IT Policies and Procedure Manual

Ver. 1.0

JCT Limited
G.T. Road, Phagwara

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Table of Contents

Introduction

The JCT Limited's IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the business which must be followed by all staff. It also provides guidelines JCT will use to administer these policies, with the correct procedure to follow.

JCT will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

These policies and procedures apply to all employees enrolled at Phagwara Unit.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Backup Policy (Servers)

Policy No: JCT/PHG/IT/BKP/001

Overview

Data backup is an important aspect of computer systems. An improper backup may result in data loss if some mishap occurs. Thus firm steps are required in an organization for the data backup policy.

Purpose

The purpose of this policy to ensure that the critical data is backed up regularly and being kept at the designated location described in the policy.

Scope

The scope of this policy covers backups of all databases (ERP and legacy applications) and user documents resides in file server located at Phagwara location. Data held and managed locally in departments is excluded unless departments have entered into specific arrangements with IT (Shared Drive on Server). Entire staff at JCT Phagwara is herby reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data *must* be stored on the network drives provided to them.

Procedure

- We having 6 tapes labeled as Monday to Saturday respectively and 5 tapes labeled as Sunday I, Sunday II, Sunday III, Sunday IV and Sunday V. Tapes labeled from Monday to Saturday overwritten on the same day (Weekly cycle) and set of weekly tapes overwritten on the same Sunday (monthly cycle) .

- Backup of all Databases (Full Backup) is taken once in early morning on the drive located on same server and then copied to the server on which backup device in installed. Complete folder having backup of all the databases then backed up to the removable tape. After completion the tape bearing backups for Monday, Wednesday and Friday are stored in fireproof safe in cash office which is at ground floor.

- Additionally we are having three tapes which are being used on 1st day of every month contains backup of month end in a way we have monthly backup of last three months.

- Backup other than databases (files backup is being taken on Sunday and holidays in a way it doesn't slowdown the performance of the server.

- Only authorized IT personnel are authorized to carry the tape from IT department to locker and vice versa.

Rajeev Baksshi

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

- Any failed backups are re-run immediately.
- Any exception to the policy must be approved by the Infosec team in advance.
- Requests for data recovery should be submitted to the HOD IT or InfoSec team via email or hard copy of the form duly filled and signed by the requester and concerned HOD.
- To ensure the backup is being taken properly and tapes are in well working condition, InfoSec Team will exercise restoration from at least one tape in a week on random basis.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Backup Policy (User Data)

Policy No: JCT/PHG/IT/BKP/001

Overview

Data backup is an important aspect of computer systems. An improper backup may result in data loss if some mishap occurs. Thus firm steps are required in an organization for the data backup policy.

Purpose

The purpose of this policy is to ensure that the critical data on user's Desktop or Laptop is backed up regularly and is being kept at the designated location described in the policy.

Scope

- The scope of this policy covers backups of all users at Phagwara location. Entire staff at JCT Phagwara is herby reminded that they are individually responsible for data held locally on their desktop or laptop computer. Due to lack of resources, as of now we don't have automatic backup solution readily available with us. Thus, a copy of critical data *must* be stored on the network drives provided to them regularly, themselves.

Procedure

- Users are advised not to save critical data on "C:\" partition of the system i.e. Desktop, My Documents, My Pictures. "C:\" partition is more prone to problems and if the operating system gets corrupt then users may lose their vital data.
- Users are suggested to have backup of their data of desktops and laptops on the network drives Or on the hard disk of their colleague having surplus vacant space, regularly themselves.
- If a user doesn't have access to network drive then he may drop a mail at IT Helpdesk mentioning his requirement en route and approved from his concerned HOD.
- Infosec Team will decide as per the requirement of the user that if space is to be provided to the user on the server Or space is to be provided to the user on his colleagues hard disk.
- IT Helpdesk person will assist users for the process of data backup if they feel any sort of difficulty.
- In case of data loss, if data recovery is to be made, then data recovery charges along with service charges will be borne by the user itself.

