Cour
Pénale
Internationale

International
Criminal
Court

Administrative Instruction
ICC/AI/2007/001

Date: 19/06/2007

ICC INFORMATION PROTECTION POLICY

The Registrar, for the purposes of establishing a classification and handling system for the protection of internally generated information and unclassified information provided to the Court, pursuant to Presidential Directive ICC/PD/2005/001, promulgates the following:

Explanatory note to the Administrative Instruction

The Court gathers, stores, processes and disseminates information. Much of this information is sensitive in the sense that unauthorised disclosure or modification might compromise the Court, its reputation, cases, witnesses, staff, officials or other interlocutors. Such information must be protected in a consistent manner.

Currently, there is uncertainty on how to protect information; Existing ad-hoc practices differ among units, sections, divisions and organs for the same information. This A.I. indicates which information must be protected and how this is to be achieved. As with any A.I., the Instruction governs staff but not Elected Officials, including the natural tension for staff directly serving Elected Officials.

The A.I. intentionally makes no difference between 'judicial' and 'administrative' documents. Court documents can be both or neither; it is the value (and associated risk) of information that is critical in determining protective measures, as compromise may impact on the judicial, investigative, legal, reputational, financial, operational or regulatory credibility of the Court. The Official Journal of the Court demands levels of confidentiality for Court records, yet many Court produced documents are not official Court records as they are not filed as such. Nevertheless, these documents also require protection.

Thus, the A.I. defines four generic protection levels are defined by the A.I.. These are applied to information regardless of its origin or format. The applied protective level is determined by the value of the information and the potential risk(s) to it A protection level defines a set of measures that seek to mitigate the likelihood (risk) that information may be compromised. The protection levels are synchronized with the judicial levels of confidentiality to ensure staff understand how to handle information once a judicial level of confidentiality has been applied by Chambers.

A protection level should not be confused with access to information. Access to information is based on a "need to know". Protection levels only determine how much protection will be afforded to help prevent unauthorised access.

Although many control measures are already in place, the A.I. does not formalize current practices. A low level of initial compliance is expected for some parts of the Court, as such requirements have not previously been imposed. A grace period is foreseen during which the Court will work towards full compliance. Staff will be supported by training, templates, tools and lists of pre-classified types of documents. The Intranet pages of the Information Security Unit contains already flowcharts and manuals that address the day-to-day questions of staff and translate the present A.I. into practical guidelines.

By its very nature this A.I. must be comprehensive and it is therefore demanding of the reader. In practice, only a small portion of the full A.I. is relevant to the vast majority of staff. Nevertheless, a consistent approach to security will benefit the entire Court and enable staff to quickly adapt to its requirements, helped by technological means that will increase the transparency of the security regime and its user friendliness.

Parts of the implementation and enforcement of the A.I. can be done through the use of automated tools. Examples of such tools are secure USB memory sticks that enable staff to carry information safely with them, log servers that centrally record user activities on the network, port blocker software that controls the copying of documents from the network and tools that stop sensitive documents from being exchanged over the internet in clear text. Such tools allow for maximal freedom for users while retaining the possibility to hold staff accountable for their actions.

Extensive consultations rounds have taken place in the drafting and tuning phase of the A.I. and lengthy consultations have even taken place with parties not foreseen in the administrative issuance process. The comments and of concerns have been processed in the A.I. in so far as deemed acceptable by the Information Security Officer within the objective of the A.I..

Please mind that this A.I. is not written in stone, it will be evaluated on a regular basis to ensure it is aligned with the needs and practicalities of the Court.

PART I – INTRODUCTION

Section 1

Definitions

1.1. Administrators – The staff members of the Court responsible for the maintenance and administration of an ICIR.

1.2. Caveat – A label that indicates the target recipients for Information. Caveats shall be translated and adapted to the possibilities and configuration of the Court's applications.

1.3. CEN II – Protection level of the (EN 1143-2:2001) International standard for the Requirements, classification and methods of tests for resistance to burglary of secure storage units (such as safes).

1.4. Classification – The assignment of a protection level to Information, as provided for in Part III of the present Administrative Instruction

1.5. Classification Retention Policy – A policy that specifies the default period that a classification will be retained until the retention period has passed or the circumstances that warranted the classification have changed.

