INFORMATION TECHNOLOGY (IT) POLICY

Corporate Office

Arkade House, Next to Children's Academy,
A.S. Marg, Ashok Nagar, Kandivali (E), Mumbai
40 0101

Introduction

Arkade Developers Limited (Arkade) Information Technology (IT) Policy provides the policies and procedures for selection and use of IT within the business, which must be followed by all the users. It also provides guidelines that will use to administer these policies, with the correct procedure to follow. ARKADE will keep all IT policies current and relevant.

Any suggestions, recommendations or feedback on the policies and procedures specified in this policy are welcome.

These policies and procedures apply to all employees of ARKADE. These policies are in adherence to the Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023.

1. User Account and Data Management Policy

Purpose of the Policy

Unique user account controls access to the company's data. They are critical to any IT security program, and the proper creation, control, and supervision of all User accounts is vital.

The Data Management policy is involved in creating data management, access and usage policies, and involving information security, Backup and retention.

This policy applies to all accounts on any system that resides at any company facility, has access to the company network.

Procedure

The IT Department is responsible for ensuring that this policy is adhered to all authorized users will be provided a unique User account for their sole use. All accounts must be uniquely identifiable by an assigned user name. All accounts must have a password that complies with the Password Policy.

- Farvision ID will be provided to the users with a unique User account id for their sole use and providing them a required access rights with a respective module depending on their job profile/role.
- Users are accountable for their actions.
- Deletion rights for any transaction entry in system are restricted for all the users.
- Users can edit/modify the document if it is in provisional mode, once the document will get approved, user will not able to edit the document anymore.
- A new user is not permitted, under any circumstances, to inherit the User ID that was originally assigned to existing user.

All the business data should be store only on the Company Data server provided by the IT team and that will be mandatory for all the users (office users and site users)

User may store only the relevant business data on the data servers – any personal data will not allow to be kept on the data server.

User will restrict the access for their system's internal drives like D drive E drive etc.

All the project site users can access the server through secured VPN connectivity.

(In case of any HO users wants to access the server data from project sites/home, they need to informed IT team prior one day to get the access for the same though secured VPN connectivity.)

Joining / Exit Procedure:

In the case of a new employee, HOD/HR should intimate the IT team prior to 5 days of new user joining date for the provision of desktop/laptop, creation of a new email account etc.

At the time of joining, assign a Laptop or desktop system to the user with his Email id / Farvision id / printer setup etc.
Respective department's head will give approval for the access rights into Farvision /necessary folders on the data servers, so that user can access and modify files on the server.

Exit process: **HR team will intimate to IT team in advance for removing the access rights in Farvision/ data folders on server/email access/email forwarder etc. from effective date.**
Password change/Discontinuation of user's email id/Farvision id etc.

2. Information Technology

❖ Administration and Software Policy

Purpose of the Policy
This policy provides guidelines for the administration of information technology application/software's and resources within the business.

Procedure
All software installation work is to be carried out only by the IT Department.

Employees are prohibited from bringing software from their own and loading it onto the business's computer hardware. Unauthorized software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

Laptops, PCs or any asset which are given to the users are the property of Arkade and need to be returned once the employee who possesses the same is no more in the Arkade's services.

Once the project site is completed, all the IT systems including printers etc. needs to be handed over to Admin/IT department.

User should have to clear the data on weekly basis from their respective folder kept in Common folder on the data server.

❖ **Information Technology Security Policy**

Purpose of the Policy
This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

Procedure

- **Physical Security**

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access in the presence of IT Team.

All security and safety of all portable technology such as Desktop, laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued with the same. Each employee is required to use locks, passwords, etc. and to ensure the system is kept safely at all the times to protect the security of the same.

In the event of loss or damage, ARKADE will assess the security measures undertaken by the concern person to determine if the employee is required to reimburse the loss or damage to their IT resources.

- **Information Security**

All the relevant data and Server data is to be backed up.

It is the responsibility of IT Department to ensure that data back-up for all the servers are conducted on Daily Backup Basis.

Users are not allowing to download any executable files from internet.

Wifi device access is permitted only for Office Laptops/Desktop systems only, users will not allow to access Wifi network on their mobile phones, ipad etc.

