University of Cyprus

Department of Computer Science

Information Security Framework

Security Policies

Security Procedures

Contents

Information Security Framework

The Information Security Framework contains general information on the high level notions of how the Department of Computer Science at the University of Cyprus sees Information Resources Security and how Information Security is organized. It is essentially the entry point for all Information Security related material for the Department of Computer Science.

The Department of Computer Science Security Framework consists of the:

- **Information Security Policies**
- **Information Security Procedures**

The Departmental Security Policy supplements the enterprise University Security Policy (whenever it will be available). The objective of the departmental policy and procedure documents is not to form a complete enterprise policy. Rather, they specify a more pragmatic and down-to-earth set of rules on how to create and maintain an educationally aware and secure information technology environment.

1.0 Purpose

Confidentiality, Integrity and Availability of Information Resources are the overarching principles with which the Department is concerned with in establishing a Security Policy.

The overall purpose of the Security Framework is to provide for:

Confidentiality, Integrity and Availability of Information Resources.

Quoting from a very famous source:

"The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. Therefore an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless." RFC 2196

2.0 Security Policies and Security Procedures

A Security Policy is not the same as a Security Procedure!

The Security Policy is a rather high level set of rules involving the subject of security. A Security Policy may also contain policies, which may seem irrelevant at first, like Backup Policies and E-Mail Policies in line with the overarching goals stated above: Confidentiality, Integrity and Availability.

The Security Policy is implemented through the use of the Security Procedures which constitute a set of technical documents describing the requirements and options in setting up a secure information technology environment.

3.0 Defence in Depth

The Department of Computer Science has adopted the high level notion of "Defence in Depth" in creating its Security Policy.

"..... in information security, defence in depth represents the use of multiple computer security techniques to help mitigate the risk of one component of the defence being compromised or circumvented. An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers within the same environment. Different security products from multiple vendors may be on different vectors within the network, helping prevent a shortfall in any one defence leading to a wider failure." http://en.wikipedia.org/wiki/Defence_in_depth

Security Policy

1.0 Objective

The objective of **Information Security Policy** (the Policy) is to ensure business continuity by preventing breaches of security.

2.0 Guiding Principles

Confidentiality, Integrity and Availability of Information Resources are the overarching principles with which the Department is concerned with in establishing a Security Policy.

3.0 Policy

The purpose of the Policy is to protect the Department's information assets from all threats, whether internal or external, deliberate or accidental.

It is the policy of the Department to use all reasonably practicable measures to ensure that:

- Information will be protected against unauthorized access.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Regulatory and legislative requirements will be met.
- Business Continuity plans will be produced, maintained and tested.
- University requirements for availability of information and information systems will be met.

4.0 Scope

The Department of Computer Science, University of Cyprus its faculty, staff, students and collaborators.

5.0 Relation to the Enterprise Security Policy

This Departmental security policy will follow and implement the general University of Cyprus Information Security Policy (which will be made available at some point). Whenever a conflict exists the general **University Enterprise Policy will prevail.**

6.0 Enforcement

Any employee or student found to have violated this policy may be subject to disciplinary action up to and including termination of employment or expulsion from the University in accordance to the disciplinary regulations adopted by the University.

The Department, also, reserves the right to take immediate action, in accordance to its adopted policies, to address any violations of this policy. Action may include any of

the following: suspension or termination of user's access, termination of assistantship and/or employment agreements and/or referral to the appropriate University disciplinary process.

7.0 List of Policy Documents

The Department has developed (or is in the process of developing) and adopted the following policies:

- General Information Security Policy
- Information Protection Policy
- Acceptable Use Policy
- Network Security Policy
- Perimeter Security
- Router and Switch Security Policy
- Remote Access and VPN Security Policy
- Wireless Access Policy
- DMZ Security Policy
- E-Mail Policy
- Baseline Host and Devices security
- Server Security Policy
- Teaching Lab Security
- Research Lab Security Policy
- Anti-virus, Anti-spam
- Backup Policy

Additional policies may be developed and made public if the need arises. Up to date information on the status of the Security Policies and Procedures can be obtained at http://its.cs.ucy.ac.cy/Policies.

8.0 Additional Material

The Security Policy is enforced through the adoption of Security Procedures. The Security Procedures are technical documents that contain details on the methods and techniques used in implementing the Security Policy. Procedures are divided into two classes: Standards and Guidelines.

- Standards are mandatory rules and actions.
- Guidelines are recommendations and best practice statements.

Appropriate Standards and Guideline documents exist (or are being developed) to cover and support the various aspects of the Policy.

Security Procedures

1.0 Objective

Security Procedures adopt, specify and list the technical and practical steps and configuration needed to be taken in very specific terms and in very particular cases to implement the Security Policy. The Security Procedures are part of the Security Framework. The objective of the security procedures is to exactly state what is required to implement the Security Policy.

Procedures are divided into two classes: Standards and Guidelines.

- Standards are mandatory rules and actions.
- Guidelines are recommendations and best practice statements.

Appropriate Standards and Guideline documents exist to cover and support the various aspects of the Policy.

2.0 List of Security Procedures

The Department of Computer Science has adopted (or is in the process of adopting) the following Security Procedures:

- Security Technical Guide
- General Security Procedures
- Linux Security Procedures
- Windows Security Procedures
- Data Backup Procedures
- Antivirus Procedures
- Research Labs Security Procedures

Additional procedures may be developed and made public if the need arises. Up to date information on the status of the Security Policy and Procedures can be obtained from http://its.cs.ucy.ac.cy under Policies.

Definitions

University --- University of Cyprus
Department --- Computer Science Department, University of Cyprus

References

- RFC 2196: Site Security Handbook (http://www.ietf.org/rfc/rfc2196.txt)
- ISO 27001 (http://www.27000.org/iso-27001.htm)
- National Security Agency - Systems and Network Attack Center. http://www.nsa.gov/snac
- The 60 minute Network Security Guide (http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/support/I33-011R-2006.pdf)
- The security policies and procedures were largely adapted from the model security documents from the SANS Institute (http://www.sans.org)

Revision History

Revisions are posted on the Information Technology Support web site of the department at http://its.cs.ucy.ac.cy/ under Policies.

Revision 1.0 - Preliminary Release: 23 February 2009
Revision 1.0a - Minor corrections and additions to revision 1.0: 12 March 2009