Rajeev Baksshi
Rajeev Baksshi
HOD(IT)

Rohit Seru
Rohit Seru
Unit Head

Authorization/Cancellation on behalf of others

Policy No: JCT/PHG/IT/Auth/001

Overview

Keeping in view of the security and a good practice of not sharing the password to anyone, authorization of various transactions (Leave, Quotations/Sanctions/Shortfall request etc) except RAMCO ERP are being done by IT if the employee is out of organization for any reason. Some of the TOP executives (ED and executives authorized by ED) are having facility to reply just ok or yes against the system generated mail and the authorization is mark in system automatically. For those who are not having authorization thru mail facility or authorizes executives can't even reply to mail, authorization is made on their behalf.

Purpose

The purpose of this policy to ensure that the critical transaction to be made by authorized persons in IT only and proper record of such transaction to be maintained.

Scope

The scope of this policy covers authorization on behalf of others by IT.

Procedure

- In case of leave requestor will send a mail to admin department with a copy to HOD. Admin dept will check the case and then forward the same to HOD IT. IT will authorize/cancel the same as per instruction and put a remark against the transaction and revert back to the sender/admin/HOD IT.
- In case of sanction notes/Quotation/shortfall etc. the requester, the level authorization to be done, Concerned HOD and HOD IT to be kept in loop.
- IT Person will make a record of the same.

Rajeev Baksshi

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Re-location of IT Asset

Policy No: JCT/PHG/IT/Reloc/001

Overview

The physical move/re-location of the Asset is the visible part of the process, but before this can be undertaken, suitable skilled person will need to be appointed. Cost certainty and quality of service is best achieved through a controlled process, which should include a scope of works, site surveys and evaluation of the responses received to including experience, methodology and requirement understanding, as well as pricing.

Good preparation and planning can be ruined at the Physical Move stage and so onsite supervision throughout, supported by detailed activity schedules, checkpoint meetings, escalation and communication procedures, as well as access and security arrangements, is vital.

Purpose

The purpose of this document is to ensure that if any asset is to be re-located that activity to be carried out by skilled person in a proper way.

Scope

The scope of this policy covers all the assets provided by IT.

Procedure

- Relocation request to be sent to IT Helpdesk.
- Helpdesk personal will visit the site and assess the requirement; if this is a minor change have no or less financial Impact, Helpdesk person will take decision on the spot and do the same.
- In case of Major change, Change requirement analysis to be submitted to HOD IT and after approval change to be carried out.

Rajeev Baksshi

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Internet Usage Policy Office Use

Doc No: JCT/PHG/IT/IUP/001

Overview

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

Access to the Internet will be provided to users to support business activities and only on an as needed basis to perform their jobs and professional roles.

Purpose

The purpose of this policy is to define the appropriate uses of the Internet by employees and affiliates.

Scope

The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

Procedure

- Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within a week.
- Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the InfoSec Team.
- Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the InfoSec Team, may be considered cause for disciplinary action.

Rajeev Baksshi

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

- Users who choose to store or transmit personal information such as passwords, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss if occurred.
- Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the HOD (IT) or Unit Head.
- User must not use unprotected devices to access internet while on corporate network. If internet on corporate network is not available and it is very necessary to access internet, InfoSec Team must be notified.
- User must not use public mailing site (gmail, rediffmail etc) for official communication. If some reason it is necessary it must be notified to InfoSec Team and a copy of the same to be marked to the corporate mail.
- Users should consider their Internet activities as periodically monitored and limit their activities accordingly.
- InfoSec Team reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.
- Any exception to the policy must be approved by the Infosec Team in advance. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Internet Usage Policy Colony Use

Doc No: JCT/PHG/IT/IUP/001

For the ease and financial impact company is providing Internet service to Thapar colony residents on chargeable basis given as under. Charges for the same will be recovered from the employee salary.

