**PRECIOUS FESTUS**

**15/eng02/026**

1. **XYZ Mobile Security Policy**

Mobile devices, such as smartphones and tablet computers, are important tools for the

Organization and XYZ Company 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.

XYZ Company 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. **Scope**

1. All mobile devices, whether owned by or owned by employees, inclusive of smartphones and tablet computers, that have access to corporate networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include corporate IT-managed laptops.

2. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorized by security management must be conducted.

**Policy**

**Technical requirement**

1. Devices must use the following Operating Systems: Android 2.2 or later, iOS 4.x 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 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.

**User requirements**

1. Users must not load pirated software or illegal content onto their devices. 6

2. 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.

 3. 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.

 4. 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.

5. Devices must be encrypted in line with compliance standards.

6. 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.

7. 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.

8. 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

**2. Industrial Espionage Scenario**

The first step to be carried out is reconnaissance which involves data infrastructure analysis which involves the understanding of the company’s network and systems architecture. The goal of reconnaissance is to identify the weak point of the target, any information gathered about the target may be the crucial piece needed to reveal the critical weakness in the defense of the target. This reconnaissance is similar to that of the military. In this phase of the attack, time will be spent observing and probing the target’s computer systems and networks to find their weakness. Any weaknesses found may lead to the successful infiltration.

These are some of the critical information which must be obtained in this phase:

1. Network information:
	1. IP addresses
	2. Subnet masks
	3. Network Topology
	4. Domain names
2. Security Policies:
	1. Firewalls
	2. Password complexity requirements
	3. Password change frequency
	4. Expired/disable account retention
	5. Physical security
3. Human Information:
	1. Vulnerable individuals
	2. Dark secrets
	3. Frequent hangouts
	4. Computer knowledge.
4. Host Information:
	1. Hardware
	2. Architecture type
	3. Operating system family and version

**3a**)

3 HAMLETS = 3rd letter =M

1 ORACLE = 1st letter =O

9 MESSENGERS = 9th letter = R

1 SHELL = 1st letter = S

4 RODENTS = 4th letter = E

1 CALABASH = 1st letter = C

3 PROPHECIES = 3rd letter = O

1 DESTINY = 1st letter = D

6 COWRIES = 6th letter = E

**Answer**: MORSECODE

**3b**)

SING THAT RAP FALL = THINGS FALL APART

**4)** key = 5, TSJSFRHGTJQTNZS = 15 words

Column Transposition Cipher Therefore: 15/5 = 3 rows

Place along each column

A B C D E

t s h j n

s f g q z

j r t t s

After: tshjnsfgqzjrtts

Caesar substitution key = 5

t = 20th – 5 =15th letter = o

s = 19th – 5 = 14th letter = n

h = 8th – 5 = 3rd letter = c

j = 10th – 5 = 5th letter = e

n = 14th – 5 = 9th letter = i

s = 19th – 5 = 14th letter = n

f = 6th – 5 = 1st letter = a

g = 7th – 5 = 2nd letter = b

q = 17th – 5 = 12th letter = l

z = 26th – 5 = 21st letter = u

j = 10th – 5 = 5th letter = e

r = 18th – 5 = 13th letter = m

t = 20th – 5 =15th letter = o

t = 20th – 5 =15th letter = o

s = 19th – 5 = 14th letter = n

**Answer:** onceinabluemoon; once in a blue moon.