E-commerce

Case study: Shaheen Power Industries (SPI) manufactures and supplies a variety of generators, inverters and batteries. SPI has a country-wide network of distributors authorised for sales, service and spare-parts. The management of SPI has been approached by E-Booster (EB) with a proposal to develop an e-commerce solution for SPI. EB's representative has suggested that both B2B and B2C e-business models could prove beneficial for SPI. The management acknowledges that there are many advantages of using these e-business models. However, it is also concerned about certain issues which may be faced during the process of development and implementation.
Required:
(a) Identify three key differences between B2B and B2C models. (03)
(b) Discuss the adverse impact which the implementation of B2B and B2C models may have on SPI's business and its relationship with the distributors and what measures may be taken to avoid such an impact while implementing the two models. (06)

B2B	B2C
Customers are other companies.	Customers are individuals.
Integration between seller and buyer systems is required.	Integration between seller and buyer systems is not necessary.
Both sellers and buyers are required to follow standard procedures while communicating with each other.	Standardisation of procedures is not required while communicating with each other.
It may involve negotiation with the counter parties over price, product specification and delivery terms and conditions.	Price, product specification and delivery terms and conditions are usually fixed.

(b) The implementation of B2B and B2C models would affect SPI's business and its relationship with its distributors in the following manner:
(i) Majority of SPI distributors may not agree to engage in B2B as it requires compatibility and connectivity of the business organisations information systems. This involves investment of cost and time.
(ii) With the launching of B2C website, SPI's relationship with its distributors may be affected if significant amount of business is carried out through the website and distributors are not adequately compensated.
(iii) If distributors leave or become demotivated, SPI may face problems in providing services and spare-parts to its customers and may need to search new service and spare-parts vendors.

In view of the identified issues, SPI may proceed as follows:
(i) SPI should consult with its distributors before taking the B2B initiative. Based on their response SPI should conduct cost benefit analysis for the B2B model and should take the decision accordingly.
(ii) SPI may divide its distributors between small and large segments. It may initiate B2B with large segment partners initially and keep doing the business in usual way with small segment partners.
(iii) For B2C model SPI may take one of the following courses of actions:
- It should not involve in direct sales and restrict the scope of B2C website to provide information and answering customer queries. For example, it may provide information about range of available and upcoming products, maximum retail prices and contact details of dealers, etc.
- If it goes for direct sales it may keep the local distributor margin in the sales price and get the product delivered to the customer via local distributor.
- It may divide its customers in segments and may choose certain segments for direct selling segments and certain for indirect sales. For example, direct sales would be feasible in the cities where dealers' network is not present or to a particular class among which e-commerce is popular.

Benefits of e-commerce:

To businesses:-
(i) It allows more business partners to be reached within a small span of time.
(ii) More geographically dispersed customer base can be reached.
(iii) Procurement processing costs can be lowered.
(iv) Inventories can be reduced.

(v) Sales and marketing costs can be reduced.
(vi) Prompt interactions with customers.

To customers:-
(i) Increased choice of vendors and products is available.
(ii) Convenience of shopping from anywhere i.e. home or office.
(iii) Round the clock shopping.
(iv) Access to more detailed information about the products, from vendors as well as from independent sources.
(v) More competitive prices because of increased price comparison capability.
(vi) Greater customization in the delivery of services.

Reasons to appoint a seasoned IT professional:

Key reasons to appoint a seasoned IT professional are as follows:

i. He would be in a better position to suggest latest techniques and equipment as well as reengineering of procedures and expedite the process of billing.
ii. He could assist the management in planning and implementation of e-business strategy in an effective and efficient manner.

Benefits of integrating various business units (stores):

1. Effective inventory management:
   Procurement can be planned covering the overall inventory position rather than each store making its own orders. On the one end this would help in getting more competitive rates and on the other end it would save the ordering cost. Internal transfer of inventory could be made where delays are expected on the part of suppliers.
2. Efficient MIS:
   Management information and reporting system will become more efficient and effective.
3. Effective sales management:
   Availability of sales data of all stores would be helpful in developing sales strategies and promotions.

B2B model.
B2B model automates the process of buying and selling among companies via Internet. The B2B transactions occur between organizations (businesses) and not between individuals.

Following are the **key characteristics** of B2B model;

(i) Need for following standards amongst business partners is a pre-requisite.
(ii) The systems and procedures of business partners are closely aligned.
(iii) There is a high level of co-ordination between the business partners.
(iv) Paperless transactions.