For Staff Members:

One Time Charge – Rs 1500/- (Non refundable)

Recurring Charge – Rs 350/- per month

For Workers:

One Time Charge – Nil

Recurring Charge – Rs 350/- per month

Procedure

1. A user willing to get internet connection in colony premises needs to submit his request in IT department through email or written application.
2. One time charges and the monthly recurring charges will be deducted from the user's salary by the factory department.
3. User is himself responsible for the transactions/data exchanged through his colony internet connection.
4. Any loss occurred by any mean will be the sole responsibility of the colony internet user.
5. At the time of activation, all users are advised by IT Helpdesk person, that they should not share their user name, password and ip address with anyone.
6. A user willing to get internet connection disconnected in colony premises needs to submit his request in IT department through email or written application.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Email Usage Policy

Doc No: JCT/PHG/IT/EUP/001

Overview

Electronic email is massively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

Purpose

The purpose of this email policy is to ensure the proper use of JCT Limited email system and make users aware of what deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Network.

Scope

This policy covers appropriate use of any email sent from a *@jctltd.com email address and applies to all employees having email Id on jctltd.com domain.

Procedure

- The 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 employee should report the matter to InfoSec Team immediately.

- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct business communication, to create/forward/ store/ retain email on behalf of JCT Limited. If for some reason it is very necessary to use third-party email systems, it must be notified to InfoSec Team and a copy of the same to be made on the jctltd.com domain.

- Using a reasonable amount of resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a email account is prohibited.

- Any exception to the policy must be approved by the Infosec team in advance. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Password Protection Policy

Doc No: JCT/PHG/IT/PPP/001

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of JCT Limited's resources. All users, including contractors and vendors with access to systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any facility, has access to the network, or stores any nonpublic information.

Procedure

- All user having access to fusionapps/Ramco/Email must use complex password. Password must be having at least 6 char length and contain one alphabet/one special char/one numeric/Case Sensitive alphabet.
- Users must not use the same password for official accounts as for other non- official (for example, personal ISP account, trading, shopping, banking and so on).
- All user-level passwords (for example, email, web, desktop computer etc) must be changed at least every six months.
- Passwords must not be shared with anyone including helpdesk personnel/InfoSec Team/seniors. All passwords are to be treated as sensitive, confidential information.
- Any user suspecting that his/her password may have been compromised must report the incident to InfoSec Team and change all passwords immediately.
- Any exception to the policy must be approved by the Infosec team in advance. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Change in Application/DB

Policy No: JCT/PHG/IT/APPCH/001

Overview

Keeping in view of the security and Integrity, any change to the live applications/DB is to be carried out in a proper way.

Purpose

The purpose of this policy is to ensure change is being made thru proper authorization.

Scope

The scope of this policy covers all change made to any live application/database.

Procedure

i. Application change initiated by user be received thru mail or in writing.
ii. Some changes may be initiated by Project owner/Administrator/HOD IT.
iii. Any change to live application/deployment of new application to be approved by HOD IT.
iv. Project owner will prepare the solution and fill the required detail in format no_____.
v. Final solution will be discussed with implementation/InfoSec team for deployment.
vi. Deployment will be carried out by Administrator/Infosec Team.
vii. Feedback of the same will be taken in writing/thru mail wherever possible.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Handover – Takeover Form (for IT Use Only)

 # This form is to be filled by IT Staff in case of any task is transferred.

Outgoing Personnel	Incoming Personnel
Name :	Name :
Emp # :	Emp # :

Handover Start Date : ..... **Handover End Date : .....**

Activities of Handover

List of Documents:

Signature
(Outgoing Personnel)

Date :

Rajeev Baksshi
HOD(IT)

Signature
(Incoming Personnel)

Date :

