1 Policies Good Characteristics

a) Mystery Door #1

COVERAGE is being described.

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

3.4.2. Password management

a. All initial and reset passwords must be generated randomly.
b. On receipt of an initial or reset password, users must immediately change the password.
c. All user-level passwords used to access general information services such as, desktop computer, email, the Internet, etc. must be changed every 40 (forty) days. This requirement may be enforced.
d. Passwords should never be written down and left in clear view near workstations or insecure locations.
e. Passwords should not be stored in plain text.
f. Passwords must never be given to anyone even if requested via phone, email or in person. Failure to comply may result in disciplinary action by the University.
g. Passwords should not be shared with anyone, including executive officers or administrative assistants.
h. Passwords used for University systems should not be reused for other systems or services.
i. Passwords must not be inserted into email messages or other forms of electronic communication without strong encryption.

Passwords believed to have been compromised, must be changed immediately and the matter referred to a supervisor **and** the IT Security Officer.

b) 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.

c) Mystery Door #3

Durability is being described.

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

Procedures

Information Security Procedure (Procedures, PDF File, 130.0 KB)

Policy applies to	University-wide All Staff
Policy Status	
Approval Authority	Vice-Chancellor
Governing Authority	Information Communication Technology Advisory Committee
Responsible Officer	Director, Information Technology
Approval Date	06/02/2015
Effective Date	06/02/2015
Date of Last Revision	01/01/2014
Effective Date of Last Revision	

* Unless otherwise indicated, this policy will still apply beyond the review date.

d) Mystery Door #4

Realism is being described.

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

5.3. Managers and Supervisors

In addition to complying with the requirements listed above for all staff and contractors, managers and supervisors must:

1. Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the Data Stewards, and that those procedures are followed.
2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
3. Ensure that each staff member understands his or her information security related responsibilities.

2 Assessing Risk

a) 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

b) 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

c) 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