INFORMATION TECHNOLOGY POLICY

Overview:

This Policy outlines the terms and conditions for use by all employees of Alok Industries Limited (hereinafter referred to as the Company or Alok) across all locations, of the Company's Information Technology assets. All employees are expected to strictly adhere to these terms and conditions.

All employees use computing devices provided by the Company with access to the Company's Information Technology network and other Information Technology facilities such as printers, scanners, facsimiles, e-mail, Intranet, Internet etc. Employees also may have access to the Company's Information Technology facilities through their mobile devices. Such access and facilities are provided to employees for the purpose of conducting Company business. Everyone must use these facilities responsibly; any misuse can potentially impact productivity, disrupt Company business and interfere with the work or rights of others. Therefore, all employees are expected to exercise responsible and ethical behaviour when using the Company's Information Technology facilities. Any action that may expose the Company to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action leading up to and including termination of employment and/or criminal prosecution.

The use of the Company's information technology facilities in connection with Company business and limited personal use is a privilege but not a right extended to various Company employees. Users of Alok's computing facilities are required to comply with all terms and conditions referred to in this Policy.

This Policy outlines the standards for acceptable use of Company's computing and information technology resources, which include, but are not limited to, equipment, software, networks, data, and telephones whether owned, leased, or otherwise provided.

Scope:

This Policy applies to all Alok employees worldwide and to all employees of Alok's subsidiaries and affiliated companies. It is the responsibility of all operating units to ensure that these terms and conditions are clearly communicated, understood and followed.

These terms and conditions also apply to software contractors, and vendors/suppliers providing services to Alok that bring them into contact with Alok's Information Technology infrastructure. Alok employees responsible for these services shall provide the contractor/vendor/supplier with a copy of these terms and conditions before any access is given.

These terms and conditions cover the usage of all of the Company's Information Technology and communication resources, including, but not limited to:

INFORMATION TECHNOLOGY POLICY

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, Laptops, terminals, workstations, PDAs, 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, pagers, radio communicators, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, Internet and intranet and other on-line services
- All software including purchased or licensed business software applications, Company-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on Company-owned equipment
- All intellectual property and other data stored on Company equipment
- All of the above are included whether they are owned or leased by the Company or are under the Company's possession, custody, or control
- These terms and conditions also apply to all users, whether on Company property, connected from remote via any networked connection, or using Company equipment

Objectives:

- Provide communication/messaging infrastructure
- Provide secured and restricted internet access
- Provide interoffice communication through intranet
- Secure the infrastructure through user authentication
- Identify the software needs to perform Company business
- Evaluate, procure and maintain system/application/security software
- Identify, procure and install infrastructure requirements
- Provide seamless computing environment to all the employees
- Secure the Company’s data
- Manage remote access through well-defined and secured environment

Infrastructure:

Computing requirements of employees are analysed and allocated based on their job profile. Individual owned devices are permitted only subject to BYOD Policy.

Employees do not have the right to demand for brand new systems or systems of any specific brand/configuration, they like. IT department in consultation with respective HoD shall decide on the configuration best suited for the role. Life of a laptop is estimated to be 5 years. Systems (<5 years old) of employees leaving the organisation shall be reallocated to new employees (preferably of the same department).

INFORMATION TECHNOLOGY POLICY

In the event of systems being replaced with new systems, employees are expected to pro-actively return the earlier system in good working condition. Any physical damage found then shall attract penalties as listed below. If the older system is not pro-actively returned within 10 days of allocation of new system, the new system shall be transferred to employee's ownership and total cost shall be debited and recovered from his/her next salary.

Every employee, irrespective of the grade, is eligible for only one computer (desktop/laptop), except in special cases approved by a key management personnel.

Desktops/Laptops are procured with pre-configured operating systems. Company's standard procurement system is followed for all IT procurements.

Laptops are allocated to users to provide uninterrupted business support, as and when required. You are expected to carry the laptop along with you. If not taken along with you, it should be kept under lock and key.

Computing devices such as desktops/laptops/printers etc are procured specifically for a location and department. Any request for transfer of assets from their allocated location/department need approval by HoD and clearance from Finance/Accounts (after necessary updation in fixed asset system). Such assets once approved/cleared shall only thereafter move out of office premises accompanied by a gate pass duly checked (physical) and approved by Admin.