Benefits of B2B model are as follows:

(i) Reducing inventory on hand. /Managing inventory more efficiently.
(ii) Enhancing just-in-time manufacturing.
(iii) Getting products to market faster.
(iv) Bringing sellers closer to their customers.

B2B model can **assist** the company in **improving its performance** in the following manner:
(i) Managing inventory more efficiently.
(ii) Suppliers can be given access to stock levels such that when stocks fall below a re-order level, the supplier will automatically send replacement stocks. Thus less employee time will be spent in reviewing stock levels, and replacement stocks will be received immediately when they are required.
(iii) Self-generated e–mails can be used to inform suppliers about new stock requirements.
(iv) Information concerning stock deliveries and receipts can be sent by Electronic Data Interchange. This will provide time and cost savings.
(v) Payment process can be expedited by making payments electronically.
(vi) Paperless environment.
(vii) Need to re-enter the data will be reduced.

Barriers in implementing the B2B model are as follows:

(i) Different culture of the transacting organizations.
(ii) Compatibility between e-commerce applications.
(iii) International trade barriers.
(iv) Lack of user authentication and lack of public key infrastructure.
(v) Lack of qualified personnel.
(vi) Legal issues. (Different laws may be applicable to different partners / stakeholders.)

Arrangements to be made with supplier before implementing B2B model:

i. Get the participants agree upon industry standards to be followed for transmission of data electronically and invest money on attaining standardization.
ii. Redesign documents, reports and procedures according to the agreed industry standards.
iii. Develop and deploy security controls on the communication channels and systems.
iv. Methods of handling exceptional, erroneous or disputed transactions.
v. Restricting the participants from changing/upgrading procedures and systems in isolation.

Benefits of B2C to business:

i. The organization would be independent of time and space barrier and could reach out more new customers.
ii. By facilitating its customers at their doorstep, the organization could retain its existing customers who may be frustrated due to long checkout queues.
iii. It would help the organization in significant cost saving as operational costs such as staffing and building will be minimized.

The company can make **use of the B2C model** in the following way:
(i) The company can make basic information of its products available at its website. Such information may include product price, availability, features of the product and any additional charges such as delivery or insurance etc. When such information is available to potential customers in an easy to understand format, it will be easier for them to make decisions and they will be automatically attracted towards company's website.
(ii) The company can provide some form of personalization of the website for repeat visits such as welcoming the customer by name or displaying a list of products already reviewed. This would help make the site more customer-friendly and probability of customers' visiting the company's website before any related purchase is made.
(iii) Providing some incentives to use the website such as loyalty points may help to attract more customers.
(iv) New customers may be reached, especially those who are not located within traveling distance of the company's sales outlet.
(v) When a purchase is made on company's website, customer information will be stored by the company's computer system. This information can be used to help provide repeat business for the organization.
(vi) Data can be mined (processed) to identify relationship in purchases.
(vii) The company can carry out business on 24/7 basis.

Challenges while running B2C website:

i. Maintaining security of data on the organization's servers during online transactions.
ii. Ensuring 24/7 availability of the B2C store by protecting the B2C site from virus and denial of service attacks.
iii. On time updating of the B2C store.
iv. Timely response to customers' queries and quick resolution of customers' complaints.

Areas that management should focus on in order to make its online store a success:

i. Navigation friendly and eye-catching:
The website should be designed in such a manner that the customer is able to access the required information quickly. Moreover, it should be eye catching to attract incidental surfers.
ii. Low response time / Fast download:

All the links and functionalities incorporated in the website should respond in a quick manner. The website contents should be downloaded quickly.

iii. Mobile version:

Mobile version of the site should be developed simultaneously and made available to customers.

iv. Customer Support Area:

There must be a Frequently Asked Questions (FAQs) section that should contain information related to customers' interest in question answer format. The website should have a 'Contact Us' page that should contain telephone numbers and an email interface through which customers may contact the company. Live chat option should also be considered for immediate resolution of customers' queries.

v. Up-to-date:

The availability of products and prices should always be kept updated on the website.

vi. Availability:

The website should be available 24 hours a day, 7 days a week; downtime, if any, should be minimal.

vii. Payment options:

All types of commonly used payment options should be available. For example, the customers should have the liberty to pay electronically or pay cash on delivery.

viii. Security:

The website should contain adequate security features (such as deployment of SSL certificates) duly verified by qualified third parties (such as Web Trust/VeriSign) on a regular basis. Moreover, adequate instructions regarding security of transaction should be made available and the customers should be encouraged to read them prior to making any transaction.

ix. Customer feedback area:

There should be a customers' feedback area where customers may give their feedback on products purchased and about customer services.

x. Personalization:

The site should have the feature to remember customer preferences and enable personalization to registered users.

xi. Product Specification:

The website should contain accurate and detail specification of available product range. It should have a feature of comparing two or more product features.

