Personal Computers (PCs), thin client devices, laptops, servers, telephones, Internet and application software to its employees for official use. The Information Technology (IT) Policy of the organization defines rules, regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them.

Purpose of the Policy

The primary purpose of the policy is to maintain, secure, and ensure legal andappropriate use of Information technology infrastructure established within, and by the firm in order to assure the usability and availability of those resources to all users. The firm recognizes the vital role information technology plays in effecting the business as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by the employees , the need for an increased effort to protect the information and the technology resources that support it , is felt by the firm, and hence this Policy.

User

Anyone who has access to IIPRD and Khurana and Khurana's Information Technology Resources, including but not limited to, permanent employees, temporary employees, interns, probationers, contractors, vendors and suppliers.

Apart from the professional, a limited amount of personal use of these facilities is permitted to the users, includingcomputers, printers, e-mail and Internet access, therefore, it is essential that these facilities are usedresponsibly by users, as any abuse has the potential to disrupt the firm business and interfere withthe work and/or rights of other users. It is therefore expected of all users to exercise responsibleand ethical behavior while using the firm's Information technology facilities.

Scope

This policy applies to everyone, in all the firm's offices throughout India, who has access to the firm's Information Technology Resources and it shall be the responsibility of all the office heads to ensure that this policy is clearly communicated, understood and followed by all users.

This Policy also applies to all contracted staff and vendors/suppliers providing services to the firm that bring them into contact with the firm's Information Technology resources. The HR / Admin department and the respective Office heads that contracts for these services shall be responsible to provide the contractor/vendor/supplier with a copy of this Policy before any access is given to them.

These policies cover the usage of all of the firm's Information Technology and communication resources, whether they are owned or leased by the company or are under the company's possession, custody, or control, including but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), laptops, workstations, wireless computing devices, telecomm equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected.
- All electronic communications equipment, including telephones, voice-mail, e-mail, fax machines, Internet and intranet and other on-line services.
- All software including purchased or licensed business software applications, firm's in-house developed applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on the firm's owned equipment.
- All intellectual property and other data stored on the firm's Information Technology equipment.

The Policy

The use of the firm's information technology resources in connection with the firm's business and limited personal use is a privilege but not a right, extended to various users. The privilege carries with it the responsibility of using the Information Technology resources efficiently and responsibly. By accessing the firm's Information Technology Resources, the user agrees to comply with this Policy. All users also agree to comply with the applicable laws and all governing contracts and licenses and to refrain from engaging in any activity that would subject the firm to any liability. K&K reserves the right to amend these policies and practices at any time without prior notice. Any action that may expose the firm to risks of unauthorized access to data, disclosure of information, legal liability, or other potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

General standards

- Responsible behavior with respect to the electronic information environment at all times.
- Compliance with all applicable laws, regulations and the firm's policies
- Respect for the rights and property of others including intellectual property rights
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information and electronic infrastructure and systems.
- Users will be fully and individually responsible for any data breach or breach of confidentiality that might take place and therefore are to handle/access/manage all data with full responsibility of its confidentiality any liability that arises therefrom.

Software Installation

The IT Team shall make sure that the computer devices have all licensed software (operating system, antivirus software and necessary application software) installed in the system before giving out the laptops to the employees. The Employees shall respect the anti-piracy laws of the country, and the policy of the organization which does not allow any pirated/unauthorized software installation on the laptops owned by the organization. In case of any such instances, the firm shall hold the individual personally responsible for any pirated software installed on the computers provided to them.

Information Technology Resources

Information Technology Resources for purposes of this Policy include, but are not limited to, the devices owned or those used under license of the organization or contract or those devices not owned by, but intentionally connected to the firm's owned Information Technology Resources such as computer hardware, printers, fax machines, voice-mail, software, e-mail and Internet and intranet access.

Passwords

- The Individual password security is the responsibility of each user and in order to ensure that these systems perform effectively, the users must choose strong passwords.
- Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them.
- Passwords must not be written down and left in a place where unauthorized persons might discover them.
- The Users shall use another user's account or password without proper authorization.

Software Licensing Policy

- All users must comply with the software licensing policy for all software, including purchased or licensed business software applications, firm's in-house developed applications, employee or vendor/supplier-written applications, computer operatingsystems, firmware, and any other software residing on the firm's owned equipment.
- No user must use/install/download anysoftware for their individual use or even for business purpose without prior express written approval of the IT Head.
- All approvals are only to be taken in written format and not verbally.
- In case any such software is found on any of the firm's system whichis not allocated to the individual user, it shall be the responsibility of the user to inform thesame to the IT department, in cases the same is not installed by the said user otherwise the firmretains the right to initiate appropriate disciplinary proceedings against the said user.
- The necessary software's for the everyday office needs are pre-installed on all the firm's systems and any request for additional needs should be addressed to the IT Head for approval.
- Apart from 3rd party software, few software are developed & copyrighted by the organization and belongs to the organization.Any unauthorized use, storage, duplication or distribution of such software is illegal andsubject to strict disciplinary action.
- The IT Department shall apply the software patches and regularly monitor the updates for both in-house developed and external software used by the firm's system, if automatic updates aren't available.
- Use of the firm's network resources to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited. No user shall make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

