**PAKISTAN STONE DEVELOPMENT COMPANY**

**IT Policy Manual**

**Table of contents:**

* Introduction: a. Mission of the organization:.………..…………..2

 b. Vision of the Organization:………………...…...2

 c. Purpose of the IT policy manual…...…….……..2

* Employee Data :………………….……………………..……………3
* Company Data:……………………………………………………….3
* Software :……………………………………….…………………….3
* Hardware :……………………………………………..……………...4
* Backup:...……………………………………………………………..4
* Data Protection :……………………………………………………...6
* Damage:………………………………………………………………6
* Internet :……………………………………………………………....7
* E-mail :………………………………………………………………..7
* Employee’s acknowledgement :……………………………………...9
* Change Document:………………………….…..………………..…10
* Notes: ……...……………………………………………….……….10

**Introduction of E-Policy:**

**Vision Statement:**

PASDEC acknowledges an obligation to ensure appropriate security for all information technology data, equipment and process in its domain of ownership and control. This obligation is shared, to varying degrees, by every member of the organization.

**Mission Statement**:

This document will:

1. Enumerate the elements that constitute information technology
2. Explain the need for information technology
3. Specify the various categories of IT data, equipment and processes subject to this policy.
4. Indicate appropriate levels of security through standards and guidelines.

**Purpose of IT Policy Manual:**

The purpose of this policy manual is to provide clear and written rules about the use of the company network system. Rules will be enforced by the random controls over the employee’s activities, disobeying rules will cause penalty or any action proposed by the management.

**Employee Data:**

 PASDEC would ensure to keep the employee information confidential and to never disclose employee information to third parties outside or within the company as long as the same is not required legally /officially. Employee data flows within the company will be limited by discretion of the concerned department and will serve as a marketing and costumer service tool. Employees who transmit information outside the company network boundary will be liable for disciplinary action including termination or dismissal from services.

**Company Data:**

Employees should always keep the company`s information confidential and ensure not to disclose company information to third parties outside the company. Employees who transmit company information outside the company network boundary will be liable for disciplinary action including termination or dismissal from services.

**Software:**

Many computers are going to be used in various departments. Employees are going to have limited access to all computers within the Company. Usable software are: Microsoft windows, Microsoft Office, Internet Explorer, any Company accounting software, HR, inventory management software and Project management software. Full access to this software will be granted to owners (IT team is owner of all the softwares) and the functional team only. Each employee will have access to these programs trough a user ID and Password only known to the user. Employees will be responsible for the use of the software during their connection to the network.

**Hardware:**

All computers will be equipped with input and output devices. Examples of some output are mouse, key board, printer, and scanner machines. The use of these devices may be solely for reason directly connected with the employee’s duties. Personal use of such devices is restricted and may be granted by managers for emergency reasons only. Computer hardware and software remains the property of PASDEC.

**Backup:**

Along with redundancy, backup is the most important part of disaster recovery. Every employee shall know what he/she needs to backup; decide when and how he will do his backups. A common scheme is to do a full backup at the beginning of each month, followed by deltas -- backups of changes -- at least fortnightly if not more often. Employee is sole responsible for availability of data at any time during his/her service span (See company data). In case if any employee wishes to keep an offsite copy of company`s data he must hand it over a copy of data backup to system administrator with a receiving note.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Data backup Label | Preceding S#, date | Backed up Data | Instructions (if any)  | Signature Owner  | Signatue System Admin  |
| Label the CD in a manner with is easy understandable both by the owner and the system admin e.g (MP-Risalpur/mar/02/16/5) | (MP-Risalpur/Feb/03/16/4) | Machinery pool Risalpur 1. list of machinery
2. Revenue
3. Current location of machinery
4. Etc etc
 | Please discard the previous data CD |  |  |

Backup of SHMA Financial shall be taken periodically keeping the following format

|  |  |  |
| --- | --- | --- |
| Monday | SHMA Financial SQL DB Archives  | Onsite  |
| Tuesday | SHMA Financial SQL DB Archives | Onsite |
| Wednesday | SHMA Financial SQL DB Archives | Onsite |
| Thursday  | SHMA Financial SQL DB Archives | Onsite |
| Friday  | SHMA Financial APP+DB | Offsite  |

It is common to duplicate the weekly backup and keep it offsite, and also to keep monthly backups.