Matters to be considered while developing e-commerce enabled website: The Company needs to plan the following matters in order to ensure customers' satisfaction:

(i) Effective interaction with its existing and prospective customers. For that it needs to:
- develop and post Frequently Asked Questions on its website;
- set fast response standards, at least to match anything offered by the competitors;
- establish ease of navigation around its website and enhance the site's stickiness.

(ii) Efficient handling of large number of orders. This may involve:
- ensuring sufficient capacity is available for dealing bulk of customer queries in a timely manner;
- setting targets for customer services for responding to customers and resolving their queries;
- making effective use of automated systems to handle such scenarios;
- ensuring the performance of relevant staff and system is scalable; and
- making arrangements with courier service to ensure timely delivery of services.

(iii) Maintain the satisfaction level of its existing customers. For this it may need to:
- ensure that accuracy of product's specification mentioned on the website;
- develop a customer feedback area at the website where customers can give their feedback on company's services and products freely; and
- plan the way to follow-up adverse customers' comments/feedback till the resolution of the matter.

(iv) Customize solutions to meet needs of different segments of customers. For this it may need to gather customers' data to identify their buying behavior and future needs.

(v) Payment flexibility and related concerns. This may include:
- offer choice of payment mechanism like acceptance of credit/debit cards and cash on delivery; and
- implement appropriate security mechanism over website

Benefits of online store:

An online store is more customer friendly than a traditional store because:
(i) The customer can shop electronically without having to leave the comfort of his home, hostel or office.
(ii) Customers can do the shopping 24 hours of the day, 365 days of the year. The barriers of bad weather and poor law and order situation etc. are minimized.
(iii) Customers sitting in far flung areas could easily place order for their required items which are not available near their place of residence.
(iv) Customers have the option to review and compare prices of similar products within few minutes without the hassle of going through the market for hours.

Measures to facilitate the customers and alleviate their security concerns:

Customer friendly
 Design the website in such a way to make search and navigation easy for customers.
Quality of goods
 Make customers' feedback and rating forum where customers may give their feedback o products purchased and DPL's customer services.
Timely delivery
 Make arrangement for products delivery with reliable courier services.
 Minimize lead time for delivery of orders but at the same time keep the customers informed about the correct delivery time.
Security of transaction
 Deploy appropriate Secure Socket Layer at its website.
 Get its website certified from institutions like Webtrust.
 Store customers' data in encrypted form.
Payment means
 Make payment arrangements with a credit card processing company to accept generally used debit/credit cards like Master and VISA etc.
 Get the payment mechanism certified by an independent authority like Verisign.
 Make payment arrangements with local banks through online transfer of funds.
 Make cash on delivery payment arrangements.

Suggested measures to ensure that website remains secure, update and available:

Security:
(i)If site maintenance and support is outsourced, get appropriate non-disclosure agreement signed. If maintenance and support is in-sourced, get non-disclosure agreement signed by all members of team.
(ii)For the security of customers' transactions, implement appropriate standards and protocols like Open Buying on the Internet (OBI), Open Trading Protocol(OTP), and Secure Electronic Transaction (SET) Protocol etc.
(iii)Get the transaction area be protected with Secure Socket Layer (SSL).
(iv)Get the website security mechanism and related procedures certified by an independent audit firm.
(v)Define appropriate policies and procedures for privacy and confidentiality issues.
(vi)Document the mechanism for securing the website and get it approved from appropriate authority.
(vii)Appoint external information system auditors for periodic audits of website security.

Update:
(i) Identify the events/activities/actions that require updating the website contents.
(ii)The departmental heads shall be made responsible for keeping the respective information on the website updated.
(iii)A senior officer should be assigned the responsibility for periodic review of the website to ensure that information given there is current.

Availability:
(i)If maintenance and support is outsourced, get appropriate service level agreement signed. If maintenance and support is in-sourced, appoint appropriate team for 24/7 schedule.

