***POLICIES***

**BYOD Policy**

• You must install the company's monitoring app on your personal devices. Apps from external parties or unknown sources, such as antivirus software, are prohibited. Additionally, only applications offered by the firm should be utilized for reading, writing, transferring, and receiving data.

• To protect the data as much as possible, only the company's cloud services may be used for storage.

• Daily backup procedures should be performed to prevent data loss. To accomplish this, one must log in to the company's backup-specific cloud.

• One should not be linked to any public network, such as a hotspot or public wifi, when transferring data or sending messages. Only using wifi access points designated for your department will operate. Don't forget to transfer data through the company's offered data encryption app.

• Data transfers outside of one's own department should be avoided. Any type of personal information, even simple text, cannot be sent. Data must be encrypted just once.

• The device must have a password to access it, and all data must be encrypted to ensure secrecy even if the owner is not there.

• You must acknowledge that the firm has unique access rights to the data on its employees' personal devices. The data on your personal device may be deleted, edited, and accessed by a firm using a variety of tools.

• Only workers in the Finance, HR, Sales, and Purchase departments are permitted to use their personal devices for work.

• Personal items like smart watches, cameras, unregistered computers, etc. are strictly prohibited within the workplace.

• Any employee who violates one of the aforementioned points in this policy will be compensated heavily.

**Access Control Policy**

***Digital Access Control***

1. A1 level management should have the ability to view, write, and modify or delete all data.

Only read access should be granted to B1 level management. They are unable to edit or remove data. Only read access should be granted to C1 level management. They are unable to edit or remove data.

2. The A1 level management should be granted access to the server rooms. Management at the B1 level shouldn't be allowed access to the server rooms. Management at the C1 level shouldn't be allowed access to the server rooms.

3. One must submit an application to the legal team or A1 level with the correct data, time, purpose, and categories of access needed in order to seek digit access.

4.Whenever a level management employee is transferred or promoted to a different position, their rights may be altered or deleted.

5.All digital access privileges should be reviewed and updated on a regular basis.

***Physical Access Control***

1. Only members of the Finance Team should be permitted access to the accounts department.

2.Only members of the HR Team should be permitted access to the inventory storage.

3.One must submit an application to the legal team or A1 level with the correct data, time, cause, and types of access needed in order to obtain physical access.

1. Periodic review of all the physical access rights should be monitored and updated.

**Password Management Policy**

• Each person needs their own account and password.

• One should reset their password at first login, and they shouldn't keep using the automatically generated one.

• Everyone has the option to change their password whenever they choose, and this should be done frequently. If the user is able to authenticate, this choice will be made available.

• The password should contain a combination of uppercase, lowercase, digits, and special characters, and it should be longer than 8 characters.

• For increased security, it is advised that everyone regularly update their passwords. It should be done once every 15 days.

• The password should be entered into the password input area in an unreadable manner, and the number of tries should be restricted.

• Old passwords should never be used since they have been recorded and cannot be used again.

• To ensure that password secrecy, it should always be kept and transferred in a secured manner.

* The account that stays ideal for more than 90 days would not be further entertained and will get disabled. Further if the same account stays ideal for more than 60 days will get permanently removed.
* Password processing should not take place on any of the automated programs , utilities , applications .

**CRYPTOGRAPHY POLICY**

**•** Cryptography enables safe data transit over networks and is mostly used to protect secrecy.

• When using a twofold encryption and decryption procedure, asymmetric key cryptography is favored over symmetric key cryptography.

Hashing methods and the RSA encryption algorithm should be employed for more secure data transport.

* The keys used for cryptography must be strong and regularly updated/changed.
* Every sensitive data transmission process should use cryptography and should not be used in case of insensitive data transmission.

**ASSET MANAGEMENT POLICY**

* Classification of assets should be done on the basis of department or rank.
* Permission management of every asset should be done to decrease the misuse of assets.
* anHaHandling of assets should be not be done without a consent letter or NOC.
* Regular maintenance of list of working and non-working assets should be done.
* A digital asset destruction should be done only by secure means such as overwriting it

**Acceptable Usage Policy**

• No one is permitted to attach any external gadgets to their possessions.

• Nothing in any of the asset configurations may be altered or modified by anybody.

• Only those who are qualified to utilize an asset should do so, or else they must first sign a NOC or a consent letter in order to do so.

* Asset owner will be responsible in case of any asset misuse is done so asset handling should be done securely.
* An individual should only perform those tasks on a asset that he/she is eligible to do.

• Asset handling should be done safely since the owner will be held accountable for any misuse of the asset.

• A person ought to limit their work on an asset to what they are qualified to undertake.

**Supplier Relation Policy**

• Important data should be stored in a secure setting.

• Cryptography methods must be used as necessary to protect data secrecy with the appropriate authorisation.

• Only a secure channel should be used to transport data in order to prevent unwanted access, integrity loss, and data breaches.

• Critical data activities carried out by suppliers should be tracked and recorded for future use.

• Must confirm that third-party organizations have a sufficient security architecture and policies in place to safeguard our data.

• Suppliers should adhere to our information security policies and only use trusted means for remote access.

**Clear Screen Policy**

* Computers / computer terminals shall not be left logged-on when unattended and shall be password-protected.
* The Windows Security Lock shall be set to activate when there is no activity for three minutes.
* The Windows Security Lock shall be password protected for reactivation.
* Users shall shut down their machines when they leave for the day.
* There shall be no screen savers set on for the individual’s desktops and laptops.

**Information Transfer Policy**

* Information transferred should maintain the integrity i.e. It should be protected from any kind of modification.
* Information transferred should be stored in a secured place to ensure protection from data breach and data loss.
* Cryptography techniques should be implemented for secure communication and authorization.
* Only trusted party/applications should be used as a medium of transfer.
* Proper guidance must be given to personnel to take appropriate precautions not to reveal confidential data.