IT Policy

For

eTrans Solutions Pvt. Ltd.

Version Control			
Document Name: eTrans Solutions Pvt Ltd – IT Policy. Version 1.3			
Author	Created/ Modified	Date	Approved by
Joydip Shome/Subrata Samanta/Ashwani Jaiswal	Created	29/8/2014	PPC
Subrata Samanta	Modified	20/2/2017	SDE

1. Purpose of Document

This document lines out the policies, procedures and guidelines followed within eTrans Solutions Pvt. Ltd (eTrans). This document applies to all employees, contractors and guest visitors to eTrans Solutions Pvt. Ltd. The implementation of this policy document is primarily the joint responsibility of the Systems Administration and HR team within eTrans Solutions Pvt. Ltd. All aspects of this document need to be understood and adhered to by all employees and Business Associates working within our system.

1.1 Need for Information Security – Part of Client Deliverables

eTrans is in the business of providing business-focused IT solutions to its Clients. All IT and IT related services delivered out of eTrans' development center are a key component of eTrans' business. This information security policy is a key document towards eTrans delivering to its Clients:

Confidentiality of Intellectual Property included software, documents, code, information and communications, data security, physical security.

Apart from client's data, all aspects of this information security document are key elements of eTrans' business as stated below:

a. Optimal use of hardware, software, internet and communication resources
b. Adherence to legal and statutory requirements,
c. Staff welfare, Smoothness of operations,
d. Brand-building
e. Business continuity.

1.2 Responsibility

All employees of eTrans are individually responsible to follow this IT Policy. It is the responsibility of all HOD's and Line Manager's to ensure the understanding of all team members and to procure their acceptance to the IT Policy.

1.3 Continual Improvement

eTrans encourages feedback and suggestions from all employees to improve on its Security Standards.

2. Internet Policy

This section describes the policy guidelines for the use of Internet in eTrans.

2.1 Restricted Sites

Visiting the following categories of websites is restricted for all employees and users of eTrans' IT infrastructure:

- Web-based chat
- Music and video download or streaming content
- Share trading
- Adult content
- Terrorist or propaganda websites
- Racist or religious hatred sites or forums

Any specific site from the above listed category, that might be needed for a specific requirement can be opened or accessed only for business purpose with prior intimation to their HODs.

Social Networking sites are allowed to be accessed.

2.2 Internet usage

eTrans' Internet connection are primarily used for facilitating the following:

1. Business-based email communications
2. File transfers between eTrans users and eTrans server.
3. For CV searches by the resourcing team.
4. For Business relevant studies.

*** Kindly Note*** Data card or any alternate Internet connection is only for official purpose and should not be primarily used for personal purpose.

2.3 Internet usage monitoring

Internet usage will be monitored to analyze Internet traffic patterns within the Organization. A list of restricted sites is implemented by the corporate firewall. This list will be updated from time to time.

2.4 Web-based voice or text Chat

Web-based chat is to be used for business purposes only that is for technical discussions between geographically dispersed teams.

2.5 Download of software

- The organisation decides upon the software required by employees on case to case basis.(Free and Licensed)
- No software application, add-ons or upgrades can be downloaded without the prior approval of the Systems Administration team.
- If any employee require any software then he/she needs to take an approval over mail from his/her HOD.
- Installation of all approved software will be done by the System Admin team only.
- System Admin Team does a periodic audit of the assets on a half-yearly basis.

Download of screen savers or executables is restricted to prevent harmful or malicious code entering the corporate network.

In general, all employees are required to avoid downloading any files through websites not specifically recommended by their line manager or the system administration team.

3. Email Policy

Email communications are to facilitate business related interactions within the Organization and with external entities including clients, vendors and other third-parties.

3.1 Restrictions on E-mail content

Any email communication sent within or outside the organization should not contain any content or remarks that can be construed as:

1. Offensive to an individual
2. Discriminatory against race, religion, gender, age, nationality or any personal preferences
3. Damaging to the Organization's policies or image

Employees are expected not to use office mail id's for registering purpose in different marketing websites.

3.2 Web-based email access

All employees should access email through Web Client or PC based client. Every mail should contain your signature with following minimum content:

--

Name
Designation
eTrans Solutions Private Limited
CIN:U63090WB2000PTC092223
Regd. Office: FD 404 Sector III
Salt Lake, Kolkata 700106
Phone: extn :
Mobile:

3.3 Email attachments

1. All email attachment should be less than 10 mb in size.
2. All the executable files should be zipped and sent.
3. Attachments should only be sent where required for official and project purposes.

