Cour
Pénale
Internationale

International
Criminal
Court

Presidential Directive
ICC/PRESD/G/2005/001

Date: 8 March 2005

The President, in consultation with the Prosecutor, for the purpose of setting out the Information Security Policy of the Court and pursuant to Section 2 of Presidential Directive ICC/PRESD/G/2003/001 promulgates the following:

Information Security Policy

Section 1

Glossary of terms

1.1. Information – all types of information, regardless of its medium, that is produced, transmitted, and stored for and by the Court.

1.2. Information System - the entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

1.3. Confidentiality - Assurance that information is shared only among authorized persons or organizations.

1.4. Integrity - Assurance that the information is authentic and complete.

1.5. Availability - Assurance that the systems responsible for delivering, storing and processing information are accessible for authorized persons when needed.

Section 2

Objective and scope

2.1. This policy addresses the protection of the confidentiality, integrity and availability of its information against threats including error, fraud, sabotage, terrorism, extortion, espionage, privacy violation, service interruption, theft and natural disaster, whether internal or external, deliberate or accidental.

2.2. The Court requires that information important to its functions is adequately safeguarded to protect the public and the Court's interests.

2.3. The President, Prosecutor and Registrar shall ensure the proper design, implementation and management of effective information security arrangements. Users of information must comply with the security provisions and restrictions placed on them by the Court.

2.4. This policy is binding for the Court and all those who seek access to its information.

Section 3

Protecting Information

3.1. Providing an appropriate level of information security requires a systematic and coordinated approach where the level of protection corresponds to the assessed level of risk. The protective measures to be taken to mitigate the perceived risks can be of a procedural, technical and physical nature.

3.2. The selection of appropriate protective measures shall be based on a sound factual, financial, lawful and ethical basis. Most importantly, they must be based on an assessment of risk.

3.3. Planning for the management of security risks shall be part of the Court's organizational culture and shall be integrated into the Court's practices, projects and plans. Risk management and good security practices shall be regarded as a fundamental part of the Court's management.

3.4. Information shall be classified, based on a formal classification system, to indicate the need, the priority and desired level of protection. Classification ensures that information is protected according to the degree of harm that could result from its unauthorized disclosure.

3.5. The Court shall translate the information security policy into administrative issuances that explicate the Court's regulation of various aspects of information security including information classification, information handling, encryption, mobile computing.

3.6. The Court shall have a process for developing and maintaining business continuity throughout the Court that ensures a managed recovery of information, and the underlying Information Systems, from a major disaster or system failure.

3.7. The Court shall actively promote amongst staff and officials awareness and knowledge of information security and the issued policies, procedures, standards and guidelines on information security.

3.8. Staff and officials shall immediately report any suspected security incidents, suspected viruses, software malfunctions, faults, weaknesses or threats observed or suspected to the information and Information Systems of the Court.

3.9. The Court shall implement a formalized information security process. The Court will accept the international recognized information security standard ISO 17799 as its guiding model.

3.10. The Information Security Officer (ISO) has been delegated responsibility for the Court's information security process and shall coordinate and monitor the information security efforts in the Court. In addition, the ISO shall provide to the ICC and its organs advice on risks, opportunities and measures with regard to information security.

Section 4

Enforcement

4.1. In order to realize the objectives of this Presidential Directive, the Court will continuously monitor its Information Systems and register all usage and transfers of information, irrespective of the method or form of such transfer.

4.2. Whenever there is a reasonable suspicion that there may have been a violation of any information security policies, procedures, standards or guidelines, the Court shall immediately investigate the matter and take such actions as are required to protect the confidentiality, integrity and availability of the information and restore the proper functioning of the Information Systems.

4.3. The manner in which any such investigation is to be conducted will be set out in an administrative instruction.

Section 5

Final Provisions

5.1. This policy will be reviewed annually or before in case of events or developments that may affect the policy.

5.2. This policy shall enter in to force on 14 March 2005.

Signed by Philippe Kirsch

President