Introduction

The Policy Will Act as a Guideline for Securing IT Asset & Software usage across Skipper Limited and will be binding on the Employees as well the IT Department

General Guidelines:

1. This Policy will be reviewed as and when required
2. This policy has to be adhered in letter and spirit by all employees of Skipper Limited and the IT department
3. All New Desktops & Laptops are to be procured with Original OS only
4. Plan to Move to O365 in a phased manner
5. Company HR Can Initiate Penal Actions if these Policy is found and proved to be violated by any employee of Skipper Limited

➢ Administrative Password Retention & Access Policy for Critical IT Equipment's

❖ In order to Secure Administrative Password of Critical IT devices and ensure its security following guidelines Should Be adhered to.

- Default passwords on all systems must be changed after installation.
- All administrator or root accounts must be given a password that confirms to the password selection criteria when a system is installed, rebuilt or reconfigured.
- Locks will be enabled for 3 failed Logins
- Password should be Complex at least 8 characters with a combination of alphabets, numbers and special characters
- Administrator password should be change periodically every 30 days
- Password should be stored in a secure Environment as per the Responsibility Matrix attached

➢ Password changes will be intimated to the Higher Management in a proper Electronic Copy after verification by the Manger IT Infra with a copy to IT Head and Directors

➢ No password shall be changed without approval of IT infrastructure Manager which should be electronically recorded and subject to Audit by IT Head or any other person or origination entrusted by the Directors

➢ PDF Writer Usage & Approval Policy

❖ This can be a Major sources of Fraudulent Practices, like modifying Company's Data & Circulating to Outside World like PO, Invoice and many others. The following guidelines needs to be strictly adhered to

- Nobody will be provided PDF Writer Exception to be granted only on case to case to Basis by IT based on Director's approval. All Existing PDF writers are to be revoked with immediate effect
- Director's approval is mandatory to edit any PDF file with presence of IT department and documentation shall be done every time. And electronically stored and subject to Audit by an origination or person entrusted by the Directors
- User should send every PDF in edit password protected mode to prevent unauthorized editing.

➢ Restriction On Usage of Unlicensed Software's Policy

- Users are not permitted to use any unlicensed software in his Desktop/Laptop.
- Director's approval is mandatory to install any Unlicensed or Trial Software every time.

➢ Physical Security and Safety Policy

- All users should use the company's devices, systems and networks in a safe manner which reduces the risk of physical injury to the person.
- Users should use the company's IT assets in a manner which does not cause physical damage to such assets.
- Users should be careful with the company's assets such as laptops, mobile, TAB devices, etc. when carrying them while traveling or in public transport.
- Any loss or theft of any IT asset should be reported to the IT Department immediately on becoming known to the user.

➢ Security Audit Policy:

- Any changes to the applications should be authorized by the concerned HOD and IT Head.

➢ Password Protection & Change Policy for Desktop, Laptops & All Applications including SAP

- Secure passwords for all company's devices, systems and software applications are mandatory.
- Password should be Complex at least 8 characters with a combination of alphabets, numbers and special characters
- Password should be change periodically in every 30 days.
- Users should not share or disclose passwords to others or write passwords down in a manner that it can be seen and accessed by others.

➢ Desktop/Laptop Security Policy

- The IT department should have desktop/Laptop security measures configured on individual machines using group policy or server based anti-virus tools
- Users should not have privileges to use removable media, install unauthorized applications or software or use the desktop in contravention of the IT policies.
- 100% Block WhatsApp on desktop/Laptop.
- Stop Google drive cloud sync with Local Machine.

➢ Network Security Policy

- The network must be designed and configured to deliver high performance and reliability to meet the needs of the operations whilst providing a high degree of access controls and range of privilege restrictions. The company's network should be protected from unauthorized access through the use of firewalls – software and / or hardware.
- Hardware based firewalls should be used to protect the company's network from external threats.
- Software firewalls on individual machines and devices should be used to protect against internal threats.
- External ports should only be opened on need basis and allowed only for restricted usage as per IT Infra manager & IT Head's approval.
- All Wi-Fi networks of the company should be secured with password based access using encryption. Access to guest devices should be controlled and should be provided based on a need to use basis.
- No non-company devices shall be allowed to be automatically connected to the company's networks.
- If any external access is to be provided to the company's networks the same should be based on Virtual Private Network (VPN) technology. This should be preferably use the Secure Sockets Layer (SSL) for additional security. No direct port based connections should be allowed.

➢ User Data Retention & Back Up Policy

- The user should keep their important data in a single folder & that should be kept in one drive as backup. Till A Proper Backup Software is installed
- IT Team would provide all email backup for last three years. The old data would be archived and handed over to user in their own custody.
- In case of separation, HR department should process the closure by filling the online FORM. IT department would not store the user's data in their custody unless higher management approval for security aspects.
- The data backup size would be capped at 30 GB per user and if the user requires over above approval from HOD is required and cost would be incurred by respective cost center.

