IVWIGHREN OGHENEOGAGA MARTHA

15/ENG02/032

500 LEVEL

COMPUTER ENGINEERING

COE 510 ASSIGNMENT

**QUESTION 1**

Below is a security policy for an XYZ company on the use of mobile devices in the company;

**XYZ’s POLICY FOR THE USE OF MOBILE DEVICES**

**1. Purpose:**

The basic purpose of having a mobile phone policy in an organisation is to define guidelines for the use of mobile phone within the company. As the cell phone is an essential commodity and can prove out to be the great asset for carrying out business.However, its excessive use can distract employee and staff. Therefore, it is important to consider the acceptable and not acceptable use of mobile phone in an organisation.

As the work environment and work are undertaken differs from employee to employee, therefore policy will apply differently to individual members. The company expects its employees to adopt a common sense approach in this regard.

**2. The Scope  of  "company cell phone policy”**

The mobile phone in the policy meant any personal cell phones, smartphones etc.  Use of mobile phones means communication through phone, exchange of messages, emails etc. However, the company policy discourages the use of mobile phones for surfing social media during office hours.

**3. Usability of  the mobile phone in office hours**  It is advised not to keep the mobile phone on the desk. If bought to the office it should be kept in a handbag etc. During office hours, a mobile phone can be used only for business purposes. It should be used minimal for personal reasons and mobile phone use must not hamper the work.

1. **4. Policy guidelines**
2. Use of mobile phone should be in the limit; excessive use of mobile phone causes the distraction in the workplace.
3. As per the “**cell phone policy at work “**there should not be any disturbance caused to colleagues.
4. The use of company-issued mobile phones must not pose any threat to the security of the company with any kind of inappropriate use.
5. There should not be any misuse of the company's internet connection.
6. Employees are not allowed to play games etc. on the mobile phone during office hours.
7. Use of mobile camera or recorder is strictly prohibited from recording company related confidential information.
8. Mobile phone should not be carried or used in the area which is already banned for the use of mobile phones etc.
9. Upload of any illegal or obscene material with the use of the company's intranet.
10. The company defines the activities wherein mobile phone can be used to carry on the organizational business.
11. The company expects its employees to use internet productively for official use during working hours.
12. Surfing of social media for personal entertainment during office hours is not allowed.
13. Employees must not access the websites which have been blocked by the company.
14. Applications such as related to weather, productivity etc are allowed but such use must not interfere with the normal working of employees in the organization.
15. Applications such as Google play store or iTunes are not allowed to be used.
16. Use of mobile phone while driving is strictly prohibited.
17. In case the company observes that the employee is using mobile phone more for personal usage, he/she may be asked to minimize usage and can also ask to contribute to the cost of monthly bill etc.
18. The mobile phone cannot be used any time to send /receive any illicit material, for harassing others, for storage of confidential information belonging to other company.
19. The cell phone must not be used while an employee is operating any instrument.
20. The Mobile phone can be used to keep the schedule and track of all official appointment.
21. It can also be used to carry out work-related research.
22. The Mobile phone may be used officially to keep track of work contacts.
23. In case the mobile phone is used inappropriately mostly, in such case device can be taken back from the employee on the ground of disciplinary issues.
24. A cell phone use is prohibited during meeting
25. Use of cell phone for harassing others may invite strong disciplinary action which may even lead to termination.
26. Use of mobile phone must be done in such a way that it does not interfere with the normal working of the business.
27. For the use of the internet and email on the phone, email and internet policy must be used.
28. The company does not hold any responsibility for the loss of mobile phone brought into the workplace.
29. The company prohibits the use of mobile phone in the area where using a mobile phone would be unsafe and would be distracting for the user or may create an unsafe working environment.
30. The company can issue mobile phone to the employees where job required to be in immediate access to customers or be in touch that otherwise are difficult to reach after office hours. In such circumstances, the mobile phone can be provided to employees.
31. All mobile phones as per Mobile phone policy provided by the company are the property of the company.
32. Employees who leave the company for any reason must return their mobile phone to the manager/HR.
33. The mobile phone when provided by the company has a right to publish the cell phone number in order to make employees more accessible for the need of business.
34. Maintenance of cell phone is employee responsibility.
35. While on international travel, it is managers/ admin. Responsibility to get the use of an international cell phone for the employee or employee can get the same from admin./hr after approval from immediate manager/ HR/HOD for the same.
36. For international roaming, the employee can be given an option to use the calling card or they are advised to purchase a local calling card.
37. It is the responsibility of the admin department that the employee uses the most effective cell phone calling plan.
38. According to companyissued cell phone agreementemployees accessing the company network with a wireless device, a password to be entered to access the device. In the event, the device becomes stolen or lost the company reserves all the right to delete company information from the device.
39. Employees are expected to manage the cost of mobile phones and other wireless devices.

**Question 2**

**How I would carry out industrial espionage without being noticed**

Industrial espionage can be defined as embracing illegal and unethical methods of collecting corporate data. It involves stealing intellectual property and trade secrets to use them for a competitive advantage.

Before I begin such a process, I have to ensure I have the trust of members of the organization. This would make it easy for me to relate to both younger and older staffs and help get classified information due to familiarity.