3.4 Software code or code related information

1. All employees and users of eTrans' e-mail system have the responsibility of not sending out by email or other means any software code or code related information including but not limited to design data, requirements, business information of eTrans' customers and eTrans confidential information.
2. Any violation of this clause will be interpreted as gross misconduct and lead to termination and legal action.
3. For specific projects, designated eTrans employees may need to sign Client specified confidentiality agreements.

This clause is binding on all individuals for all times during and after their employment or contract with eTrans.

3.5 Email disclaimer

All users of eTrans' email system should include the following disclaimer in all email communications.

Disclaimer:

This email is intended solely for the individual addressed and the

information contained in this email message and/or attachments to it may contain confidential or privileged information. If you are not the addressee or have received the email in error, you should notify the sender immediately and permanently delete this e-mail from your system. The sender or eTrans Solutions Pvt. Ltd is not responsible for any errors or omissions in the contents of this message on account of transmission.

3.6 Email monitoring

1. All company emails are subject to monitoring.
2. Inter communication mails should be marked to HOD's
3. Adherence to circulation as per practice

3.7 Email quota

All users are allocated an email quota based on their role related requirements. Any request for increasing the email quota should be made in writing to the line manager or the systems administration team. The email quota for users will be monitored from time-to-time to assess email usage patterns.

4. Data Security

4.1 Use of Computers

Desktop and Laptop computers are to be used for work related activities. Use of computers for personal reasons such as web-browsing can be done only after working hours.

4.2 Software Code

Any code, design or documentation created at eTrans' Clients for its Clients is eTrans' Intellectual Property (IP). All users should take utmost care towards protecting this IP. Whilst monitoring and security systems are in place to protect Client and eTrans 's IP, any instance of breach or suspected breach of confidentiality of software code or code related information should be notified to the line manager with immediate effect.

4.3 Copying of files on media drives

1. Copying of company's data should only be done on company's provided media.
2. Any company's media drive should not be used for personal purpose.

4.4 Centralized print/scan facility

For scanning or printing of files only the office system should be used.

4.5 Hardware Accessories, Storage Devices and Network Accessories

All computers, computing accessories and network devices required by users will be provided by eTrans. Any requirement for additional hardware or accessories should be made to the concerned line manager or the Systems Administration team. Users should not use any devices or accessories without the written approval of the Systems Administration team.

4.6 Clear-Desk Policy

A clear-desk policy should be practiced by all users of eTrans' IT infrastructure. This helps achieve the objectives of:

1. Better working environment
2. Prevention of loss and theft
3. Improving the image of the office to employees and visitors

4.7 Mobile computing, communication devices and Tele working.

Only eTrans authorized equipment and accessories should be used within the eTrans infrastructure. Use of any mobile or unauthorized communication device constitutes a violation of the harmful code policy and data security policy. This restriction applies to (including but not limited to):

1. Mobile phones synchronized to desktops/laptops,
2. PDAs & other hand-held devices
3. Remote Access to servers is only accessible to Network Administrators.

4.8 Reporting Data Weaknesses or Security incidents

Any user who is in the knowledge of a security threat or weakness should report the same to his or her line manager or the Systems Administration team. Whilst all users are encouraged to report data or network vulnerability, any changes should be routed through the Systems administration team. Any changes made to hardware, network or security devices and systems may be construed as tampering.

5. User Rights and User Access Policy

1. Users are responsible for the security of the data they are handling.
2. If a user is moved from one project to another, his or her user rights will be accordingly modified.
3. Project related documentation will be made available only to designated individuals within that project.
4. For security reasons user are asked not to share their password with others.
5. Users are expected to access their own user ids.

5.1 Documents, Code and Test Data access based on User Groups

System related documents, code and any confidential documents related to the project can be accessed by the designated personnel for that project.
The intellectual Property Rights of all Soft Assets belong to eTrans.

5.2 Use of Laptop computers

1. The laptop owners are liable for the security, safety and cleanliness of the laptop.
2. Employees are specially asked to keep a track of their laptop when they are in tour.

Apart from this the use of desktop computers is encouraged for all offices of eTrans.

6. Physical Access Policy

Physical access restrictions are an integral part of the security policy at eTrans. eTrans' offices and facilities are meant solely for eTrans' employees, contractors and official visitors (after clearance).

6.1 IDC/Server Access

The server room is a restricted entry zone. Only authorized systems administration personnel are allowed to access this area. Entry is restricted for all individuals without the presence of a representative from systems administration. Systems

administration is responsible for restricting access to the server rooms.

7. Print Policy

Printers and printer consumables are meant for printing official documents. All users are advised to exercise discretion in the use of this shared facility.
eTrans encourages Green policy of minimum printing.

