**VSC IT D S**

**A S P S C : 9/5/06**

**R :**

**R : 9/5/2013**

## I. D

Information is said to be secure if is protected against disclosure to unauthorized individuals, cannot be altered by unauthorized individuals and is available when required.

## S D

There are three aspects of information security that our definition is intended to cover:

**C a** : Information that is secure should not be readable by unauthorized individuals.

**I** : Information that is secure should not be modifiable by unauthorized individuals.

**A a a** : Information that is secure should be available to authorized individuals when it is needed.

## IV. O a a D S

To make the definition specified in the beginning of this document more precise, and to provide a way to objectively verify when information is being handled in a secure manner, we offer the following operational definition of "secure." Our operational definition is expressed in terms of attack models.

We define two different attack models: one for attacks against information as it is being transmitted and another for attacks against information as it is stored.

We adopt the standard Dolev-Yao (D

defeat the D-Y attacker on a single network connection (although n

- Find previously undocumented and unknown vulnerabilities in existing computer systems.
- Defeat any physical locks.

For example, a D-S attacker can enter any unlocked office and immediately read and later remember all documents left out on the desk. The attacker would also immediately know any hidden information in the room, such as passwords stuck under a keyboard or stored in unlocked desk drawers or filing cabinets. The attacker could sit down at the office computer and, perhaps using the hidden information obtained earlier, immediately operate all software on the machine with the skill level of an expert. The attacker could do all of these things instantaneously, even if the authorized user of the office stepped out for only a few moments.