Only confirmed employees will be entitled to laptops. The system of allocating new desktops/laptops shall be based on seniority of employees in terms of their grade. Exceptions, if any, need to be managed by swapping systems within the department by HoD, with formal intimation to IT department. Laptop users shall not be eligible for accessories such as keyboard, mouse, monitor etc. Employees who need such accessories may procure and maintain the same at their own cost and risk.

USB ports/SD slots are disabled on all systems, except in special cases approved by a key management personnel.

In case of termination/resignation of an employee, the Company reserves the right to immediately:

i. take possession of the concerned employee's computing device without any prior intimation to the concerned employee and erase all information stored on the said device, including personal data if any and

ii. deny access to any of the company's Information Technology infrastructure to the concerned employee

If the employee fails to return the laptop after termination/resignation, cost shall be recovered from the full and final settlement as under:

I. 100% of the cost if the laptop is <=2 years old

II. 60% of the cost or Rs.25,000 whichever is higher if the laptop is 2-3 years old
III. 50% of the cost or Rs.20,000 whichever is higher if the laptop is 3-5 years old
IV. 40% of the cost or Rs.15,000 whichever is higher if the laptop is 5+ years old

Any damage to a computing device, regardless of the cause of such damage, shall be recovered fully from the concerned employee. All required repairs need to be strictly done through IT department at product's authorised service centre. Employees are not permitted to do any fixing/enhancement to systems allocated to them, under any circumstances.

In instances where a damaged device is required to be replaced due to:

i. Severity of the damage, then the entire replacement cost is liable to be recovered from the employee.
ii. Obsolescence of the damaged device, a flat amount of Rs 10,000/- shall be recovered from the concerned employee

The Company reserves the right to periodically examine any system and other usage and authorization history as necessary to protect its computing facilities. The Company disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

The Company will have unrestricted access to all desktops/laptops i.e. all computing devices at all times without prior intimation to the concerned employee(s).
The Company is not responsible for any loss of data from an employee's computing device due to any reason whatsoever.

Employees are strongly advised to refrain from storing any personal or business critical data on their devices.

To ensure physical security of the computing devices allocated to you for business and also save substantially on energy costs, it is mandatory to shut down the devices while leaving office for the day. When the system is not in use for a long period say, exceeding 30 minutes (for eg. lunch break, leaving desk for meetings etc.), you may either switch off your computer or enable the energy saving mode.

Please configure your energy settings so that your computer goes to "sleep" after periods of inactivity or "hibernate". Sleep/Standby is a power-saving mode that allows a computer to quickly resume full-power operation (typically within several seconds) when you want to restart work. While Sleep mode puts your work and settings in memory and draws a small amount of power, Hibernation mode puts your open documents and programs on your hard disk, and then turns off your computer. Of all the power-saving modes in Windows, Hibernation uses the least amount of power.

In instances where the above is not complied with, half day's salary of the concerned employee (for any noncompliance during the month) shall be deducted (for the month) and credited to the "Staff Welfare Fund". In addition to this, in the event of any damage to the computing device being left on in violation of the Policy stated above, recovery shall be done as mentioned above (damage to a computing device).

Considering the potential destruction, theft and misuse of Company information, all employees are responsible to prevent unauthorised access to such information available on their respective computing devices.

Preserving the access to information resources is a community effort that requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable and ethical use:

- Use only those computing and information technology resources for which you have authorization.
- Protect the access and integrity of computing and information technology resources.
- Abide by applicable laws and Company Policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
- Use computing and information technology resources only for their intended purpose.
- Respect the privacy and personal rights of others.

Use only those computing and information technology resources for which you have authorization.

For example, it is a violation:

- To use resources you have not been specifically authorized to use by your HoD.
- To use someone else's account and password or share your account and password with someone else
- To access files, data, or processes without authorization
- To purposely look for or exploit security flaws to gain system or data access

Protect the access and integrity of computing and information technology resources.

For example, it is a violation:

- To use excessive bandwidth
- To release a virus or worm that damages or harms a system or network
- To prevent others from accessing an authorized service
- To send email that may cause problems and disrupt service for other users
- To attempt to deliberately degrade performance or deny service
- To corrupt or misuse information
- To alter or destroy information without authorization

INFORMATION TECHNOLOGY POLICY

Abide by applicable laws and Company Policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.

For example, it is a violation:

- To download, use or distribute copyrighted materials, including pirated software.
- To make more copies of licensed software than the license allows.
- To upload, download, distribute or possess pornography

Use computing and information technology resources only for their intended purposes.

