**NAME : EKERUCHE CHINWE BRIDGET**

**MATRIC NO : 15/ENG02/020**

 **COURSE CODE : COE 510**

**COURSE TITLE: COMPUTER SECURITY TECHNIQUES**

# QUESTION 1

## SECURITY POLICIES :

### Technical Requirements

1. Devices must store all user-saved passwords in an encrypted password store.
2. Devices must be configured with a secure password that complies with ’s password policy. This password must not be the same as any other credentials used within the organization.
3. Only devices managed by IT will be allowed to connect directly to the internal corporate network.
4. These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

### User Requirements

1. Users must report all lost or stolen devices to IT immediately.
2. If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with ’s incident handling process.
3. Devices must not be “jailbroken” or “rooted”\* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
4. Users must not load pirated software or illegal content onto their devices.
5. Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact IT.
6. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
7. Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
8. Devices must be encrypted in line with ’s compliance standards.
9. Users may must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify IT immediately.

 11. The above requirements will be checked regularly and should a device be noncompliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.

# QUESTION 2

Industrial espionage is defined as an individual or private business entity sponsorship or coordination of intelligence activity conducted for the purpose of enhancing a competitor's advantage in the marketplace.

##  HOW TO CARRY OUT AN INDUSTRIAL ESPIONAGE WITHOUT BEING NOTICED

1. **Mole planting:** a double agent is embedded and gains the trust of **XYZ** company
2. **Eavesdropping:**  ranges from wiretapping phones to intercepting WIFI signals and emails.
3. **Hiring competitors’ employees:** hiring away critical employees from **XYZ** company.
4. **Bogus job interviews:** Fake interview of candidates solely for the purpose of collecting key information **XYZ** current employers.
5. **Research under false pretenses:** using research paper as ruse to gain key information from **XYZ** company.
6. **Corporate communication intercepts:** Intercepting telephone calls through public switch exchange.
7. **Using familial connections:** conversations with unsuspecting relatives working for **XYZ** company
8. **Trade fair conversations:** establishing a contact at trade fairs, particularly with experts having a high level of understanding of innovative technology.

### Computer Espionage

1. **Copy files**: Easily copy computer files with miniature USB drives and pass them on to other individuals, businesses or governments.
2. **Computer hacking**: attempts to illegally gain access to a computer file or network or to do so without proper authorization.
3. **Information requests**: Requests for sensitive information, particularly over the internet, to unsuspecting low or mid-level personnel.

##  SECURITY MEASURES ;

In order to prevent the likelihood of other hackers performing the action in the future , some security measures must be put in place . they are as follows;

****Conduct a risk assessment.****

Find potential targets. You need to know what trade secrets and other valuable data your company possesses and how much they’re worth. You can evaluate your trade secrets by comparing them with products already available on the market or with known assets of your competitors.

Once you identify your most valuable data, you can guess who may want it. Once you know possible threats and potential attack vectors, you can detect vulnerabilities in your own defenses. Risk assessment is key to a risk-based approach to security, which should be part of the security strategy of every organization. You should also work out an [incident response plan.](https://www.ekransystem.com/en/blog/incident-response-plan-tips) It will help you respond in case of a data breach and minimize its impact on your business.

**Establish an effective security policy**

You should ask yourself if  all your employees follow your security policy? All security rules should be formalized in a clearly written security policy. This policy should include rules prohibiting password sharing and employees bringing their own devices to work, among other things. Make sure all your employees are aware of it, starting with upper management.

**Maintain an efficient data access policy**

 Many companies provide access to critical data and infrastructure by default. While it may be more convenient, this policy is not secure.Your company should follow the [principle of least privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege) and prohibit access to all data unless necessary. Applying the so-called “need to know” principle means that you provide access only to employees who really need information. If unauthorized employees occasionally need to work with confidential information, they can do it under the supervision of authorized staff.By limiting the number of people with access to critical data, you strongly limit the risks of your competitors obtaining this data.

 **Secure your infrastructure**

 Establish a secure perimeter around your company network. Conventional corporate cybersecurity software, such as firewalls and antivirus software, is your **first line** of defense. Make sure to separate your valuable data from your corporate network and limit access to it. Protect your border routers and establish screen subnets. A secure perimeter with a layered approach is the best way to protect yourself from industrial and economic espionage through hacking and malware.

**Educate employees**

 The best way to prevent your employees from inadvertently helping the enemy is to educate them. Tell them about potential threats your company faces.

 Make employees aware of the role they play in the security of your organization.

Teach them about simple security practices to use in their daily workflow. This will help protect your staff from social engineering and will prevent simple security mistakes, such as [sticking with default passwords](https://www.ekransystem.com/en/solutions/privileged-user-monitoring).

**Conduct background checks**

 Before hiring someone, the HR department usually conducts a [background check](https://en.wikipedia.org/wiki/Background_check).

This minimizes risks of finding a mole in your organization.It can be helpful to repeat these checks once in a while – especially for employees with privileged access – to ensure that they don’t become spies. A sudden surge in standards of living, unexpected trips, or paying off debt are among potential causes for concern.

**Create a proper termination procedure**

 In many cases, company espionage is performed in the last couple weeks of work. Employees’ credentials are often still active after termination, so they can still access sensitive data for malicious purposes. Create and implement a proper termination procedure to protect your company from potential acts of industrial espionage by former employees.

**Monitor employee activity**

You’ll never know whether your employees are acting maliciously, intentionally, or inadvertently unless you monitor their online presence.It’s especially important to keep an eye on privileged users, such as system administrators and upper management. They can easily gather intelligence while performing their normal tasks and explain any abnormal behavior as a mistake.

# 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 TRAP FALL is an anagram for “ THINGS FALL APART”

QUESTION 4

Encrypted message TSJSFRHGTJQTNZS

1. Caesar substitution cipher (key 5)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

From the English alphabets above Caesar shift of 5 gives:

VWXYZABCDEFGHIJKLMNOPQRSTU

Decrypted Caesar cipher – ONENAMCBOELOIUN

1. Columnar transposition cipher (key 5)

**Using Key = abcde**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **a** | **b** | **c** | **d** | **e** |
| **1** | **2** | **3** | **4** | **5** |
| **o** | **n** | **c** | **e** | **i** |
| **n** | **a** | **b** | **l** | **u** |
| **e** | **m** | **o** | **o** | **n** |

Plain text – ONCE IN A BLUE MOON