EUROPEAN COMMISSION
DIRECTORATE-GENERAL
INFORMATICS

Director General

DIGIT

Directorate-General for Informatics

INFORMATION SECURITY POLICIES

INFORMATION SECURITY POLICY STRUCTURE

Step:	30.10 Publication
Version:	1.1 - 05/09/2008
Reference Number:	POL_STRUCT
Owner:	Francisco García Morán - Director General
Author:	Philippe Schultz - DIGIT LISO
Revised by:	DIGIT Information Security Steering Committee
Approved by:	Francisco García Morán - Director General
Classification:	LIMITE

Commission européenne, L-2920 Luxembourg. Telephone: (352) 43 01-1.

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.

Table of Contents

DOCUMENT HISTORY

Step	Version	Date	Comments	Modified Sections
00.10	0.1	28/06/2007	Draft version by DIGIT LISO	
00.20	0.2	10/10/2007	Review document structure by DIGIT LISO	all
00.20	0.3	21/12/2007	Review document structure by DIGIT LISO	all
30.10	1.0	26/05/2008	Review following Information Security Steering Committee of 26/05/2008	all

1. INTRODUCTION

The Security Policies represent DIGIT philosophy and strategic thinking of the management in term of information systems security.

Their aim is to communicate a coherent security standard to any stakeholder including management, users, technical staff and external parties.

They provide the Directorate General with clear and concise governance to achieve information risk mitigation and they are the foundation for a comprehensive and effective security program.

To develop policies, DIGIT uses a top-down approach to be consistent with corporate-level policies and integrate legal requirements such as applicable Commission Decisions, Communications, Administrative Notices. This approach also ensures consistence within the organisation and compliance.

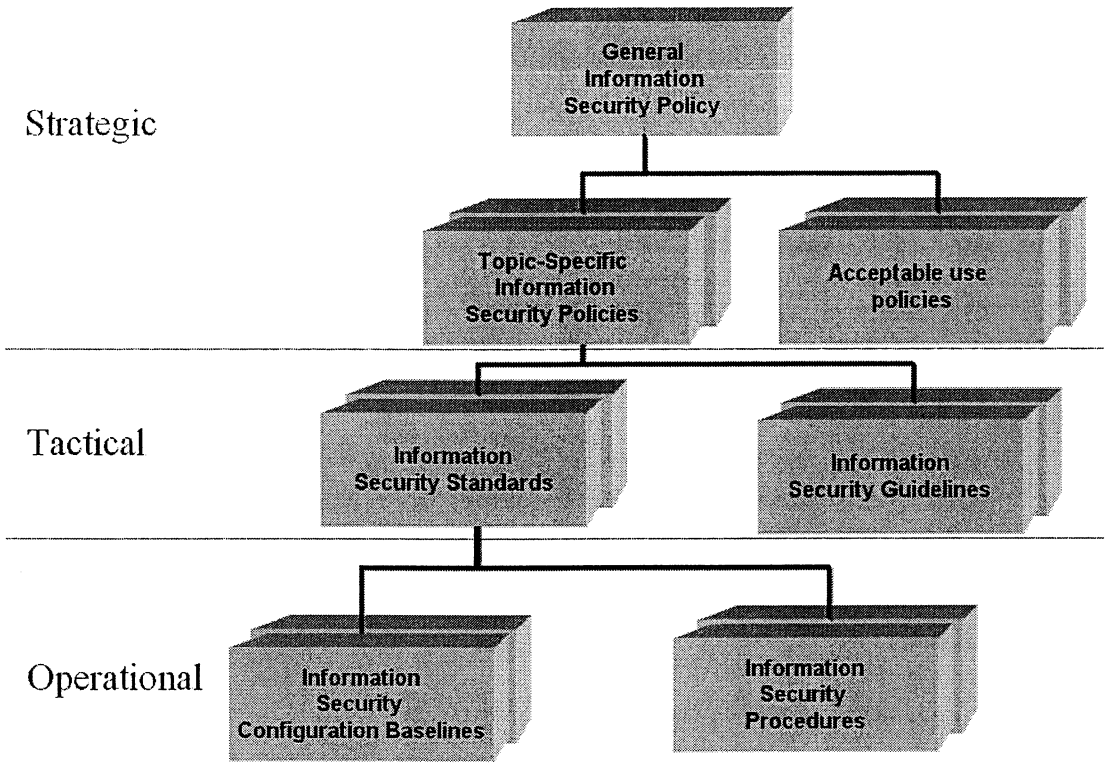
Every policy is developed by balancing the level of control with the level of productivity to avoid the cost of a control exceeding the expected benefit.

