E

WIPO

SCIT/7/12
ORIGINAL: English
DATE: April 26, 2002

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

STANDING COMMITTEE ON INFORMATION TECHNOLOGIES

PLENARY
Seventh Session
Geneva, June 10 to 14, 2002

OVERVIEW OF WIPO'S INFORMATION SECURITY POLICIES

Document prepared by the Secretariat

INTRODUCTION

1. The widespread implementation and use of information and communication technologies, including networks and distributed processing environments, are accompanied by new issues. Networks provide greater flexibility for accessing and sharing information and resources and for enabling processing at the desktop. However, these advantages lead to increased exposure of sensitive information and, therefore, it is necessary to implement strategies in order to ensure the confidentiality, integrity and availability of information and information systems.

2. This document contains an overview of WIPO's information security policies and the strategies to implement them.

SCOPE

3. The WIPO information security policies apply to all WIPO employees, staff members, internal consultants, temporary staff and external contractors working for WIPO. WIPO employees shall ensure that contracts with other individuals and enterprises who, by nature of their relationship to WIPO, are entrusted with sensitive information, are made subject to the security policies unless otherwise authorized. The policies address all aspects of information security, including the initial design of an information system through to its implementation and operation. They also address any device used to store, process or communicate WIPO information. The policies are applicable independently of the way information is represented (written, spoken, printed, electronic and other forms), of the technology used to handle it and its location (e.g., in the office, at a remote location, on an airplane).

SECURITY MANAGEMENT

4. Security management seeks to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to data, and unauthorized disclosure of the information. Security management is achieved through making effective policies, strict implementation of standards and procedures to ensure the confidentiality, integrity and the availability of WIPO information, software applications, systems and networks to authorized users.

Confidentiality

5. Confidentiality relates to the protection of the information from unauthorized access regardless of where it resides or how it is stored. Information that is sensitive needs to be protected to a higher level than other information. The WIPO information security policies provide a framework for classifying data with indications of the associated security requirements.

Integrity

6. Integrity is the protection of information, software applications, systems and networks from unintentional, unauthorized, or accidental changes. It is also important to protect the processes or programs used to manipulate data. Information should be presented to information owners and users in a secure, accurate, complete and timely manner. Key to achieving integrity is the identification and authentication of all users accessing information through the use of manual and automated monitoring.

Availability

7. Availability is the assurance that WIPO information and resources are accessible by users as authorized. There are two issues relative to availability: denial of services caused by a lack of security controls (e.g., destruction of data or equipment, computer virus), and loss of services from information resources due to natural disasters (e.g., storms, floods, fires). Denial of service is addressed as part of security management. Loss of services is addressed as part of the business continuity planning process.

ROLES AND RESPONSIBILITIES

8. Responsibility for information security on a day-to-day basis is every employee's duty. Staff members must remain aware of the need for the protection of WIPO's information assets. To coordinate the information security activities in WIPO, three categories of roles have been defined, at least one of which applies to each worker. These categories define the general responsibilities within WIPO for information security:

(1) *Owner* – WIPO is the overall owner of all information, computer applications and systems within the context of the information security policies. Within that framework, owners are those individuals charged with the ownership of the information or information systems utilized by their respective functional Unit. Owners include senior management, program managers, project managers or their representatives who bear responsibility for acquisition, development and maintenance of systems that process WIPO information. Owners are responsible for determining access rights and security criteria for information under their control.

(2) *Custodian*s - Custodians have physical or logical possession of WIPO information, or information that has been entrusted to WIPO. IT staff members, and/or system administrators, can be looked upon as custodians. In the case of information stored on a personal computer, the individual PC user would be the custodian. Custodians assume the responsibilities of owners in the absence of specific ownership.

(3) *User* - The Users are individuals who process information in their day-to-day work that is owned or under the custody of others. Users are responsible for observing the security policies, standards and rules established by the owners. In the event of questions of access to information, the Users must defer to the Owners or Custodians of the information. Users may be employees, temporary staff, contractors, consultants or third parties with whom special arrangements have been made.

9. Due to the sensitive and important nature of information security policies, and for the purpose of effective implementation thereof, the Information Technology Projects Division, is currently structured as follows:

Chief Information Officer (CIO)

10. The CIO's role in information security is to communicate to senior management the business risks of implementing new and distributed technology and the necessity for developing the appropriate information security policies, procedures and infrastructure.

Information Security Officer

11. The Information Security Officer of WIPO has overall responsibility for information security matters. These responsibilities are to:

- ensure that appropriate user access and authentication controls are in place;
- ensure that the documented security policies, standards and procedures are reviewed, updated and maintained;
- evaluate security exposures, misuse, or non-compliance situations and ensure implementation of security controls to address them;
- develop and implement a Security Awareness Program.

Helpdesk

12. The Helpdesk is responsible for providing initial responses to security-related questions in accordance with policies, standards and procedures and, where appropriate, the redirection of security-related issues to the appropriate division management in accordance with WIPO's information security incident escalation procedure. The Helpdesk is a central user registration authority and, together with the security administrators, provides password management.

Divisional Management

13. Divisional Management in this document refers to all WIPO program or division managers who are responsible for the physical or practical implementation of security policies of WIPO in their own functional business areas. Divisional management is responsible for establishing the overall security strategy for their division's information. This includes determining the security classification of the information owned by the division, including the level of sensitivity and availability required for the information. The divisional management is also responsible for authorizing the level of access to information under their responsibility.

