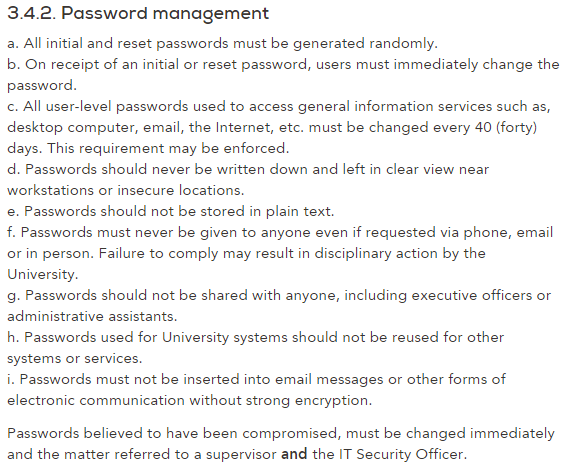
1 Policies Good Characteristics

1. Mystery Door #1

COVERAGE is being described.

Example: the Password management policy of the Australian catholic university:



1. Mystery Door #2

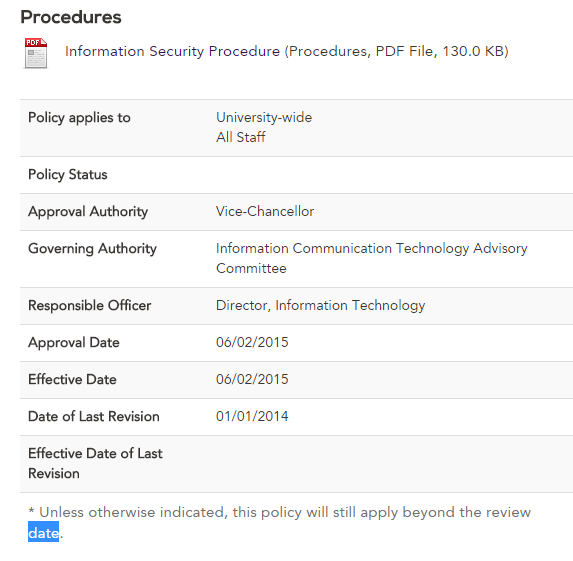
Clarity is being described.

Example: nearly every restaurant has a board writing ‘stuff only’ hanging on the door to their kitchen, that’s very clear to understand.

1. Mystery Door #3

Durability is being described.

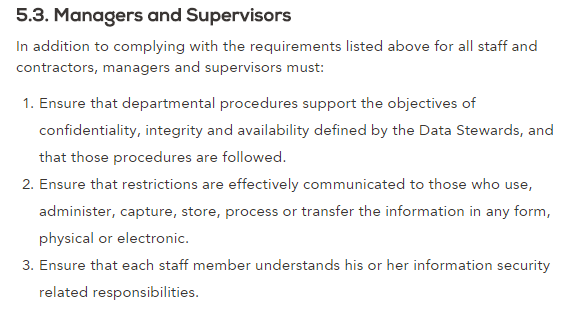
Example: the information security policy of the Australian catholic university:



1. Mystery Door #4

Realism is being described.

Example: the roles of Managers and Supervisors of the Australian catholic university:



2 Assessing Risk

1. Restricted Door

Impact: high(3), if someone maliciously entered the unlocked office room and nobody was present, he can do whatever he want, and that may include stealing devices, documents, or damaging them, etc. That’s a lot of damage for economical loss.

Probability: high(7), as although there won’t be many people trying to open a locked door, there will always be thieves or people happened to push the door(maybe for a rest). Once this happens, the attack will be happening.

overall exposure: 3\*7 = 21

1. Open Laptop

Impact: med(2), considering if you don’t store your important informations in your laptop, there won’t be many impact of information leakage. Although your data could still be deleted by malicious people.

Probability: very high(8). Every human beings have their curiosity to check unknown items, and that includes other’s personal computer. If this situation happens elsewhere, the probability may be 10. But this is in university campus, and educated students should show more respect for other’s personal stuff. But, we can’t trust on that, the probability for the attack is still very high.

Overall exposure: 2\*8 = 16

1. Trains Trains Trains

Impact: low(1), as although the free train wifi is public and not secured, you don’t need to connect to the internet for coding. And, if you don’t enter security informations like password on the internet, malicious people won’t get it.

Probability: low(3) .The train wifi owner itself is government, they won’t steal our data transmission, so we can trust them. Also, there won’t be many people proposed to trying to steal other people’s web information in a train, and that’s the train you have boarded.

Overall exposure: 1\*3 = 3

3. Ethics

Example:

<http://news.163.com/10/1014/08/6IULE52600014JB5.html>

‘Chinese news: people employed to write Trojans to hijack other people’s QQ (social chatting software), 5 million people was hacked.’

Are you ethically responsible for the code you write or the things you create when employed?

Answer: YES.

Where does the law stand on the same issue, is it dierent?

Answer: the employee is punished as well as the employer.

You can’t change other people’s open source software to profit for yourself.

You must follow different countries’ laws when designing software for them. for example:

– some countries (try to) forbid encryption/decryption,

– some countries forbid reverse engineering,

– some countries forbid format conversion