For example, it is a violation:

- To use computing or network resources for advertising or other commercial purposes.
- To distribute copyrighted materials without express permission of the copyright holder.
- To send forged email.
- To send terrorist threats or "hoax messages".
- To send chain letters.
- To intercept or monitor any network communications not intended for you.
- To attempt to circumvent security mechanisms.
- To use privileged access for other than official duties.

Respect the privacy and personal rights of others.

For example, it is a violation:

- To use electronic resources for harassment or stalking other individuals.
- To tap a phone line or run a network sniffer without authorization.
- To access or attempt to access other individual's password or data without explicit authorization.
- To access or copy another user's electronic mail, data, programs, or other files without permission.
- To disclose information about Company.

Communication/messaging infrastructure:

All employees who need to communicate internally or externally have been provided Office 365. Alok respects the contents of your files and does not review file content. However, system administrators may become aware of file content while dealing with some system problems.

Please refer our “Email Policy” and “Email Protection Precautions” published on intranet (HR - Policies - Information Technology Polices) for further details.

INFORMATION TECHNOLOGY POLICY

Secured and restricted Internet access:

Internet access is provided only on need basis subject to approval from respective HoDs. Certain domains are blocked for all the users.

Locations access internet though local internet connections. Firewalls are installed to prevent intrusions and protect network from hacking.

Full time connectivity is provided only to those who need Internet for their day-to-day business activities. The system administrator is authorized to change the time slot or provide connectivity to any user, only on written request (duly approved by HoD) clearly indicating the reason/usage requirements.

System keeps a log of all the activities being done on net. Users are requested to strictly follow the Company Policy in this regard. Any violation of the Company Policy in this regard may result in disconnection of Internet access.

Intranet:

Locally hosted intranet is used to share General Company/Employees information. Employee specific information such as attendance, late marks etc., request for OD, leave etc. are also available on intranet. All employees can access intranet through the link “http://192.168.1.48/index.asp” from office network and “http://125.99.89.152/index.asp” from external networks.

Infrastructure Security:

The entire IT infrastructure is protected through “access card system”, firewall, anti-virus and anti-spam software. The network is available only to local users and connections through secured VPN client.

Software needs:

The software needs of the organization is analysed by IT department along with respective functional groups. After finalizing the requirements, applications are either developed in-house or procured externally depending on the internal resource availability and complexity of the system.

Infrastructure and organizational stability, Capital, Integrating with other software products, Maturity, Technology, Partner network, Resource availability etc. are the key factors on which software products and partners and selected.

Software for any special purpose is procured in consultation with the department head and management. These requirements are mainly application in designing and production areas.

INFORMATION TECHNOLOGY POLICY

Business applications are typically maintained in-house and adequate training is provided to the team during implementation. The software environment is further strengthened by entering into service agreement with product companies.

Only IT department is authorised to download/install any application on systems in the office network. It is a violation, if you download/install any application or make any configuration changes in applications installed on your system of your own.

Information security and Backup:

Information security is implemented through various physical/application/database specific tools.

Access to data centre, communication rooms are restricted through face recognition systems and physically monitored through CCTV. Applications such as Office 365, SAP etc. have their own role specific authorisations restricted through login id and password. Other structured data stored on central server is also accessible only through user authentication.

External devices such as USB drives, DVR/W drives etc. are disabled by default, except for those authorised by management.

Data is regularly backed up on external devices such as hard disks, other servers, CDs, data cartridges etc. Media is then stored in fire proof storages to safe guard against natural calamities.

SAP being the backbone of our business, 3 different technologies are implemented for data backup.

- Daily backup of online database and regular backup of archive logs on data cartridges.
- Online replication of database using Oracle log shipping on storage at a different geographical location through a dedicated communication link.
- Online replication of file systems using “double take” software on a landscape hosted at a different geographic location.

Data on local hard disks of desktops/laptops are not part of the automated backup system. Users are advised not to store any important data on the local storage. This data may not be recovered in the event of any system failure. Any important file kept on local storage, should be backed up regularly on CD/DVD by the user. IT shall not be responsible for the security of locally stored data.

File server installed at the data centre facilitates storage of shared structured/unstructured data such as word, excel files etc. This data is replicated and backed up regularly. Storage of any personal data such as songs, videos, photos, unauthorised software etc. are strictly not permitted on any systems in the network (file server/desktop or laptop). As part of the periodic clean-up, all such files are automatically deleted by IT department. All users are requested to do regular housekeeping by deleting unwanted files and not making multiple copies of files in various folders. Temp folder on this server is not backed up and hence do not store any important data in this folder.