1.6. Classified Information – Information assigned a protection level higher than UNCLASSIFIED.

1.7. Compromise – The loss, improper access or use, and unauthorized disclosure, alteration and destruction of information.

1.8. Confidentiality - Assurance that Information is shared only among authorized individuals or organizations authorised to access the Information.

1.9. Court Records - ICC Records filed with or by the Registry as part of a situation or case.

1.10. DIN 32757-1 - Industry standards for document shredding.

1.11. Documents - Recorded information regardless of physical form or characteristics. 'Documents' is used interchangeably with ICC Records for the purpose of readability.

1.12. Endorsement Codes – Markings that allow for supplementary directives on how Information shall be handled (such as 'Do not copy' and 'Not to be released after').

1.13. Head – Head of Organ, Division, Office, Section or his/her assigned delegate for a certain task.

1.14. ICC Records - Books, papers, photographs, machine readable materials, maps, or other documentary materials, regardless of physical form or characteristics, which are in the possession of the Court and have documentary or evidential value. Such materials, created, received or accumulated in connection with the transaction of official use, are preserved because of their informational value as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities. Portable computing devices (for example, laptops and PDAs) with resident memory are regarded as ICC Records within the context of this A.I.

1.15. ICIR - ICC Classified Information Register. This register is kept to administer the lifecycle (creation, receipt, classification, storage, retrieval, modifications, transfer, scanning, copying, destruction transmission, re- and declassification) of Documents marked as [ICC] SECRET.

1.16. ICT System – The assembly of equipment, software, methods and procedures, and if necessary, personnel, organized to process Information.

1.17. Information – ICC Records in any medium or form.

1.18. Information Custodian – The custodian of Information is the Head of the Organizational Unit responsible for providing operational support for information systems to Information Owners by administrating or maintaining the information system. Information Custodians implement the protection requested by the Information Owner.

1.19. Information Owner – The Information Owner is the Head of the Organizational Unit responsible for the information. Ownership does not imply property ownership within the context of Information Security. Where appropriate, ownership may be shared by Heads. Information Owners determine the usage, access rights and protection criteria for information for which they are responsible.

1.20. Information Security Officer - The Information Security Officer of the Registry's Security and Safety Section.

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

1.22. NDA - Non-Disclosure Agreement.

1.23. Organizational Unit – An Organ, Division, Office, Section, Team or Unit.

1.24. Originator – The person or organizational unit within the Court that created the Information or received Information from a Provider.

1.25. Provider – The person or entity, independent and external to / from the Court, which supplied Information to the Court.

1.26. Secure Printing – A printer feature that ensures that printing only takes place after Staff properly identified itself as being in close proximity to a printer.

1.27. Strong Password - A password consisting of at least 8 characters including 1 special[1] character and 1 numeric character.

1.28. Staff - For the purposes of this Administrative Instruction, the term "staff" shall include all Elected Officials, staff and individuals affiliated with or having a contractual relationship with the Court, such as independent contractors, gratis personnel, interns, consultants, volunteers, interpreters, and other contractual personnel who are entrusted with authorised access to ICC Information in the course of performing their official duties.

Note: Elected Officials are exempted from the regular disciplinary process but are subject to the administrative processes and requirements of the Court.

Section 2

General

2.1. This Administrative Instruction sets out the minimum standards for protecting the confidentiality of Information within the operations of The International Criminal Court ("the Court"), for classifying Information and the consequent appropriate handling of Classified Information.

2.2. The present Administrative Instruction shall apply to Information that the Court uses in the execution of its functions and applies to all current and former staff members of the Court.

2.3. This Administrative Instruction applies to Information that is generated internally by the Court or is provided to the Court not declared or protectively marked by the Provider as a State Secret.

2.4. This Administrative Instruction does not apply to Information that is provided to the Court declared as or protectively marked as a State Secret by the Provider. In such case, the Information shall be treated according to the A.I. on State Secrets ("Information Classification and the Handling of Classified Information Provided by States and International Organisations").