For the Internet accessibility – only secured work-related site are accessible to all the users, if someone requires a particular blocked website to be whitelist, user must have to take a approval from respective HOD with keep management and HR in cc and inform to IT team.
Blocking Website category may include:

All the social media sites, spamming / phishing websites, other webmails sites like gmail, yahoo mail, rediff mail etc.,

The ITO will monitor user activity through monitoring and filtering software to prevent access to sites which are illegal or against Arkade's policies.

- **USB Drive Accessibility:**

For all the desktop/laptop users will not allow to transfer any data through any external devices like. Pendrive, hdd, card reader, mobile device etc. whereas all the USB ports have been set up as in read only mode for all the systems. If anyone wants to access/transfer the data through USB they must have to take an approval from respective HOD with keep management and HR in cc and inform to IT team. Digital signature dongle will be working even if the USB ports are in read only mode.

All technology assets that has internet access must have anti-virus software installed. It is the responsibility of IT Dept. to install anti-virus software and ensure that this software remains up to date on all technology used by the business. The Company has also in place a continuous security monitoring system to enhance resilience against cyber threats.
All information used within the business is to adhere to the privacy laws and the business confidentiality requirements.
Personal Laptops/Tabs are not allowed in the office as well as on the Project Site.

- **Information Security Audit:**

Periodic security audits of the Company's IT infrastructure shall be conducted at least once annually or as required. The audit findings, including identified risks and recommended actions, shall be reviewed by management, and necessary corrective measures shall be implemented in a timely manner.
The information security risks may include cyber-security threats, data loss, system failures, vendor risks, cloud-related risk etc.

- **Information security incidents or suspected information security incident reporting**

All employees, users, and stakeholders shall promptly report any actual or suspected information security incidents to the IT Department immediately upon becoming aware of such incidents. Once such an incident is reported, the IT Department shall investigate on the matter. If any serious incidents are found, legal actions will be initiated. Also, IT Department ensures that proper backups are being restored.

A "reportable incident" includes any actual or suspected event that may compromise the confidentiality, integrity, or availability of the Company's information systems or data.

❖ **Information Technology Email Policy**

Purpose of the Policy

The purpose of this email policy is to ensure the proper use of ARKADE email system and make users aware of what ARKADE deems as acceptable and unacceptable use of its email system.

This policy covers appropriate use of any email sent from ARKADE email address and applies to all employees.

Procedure

ARKADE email account should be used primarily for Company business-related purpose, non-Company related commercial uses are prohibited.

Email Id will be allotted above office asst. level for all the departments.

Email should be retained only if it is required for business record; all unnecessary emails (like any promotional emails/junk emails) are expected to be deleted by the employees.

Users can able to receive the emails from all the outside domain email ids, but they cannot send emails to outside domain email ids like on gmail.com, yahoo.co.in etc. They can send emails only within the arkade.com domain email ids.

If anyone required to send an email to any outsider email id, please take a prior approval from their respective HOD and HR. For HOD's need to take approval from Management and HR.

While on the primary stage, user should have to submit the outsider email ids list to get whitelisting those email ids in Email server for further communication.

The ARKADE email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

Employees who receive any emails with this content from any domain, employee should report the matter to their supervisor or It dept immediately.

ARKADE IT may monitor emails without any prior notice.

3. Confidentiality

Company confidential information must not be shared outside of the Company, without authorization, at any time. One should not conduct personal business using the Company's computer or email.

The Company ensures that, limited access is being given to department wise data, so as to maintain confidentiality.

4. Document Retention

All the documents shall be maintained in appropriately secured applications or severs. It is required to ensure not to delete any information that may be required. Also, ensure to properly dispose the data which are not required anymore.

5. Training and Awareness

The IT Department imparts induction training with respect to the systems and guidelines. Also, the employees are given standard guidelines regarding system security in writing, which are acknowledged by the employees.

6. Responsibility

The IT Department is responsible for the implementation of this Policy.

7. Review

The Company reserves the right to modify and/or review the provisions of this Policy from time to time, in order to comply with applicable legal requirements or internal policies, to the extent necessary.