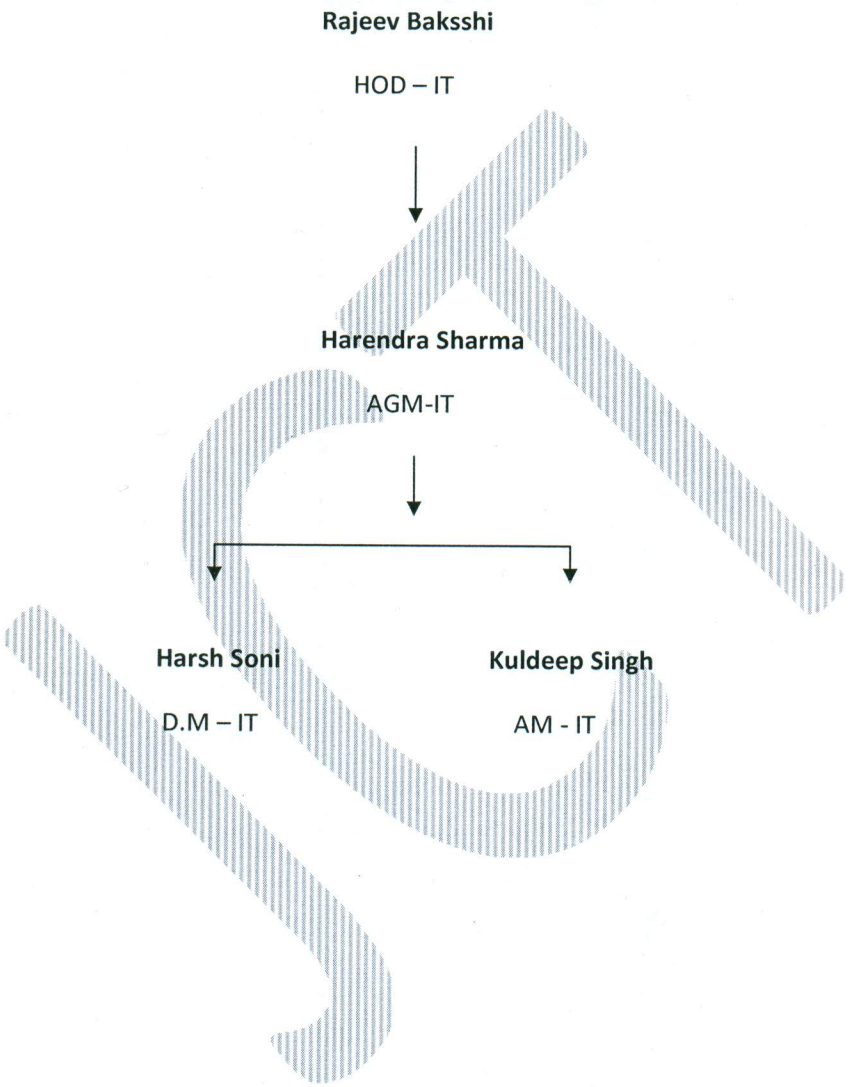
Signature
(Reviewer)

Date :

Rohit Seru
Unit Head

Annexure-1:

InfoSec Team:



Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Group Policy

Policy No: JCT/PHG/IT/GP/001

Overview

Keeping in view of the security and best practices, some polices are to be defined at domain level.

Purpose

The purpose of this policy is to improve the centralized security/unauthorized access at user/computer level from domain controller.

Scope

The scope of this policy covers all users/computer at Phagwara.

Procedure

1. **Account Lock:** Putting wrong password five consecutive times within 30 min will lead to account lock for a period of 24 Hr. To unlock the account user have approach the InfoSec team by giving the suitable reason for the same.

2. **Password Age:** Maximum password age will be 180 days. After this period when user will try to logon into the system, he/she will be forced to change the password.

3. **Screen Lock:** After 10 min of inactivity on the system, screen will be locked automatically.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Laptop Policy

Policy No: JCT/PHG/IT/LAP/001

Overview

To define the policy and process of providing laptops to need-based employees of JCT Limited, Phagwara.

Purpose

Purpose of providing laptop is to ensure that employees have uninterrupted access to data during their frequent travel and constant communication so that they could respond immediately to business queries and issues, without any delay.

Scope

The scope of this policy covers all laptop users at Phagwara.