[1] The following characters are considered to be special characters: ~`!@#$%^&*()_-+={}[]\|:;?><,./

2.5. In cases where full compliance with this Administrative Instruction is not possible due to exceptional circumstances beyond Staff's control, Staff shall take all reasonable steps to comply with the spirit of the Administrative Instruction.

Note: The above provision provides flexibility to staff on missions and travel that is faced with the practicalities of their environment. It also caters for the situation where the Court did not yet provide necessary means. Please note that an appeal on this provision leads to an onus of proof.

2.6. The provision of Information to the Court shall be matched by credible reassurances for the Provider that proper measures are taken to prevent unauthorized disclosure of Information and that any Information, once provided to the Court, shall be appropriately protected.

2.7. Each Organizational Unit shall establish administrative procedures for the control of Information for which it is accountable, based on the provisions of this Administrative Instruction and an assessment of the Organ's processes and perceived risks. These administrative procedures shall be used to protect Information from unauthorized disclosure by controlling access to Information and ensuring compliance with the requirements on handling, marking, storage, transmission, and destruction as set out in this Administrative Instruction.

Note: The Organizational Unit are responsive for the protection of the Information they own within the context of the Court or which is (temporary) in their custody. The above provision provides flexibility to the Organizational Units by enabling them to translate the generic security provisions into measures that fit their processes. It is up to the Organizational Units to decide how to organize this, as this could be different per Organizational Unit.

PART II – PROTECTION LEVELS

Section 3

Protection levels

3.1. Information shall be afforded protection, based on the established protection level which corresponds to the level of sensitivity of the Information.

3.2. The following factors shall be considered in conjunction with each other in order to determine the level of sensitivity of Information:

(a) The degree of potential damage which disclosure could cause to the Court, the Provider or individuals;

(b) The degree of potential advantage disclosure could offer to the Court, the Provider or individuals.

3.3. Based on the principles set out in Subsection 3.2 above and the specific classification criteria set out in Section 5 below, Information shall be protected according to the following protection levels, in increasing order of strictness:

(a) "UNCLASSIFIED" - for Information of which public dissemination would not damage the Court, that is approved for public dissemination or that is available from public sources.

Note: Within the context of the Court, approving information for public dissemination is a conscious decision and the absence of a marking that suggests otherwise does not warrant the assumption that information is unclassified. See also subsection 5.15.

(b) "[ICC] RESTRICTED" - for Information that is determined to be for internal use within the Court;

(c) "[ICC] CONFIDENTIAL" – for Information that is determined to be kept confidential to certain parties;

(d) "[ICC] SECRET"- for Information that is determined to be kept as a secret amongst selected individuals;

Note: The levels of protection afforded to non-state secrets do not try to match or be symmetric to the levels defined for state secrets; the protection levels for state secrets are completely unrelated to the levels of protection afforded to non-state secrets.

3.4. For Information provided to the Court, the level of protection defined by the Provider's assigned protection level shall be used to determine the corresponding protection level of the Court.

Section 4

Classification and efficiency considerations

4.1. Information shall be given a protection level which shall be as low as possible, but as high as necessary. Applying too high a classification may inhibit access, lead to unnecessary protective controls, and impair the efficiency of the activities of the Court. Conversely, applying too low a classification may put Information at risk of Compromise, due to a lack of appropriate security controls.

4.2. Information shall be classified to its appropriate level which is not necessarily the classification of the information it based on, responds to or is referring to.

4.3. Where possible and applicable, information that requires a high protection level shall be placed in appendices in order for the main texts to be distributed more widely and with less stringent security measures.

4.4. Information shall be classified on the basis of its contents and the risks associated with the Compromise of the content as set out by the criteria in Section 5.

Section 5

Protection levels and application criteria

5.1. The level of protection afforded to Information received from a Provider shall be linked to the level of sensitivity indicated by the protection level assigned by the Provider.

UNCLASSSIFIED

5.2. The Court shall strive to receive and generate Information that can be marked as UNCLASSIFIED in order to maximize the utility of the Information for the Court's purposes and to have maximum discretion with respect to the handling of the Information.

5.3. Information not falling into any of the protection levels defined below shall be considered unclassified and shall be marked UNCLASSIFIED with the exception as defined in subsection 7.4.

