

# IFIP TC-11

The International Federation for Information Processing (IFIP) is a multinational federation of professional and technical organizations (or national groupings of such organizations) concerned with information processing. IFIP consists of approximately 50 member organizations, representing some 60 countries. Eleven societies, associations, federations or councils are affiliate members to IFIP.

IFIP was founded under the auspices of UNESCO. Its official relationship with that organization is classified as category B, that is able to advise in a particular field. IFIP established official relations with the World Health Organization in February 1972 and maintains informal relationships with other members of the UN family. IFIP has the status of a Scientific Affiliate of the International Council of Scientific Unions (ICSU).

In 1970, IFIP together with four sister federations, IFAC, IFORS, IMACS and IMEKO, established a Five International Associations Co-ordinating Committee (FIACC) which provides a basis for the cordial and successful co-ordination of a variety of activities of mutual interest. IFIP also participates in an advisory capacity in the work of CCITT, the International Telegraph and Telephone Consultative Committee.

IFIP Technical Committee 11 on Security and Protection in Information Systems was created in 1983 under the chairmanship of the late Kristian Beckman of Sweden. Representatives from 28 countries that are members of this committee meet at least once a year at the IFIP SEC conferences that are held in different member countries.

## **IFIP TC-11 Aim and Scope**

The aim of TC-11 is to increase the reliability and general confidence in information processing as well as to act as a forum for security managers and others professionally active in the field of information processing security.

The scope of TC-11's activities will include:

- the establishment of a common frame of reference for security in organizations, professions and the public domain;
- the exchange of practical experience in security work;

- the dissemination of information on and the evaluation of current and future protective techniques;
- the promotion of security and protection as essential elements of information processing systems.

In order to accomplish its objectives, TC-11 has established a number of working groups (WG's) to address specific areas of security interest. Special task forces (TF's) are installed when a topical subject requires a reaction or standpoint from TC-11.

### **IFIP TC-11 general information**

Chairman: prof.dr. Sebastiaan von Solms, Rand Afrikaans University,  
Johannesburg, South-Africa  
Vice-chairman: prof.dr. Reinhard Posch, Technical University Graz, Austria  
Secretary: mr. John Beatson, Wellington, New Zealand

The official journal of TC-11 is **Computers & Security**, published by Elsevier Advanced Technology. ISSN 0167-4048

### **More information**

All current information about IFIP can be found on or via IFIP's homepage:  
<http://www.ifip.or.at>

All current information about TC-11 can be found on or via TC-11's homepage:  
<http://www.ifip.tu-graz.ac.at/TC11>

The IFIP secretariat can be reached at:

Hofstrasse 3  
A-2361 Laxenburg  
Austria, Europe

Telephone: +43 2236 73616  
Telefax: +43 2236 73619  
E-mail: [ifip@ifip.or.at](mailto:ifip@ifip.or.at)

# IFIP TC-11 working groups

## WG 11.1 INFORMATION SECURITY MANAGEMENT

Chair: prof.dr. Rossouw von Solms, Port Elizabeth Technikon, South-Africa

### **Aim**

As management, at any level, may be increasingly held answerable for the reliable and secure operation of the information systems and services in their respective organizations in the same manner as they are for financial aspects of the enterprise, the Working Group will promote all aspects related to the management of information security.

These aspects cover the wide range, from the pure managerial aspects concerning information security, like upper management awareness and responsibility for establishing and maintaining the necessary policy documents, to more technical aspects like risk analysis, disaster recovery and other technical tools to support the information security management process.

### **Scope**

The scope of the working group shall be to:

- study and promote methods to make senior business management aware of the value of information as a corporate asset, to realise the risks involved with this corporate asset, and to get their commitment to implementing and maintaining the necessary objectives and policies to protect these assets;
- study and promote methods and ways to measure and assess the security level in a company and to convey these measures and assessments to management in an understandable way;
- research and develop new ways to identify the information security threats and vulnerabilities which every organization must face;
- research and identify the effect of new and changed facilities and functions in new hardware and software on the management of information security;
- study and develop means and ways to help information security managers to assess their effectiveness and degree of control;
- address the problem of standards for information security.

