40

RAJARATA UNIVERSITY OF SRI LANKA
FACULTY OF APPLIED SCIENCES

B.Sc. (General) Degree in Information and Communication Technology
Second Year - Semester II Examination – September/October 2020

ICT 2207 – MANAGEMENT INFORMATION SYSTEMS

Time: Two (02) hours

Answer **ALL** the questions.

1

a) What is an information system?

(03 marks)

b) What are the main components of an IT infrastructure?

(04 marks)

c) What are the strategic business objectives of information systems? Briefly describe each of them.

(06 marks)

d) What is MIS audit?

(04 marks)

e) "Organizational politics directly affect the Organizational information systems."
Is above statement true or false? Discuss your answer.

(08 marks)

2

a) What are the dimensions of information systems?

(03 marks)

b) Why are information systems so essential for running and managing a business today?

(06 marks)

c) Discuss behavioral view of organization.

(06 marks)

d) In relation to MIS, describe each of following applications and evaluate their benefits.

i. Supply chain management systems
ii. Database management systems
iii. Decision Making systems

(06 marks)

e) What are the four (04) generic strategies for dealing with competitive forces enabled by the use of IT? Briefly describe each of them.

(04 marks)

3

a) Information technology enhances business process in two (02) main ways. What are those ways?

(04 marks)

b) Briefly describe types of E- Commerce.

(06 marks)

c) What are the business values of Customer Relationship Management?

(07 marks)

d) Give a design of an MIS for inventory control system of an automobile company.

(08 marks)

4

Read the case study and answer following questions.

When you were at work, how many minutes (or hours) did you spend on Facebook today? Did you send personal e-mail or visit some sports Web sites? If so, you're not alone. According to a Nucleus Research study, 77 percent of workers with Facebook accounts use them during work hours. An IDC Research study shows that as much as 40 percent of Internet surfing occurring during work hours is personal, while other studies report as many as 90 percent of employees receive or send personal e-mail at work.

This behavior creates serious business problems. Checking e-mail, responding to instant messages, and sneaking in a brief YouTube 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!

Many companies have begun monitoring their employee use of e-mail, 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 e mail 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. Some employees may even be billing time they spend pursuing personal interests online to clients, thus overcharging them.

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 that computing resources were limited by a lack of bandwidth caused by employees using corporate Internet connections to watch and download video files. MONITORING EMPLOYEES ON NETWORKS: UNETHICAL OR GOOD BUSINESS?

When employees use e-mail or the Web (including social networks) 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, sexually explicit, 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 e-mail or blogs. A recent survey conducted by the American Management Association and the ePolicy Institute found that 14 percent of the employees polled admitted they had sent confidential or potentially embarrassing company e-mails to outsiders.

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 appropriate tool for maintaining an efficient and positive workplace. Some companies try to ban all personal activities on corporate networks—zero tolerance. Others block employee access to specific Web sites or social sites or limit personal time on the Web.

For example, Enterprise Rent-A-Car blocks employee access to certain social sites and monitors the Web for employees' online postings about the company. Ajax Boiler in Santa Ana, California, uses software from SpectorSoft Corporation that records all the Web sites employees visit, time spent at each site, and all e-mails sent. Flushing Financial Corporation installed software that prevents employees from sending e-mail to specified addresses and scans e-mail attachments for sensitive information. 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 employees for Internet misuse, 64 percent did so because the employees' e-mail contained inappropriate or offensive language, and more than 25 percent fired workers for excessive personal use of email.

No solution is problem free, but many consultants believe companies should write corporate policies on employee e-mail 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 e-mail, blogging, or Web surfing. The policies should also inform employees whether these activities are monitored and explain why.

43

IBM now has "social computing guidelines" that cover employee activity on sites such as Facebook and Twitter. The guidelines urge employees not to conceal their identities, to remember that they are personally responsible for what they publish, and to refrain from discussing controversial topics that are not related to their IBM role.

The rules should be tailored to specific business needs and organizational cultures. For example, although some companies may exclude all employees from visiting sites that have explicit sexual material, law firm or hospital employees may require access to these sites. Investment firms will need to allow many of their employees' access to other investment sites. A company dependent on widespread information sharing, innovation, and independence could very well find that monitoring creates more problems than it solves.

a) Should the managers monitor employees' e-mail and Internet usage? Discuss why or why not?.

(07 marks)

b) Define an effective e-mail and web usage policy for a company.

(08 marks)

c) Should the managers inform employees that their web behavior is being monitored? Or should the managers monitor secretly? Discuss why or why not?

(10 marks)

---END---