5.4. The protection level 'UNCLASSIFIED' shall be applied to Information provided by the parties to the legal proceedings as 'PUBLIC' unless ordered otherwise by the relevant Chamber.

[ICC] RESTRICTED

5.5. The protection level '[ICC] RESTRICTED' shall be used for Information where the Compromise of such Information would reasonably be expected to be disadvantageous for the Court. Such disadvantage would, inter alia, be indicated by:

(a) Facilitation of unjustified gain or advantage for individuals or organizations; or

(b) Limited financial loss by the Court; or

(c) Disadvantages for the Court in commercial or political negotiations; or

(d) Undermining the public perception of the Court and its operations.

5.6. The protection level '[ICC] RESTRICTED' requires a level of protection that shall reasonably prevent Compromise.

5.7. Information shall be classified by default as [ICC] RESTRICTED unless its meets the criteria for [ICC] CONFIDENTIAL, [ICC] SECRET or UNCLASSIFIED.

Note: [ICC] RESTRICTED is the Court's equivalent of 'Internal use only' and will mainly be used for documents concerning the operation and administration of the Court and its processes. It has no judicial counterpart and therefore cannot be applied to Court Records.

[ICC] CONFIDENTIAL

5.8. The protection level '[ICC] CONFIDENTIAL' shall be used for Information where the Compromise of such Information reasonably be expected to prejudice the interests of the Court. Such prejudice would, inter alia, be indicated by:

(a) Damage to the effectiveness, reputation, stability or security of the Court, States, Intergovernmental Organizations or Non-Governmental Organizations; or

(b) Detrimental effect on the support of the Court in a specific case, situation or programme; or

(c) Detrimental effect to an investigation or trial;

(d) Prejudice to individual wellbeing or liberty.

5.9. The protection level '[ICC] CONFIDENTIAL' requires a level of protection that shall ensure:

(a) The prevention of casual and wilful Compromise; and

(b) Actual or attempted Compromise shall be detected.

5.10. The protection level '[ICC] CONFIDENTIAL' shall be applied to Information provided to the parties to the legal proceedings as 'CONFIDENTIAL' unless ordered otherwise by the relevant Chamber.

[ICC] SECRET

5.11. The protection level '[ICC] SECRET' shall be used for Information the Compromise of which would reasonably be expected to seriously harm the interests of the Court. Such harm would, inter alia, be indicated by:

(a) Material damage to the effectiveness, reputation, stability or security of the Court, States, Intergovernmental Organizations or Non Governmental Organizations; or

(b) Material damaging consequences to an investigation or trial; or

(c) A direct or indirect threat to, or loss of, life, regardless of their relation with the Court.

5.12. The protection level '[ICC] SECRET' requires a level of protection that shall ensure:

(a) There shall be no Compromise; and

(b) Actual or attempted Compromise shall be detected and those responsible shall be identified.

Note: The afforded level of protection aims at no compromise. Nevertheless, there can and will always be circumstances leading to a compromise. In such case, the compromise must be detectable and control measures must be in place to ensure the availability of traces to aid the investigation.

5.13. The protection level '[ICC] SECRET' shall be applied to Information provided by the parties to the legal proceedings as 'UNDER SEAL' unless ordered otherwise by the relevant Chamber.

GENERAL

5.14. Information not marked shall be treated as [ICC] RESTRICTED by default.

5.15. Information provided to the Court shall be afforded [ICC] RESTRICTED, unless or until the Provider specifies a particular handling or level of sensitivity or the Information is available in the public domain.

5.16. The prefix 'ICC' in the nomenclature of these levels is used purely to facilitate the handling of Classified Information, in clearly identifying levels as being those applied by the Court in order to avoid any conflict or misunderstanding with other classification systems.

5.17. The use of the 'ICC' prefix may be omitted at the risk of confusion between the usage of [ICC] RESTRICTED, [ICC] CONFIDENTIAL and [ICC] SECRET as protection levels and the usage of 'restricted ', 'confidential' and 'secret' as adjectives.

5.18. The use of the 'ICC' prefix does not in itself imply any particular scope of dissemination.

Section 6

Caveats and Endorsement codes

6.1. Caveats shall be used to indicate directives on the dissemination of the Information by specifying the authorised recipients of Information.