➢ Remote Access / VPN Access

- It is the responsibility of users with VPN privileges to ensure that unauthorized Users are not allowed access to the Company's internal networks.
- Remote access should be password protected & IT support team should take permission of users to connect their Desktop/Laptop
- VPN use is to be controlled using login ID and password authentication.
- All computers connected to the Company's internal networks via VPN must use the most up-to-date anti-virus software and operating system patches.

- VPN Users will be automatically disconnected from the Company network after a period of inactivity. The User must then logon again to reconnect to the network.
- Users of computers that are not company-owned must comply with Company VPN, anti-virus, operating system patches, and network requirements.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the Company network, and as such are subject to the same rules and regulations that apply to Company-owned equipment, i.e., their machines must be configured to comply with the Company Information Security Policies.

➢ Data Centre Physical Access Policy

- Unless otherwise required no other departmental personnel should be allowed into the server room / data center which houses the central IT infrastructure.
- Data Center should be accessed by biometric authentication and CCTV Survilence
- The server room / data center should have fire warning and retardant systems installed.
- Rodent control and water damage prevention should also be installed.
- Vendor's Entering Data Centre Should Be Maintained with Name, Address, Phone No ,Date ,In & Out Time Counter Signed By Local IT Head .This should be available for Audit .

➢ Removable Media Usage Policy

- External storage like Pen drive, External HDD should be blocked for every user to prevent from virus and unauthorized use of business data.
- Access to Pen drive/External storage for a user/ functional unit/department or group of user would be provided on the basis of substantiated business needs agreed upon by Director.
- All removable devices will take under IT custody after review every system.
- The IT department should ensure the use of Data Leakage Prevention and Endpoint Security and other similar tools and technologies are installed to prevent the usage of removal media

➢ Domain Controller & Single Sign On Policy

- A Domain Controller Is To be Installed In Cloud
- All IT' Policy's Should Be Implemented using the Domain Controller
- Access To All Applications including mail & SAP should be through Domain Controller Landing Page with Single Sign On

➢ Incident management Policy

  - ❖ An IT security incident is an event affecting adversely the processing of information in the company.
- Any incident happens due to unknown reason, unknown sources and unplanned outage not more than one hour shall be considered.
- Local IT Team shall make root cause and send to IT infra manager for further issues related to same cause.

- **Vendor Access Policy**
  - ❖ Vendor's access to skipper IT infrastructure is completely restricted.

- Passwords of any IT Infrastructures should not be made available to the vendors.
- If vendor need an access that has to be approved by IT Infra Head & IT Head based on need & job performed will be under local IT supervision & evidence of the same to be kept electronically for future audit.
- Proper NDA should be signed with all Vendors who have access to our Data like Vector, Kloud Q, Arokia, Light House, PWC etc.
- All changes/Modification should be documented by IT department for further implementation and resolution.
- Third party software like Anydesk etc. Should have password set for remote access and should be used under the supervision of local IT team.

Responsibility Matrix

Policy	Responsible person	Over all Responsible person	Principal Responsible person	Reporting Frequency	Report send to
Administrative Password Retention & Access Policy for Critical IT Equipment's	IT Infra Manager	IT Infra Manager		30 Days	Directors with the copy to IT Head
PDF Writer Usage & Approval Policy	All Local IT Team	IT Infra Manager	Users	30 Days	Directors with the copy to IT Head
Restriction on Usage of Unlicensed Software's Policy	All Local IT Team	IT Infra Manager		30 Days	Directors with the copy to IT Head
Physical Security and Safety Policy	All Employees			30 Days	Directors with the copy to IT Head
Security Audit Policy:	All Local IT Team	IT Infra Manager		30 Days	Directors with the copy to IT Head
Password Protection & Change Policy for Desktop, Laptops & All Applications including SAP	All Local IT Team	IT Infra Manager	Soumen Samanta for SAP & Ratan Lal Keshri for APPs	30 Days	Directors with the copy to IT Head
Desktop Security Policy	All Local IT Team	IT Infra Manager		30 Days	Directors with the copy to IT Head
Network Security Policy	All Local IT Team	IT Infra Manager		30 Days	Directors with the copy to IT Head
User Data Retention & Back Up Policy	All Users	IT Infra Manager		**30 Days**	Directors with the copy to IT Head
Remote Access / VPN Access	All Users	IT Infra Manager		30 Days	Directors with the copy to IT Head

Data Centre Physical Access Policy	All Users	IT Infra Manager		3 month	Directors with the copy to IT Head
Removable Media Usage Policy	All Local IT Local IT Team	IT Infra IT Infra Manager		30 Days	Directors with the copy to IT Head
Incident management Policy	All Local IT Local IT Team	IT Infra IT Infra Manager		30 Days	Directors with the copy to IT Head
Vendor Access Policy	Local IT Team as on required	IT Infra Manager		30 Days	IT Head