(ii)Make arrangements for a suitable help desk function.
(iii)Prepare and test disaster recovery and business continuity plans.
(iv)Periodically monitor website traffic and its response in peak hours.

Questioner to access viability, resource requirements and customer support requirements of e-commerce project:

Project Viability:
(i) What is the estimated capital expenditure and recurring costs?
(ii)What advantages will CSL gain from becoming accessible on the web?
(iii)What disadvantage(s) might CSL encounter from becoming accessible on the web?
(iv)What are the legal requirements/restrictions imposed by the government which must be met?

Required Resources:
(i) What hardware will be required? Has it been arranged?
(ii)What software would be required? Has it been purchased?
(iii)What type of communication service (Email, discussion board, phone, toll free number, postal mail) would be used?
(iv) What type of security services/protocols would be required? (SSL, SET and IPSEC etc.)

Customer services and support requirements:
(i)What support would be available to customers (FAQs, query via email, online chat, toll free number)?
(ii)How would the orders be fulfilled/delivered?
(iii)What payment options would be available to customers (check, credit/debit card, electronic funds transfer)?
(iv)Which currencies would the entity accept for payment?
(v)How would the entity handle custom duties?
(vi)Would the entity offer import and export assistance to its customers?
(vii)Which other languages (if any) could/should be made usable on the website?

The objectives of e-government are as follows:

1- to fulfill the citizens and businesses needs and expectations satisfactorily with minimum hassle/efforts (in terms of time and again visiting the offices, standing in long queues, limited number of service hours etc.) and minimum personal interaction between the citizens/businesses and the government personnel (to minimize corruption such as bribe).
2- to facilitate a speedy, transparent, accountable, efficient and effective process (in the back office) for performing government administration activities.

The four phases of e-government model:

First Phase (Publish or Presence phase)
In this phase, the government departments introduce their websites to provide the public with relevant information. The format of government websites in this phase is similar to that of a brochure. The value to the public is that information is publicly accessible; processes are described and become more transparent which lead to improved services.
Second Phase (Interaction phase)
In this phase the interaction between government and the public is stimulated with various applications. People can ask questions via e-mail and download forms and documents. Submission of applications can be done online on 24 hours basis. Internally, government organizations use LANs, intranets and e-mail to communicate and exchange data with each other during this phase.
Third Phase (Transaction Phase)
In this phase, complete transactions are carried out online without going to the office. For example, filing of income tax returns, filing property tax, renewal of licenses, visa and passports and online voting etc. This phase is made complex due to security and personalization issues.
Fourth Phase (Transformation phase)
In this phase all information systems (of government) are integrated and the public can get G2C and G2B services at one (virtual) counter. One single point of contact for all services is the ultimate goal.

Following issues may create **hindrance** in the **effective implementation of e-government** in a developing country:

(i) Political instability including leadership and political commitment.
(ii) Lack of citizens' trust over security of government's websites.
(iii) Lack of information and communication infrastructure including country-wide availability of economical and reliable Internet service.
(iv) Resistance to change from government employees.
(v) Low education level of citizens.
(vi) Low economic status of the citizens.

The government of a developing country may face the following **challenges** while implementing G2C strategies:
(i) Creating infrastructure for providing economical access to the government websites to all citizens specially those living in remote towns and villages.
(ii) Security of government websites.
(iii) Creating awareness among masses as regards the uses of e-commerce technology and related issues.

Government to citizen (G2C) e-commerce model may be implemented in the following **areas:**

(i) Lodging complaints and giving feedback on various projects of the government.
(ii) Keeping citizens' update on ongoing developments like tax reforms, construction of dams, education policy etc.
(iii) Online submission of tax returns.
(iv) Online payment of utility invoices.
(v) E-voting in local bodies or in general elections.
(vi) Online submission of job applications.
(vii) Online tracking of CNIC and Passport application status.

Reasons for revision of web hosting contract when going for online payment solution:
When the entity will go for the online payment solution, it will need to develop and install customized application on its website, connect it to the payment solution provider's website, and implement mandatory controls to ensure secure processing of payment.
Such features and controls may require additional storage space, uploading/downloading limits and support for development tools etc. Hence, the entity would need to review its existing webhosting contract and to make necessary amendments accordingly.

Role of customized software in processing online payment:
The customized application would enable the students to create their accounts (get them registered) at the university's website. The application would identify and distinguish each student through a unique field (ID) e.g., their enrollment number. They would be authenticated through their passwords, after which the payment requests of the students would be forwarded automatically to the payment service provider. The application will also keep track of the students' payments using their unique ID.