IMPLEMENTATION

Information Resources

14. The information systems infrastructure shall be protected in a manner to ensure that unauthorized persons are not able to access the system, nor cause physical damage nor modify internal components that could affect the results of information processing. Environmental and security controls shall be appropriate for the level of risk. An assessment that balances risk with the cost of implementing the control should be completed when determining what security and environment controls are appropriate.

15. Information assets are classified in order to provide a means of communicating the level of protection to be provided. Information security requirements vary with the sensitivity and level of importance of the information or the systems associated with that information.

16. Users are responsible for adhering to copyright, patent laws and license agreements for intellectual property, the contents of which they know or ought to know. Owners shall ensure that custodians and users are made aware of the relevant provisions of license agreements.

17. Periodically, the data owner, custodian and the Information Security Officer shall review the current set of access rights and update capabilities granted to each individual in the system in order to ensure that the appropriate level of access has been granted and that no changes are necessary.

Access to Systems and Information

18. Access to information and systems is provided based on business requirements. Owners, as part of their management responsibility, are required to review all requests for access to information or systems, and to verify that such access meets a legitimate business need. Approval for access needs must be communicated to the custodian.

19. All requests for information between divisions must meet the same business requirements criteria. When making the decision to either grant or deny access, the owner should consider the benefits to WIPO of granting access, the type of access required and any risks associated with such access.

20. When approval for external access to confidential or secret WIPO information is granted, detailed instructions must be provided to the recipient, notifying them of any security requirements including the need to maintain the confidentiality of the information, any limitation in respect of distribution of the information within their organization and the procedures for the destruction or return of the information following the period of access.

21. When a division manager is notified of an employee termination/resignation or transfer, he/she should review the disposition of the user's data and the files residing on the network and application directories with the user prior to the transfer or separation from WIPO. The manager shall notify the Helpdesk in writing of those files to be transferred or destroyed. Disposition of any data shall follow the guidelines defined by the Documentation Retention Policy or, pending implementation of the Documentation Retention Policy, the Program Manager and WIPO's Information Security Policies Manual (ISPM).

Security Monitoring

22. It is the responsibility of network, system and application administrators to implement appropriate measures to detect attempts to compromise the confidentiality or integrity of information or information systems. When implementing monitoring capabilities, consideration should be given as to, what situations are to be monitored based on the extent of risk, the most effective means for monitoring security activities, the resources available for monitoring and the system constraints that limit the ability to monitor security-related events. As part of these measures, virus detection software within the local area network environment, as well as on systems that are at high risk of infection, should be kept up-to-date.

Information Security Awareness Program

23. It is the responsibility of management to ensure that all users of information understand how to protect WIPO's information assets (including information and information resources) and how to comply with the security policies, standards and procedures.

24. The Information Security Officer with assistance from the HRMD is responsible for developing and implementing an information security awareness program that promotes employee awareness.

CONTROLS

Risk Assessment

25. Risk assessment involves identifying the sensitivity and criticality of information and the consequences to WIPO if information is disclosed, modified or destroyed. Risk assessment techniques can include formal methods of determining the financial and operational impact of a security incident, as well as less formal assessment techniques. A risk assessment process should include the following elements:

- the determination of an inventory of information assets that need to be protected;
- evaluation of the sensitivity of the information and the consequences if information is disclosed;
- evaluation of the criticality of information and the consequences to business processes if information and information processing systems are not available;
- a confirmation by management of the extent of risk that will be accepted, mitigated, or transferred;
- development of a risk control strategy;
- determination of compliance with WIPO information classifications.

26. It is the responsibility of management to understand the level of risk to WIPO relating to confidentiality, integrity and availability of information and to the controls necessary to effectively mitigate this risk. Risk control measures should address the information, the processes that are used to create, modify, report or distribute it, and the environments under which these processes exist. This process should also incorporate the classification of information, in accordance with WIPO information security standards, into one of the following categories:

- Secret
- Confidential
- Internal Use Only
- Public

27. The WIPO ISPM provides a framework for classifying the confidentiality, integrity and availability rankings for information and the necessary security requirements for each classification.

Functional Security Policies

28. The WIPO ISPM contains the functional information security policies. It defines the framework for WIPO's information security strategy, architecture and implementation, focusing on the technology for storage, processing and transmission of information as well as on the administrative and operational practices for its protection in all forms, both inside and outside WIPO. It is established and maintained by the Information Security Officer and approved by the Director General.

Information Security Standards

29. The WIPO Information Security Standards Manual (ISSM) document establishes the methods for achieving the security objectives of the WIPO ISPM. Based on those standards, platform and application specific security baselines shall be developed. The ISSM is established and maintained by the Information Security Officer and approved by the CIO.

Information Security Procedures

30. For the implementation of WIPO's information security policies and standards, various security procedures shall be developed. They will define the step-by- step actions to be followed for performing a specific information security activity.

Divisional Procedures and Guidelines

31. Each division should develop and maintain additional divisional procedures and guidelines that support the overall information security policies, if necessary to meet specific needs.

32. The SCIT Plenary is invited to note the information contained in this document.

[End of document]