Procedure

1. Company will provide the Laptop of the brand and configuration as per company norms, (Configuration will be reviewed by the Company's IT department, as and when required) worth Rs.50,000/-.
2. If an employee chooses to get a Laptop with operating system valuing more than Rs.50,000/-, then prior approval of ED is required.
3. Every employee will be personally responsible for the Laptop's breakdown, technical problem, theft, misuse or any such act that hampers working of laptop due to his negligence or mishandling. In such a case the expenses occurred will be borne by the user himself.
4. IT Head will be the final authority to judge/affix the responsibility of the employee in regard to his/her negligence or mishandling.
5. In any case if it is found that additional software/data has been loaded without the written permission of the IT Department and due to this any loss occurs to the machine, full recovery will be made from the concerned employee.
6. Laptop holder will be solely responsible for the backup of the data on the hard disk.
7. In case of Piracy, Laptop holder will be personally responsible.

Rajeev Baksshi

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

8. Employee has the option to change the Laptop after the time span of 4 years from the date of purchase of the Laptop.

9. At the time of leaving the organization Or at the time of change of Laptop, the concerned employee has the option to purchase his existing old laptop at its WDV (Depreciation calculation is based @ 16.21% p.a. SLM calculated on monthly basis as per the Companies Act.)

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

Removable Storage Policy

Policy No: JCT/PHG/IT/STOR/001

Overview

Removable media (Pen Drive/External Hard Disk/Memory Card) is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained at JCT Phagwara and to reduce the risk of acquiring malware infections on computers operated by the employees of JCT Phagwara.

Scope

The scope of this policy covers all desktops and laptops at Phagwara.

Procedure

1. Removable media is disabled by default on all desktops and laptops at JCT Phagwara.
2. In case of requirement of data to be copied to external media, IT Helpdesk person will assist them but with the prior consent of the concerned HOD.
3. If a sales personal that has been provided with an official laptop is moving outside then IT helpdesk person will enable mass storage device on that laptop for that specific period but with the prior consent of the concerned HOD.
4. If removable media is to be enabled on desktop or laptop of an employee on permanent basis due to nature of job then prior approval from ED is required.
5. Sensitive information should only be stored on removable media when required in the performance of your assigned duties or when providing information required by banks and government departments.
6. Some employees have been provided with external Hard Disk for backup purpose. Such hard disks are to be kept in a locker at IT department and when in need, should be given and a record of the same also should be maintained. The hard disk is to be returned back to IT department before the closing of the same business day.
7. Any exception to the policy must be approved by the Infosec team in advance.
8. Personal IT device such as laptop/desktop/printer/scanner/hard disk/ access point/switch etc, are not allowed to bring into the office premises. If for some reason these are required, should be brought to the notice of InfoSec Team in advance.

Rajeev Bakshi
HOD(IT)

Rohit Seru
Unit Head

Disaster Recovery Plan

Policy No: JCT/PHG/IT/DR/001

Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives an organisation a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by JCT Limited that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

Procedure

1. Backup of all Databases is taken once in early morning on the drive located on same server and then copied to the server on which backup device in installed. Complete folder having backup of all the databases is then backed up to the removable tape. After completion, the tapes bearing backups for Monday, Wednesday and Friday are stored in fireproof safe in cash office which is at ground floor. Apart from this, the tapes for the days (Tuesday, Thursday, Saturday and Sunday) are kept in the server room. These tapes can be used to restore the database as and when required.

2. To ensure the backup is being taken properly and all tapes are in well working condition, InfoSec Team will exercise restoration from at least one tape in a week.

3. Users having critical data have been provided with storage space on server and this data is backed up on removable tape every weekend. In case of requirement, the data can be retrieved accordingly.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head

4. Most of the critical network uplinks are backed with standby uplinks which are checked by the Helpdesk team randomly every month.

5. Most of the critical network links have also been provided with surge arrestors to prevent the damage caused due to heavy lightening. The earthing of the surge arrestors is checked by Helpdesk Team randomly every month.

6. The main internet link is backed up by another backup link, in a way that day to day work does not hampers in the office area.

7. As of now, these are the only measures that we have taken for the disaster recovery within the provided range of infrastructure. In future, if the financial condition of the company allows, we shall have automated backup to a remote location.

Rajeev Baksshi
HOD(IT)

Rohit Seru
Unit Head