Following **controls** should be implemented in order to ensure smooth and secure availability of the online fee payment system:

(i) Installing secure socket layer over student's login and payment processing pages.
(ii) Storing students' passwords in irreversible encryption.
(iii) Storing students' personal information in encrypted format.
(iv) Backup and contingency plan for ensuring availability of the online payment feature.

The university would need to consider the following **factors while selecting a bank** for opening internet merchant account:

(i) Cost: The University should consider which bank is offering most competitive rates for providing the required service. This may include account set up cost, annual maintenance cost and cost per transaction.

(ii) Reporting and administration facilities: RU may need to check the tools offered by the banks to manage merchant services. This may include access to real-time transaction statements, ability to extract data for research and planning e.g., number of declined transactions per month, reasons for decline etc.

(iii) Technical support: The University may consider the extent and level of technical support provided by the bank. This may include availability of support on 24×7 basis, strength and qualification of technical support team and problem reporting and resolution mechanism etc.

(iv) Security: The University may need to consider the controls that have been implemented by the bank for ensuring the security of students' credit card details. This may include enquiring about the controls implemented for ensuring security of students' data, to which security standards the payment system is compliant and fraud protection controls etc.

(v) Availability: The University would need to consider the measures taken by the bank to ensure availability of the payment system. This may include reviewing the backup and contingency planning.

(vi) Market reputation: The University may need to survey market and/or take feedback from the bank's existing customers on all of the above stated factors to assess the reliability of the bank.

Risks associated with e-commerce and related mitigating measures:

Risks	Mitigating Measures
Privacy: Customers' private and confidential information may become public and the seller risks facing legal prosecution in case the customers' data is compromised.	Seller should store customers' data in encrypted form. Seller should declare that he would not disclose customers' data to third parties or any other agency unless required by the law. Seller should get the website certified by the Web Trust.
Integrity of transaction: Information submitted by the customers may be tampered during or after the transaction.	Seller should deploy Secure Socket Layer (SSL) on the website, especially on those pages where customers' data is collected. Seller should make use of public key cryptography and allow customers to encrypt the data with his public key.
Fraud: The seller may indulge in fraud or the website may not be authentic.	Buyer should not follow hyperlinks received from marketing emails to visit the seller's website. Buyer should install fishing filter embedded web browsers.
Non-repudiation: Buyer may deny that he has placed the order.	The seller should get the customers registered with its website and assign them digital signatures before making any transaction. These signatures should be used for communication with the seller.
Availability: Website may become unavailable due to virus attack, email/message bombardment on system or system malfunction.	Deploy firewall with effective policies to prevent unwanted traffic. Deploy reputed antivirus and update it regularly. Develop and implement an effective disaster recovery and business continuity plan for the e–commerce website. Ensure periodic testing and updating of the plan.
Trust: Seller may deceive the buyers and the delivered order may be of very low/poor quality than its description mentioned at the online store.	Customers should be alert to this possibility and satisfy himself through available means, before carrying out such a transaction.

Risks in adopting EDI and related controls include:

Risk 1: Transaction Authorization: Since the interaction between parties is electronic, there is no inherent authentication occurring. Computerized data can look the same no matter what the source and do not include any distinguishing human element or signature.
Controls:
(i) Digital signatures should be in the transmission to identify the source.
(ii) Data should be encrypted using algorithms agreed to by the parties involved.
(iii) The receiving organization must have controls in place to test the source and reasonableness of messages received. This may be based on trading partner's transaction history or documentation received that substantiates special situations.

Risk 2: Where responsibilities of trading partners are not clearly defined in the agreement, there could be uncertainty related to specific legal liability.
Controls:
(i) Responsibilities of trading partners should be clearly defined in the agreement and reviewed periodically.
(ii) Legal consequences of disputed transactions and their legal liabilities should be clearly defined.

Risk 3: Unauthorized interception of data by third parties.
Controls:
(i) Direct or dedicated transmission channels among the parties should exist to reduce the risk of tapping into the transmission lines/use of secure socket layer.
(ii) Data should be encrypted using algorithms agreed on by the parties involved.

Risk 4: Deletion of transactions.
Controls:
(i) Log each inbound transaction on receipt.
(ii) The use of control totals on receipt of transactions to verify the number and value of transactions to be passed to each application and reconcile totals between applications and with trading partners.
(iii) Arrange for security over temporary files and data transfer to ensure that inbound transactions are not erased between time of transaction receipt and application updates.