* **Client information.** I will be able to access Client information this involves data of your clients, including their financial information, can be used to steal business or can be leaked to damage the reputation of your company.
* **Trade secrets**  This generally involves protected information about existing products or products in development. This information will help me make my products more competitive or even bring a similar product to the market faster
* **Financial information.** Financial information about your company can be used to offer better deals to your clients and partners, win bids, and even make better offers to your valuable employees.
* **Marketing information.** This will allow your competitors to prepare a timely answer for your marketing campaigns, which, in turn, may render them ineffective.

There are many ways industrial espionage are carried out but in this case this will be called **INSIDER THREAT**. This is a much safer bet and harder to detect as I will be a mole inside the company having priviledged access to classified information

People can also perform or aid in corporate espionage inadvertently. Various social engineering techniques can be used to gather secret information or extract credentials from employees.

Also there is the use of malware;

* A random USB stick left in a hallway for a curious employee to pick up and use or a carefully written email that prompts the recipient to click on a link are only two of a large number of ways through which malware can infect your system, giving your competitors full access to sensitive data.
* Using a keyboard Trojan / spyware, I would access the computers of the head of all the targeted departments to access their company email and password to enable me send out an official email to all staff asking them to fill a detailed survey and send progress reports for classified information which I had been able to gather during the social engineering phase. This email will be sent out with Remote Access Trojans (RAT) which will give me full control over all staff systems and revert all filled surveys and reports to my system. Once my job is done the email be set in such a way that it can automatically expire.

**Security measures to prevent the likelihood of other hackers performing this action in the future.**

**Identify Your Companies Trade Secrets**

The first step to protecting a company’s trade secrets is to identify exactly what those secrets are. This not only involves looking inward, but looking outward as well. Firms cannot deduce the true value of their trade secrets until they understand how these secrets stack up against the technology and best practices of their competitors. By properly evaluating their intellectual property, firms will be more able to establish priorities and allocate security resources to better protect their most vital secrets.

**Identify the Threats**

Before firms develop strategies to counter industrial espionage, they need to understand what organizations present the largest threat. For instance, a company’s competitors may pose the most obvious danger. However, it should be kept in mind that visitors, customers, business partners, hackers, activist groups, and even foreign national governments are all potential threats and should be considered when building a counterespionage plan.

**Ensure Physical Security**

The same measures that are effective against run-of-the-mill criminals are also effective at protecting businesses from industrial spies. As such, firms should ensure the physical security of their offices, equipment, and infrastructure. This means setting up surveillance systems, securing entry points, and hiring or contracting specialized personnel. It is particularly important that firms identify the most sensitive information and facilities and ensure that these are given extra layers of protection.

**Establish Policies for Controlling Information**

In many instances, the unwanted disclosure of secrets could have been easily avoided if firms had simply put more thought into controlling the flow of information. Firms should establish policies on what information employees can share inside and outside the workplace. They should also establish procedures for control, reproduction, and storage of sensitive data. Particular attention should be paid to what is disseminated over the Internet and social media sites. Additionally, firms should develop procedures for the proper disposal of paper documents, IT hardware, and other sensitive equipment.

**Train the Workforce**

While firms may enact policies on the proper storage, control, and dissemination of information, they also need to ensure that their employees are trained to follow these procedures. Firms should conduct periodic training and awareness campaigns to inform employees about the threat from industrial espionage and the importance of information security.  Employees should understand that the threat from espionage is internal as well as external. As such, they should instruct workers on the correct procedures for identifying and reporting suspicious activity.

**Compartmentalize Information**

Not all information needs to be accessible by every employee in a company. That is why information should be compartmentalized on a need to know basis. Even senior members of a particular corporation may not need to know every technical detail about business operations. As such, firms should put in place policies to segregate which employees have access to which information, with special attention given to those employees who have access to a company’s most vital trade secrets.

**Conduct Background Checks and Monitoring**

Firms should conduct a background checks on all employees with access to sensitive data. This may even include often-overlooked individuals such as janitors, caterers, and groundkeepers. Specifically, firms should attempt to identify any possible factors that could make a particular worker more prone to illegally disclosing information

**QUESTION 3**

3a. decrypt the following codes

3 HAMLETS – the third letter in the word HAMLET is ‘M’

1 ORACLE - the first letter of the word ORACLE is ‘O’

9 MESSENGERS – the ninth letter of the word MESSENGERS IS “R”

1 SHELL – the first letter of the word SHELL is “S”

4 RODENTS – the fourth letter of the word RODENTS is “E”

1 CALABASH – the first letter of the word CALABASH is “C”

3 PROPHECIES – the third letter of the word PROPHECIES is ‘O’

1 DESTINY - the first letter of the word DESTINY is “D”

6 COWERIES – the sixth letter of the word COWERIES is “E”

The above decryption will give “MORSE CODE”

3b. SING THAT RAP FALL is an anagram for ‘THINGS FALL APART’

**QUESTION 4**

The encrypted message reads TSJSFRHGTJQTNZS

1. using Ceaser substitution cipher

Regular alphabets: A B C D E **F** **G** **H** I **J** K L M **N** O P **Q** **R S** **T** U V W X Y **Z**

Applying shift key 5 : V W X Y Z **A** **B C** D **E** F G H **I** J K **L M** **N** **O** P Q R S T **U**

To decrypt the above text, comparing the letters of the alphabet to the new order after the shift key was applied, and this was what I got : **O N E N A M C B O E L O I U N**