**WG 11.2          SMALL SYSTEMS SECURITY**

Chair: prof.dr. Jan Eloff, Rand Afrikaans University, Johannesburg, South Africa

**Aim**

To investigate methods and issues in the area of information security, particularly related to small systems; and to advance knowledge and awareness of the subject through publications, conferences and other means. The aim is to address small systems security from both a functional and technical perspective.

**Scope**

The scope of the working group shall be to:

- promote the design of the new information security techniques and methods in systems where the functionality and responsibility for secure systems are distributed to the end user;
- investigate and report on the information security aspects of information technology products and information services for end users and consumers;
- address the information security aspects in systems which could technically be described within the range from bits-like systems such as intelligent tokens up to desktop type workstations;
- design guidelines and promote methodologies for the implementation of information security in small organizations;
- investigate intelligent token and smart card applications in information security with the aim of making the user less dependent on a shared environment.

**WG 11.3          DATABASE SECURITY**

Chair: prof.dr. John Dobson, University of Newcastle, Newcastle upon Tyne, UK

**Aim and Scope**

The aim and scope of the working group shall be:

- to advance technologies that support:
  - the statement of security requirements for database systems;
  - the design, implementation, and operation of database systems that include security functions;
  - the assurance that implemented database systems meet their security requirements;
- to promote wider understanding of the risks to society of operating database systems that lack adequate measures for security or privacy;
- to encourage the application of existing technology for enhancing the security of database systems;

## **WG 11.4 NETWORK SECURITY**

Chair: prof. dr. Sokratis Katsikas, University of the Aegean, Samos, Greece

### **Aim**

to study and promote internationally accepted processes which will enable management and technicians to fully understand their responsibility in respect of the reliable and secure operation of the information networks which support their organizations, their customers or the general public;

to study and promote education and training in the application of security principles, methods, and technologies to networking.

### **Scope**

to promote the awareness and understanding of the network aspect of information systems security;

to provide a forum for the discussion, understanding and illumination of network security matters;

to study and identify the managerial, procedural and technical aspects of network security; and hence to define the network security issues;

to study and describe the risks that arise from embedding an information system in a network environment;

to advance technologies and practices that support network security controls, make possible the statement of requirements for network security, and in general, advance the foundation for effective network security;

to contribute, as feasible and appropriate, to international standards for network security.

## **WG 11.5 SYSTEMS INTEGRITY AND CONTROL**

Chair: Leon Strous, De Nederlandsche Bank, Amsterdam, The Netherlands

### **Aim**

To promote awareness of the need to ensure proper standards of integrity and control in information systems in order to ensure that data, software and, ultimately, the business processes are complete, adequate and valid for intended functionality and expectations of the owner (i.e. the user organisation).

### **Scope**

- study and promote the research and use of standard mechanisms / measures to ensure that data integrity requirements in information systems and their use in business are satisfied;
- study and promote the use of standard evaluation criteria to define the integrity and control requirements;

- study and promote the use of advanced tools and techniques as a means to identify integrity and control weaknesses;
- study and promote the use of advanced tools and techniques to support the work of internal and external auditors;
- promote the mutual understanding of the edp-audit, security and development functions between personnel engaged in those functions and to the wider business community.

## **WG 11.8            INFORMATION SECURITY EDUCATION**

Chair: prof.dr. Louise Yngström, University of Stockholm, Sweden

### **Aim**

To promote information security education and training at the university level and in government and industry.

### **Scope**

The scope of the working group shall be to:

- establish an international resource center for the exchange of information about education and training in information security;
- develop model courses in information security at the university level;
- encourage colleges and universities to include a suitable model course in information security at the graduate and/or undergraduate level in the disciplines of computer science, information systems and public service;
- develop information security modules that can be integrated into a business educational training programme and/or introductory computer courses at the college or university level;
- promote an appropriate module about information security to colleges and universities, industry and government;
- collect, exchange and disseminate information relating to information security courses conducted by private organizations for industry;
- collect and periodically disseminate an annotated bibliography of information security books, feature articles, reports, and other educational media.