Disposal of IT Assets:

All surplus or obsolete IT assets and resources must be discarded according to legal/accounting requirements and environmental regulations through appropriate external agents. It is mandatory for IT department to update accounts/inventory departments to ensure proper accounting of such disposals.

This procedure applies of all non-leased IT hardware, including PCs, laptops, printers, handheld devices, servers, hubs, switches, routers, and so on. Company owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this procedure. Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

IT department is responsible for backing up and then wiping clean of Company data from all IT assets slated for disposal, as well as the removal of Company tags and/or identifying labels.

Acceptable methods for the disposal of IT assets are as follows:

- Sold in a public forum.
- Auctioned online.
- Sold as scrap to a licensed dealer.
- Used as a trade-in against cost of replacement item.
- Reassigned to a less-critical business operation function.
- Donated to schools, charities, and other non-profit organizations.
- Recycled and/or refurbished to leverage further use (within limits of reasonable repair).

Printers/Scanners/Photocopiers:

Multi-functional printers are installed at convenient locations across the office. These being shared devices, print jobs get queued and then printed after users physically choose to print the same. Access to printers is provided depending on the geographical proximity of users, quantum of printing etc. Users need to get printers configured through IT department to use these devices for printing/scanning.

Use of personal printers is discouraged. However, in case of unavoidable requirements, they are provided on special request (duly approved by management).

Printing, photocopying and scanning facility should be used for official purpose only. Secured printing feature to be used to avoid print being taken by others. Use double side printing to optimise consumption of paper. Always destroy confidential information printed but not required for further use.

Antivirus:

Kaspersky end point security is enabled on all computer systems across locations. IT departments conducts periodic checks on systems to ensure that they are up-to-date and enabled for services such as “Auto Protect”, “Internet Worm Protection”, “Email Scanning” etc.

New patches are released often and the program is configured to automatically download the patches and update systems in the network. However, new viruses attack without any warning and there is a very high possibility that the antivirus program does not recognize the virus and destroys it. Despite all these protections, we are still at a high risk unless we are very alert.

Users are requested to check the date of the last updated virus definition and contact the system administrator, in case of any inconsistencies.

The main sources of viruses are Internet, emails, CDs and other external storage devices. An infected system can disturb all the systems in the network connected either through LAN (Local Area Network) or WAN (Wide Area Network).

Do not open any “doubtful” emails or pop-ups, if you are not sure/clear about the authenticity of the same. Many viruses/spams are propagated through mails with familiar names and subjects. Often, the underlying email id of such familiar sender will be unknown. Typically these mails will have some attachments, which are different from what you normally receive. Beware of attachments such as zip files, img files etc.

If you feel at any point that your system may be infected, shutdown the computer and inform the systems administrator. Do not use the system till the administrator checks and certifies the system.

A simple ignorance can cripple the entire IT infrastructure and hence you need to be extra vigilant in this.

INFORMATION TECHNOLOGY POLICY

Closed Circuit Television (CCTV) Monitoring & Recording:

The purpose of CCTV monitoring is to deter crime and to protect the safety and security of our resources. CCTV monitoring will be conducted in a professional, ethical and legal manner. Recordings may be retained for a period not to exceed 30 days and may then be overwritten, unless retained as part of an investigation or other bona fide use as approved by the management. Personnel involved in monitoring shall validate consistent recording of all cameras on a daily basis. Preventive maintenance of cameras and recording system shall be done at least once a quarter to ensure seamless functioning of the system.

Business continuity:

Business continuity plans to address remote work during natural disasters, pandemics etc are handled through remote access to applications and central IT resources. Secured VPN clients through firewall mitigates cybersecurity risks. Application connection is further validated through login credentials to ensure data security and operational effectiveness.

Virtual Meetings:

The full lifecycle of virtual meetings is automated through Microsoft Teams. Features such as recording, screen-sharing etc. make it easier to collaborate. The recording is automatically saved to Microsoft Stream which can be downloaded and shared. Both the meeting organizer and internal attendees can start or stop the recording.

Following are strictly prohibited and considered as violations:

1. Disable any encrypted tools installed on any systems in the office network (laptops, desktops or servers)
2. Interfacing the system to download/upload information from your system or any another system without authorization. This will have serious consequences.
3. Upload any company related information in the internet and social media without prior approval from management.

In case any employee is found violating any of the terms and conditions of the Policy contained herein, the Company reserves the sole discretion to deal appropriately with such violations, which may include monetary penalties and/or termination of employment.