Apart from that eTrans also focus on the following items:

1. Printing pages from Internet website apart from project related reading from public websites
2. Any project related confidential documents including code, design and other related documents
3. Printing of colored documents when not needed
4. Printing of multiple copies unless required.
5. Any material that can be deemed offensive, discriminatory or abusive

8. Password Policy

All users are required to safeguard their personal passwords. The following practices are to be adhered for passwords:

1. Follow the guidelines provided in formulating secure passwords
2. Avoid using obvious passwords
3. Do not share your password with anyone
4. Change your password regularly or if you feel it may have been compromised
5. Group passwords should be changed each time there is a change in the constitution of the group sharing the password

The password policy is : -

1. The password's length is more than 8 characters.
2. Password must contain one upper, one lower, one digit and one number.
3. After 90 days system will automatically ask for new password.
4. Avoid reusing a password.
5. Avoid using the same password for multiple accounts.
6. Don’t use automatic log on functionality.
7. Store passwords on a secure computer system.

Please change Mail password from your web access as per policy.

9. Backup Policy

- Server side back-up for data is done by automated schedule job on an incremental basis daily and fully on a weekly basis .
- All users are advised to take back-ups of their files on officially provided file server on a daily basis.
- For certain computers with high priority data the backup has been automated.
- The following back-up activities are performed by systems administration:

1. Database Server back-up
2. Application Server back-up
3. Code back-up

- Backup is to be taken from File Server as per daily incremental basis.
- Office User should take backup of their own important work files and mail weekly in his / her specified folder in the File Server
- Some critical business users (employee) whose documents are most urgent, an automated script will take backup of their system on a daily basis when connect to the office network.

10. Guidelines for use of IT Systems

eTrans' IT systems are a shared resource and the responsible use of these shared resources is an organisation-wide responsibility. Some guidelines have been included here in addition to the policies described in this document.

10.1 Use of CDs/ DVDs and other storage

Any external drive, plug-in or software is a potential source of virus and can compromise the organization security. Users are advised to avoid use of a) Personal CDs/DVDs, b) Audio devices that integrate with computers MP3 players for downloading or uploading files and c) Movie or still photography cameras on computers.

10.2 Switching off of IT equipments and power points

Power usage has to be optimized from the point of view electricity consumption and the performance of equipment. Users are advised to switch of equipment at the end of the working day and whenever there is an anticipated long period of inactivity. UPS and power back-ups should be used with discretion to optimize the life of these important network accessories.

10.3 Computer Care

The allocated laptops & desktop computers are the individual's personal asset for the time spent for office work.
The maintenance procedures required for optimum machine performance should be performed by the individuals.
1. Cleaning the monitor and keyboard
2. Organizing file on hard-drive.
3. Disk clean-up.

Any failed equipment or naked wires should be reported to Systems administration immediately. No inflammable material or items should be brought into the server room and RnD Lab of eTrans premises.

eTrans operates a complete no-smoking policy within the office premise.

11. Confidentiality of Organizational and Customer Data

11.1 Applicable laws

All eTrans employees and contractors are bound by the confidentiality and security laws mandated by the geographies that eTrans' operates.

11.2 Intellectual Property

There is liability placed on the concerned individual employee for breach of

any Intellectual Property rights. This implies in the main:

Code, designs and confidential material created and used by eTran's for product development should not be compromised or leaked out
Any designs or patents should not be copied or sold/ distributed.
No data related to a customer should be publicized without authorization.

11.3 Data Protection Act

1. No data should be provided to tele-caller
2. No personal information relating to a person or a group of people should be divulged without the written consent of the concerned individuals

As a broad principle, all eTrans employees and contractors are advised to seek prior written consent before using any personal or Client related data.

12. Acceptance of IT Policy by Employees

All employees by default are deemed to accept the eTrans IT policy. users of eTrans' . Periodic audit by Functional/Line managers is recommended to check the compliance.

13. Procedure for reporting non-compliance

Whilst this document lines out the IT Policy in place within eTrans, eTrans encourages:

1. involvement of Group for continuous improvement in IT security Policy,
2. all users to report any instances of non-compliance to improve the process and strengthen eTrans' image as a security process driven organization, and
3. all users to give suggestions for improvements at all times.

14. Capacity Management

Capacity Management process would include the following steps and rules.

1. Monitoring of the Hard disk on a regular basis.

2. Hard Disk threshold limit for every server is 85 %.

3. If the space reaches the threshold limit then System Administrator plans for new hard disk procurement and gives a report to Head – System & Database Administrator for initiating the process of hard disk purchase

4. All the process should be approved by CTO

5. Change the Hard disk before the space reaches up to 90%