Internet and Intranet Usage Policy

- Internet software may only be installed / used by or with the approval of the IT Head.Software patches or updates may only be downloaded, subject to approval and ensuringstrict adherence to the vendor's security and usage guidelines.
- Access to the internet and its resources is provided for the primary purpose of conducting business on behalf of the firm but certain reasonable personal use of the Internet is permitted, according to constraints set out by the Anexgate Firewall.
- The IT department reserves the right to block access to any Internet resource without any prior notice. In case anyone required access to a certain restricted site, the same may be dealt asspecial case provided the same is identified as an use strictly for official purpose. The approval for the same needs to be obtained by theDepartment Head / Branch Manager from the IT Head.
- No user shall engage in any such activity that would potentially corrupt the firm's IT systems with imported viruses. Such activity consists of, but is not limited to, downloading files from unauthorized servers, games, entertainment software or other

inappropriate files (for example,video or audio materials for personal use), playing games against opponents or gamblingover the internet.

- The users shall not conduct any form of "hacking" or use malicious code topenetrate or attempt to penetrate other computers or to deliberately release viruses orother harmful programs within either the firm's network or the internet or bypasssecurity features.

Information Security Policy

- Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction.
- The firm protects data integrity based on data classification and secures the organization's information systems through the use of thin-client architecture. It helps in securing and maintaining the client data, locally within the office premises.
- The thin-client system facilitates immediate access to virtual desktops and applications and offers centralized computing capabilities and any hardware or software upgrades and application changes are easily be made in the data center.
- A number of methods like access control, authentication, monitoring and review are used in ensuring data security in the organization.
- The IT Department shall, on a regular basis, reviews servers, firewalls, routers and monitorsthe IT system that includes monitoring of access logs and intrusiondetection software logs.
- Access to the network, servers and systems in the organization should be achieved byindividual logins and will require authentication. Authentication includes the use ofpasswords, biometrics or other recognized forms of authentication.
- The firm's firewall system helps in filtering and blocking in any form of intrusions and is implemented on all servers and workstations, while also disallowing most-third party websites unless they are required by the respective team to perform their work.
- Client data that are private and confidential shall be encrypted and password protected, both while the data is in system and when there is any sort of movement of such data over insecure channels.

Email Usage Policy

- All the employees of K&K are provided with an office E-mail account, and the same is protected with a password which is provided to the individual user. The use of E-mail should be restricted only for the business purpose; however personal mail can also be exchanged to a limited quantum provided that such exchange does not amount to breach of this IT policy or otherwise materially affects the firm's operations.
- An employee found using e-mail service, which is objectionable by any means; the access can be terminated by IT department without any prior information.

- In use of the email, the employees should be aware that exchange of information with external sites may not be secured with there being high risks of spam, Trojans, malicious codes etc. Hence the exchange of information should be limited to reliable sites.
- All material contained on the email system belongs to the firm and users should consider messages produced/received by them on the firm's email account to be secure. The confidentiality of email data should be maintained by every individual user.
- It is of paramount importance that the security regarding access to the email system is protected. User identities and personal passwords must not be shared with others and the users should be cautious of providing their email addresses to external parties, especially mailing lists.
- The users are allowed a reasonable personal use of the email system but such use shall not interfere with the firm's operations, or take precedence over the user's job accountabilities.

Phone Usage Policy

- Landline phone systems are installed in the firm's offices to communicate internally with other employees and make external calls.
- The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the firm.
- The IT Dept. is responsible for maintaining telephone connections in offices. For any problems related to telephones, they should be contacted.
- Employees should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the firm's phone services.

Antivirus and Firewall

- Licensed antivirus and firewall software (Anexgate) is installed on all PCs and laptops owned and distributed by the firm.
- The software is a gateway system that is connected via LAN and filters and protects internal and external data, information, applications from unauthorized access, altercation and destruction.
- Employees are expected to make sure their Antivirus and Firewall is updated regularly. The IT Dept.should be informed in case of any problem relating to it.
- Any external storage device like pen drive or hard disk connected to the PC needs to becompletely scanned by the Antivirus software before opening it and copying files to/fromthe device.

Data Backup

In order to prevent loss of information and data by destruction of the magnetic means in which it is stored, a periodic backup procedure shall be carried out. The responsibility for backing up the information located in shared access servers is of the IT head. The firm's system management backs up all the information and servers in the databases through an automated procedure, however, the data backup in computers and laptops is the responsibility of the users whom the computer has been assigned. Additionally, the users shall wherever possible keep certain important official data in an external storage device for extra security of such information.