Note: The essence of protecting confidentiality is that one tries to lock out unauthorised users. Hence, information can only be classified as sensitive in combination with its authorised users. When dealing with digital information, the caveats are implemented through for instance access groups and roles in applications and network folders.

6.2. Endorsement Codes shall be used to allow for supplementary directives on how Information shall be handled.

Note: Endorsement Codes allow for handling codes to instruct staff on specific handling requirements like a disclosure under embargo.

6.3. Caveats and Endorsement Codes shall be assigned during the creation of Information or when the Information is registered.

6.4. The Endorsement Code 'Ex Parte' shall be used in combination with a description of the authorised audience

6.5. Caveats may be translated and adapted to the possibilities and configuration of ICT Systems.

Section 7

Markings

7.1. The Court shall mark Information with:

(a) A protection level;

(b) Caveats;

(c) Endorsement Codes.

Note: The explicit marking of material is a common practice in the judicial processes of a Court. One can choose out of the four levels defined in this A.I. or their judicial equivalent (see 5.4, 5.11 and 5.14)

7.2. Markings shall be applied to all copies of classified Information.

7.3. The protection levels [ICC] CONFIDENTIAL, [ICC] SECRET shall be used in combination with a Caveat that specifies the authorized recipients.

Note: Information is only of value when it is accessible by those with a need to know. The protection level only specifies how much effort is afforded to protect against compromise; one must still specify the authorized audience (for instance ex-parte or OTP only).

7.4. Information intended and approved for public release does not have to be marked visibly as UNCLASSIFIED when its format clearly identifies its public nature.

Section 8

Classification of Information

8.1. Information shall be classified according to the protection level criteria set out in Section 5 of this Administrative Instruction.

8.2. Each Organizational Unit may issue clarifying guidelines with regards to the classification of Information.

8.3. The classification of Information shall be determined by the following authorities:

(a) In the case of Information generated by the Court, the Originator of the Information shall assign a protection level under the responsibility of the Owner; or

(b) In the case of Information provided by an external Provider, the Provider shall have the authority to designate its initial protection level; or

(c) If a Provider provides Information which appears to have a protection level but without indicating a level of sensitivity or protection level, the Head of the receiving Organizational Unit shall, subject to Section 5 above, apply a protection level and treat the Information accordingly.

8.4. In making the determination as set out in subsection 8.3.c, the Originator may consult, if necessary, the Classification Officer of the Organizational Unit accountable for the Information to be classified.

8.5. If a recipient of Classified Information suspects improper classification or inappropriate classification markings, this suspicion shall be brought to the attention of the Originator, Provider or the Classification Officer of the Organizational Unit accountable for the Information by the recipient. The recipient may provide a suggestion for the classification/marking which he/she believes appropriate.

Section 9

Classification officers

9.1. Every Organizational Unit shall assign the role of a Classification Officer within the Organizational Unit that shall provide Staff of the respective Organizational Unit with advice with respect to the classification of Information. Alternative, a Classification Officer may be assigned to the Organizational Unit by a superordinate Organizational Unit.

Note: The Classification Officer has an advisory role to the head of the relevant Organizational Unit.

9.2. The Classification Officer shall maintain for this purpose classification guidelines for the types of documents that are commonly or routinely handled within the respective Organizational Unit.

9.3. The Classification Officer shall respond to requests for classification guidance or may refer the request to Information Security Officer.

9.4. The Classification Officer shall support the respective Organizational Unit in responding to requests for Information outside the standard practices for information exchange between the Organizational Unit and the requestor:

(a) By performing -or arranging for- a classification review of Information that is considered to be responsive to the request; and

(b) By making recommendations regarding the declassification or sanitizing of Information before release.

Section 10

Duration of classification

10.1. When providing classified Information, the Originator or Provider may indicate the duration of classification that shall apply to the Information. If no indication is given, the duration of the classification shall be assumed to be the same as the Classification Retention Policy for the type of Information provided. In case there is no applicable Classification Retention Policy, the retention of the classification will be maintained until the information is superseded or has become obsolete.

