PGDM- IB, 2017- 19

Information Systems Management for Business

IB- 206

Trimester – II, End-Term Examination: December 2017

Roll No: _____

Time allowed: 2 Hrs 30 Min
Max Marks: 50

Instruction: Students are required to write Roll No on every page of the question paper, writing anything except the Roll No will be treated as **Unfair Means.** All other instructions on the reverse of Admit Card should be followed meticulously

Section A (Attempt 3 out of 5 questions) **3*5= 15 Marks**

1. Describe the characteristics of management information systems (MIS) and explain how MIS differs from TPS and from DSS
2. It has been said that the advantages that leading edge retailers such as Dell and Walmart have over their competition isn't technology, it's their management. Do you agree? Why or why not?
3. What are the challenges faced by any firm while implementing information systems? What are your recommendations to overcome them?
4. Describe the ethical issues raised by technology trends-
    a. computing power doubles every month,
    b. data storage costs rapidly declining,
    c. data analysis advances,
    d. networking advances and the internet
5. Describe each of the four kinds of organizational change that can be promoted with information technology

Section B (Attempt 2 out of 3 questions) **2*10= 20 Marks**

1. List and describe four competitive strategies enabled by information systems. Illustrate with examples, how information systems can support each of these competitive strategies.

2. What are the principal e-commerce business and revenue models? What issues must be addressed when building an e commerce presence?

3. Flipkart is an e-commerce site that sells goods and accepts credit card payments.
    a) Discuss the security threat to this website and their potential impact.
    b) Establish a framework for security and control
    (information systems controls, risk assessment, security policy)
    c) Establish disaster recovery planning and business continuity planning

32

Turn Over

Section C (Compulsory Case Study) **15 Marks**

Monitoring Employees on Network: Unethical or Good Business

As Internet use has exploded worldwide, so have the use of email and the web for personal business at the workplace. Several management problems have emerged: First, checking email, responding to instant messages, or sneaking in a brief Youtube or MySpace video create a series of nonstop interruptions that divert employee attention from the job tasks they are supposed to be performing. According to Basex, a New York City business research company, these distractions take up as much as 28 percent of the average U S worker's day and result in $650 billion in lost productivity each year. In India, a websense survey of major cities in India across industries has revealed that an employee visits the internet for personal purposes on tuning in losses to the companies of Rs. 1.6 lakh (PTI).

Second, these interruptions are not necessarily work related. A number of studies have concluded that at least 25 percent of employee online time is spent on non-work related Web surfing, and perhaps as many as 90 percent of employees receive or send personal e-mail at work.

Many companies have begun monitoring their employee use of email, blogs and the Internet, sometimes without their knowledge. A recent American Management Association (AMA) survey of 304 U.S. companies of all sizes found that 66 percent of these companies monitor employee e-mail messages and web connections. Although U. S. companies have the legal right to monitor employee Internet and email activity while they are at work, is such monitoring unethical or is it simply good business?

Managers worry about the loss of time and employee productivity when employees are focusing on personal rather than company business. Too much time on personal business, on the internet or not, can mean lost revenue or overbilled clients. Some employees may be charging time they spend trading their personal business to clients, thus overcharging the clients.

If personal traffic on company networks is too high, it can also clog the company's network so that legitimate business work cannot be performed. Schemmer Associates, an architecture firm in Omaha, Nebraska, and Potomac Hospital in Woodridge, Virginia found their computing resources were limited by a lack of bandwidth caused by employees using corporate Internet connections to watch and download video files.

When employees use e-mail or the web at employer facilities or with employer equipment, anything they do, including anything illegal, carries the company's name. Therefore, the employer can be traced and held liable. Management in many firms fear that racist, or other potentially offensive material accessed or traded by their employees could result in adverse publicity and even lawsuits for the firm. Even if the company is found not to be liable, responding to lawsuits could cost the company tens of thousands of dollars.

Companies also fear leakage of confidential information and trade secrets through email or blogs. Ajax Boiler, based in Santa Anna, California learned that one of its senior managers was able to access the network of a former employer and read the email of that company's human resource manager. The Ajax employee was trying to gather information for a lawsuit against the former employer.

33

Turn Over

Companies that allow employees to use personal e-mail accounts at work face legal and regulatory trouble if they do not retain those messages. E-mail today is an important source of evidence for lawsuits and companies are now required to retain all of their e-mail messages for longer periods than in the past. Courts do not discriminate about whether emails involved in lawsuits were sent via personal or business email accounts. Not producing those emails could result in a five-to-six figure fine.

U S Companies have the legal right to monitor what employees are doing with company equipment during business hours. The question is whether electronic surveillance is an important tool for maintaining an efficient and positive workplace. Some companies try to ban all personal activites on corporate networks- zero tolerance. Others block employee access to specific website or limit personal time on the web using software that enables IT departments to track the web sites employees visit, the amount of time employees spend at these sites, and the files they download. Ajax uses software from Spectorsoft Corporation that records all the websites employees visit, time spent at each site, and all emails sent. Schemmer Associates uses OpenDNS to categorize and filter web content and block unwanted video.

Some firms have fired employees who have stepped out of bounds. One-third of the companies surveyed in the AMA study had fired workers for misusing the Internet on the job. Among managers who fired workers for Internet misuse, 64 percent did so because the employee's email contained inappropriate or offensive language and more than 25 percent fired workers for excessive personal use of email. In India, major IT/ ITES companies have banned any use of Internet for personal purposes and have put intranet messaging to serve company interactions. Any violation is met with dire consequences of being fired.

No solution is problem free, but many consultants believe companies should write corporate policies on employee email and Internet use. The policies should include explicit ground rules that state, by position or level, under what circumstances employees can use company facilities for email, blogging, or web surfing. The policies should also inform employees whether these activities are monitored and explain why.

The rules should be tailored to specific business needs and organizational culture. For example, investment firms will need to allow many of their employees to access to other investment sites. A Company dependent on wide-spread information sharing, innovation and independence could very well find that monitoring creates more problems than it solves.

Questions **3*5= 15 Marks**

1. Should managers monitor employee e-mail and internet usage? Why or why not?
2. Describe an effective e-mail and web use policy for a company.
3. How would you feel if your employer used a software to monitor what you are doing on the job? Explain your response

34