Eastern University, Sri Lanka
Faculty of Commerce and Management
Postgraduate Studies Unit
First Year First Semester Examination in Master of Business Administration - 2016/2017 (July, 2017) (Proper/Repeat)
MBA 1033 Managing Information and Technology

Answer all questions **Time: 03 Hours**

Q1. Read the following information carefully and answer the questions given below:

Monitoring Employees on Networks: Unethical or Good Business?

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. A Ponemon Institute study reported that the average employee wastes approximately 30 percent of the workday on non-work-related Web browsing, 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, or sneaking in a brief YouTube video creates 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 result in $650 billion in lost productivity each year!

Many companies have begun monitoring employee use of e-mail and the Internet, sometimes without their knowledge. A 2010 study from Proofpoint Plus found that more than one in three large U.S corporations assign staff to read or analyse employee e-mail. Another recent survey from the American Management Association (AMA) and the ePolicy Institute found that two out of three of the small, medium, and large companies surveyed monitored Web use. Instant messaging and text message monitoring are also increasing. 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 translates into 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. Procter & Gamble (P&G) found

that on an average day, employees were listening to 4,000 hours of music on Pandora and viewing 50,000 five-minute YouTube videos. These activities involved streaming huge quantities of data, which slowed down P&G's Internet connection.

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 run up huge legal bills. Symantec's 2011 Social Media Protection Flash Poll found that the average litigation cost for companies with social media incidents ran over $650,000.

Companies also fear leakage of confidential information and trade secrets through e-mail or social networks. Another 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, closely monitor e-mail messages, or limit personal time on the Web. For example, P&G blocks Netflix and has asked employees to limit their use of Pandora. It still allows some YouTube viewing, and is not blocking access to social networking sites because staff use them for digital marketing campaigns. 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. Financial services and investment firm Wedbush Securities monitors the daily e-mails, instant messaging, and social networking activity of its 1,000-plus employees. The firm's e-mail monitoring software flags certain types of messages and keywords within messages for further investigation.

A number of firms have fired employees who have stepped out of bounds. A Proofpoint survey found that one in five large U.S. companies fired an employee for violating e-mail policies in the past year. Among managers who fired employees for Internet misuse, the majority did so because the employees' e-mail contained sensitive, confidential, or embarrassing information. No solution is problem free, but many consultants believe companies should write corporate policies on employee e-mail, social media, and Web 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. 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, 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.

(Sources: Emily Glazer, "P&G Curbs Employees' Internet Use," *The Wall Street Journal*, April 4, 2012; David L. Barron, "Social Media: Frontier for Employee Disputes," *Baseline*, January 19, 2012; Jennifer Lawinski, "Social Media Costs Companies Bigtime," *Baseline*, August 29, 2011; Don Reisinger, "March Madness: The Great Productivity Killer," *CIO Insight*, March 18, 2011; "Seven Employee Monitoring Tips for Small Business," IT BusinessEdge, May 29, 2011; Catey Hill, "Things Your Boss Won't Tell You," *Smart Money*, January 12, 2011).

Case Study Questions:

(a) Should managers monitor employee e-mail and Internet usage? Why or why not?

(07 Marks)

(b) Describe an effective e-mail and Web use policy for a company.

(07 Marks)

(c) Should managers inform employees that their Web behaviour is being monitored? Or should managers monitor secretly? Why or why not?

(06 Marks)

(Total 20 Marks)

Q2.

(a) Define the term **"Green Computing or Green IT"** in your own words. **(03 Marks)**

(b) Why Green Computing or Green IT is highly needed for business organizations nowadays?

(04 Marks)

(c) Why it is important for companies to measure their energy use and inventory and track their information technology assets both before and after they start their green initiatives?

(03 Marks)

(d) What features of organizations do managers need to know about to build and use information systems successfully?

(05 Marks)

(e) Assess the relationship between Business Continuity Management (BCM) and Information System Continuity Management (ISCM).

(05 Marks)

(Total 20 Marks)

Q3.

(a) Recently, ninety-nine countries are hit by 75,000 attacks using US National Security Agency superweapon dubbed (named) the 'atom bomb of malware' stolen by mysterious hacking collective called 'The Shadow Brokers'. In order to protect the IT resources, what are the most important controls, tools and technologies available for safeguarding information resources of an organization?

(10 Marks)

(b) Identify the **six *strategic business objectives of information systems*** and **four *information system strategies for dealing with competitive forces***. Compare the both aspects and determine their similarities or uniqueness.

(10 Marks)
(Total 20 Marks)

Q4.

(a) Explain the relationships among **task, technology, people,** and **structure** in an organisation. Group these elements into two main approaches which will help to form **Contemporary Approaches to Information Systems.**

(10 Marks)

(b) Indicate the principal components of Telecommunications Networks and Key Networking Technologies of your organization and explain how these components and technologies affect your organization's performance?

(10 Marks)
(Total 20 Marks)

Q5.

(a) Explain the challenges of managing IT infrastructure in general as well as specific to your organization and propose some management solutions?

(10 Marks)

(b) Discuss the key issues or problems of managing data resources in your organization and explain how they can be solved by using Database Management System and new technologies?

(10 Marks)
(Total 20 Marks)