10.2. Classifications shall be reviewed after the retention period has passed.

10.3. Classifications shall be reviewed if the circumstances that warranted the classification have changed.

10.4. Classifications may be reviewed periodically by the Originator in order to establish whether the classification may be revised or terminated.

10.5. The classification of Information shall cease to apply only when the Information is destroyed in its entirety, not when merely some but not all instances or elements of the Information are destroyed.

Section 11

Reclassification

11.1. Reclassification of Information may be required when the Information is amended, supplemented superseded or revised so as to create a substantial change in its sensitivity.

11.2. For Court Records, the determination of (re)classification shall be made only by the relevant Chamber.

11.3. In the case of a request for a change in the protection level of Information originating from the Court, the appropriate Classification Officer shall make such determination, abiding by the criteria established for the application of protection levels with reference to the stated operational need.

11.4. The Court may request a change from the Provider in the classification of provided Information. Such a request shall be based on a clear operational need. Before confirming such change, the Court and Provider may consult on the consequences of the proposed change.

11.5. If the Originator or Provider changes the classification of the information, (s)he shall inform the addressees.

Note: The act of giving notice may be automatically incorporated into the default procedures, as for instance, the case with decisions of Chambers on court records filed by Chambers and the parties.

11.6. When Information classified [ICC] SECRET is declassified the ICIR record of the document shall be updated to show the date of declassification. The record shall be retained by the ICIR and Staff currently holding a copy of the document shall be notified of the declassification.

11.7. Reclassified Information shall be marked in a conspicuous manner in order to alert the holder handling the Information on the actual classification.

Section 12

Retention periods

12.1. Information is to be retained for the period specified by the relevant ICC retention schedule. After that period, such information may be archived following the relevant archiving policies or be destroyed.

12.2. The retention schedule for Information is set under responsibility of the Information Owner.

12.3. The default ICC retention period is set to 10 years unless applicable regulations require a longer or shorter retention period.

12.4. Court Records shall be maintained ad infinitum.

Section 13

Classification of passwords, keys and cryptographic devices

13.1. The protection level for passwords, keys and cryptographic devices shall be at the same level as the highest level of the Information protected by those passwords, keys and cryptographic devices.

PART III – HANDLING OF CLASSIFIED INFORMATION

Section 14

Handling provisions

14.1. Part III of the present Administrative Instruction sets out the principles governing the provision of access to and procedures for the handling and dissemination of Information.

14.2. A protection level does not in itself determine the scope of access to classified Information, but defines the manner in which it shall be handled and protected against unauthorized reproduction and dissemination.

Section 15

Access to Information

15.1. Staff whose duties give them access to Classified Information shall hold a personal security clearance issued by the Vetting Desk of the ICC Security and Safety Section or hold an external clearance recognized by the Court.

Note: Contractors, interns, visiting professionals may need (or already have) access to the most sensitive types of information, including the identities of witnesses. Hence, the Court has an obligation to make an effort to ensure the trustworthiness of those to be entrusted with such sensitive information. For this reason the Court has implemented a security clearance process through the SSS vetting unit. The personal security clearance process is unrelated to the clearances offered through national security agencies and does substitute the types of clearance that states and the EU would look for.

Note: The personal security clearance process yields an opinion of the SSS. There is no differentiation between levels of clearance. This is not feasible within the research possibilities of the Court and would not align with the information flows within the Court; for instance a vast amount of Staff have access to Under Seal documents as part of their role in the processes of the Court. Therefore a one-size-fits-all that aims for the highest level of assurance (under seal/secret) is the most appropriate choice.

Note: The personal security clearance process draws upon several sources of information. The AIVD has fallen away as a source and a replacement source is underway. Other sources remain pertinent.

15.2. Those who have access to Classified Information shall sign a Non-Disclosure Agreement (NDA) upon commencement of their duties. The obligations under the NDA do not cease upon separation of service.

Note: The NDA for staff is done and administrated through HR. SSS looks after instructions to individual maintenance contractors. Procurement puts NDA-type provisions in place for contracting parties.

15.3. Organisational Units may implement supplementary NDAs consistent with this Administrative Instruction in order to further regulate access for particular tasks or purposes.

