**NAME: MACDONALD PEREZ**

**MATRIC NO: 15/ENG02/035**

**DEPT: COMPUTER ENGINEERING**

**SECURITY POLICY ON THE USE OF MOBILE DEVICES IN JOBTASKA**

**Introduction**

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and **Jobtaska** supports their use to achieve business goals. However, mobile devices also represent a signiﬁcant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization’s data and IT infrastructure. This can subsequently lead to data leakage and system infection.

Jobtaska has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications.

**Purpose**

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to use a private or **Jobtaska** provided mobile device. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

• Laptop/notebook/

• Tablet computers such as iPads

• Mobile/cellular phones

• Smartphones

• PDAs

• Any mobile device capable of storing District data and connecting to an unmanaged network.

The goal of this policy is to protect the integrity and confidential data that resides within Jobtaska technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to the District’s public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Jobtaska direct control to backup, store, and otherwise access District data of any type must adhere to Jobtaska-defined processes for doing so.

**APPLICABILITY**

This policy applies to all Jobtaska employees, including full and part-time staff, contractors and other agents who utilize either Jobtaska-owned or personally-owned mobile device to access, store, back up, relocate or access any District resources / info. Such access to the district resources / info is a privilege, not a right. Consequently, employment at Jobtaska does not automatically guarantee the initial and ongoing ability to use these devices to gain access to District networks and information.

**POLICY**

It is the responsibility of any employee of Jobtaska who uses a mobile device to access District resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct Jobtaska business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user’s account. Based on this, the following rules must be observed:

**Technical Requirements:**

1. Device must use the following operating system: Android 8.0 or later, IOS 10.0 or later.
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be conﬁgured with a secure password that complies with Jobtaska’s password policy. This password must not be the same as any other credentials used within the organization.
4. Only devices managed by IT will be allowed to connect directly to the internal corporate network.
5. 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 may only load corporate data that is essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to Jobtaska IT department immediately.
3. 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 Jobtaska’s incident handling process.
4. 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.
5. Users must not load pirated software or illegal content onto their devices.
6. 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 Jobtaska IT department.
7. 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.
8. 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.
9. Devices must be encrypted in line with Jobtaska’s compliance standards.
10. 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 Jobtaska 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.
12. The user is responsible for the backup of their own personal data and the company will accept no responsibility for the loss of ﬁles due to a non compliant device being wiped for security reasons.

**POLICY NON-COMPLIANCE**

Failure to comply with this Policy may, at the full discretion result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

2.

**MY ROLE AS AN INDUSTRIAL ESPIONAGE ON COMPANY B**

As a highly sophisticated Security Expert, I have been hired by Company A to perform a role of an industrial Espionage on company B. Due to the fact that Company A and Company B are rival companies in the cyber security world and Company B stocks have mysteriously surpassed Company A stocks within the last six months this implies that Company B has implemented a new modus operandi in their act of operation. That is why I have been sorted after to act as an Industrial Espionage to Company B. I will hereby discuss the role I played and how I carried out my attacks on Company B.

I started off by scouring information openly available on the internet about the company, what bloggers have said about the company both the good and the bad part, I searched for peoples reviews about the company especially on social media platforms like twitter, Facebook and Reddit where you get Firsthand review from. Then I went on platforms like LinkedIn to search for the companies employees, I try to connect with them on LinkedIn. With LinkedIn I get some of the company’s employee’s First name and last name, with the first name and last name I am able to search for the company’s employees on social media platform like Facebook, Instagram and Twitter. With their social media profile I can be able to get some personal information about some of the company’s employees like where they stay (Not necessary their home address), if they are married or not and if they are married to who, to learn about some of the company’s employees daily routine if they like for example if they like to visit the gym after work or if they are the type that parties every weekend, locations they eat during lunch breaks, music and movies they like, if they have siblings and if yes how many are they and some personal information about their siblings will be helpful etc. I put together all these information’s on the company employees and if its not enough I move into hacking their social media accounts and after obtaining all these information’s on the company’s employees I look for the most vulnerable employees. The sole purpose of gathering all this information is for carrying out the act of social engineering.

Social engineering refers to the design and application of deceitful techniques to deliberately to manipulate human targets. In a cyber security context, it is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information The basis of a social engineering attack is to avoid cyber security systems through deceit, exploiting the weakest link, the people involved. Throughout the interaction, victims are unaware of the destructive nature of their actions. The social engineer exploits innocent instincts, not criminal. Explicit methods such as threats or bribery do not fall within the scope of social engineering. A talented practitioner of this discipline understands and perceives social interaction patterns to manipulate the psychological aspects of the human mind. With this resolution, the attacker is capable of executing an efficient and cheap security compromise, without the need to invest in breaking technical security measures. Nevertheless, an educated social engineer on computer science may also complement technological means to the attack in order to accomplish the malicious intentions.