Risk 5: Duplication of transactions due to human or system error.
Controls:
(i) Automatic generation of unique transaction ID for each transaction.
(ii) Check on unique transaction ID before sending each transaction (at the sender's system).
(iii) Check on unique transaction ID before accepting each transaction (at the receiver's system).

Risk 6: Loss of confidentiality and improper distribution by EDI provider.
Controls:
(i) Legal consequences of disputed transactions and their legal liabilities should be clearly defined in the agreement.
(ii) The policies and procedures established by the EDI provider should be reviewed periodically to evaluate their effectiveness in avoiding/minimizing leakage of data or information.

Following **benefits** are achieved using **digital signatures:**

(i) Data Integrity: Any change to the digitally signed document renders the signature invalid. This ensures the recipient integrity of the message.

(ii) Authentication and Encryption: The recipient can ensure that the message has been sent by the claimed sender since only the claimed sender has the secret (private) key to encrypt the message.

(iii) Non-repudiation: Since the digital signatures on one document cannot be transferred to other document, hence the claimed sender cannot later deny generating and sending the message.

Process for exchange of digitally signed e-mails:

The required process would involve the following steps:
(i) A hash-value of the message is calculated.
(ii) The message is then encrypted using sender's private key and sent to the receiver.

(iii) On receipt, the sender decrypts the message. The decryption requires authorization by way of public key of the sender that corresponds to the private key used during the signing of the message.
(iv) The hash-value is computed again using the same algorithm as was used during the signing process. If the two hash-values are identical, the verification is successful otherwise it means that the digital signature is invalid i.e. the message has been altered during transmission.

Since public key may be obtained from the issuing trusted source/certification authority, hence someone else who has access to the message can also decrypt the message, i.e., confidentiality of the message may be compromised. This risk can be minimized if, the sender, after encrypting the message with his private key encrypt it again with the recipient public key. In this case the receiver would use sender public and his private key to decrypt the message. Rest of the process remains the same.

The organization should take the following **steps to ensure** that it is **complying with relevant privacy laws:**
(i) Identify the concerned laws and regulations governing the issue of privacy.
(ii) Study and understand the legal requirements of each such legislation.
(iii) Critically review the privacy policy and related problems to ascertain that it takes into consideration the requirement of applicable privacy laws and regulations.
(iv) Verify that the correct security measures are adopted and are being implemented.

Principles to be included in privacy policy:

Following principles should be considered while collecting personal information:
Openness: There should be a general practice of openness about policies related to personal information and those should be adequately disclosed to all stakeholders.
Collection limitation: The collection of personal information should be obtained by lawful and fair means and with the knowledge and consent of the subject.
Purpose specification: The purpose for collecting personal information should be disclosed at the time of collection. Further uses should be limited to those purposes.
Use limitation: Personal information should not be disclosed for secondary purposes without the consent of the subject or by authority of law.
Individual participation: Wherever possible, personal information should be collected directly from the individual.
Regular updating: Individuals should be allowed to inspect and correct their personal information.
Security safeguards: Personal information should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.
Limited Access: Access to personal information should be limited to only those within the organization with a specific need to see it.
Accountability: Someone within the organization, such as the Chief Privacy Officer or an information manager, should be held accountable for complying with its privacy policy.

The generally accepted privacy-protection principles are as follows:
(i) Consent: The collection of personal information should be obtained by lawful and fair means and with the knowledge and consent of the data subject (individual).
(ii) Purpose specification: The purpose for collecting personal information should be disclosed at the time of collection.
Further uses should be limited to those purposes.
(iii) Use limitation: Personal information should not be disclosed for secondary purposes without the consent of the data subject or by authority of law.
(iv) Data quality: Only the relevant data for the extent necessary for the specific purpose should be collected. The collected data should be accurate, complete and kept up-to-date.
(v) Security safeguards: Personal information should be protected by reasonable security safeguards against such risks as loss/ destruction, modification, unauthorized access/ disclosure etc.
(vi) Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data, the main purposes of their use, and the identity and usual residence of the data controller.
(vii) Individual participation: People should be able to establish whether data exists about them in a personal data system. If such data exists, they should be able to examine it and correct or delete data about themselves that is inaccurate, incomplete, out of date or irrelevant.
(viii) Accountability: People who exercise control over personal data should be held accountable for ensuring that appropriate measures for complying the above stated principles are in place and working.