2. PURPOSE

This document presents how DIGIT has developed and structured its information systems security policies with the objective to ease its communication, understanding, and implementation.

3. POLICY STRUCTURE

The following structure has been adopted:



3.1. General Information Security Policy (GISP)

The GISP sets out DIGIT's intentions and principles regarding information security in broad and gives an overview of terms covering many subjects.

It establishes the strategic plan (ultimate end-point) for information systems security (INFOSEC)

It includes statements covering
- legal and regulatory obligations,
- role and responsibilities,
- strategic approach and principles.

In support to this GISP, several other policies are developed as following to provide the security framework as following.

The LISO has the lead on the development of the GISP

3.2. Topic-Specific Information Security Policies (TSISP)

As the GISP is broad level, TSISP are developed to address, in a more detailed form, specific areas of information security.

Theses polices are designed to define the security strategic framework for domains such as

- Access controls
- physical and environmental security
- Business Continuity Management
- Networks
- Security monitoring
- Information Security Incident management
- Asset Management
- Device lifecycle
- Information Systems development Security (Information Systems acquisition, development and maintenance)
- Human Resources Security
- Communications and Operations management
- Risk Assessment and treatment

3.3. Acceptable use policies (AUP)

In addition to TSISPs, acceptable use policies provide a behaviour framework for actors in regards with specific information systems or services such as the e-mail or the Internet.

AUPs cover the rules and regulations for appropriate use of the computing facilities.

3.4. Information Security Standards (ISS)

In support to general and topic specific policies, standards provide uniform way to implement higher level policies requirements into much more concrete details.

They include collections of system-specific or procedural-specific requirements that must be met such as

- the translation of security objectives into technological details (per technology)
- detailed requirements to be integrated into processes/procedures

Therefore, such standards provide tactical support (steps to achieve the strategic goal).

They are compulsory, enforcement is mandatory.

3.5. Information Security Guidelines (ISG)

Guidelines are discretionary recommendations in areas such as strong passwords selection.

Such guidelines include collections of system specific or procedural specific "suggestions" for best practice.

They also provide tactical support (steps to achieve the strategic goal).

3.6. Information Security Configuration Baselines (ISCB)

Baselines establish the implementation methods for security mechanisms and products.

They provide detailed information of policy implementation, for a unique technology or platform.

Such baselines provide operational support.

As standards, baselines are compulsory, enforcement is mandatory.

3.7. Information Security Operating Procedures (SecOps)

Procedures define step-by-step required actions to achieve a specific task such as

- Incident reporting
- Users and users rights management

Such procedures provide operational support.

As standards and baselines, procedures are compulsory, enforcement is mandatory.

4. POLICY DEVELOPMENT LIFECYCLE

To achieve continuous improvement, policies are developed using a quality management process (management system), described in detail terms in DIGIT Information Security Management System document.

DIGIT policies are developed based on tasks assigned by the senior management, with taking into consideration applicable decisions, communication or policies defined at corporate level by the entities having authority on these documents.

Moreover, each document is elaborated following the procedure described hereafter.

Step by step process is described in an ad-hoc Information Security Procedure (ISP) document.

4.1. Strategic and Tactical level policies development life-cycle

The LISO has the responsibility to develop, coordinate or oversee the development of DIGIT information security policies at strategic and tactical level.

This includes

- the General Information Security Policy (GISP)
- Topic-Specific Information Security Policies (TSISP)
- Acceptable use policies (AUP)
- Information Security Standards (ISS)
- Information Security Guidelines (ISG)

The following lifecycle is applicable

- LISO draft the policy document
- Policy is submitted to operational units for comments and review
- Policy is reviewed by the Security Steering Committee (SSC)
- Policy is approved by the Director General based on the advise from the SSC
- Document is published

4.2. Operational level policies development life-cycle

Sectoral teams have the responsibility to develop information security policies at operational level.

This includes

- Information Security Configuration Baselines (ISCB)

- Information Security Operating Procedures (SecOps)

The following lifecycle is applicable:

- The sectoral service draft the policy document
- Policy is reviewed by the LISO for compliance checking with high-level policies (TSISP and ISS documents)
- Policy is approved by the Information Security Steering Committee based on the advise from the LISO
- Document is published