In case where the hard copy is the sole mode of record keeping or where the hard copy is obligatory for record keeping, the site in charge is responsible for maintaining the backup through scanned copies. The IT team has to make sure the availability of backup of all project sites and regional offices in case of disaster recovery operations. Bi monthly incremental data backup is recommended for the project sites and regional offices. Before handing over the site data to IT admin team the data owner (Site in charge) must label the backup data in prescribe format.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Data backup Label | Preceding S#, date | Backed up Data | Instructions (if any)  | Signature Owner  | Signatue System Admin  |
| Label the CD in a manner with is easy understandable both by the owner and the system admin e.g (MP-Risalpur/mar/02/16/5) | (MP-Risalpur/Feb/03/16/4) | Machinery pool Risalpur 1. list of machinery
2. Revenue
3. Current location of machinery
4. Etc etc
 | Please discard the previous data CD |  |  |

**Data Protection:**

Pakistan Stone development Company (PASDEC) follows the three tier strategies for data protection which includes onsite backup, offsite backup and private cloud solutions.

Rationale to follow the three tire data protection strategy is to address the local, small to large and mega scale disasters. The protected data contained in each category shell stand identical so that the zero tolerance recovery is obtained.

Data protection for Onsite backups are maintained on individual servers where as offsite backups are taken on CDs and stored in bank lockers. Private cloud space of approx 2 TB will be made available the BCDR (business continuity and disaster recovery) purpose to address the large scale disasters.

Sidat Hyder Murshid Financials (SHMA Financials) backups are made to disks for on-site and copied to CDs for offsite and same are uploaded to Private Cloud solutions. Machinery Management System (MMS) backup are to be maintained by the hosting company and a copy of the backup made to CDs and sent off site on regular intervals. The management and operational departmental data in PDFs, Word Docs, Excel Sheets and PPTs formats etc are scanned /copied on file server and are replicated for offsite lockers and Private Cloud solutions

**Damage:**

The health and well-being of all IT resources are the responsibility of its users who must guard them against abuses which disrupt or threaten the long-term viability of the systems at PASDEC. The organization requires the employees to act in accordance with these responsibilities, policy, relevant laws and contractual obligations, and the highest standard of ethics. The misuse of these resources are unethical and unacceptable, and just cause for taking disciplinary action within the regulations of the PASDEC, and/or legal action, any activity which, without the prior permission of a properly recognized authority:

* accesses, modifies, tampers with or destroys or in any way jeopardizes the integrity of any stored program or data;
* uses, modifies, tampers with, damages or destroys any computer equipment, which shall include moving, opening or disconnecting the equipment, or attaching other equipment:
* removes, defaces, or destroys printouts, documents or support material;
* copies, modifies, deletes, disseminates, breaches confidentiality or copyright requirements, or uses any part of information not provides by or generated by or addresses to the persons involved, which may become available to them in whatever form through their use of office computer facilities.

**Internet:**

The use of internet is permitted as long as employees act appropriately and lawfully. Acceptance account information and agreement to follow this policy, employees will be granted Network and Internet access on their desktops. Employees using internet must adhere to the etiquettes. PASDEC will determine prohibited and allowed internet activities. The Following activities violate PASDEC Computer’s Network and internet usage policy.

(a)Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, political, abusive, or misleading language or materials.

(b)Revealing Personal information

(c)Causing harms to other’s property. Ex. Downloading copyrighted materials.

**E-Mail:**

PASDEC provides all of its employees of electronic communication tools such as e-mail. Violation of below mentioned rules shall result in disciplinary action including termination or dismissal from services and initiatives of legal proceedings. Usage of official email is primarily for business purpose. PASDEC has the right to monitor any activities; therefore employees should not expect any privacy while communicating from the company e-mail system.

1. All use of email must be consistent with PASDEC policies and procedures of ethical conduct, safety, compliance with national laws and proper business practices.
2. PASDEC email account should be used primarily for business related purposes. Non- related commercial uses are strictly prohibited and violence of such may cause disciplinary action disciplinary action including termination or dismissal from services.
3. All data contained within an email message or an attachment must be secured according to the data protection standard (see employee data and company data).
4. Email should be retained only if it qualifies as a business record. Email is a PASDEC business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
5. The PASDEC email system shall not to 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 PASDEC employee should report the matter to their supervisor immediately.
6. Users are prohibited from automatically forwarding PASDEC email to a third party email system (noted in 7 below). Individual messages which are forwarded by the user must not contain PASDEC confidential or above information.
7. Users are encouraged not to use third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct business, to create or memorialize any binding transactions, or to store or retain email on behalf of PASDEC. Such communications and transactions should be conducted through proper channels using -approved documentation.
8. PASDEC Employees shall have no expectation of privacy in anything they store, send or receive on the PASDEC email system.
9. PASDEC may monitor messages without prior notice. PADEC is not obliged to monitor email messages.

**Employee’s acknowledgement:**

By virtue of this policy, all PASDEC employees agree to all the rules implied in the IT Policy. Employees understand that the use of user ID and password will make them responsible for any violation of the regulations above written.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SNO** | **Change Order** | **Insert** | **Page** | **Sig / Sig** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**NOTES**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**