I set myself up too meet one of the company’s employees I find vulnerable at her favorite coffee shop while she’s observing lunch break, a female in her 30s and single. I get to introduce myself and with the sole purpose of getting her number and getting to take her out on a date later that week. The next day I subscribe to a gym where another of the company’s employee which I find vulnerable works out he’s a male in he’s 30s and works in the IT department, I introduce myself as a friend with the intentions of becoming gym partners.

I get to take her out on a date and start talking with her with the intentions of getting close to her and build rapport (This might take weeks or months) to get close to her. Few weeks after talking we get into a relationship and I become her confidant, in this process I use advanced social engineering to get information about the company and sometimes I get to visit her at work and take notes on how the building is structured and the data room. I get to develop a malware and install it on her computer in order to monitor the data and get information, within a few weeks I was able to get details on some of the investors and some companys information but not the modus operandi.

Malware is the collective name for a number of malicious software variants, including viruses, [ransomware](https://www.forcepoint.com/cyber-edu/ransomware) and spyware. Shorthand for malicious software, malware typically consists of code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.

Malware has actually been a threat to individuals and organizations since the early 1970s when the Creeper virus first appeared. Since then, the world has been under attack from hundreds of thousands of different malware variants, all with the intent of causing the most disruption and damage as possible. They are several types of malware which are ;

**Virus**

Possibly the most common type of malware, viruses attach their malicious code to clean code and wait for an unsuspecting user or an automated process to execute them. Like a biological virus, they can spread quickly and widely, causing damage to the core functionality of systems, corrupting files and locking users out of their computers. They are usually contained within an executable file.

**Worms**

Worms get their name from the way they infect systems. Starting from one infected machine, they weave their way through the network, connecting to consecutive machines in order to continue the spread of infection. This type of malware can infect entire networks of devices very quickly.

**Spyware**

Spyware, as its name suggests, is designed to spy on what a user is doing. Hiding in the background on a computer, this type of malware will collect information without the user knowing, such as credit card details, passwords and other sensitive information.

**Trojans**

Just like Greek soldiers hid in a giant horse to deliver their attack, this type of malware hides within or disguises itself as legitimate software. Acting discretely, it will breach security by creating backdoors that give other malware variants easy access.

**Ransomware**

Also known as scareware, ransomware comes with a heavy price. Able to lockdown networks and lock out users until a ransom is paid, ransomware has targeted some of the biggest organizations in the world today — with expensive results.

After several months of communicating with the male employees, after implementing social engineering I discovered he was discontented with his salary and lacked enthusiasm towards hes job, with this knowledge I made an anonymous bid to the employee without him knowing its me and the offer was too much for him too refuse forcing him to send in the companys modus operandi, hereby my work as an industrial espionage is completed.

**WAYS OF AVOIDING INDUSTRIAL ESPIONAGE**

* **Personnel Security:**

All employees with the potential access to the important files should be carefully investigated

for their background. It is good to have an electronic system access to the facilities, where

everyone who enters the office uses an electronic ID to open doors or copy the data. The

company should support the intercommunication of administrative and human resources

departments. All unusual activities should be analyzed and investigated as soon as possible.

* **Technical Security :**

The implementation of technical protection provides electronic systems security. These

countermeasures ensure the proper work of confidential standards of the company with integration into a computer network. All these technical methods are well known and work successfully within the electronic systems of many organizations.

* **Physical Security :**

The threat of physical stealing of the information is a serious issue. Hence, the access to the company’s facilities and archives must be strictly controlled and

regulated. It can be ensured by the limitation of access for third parties, such as clients or partners and the employees. The organization should avoid the free access to corporate facilities, especially the archives with the critical information. If the company is big, it is a good idea to require all the employees to wear the corporate badges with a status indication (employee, visitor, partner etc.). This will avoid the awkward moments and the mock competence by violators. Moreover, the policy of the company should encourage people to check the badges of the individuals who they are not familiar with. Not the last issue to name is control of the trash which comes out the office to avoid the outflow of the information through the garbage disposal system.

* **Operational Security**

Operational security is based on the business model of the company or the value chain

activities of the organization. The strict procedures of the transition and control of the

information must be supported by the clear understanding of the marketing processes, research

activities, product development, manufacturing, and distribution. The compromised

information must be secured with additional control

* **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.

* **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.

* **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.

* **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.

* **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.

**3a**

3 HAMLETS - M

1 ORACLE - O

9 MESSENGERS - R

1 SHELL - S

4 RODENTS - E

1 CALABASH - C

3 PROPHECIES - O

1 DESTINY - D

6 COWRIES - E

**ANSWER: MORSE CODE**

**3b**

SING THAT RAP FALL is an anagram that translates to THINGS FALL APART

**4**

Encrypted message TSJSFRHGTJQTNZS

1. **Ceasar 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