15.4. The ICC Security and Safety Section shall instruct those with access to Information classified as [ICC] RESTRICTED or above, upon their arrival at the Court and at regular intervals thereafter, on the handling of such Information.

15.5. Heads shall arrange for instruction of those with access to Information classified as [ICC] RESTRICTED or above, upon their arrival at the Court and at regular intervals thereafter, on the handling of such Information where such handling is specific to their Organizational Unit.

Section 16

Dissemination principles

16.1. The dissemination of Information shall be governed by the following principles:

(a) access to Information shall be regulated in accordance with its protection level; and

(b) the dissemination of Information shall be on a need-to-know basis. An individual's specific function or tasks shall be the principal determinant of that individual's need to know and of the consequent scope of access to Information.

16.2. Staff shall not discuss or disclose classified information with anyone except individuals to which access has been granted by the Head accountable for the Information, in which case such discussions or disclosure will involve only such Information as is reasonably necessary to accommodate the purposes for which access was granted.

Section 17

Disclosure of Information to External Parties

Note: The release of Information to third parties has been partly regulated and shall be in compliance with rule 101.7.b of the Staff Rules and Regulations. The present section focuses on the conditions to release Classified Information.

17.1. The Court may release Classified Information to external parties subject to the following conditions:

(a) The Information retains its protection level; and

(b) The Court retains discretion over the use of the Classified Information; and

(c) The external party shall protect and safeguard the Information according to its own security regulations for information holding an equivalent security level; and

(d) The Information shall not be used for purposes other than those agreed to by the Court.

17.2. The Court shall take due care to ensure that external parties are compliant with their own security regulations.

17.3. Release of Information that affects the privacy of Staff shall be authorised by the Head of the Human Resources Section, in addition to the Head of the respective Organisational Unit. In such case, the Head of the Human Resources Section shall ensure the exchange adheres to the following conditions:

Note: Authorisation is implicit when such exchange is initiated by the Human Resource Section in the light of their duties regarding the administration of Staff.

(a) The Information is fairly and lawfully processed; and

(b) The Information is processed for limited and agreed upon purposes; and

(c) The Information provided is adequate, relevant and not excessive; and

(d) The Information is accurate; and

(e) The Information is not kept for longer than is necessary; and

(f) The Information is released to parties with adequate data protection regulation.

Note: The above provision is aligned with the data protection principles as applied by the International Labour Association.

17.4. The release of private Information of Staff that falls outside the duties of the Court regarding its operations, and the safekeeping and administration of its Staff shall require the consent of the individual Staff, or the Staff Representative Body when a material amount of staff is involved.

Note: The provision serves to protect the privacy of individuals but also to avoid the creation of unjustified data protection obstacles to economic relations and the transborder flow of data. Only Information that goes beyond the administrative needs of the Court, for instance personal staff opinions gathered through surveys or the background information required for the vetting process, needs approval. Please note that this provision is in effect already in place to a large extent.

Section 18

Translations and Transcriptions

18.1. Information may be translated or transcribed, provided the translation or transcription inherits the protection level, markings and Endorsement Codes of the originating Information and is handled accordingly.

Section 19

ICT Systems

Note: The Court is fully dependent on ICT Systems and has declared information security to a spear point. This section aims to ensure that the information security aspect is addressed from the first idea to the disposal of a system. It also defines the global responsibilities between the ones that are responsible for information and the ones that provide the necessary services use and protect the information.

Note: More detailed requirements per information system (like TRIM, RingTail) are to be elaborated on a lower level; for instance in service level agreements. These agreements should hold provisions on who is responsible for what. Information security requirements on access control and accountability can be found in the draft A.I. on Access Controls.

19.1. The Court may deploy ICT Systems for storing, processing and transmitting Information.

19.2. The protection of Information shall be envisaged, maintained and documented throughout the life cycle of an ICT system's life cycle.

19.3. The following stages of an ICT system life-cycle are identified: Planning, Development and procurement, Implementation, Operation, Enhancement, withdrawal from service, and disposal of equipment.

Note: Security is an integral part of any ICT System and should be part of the solution for its conception.

19.4. The Information Owner accountable for the Information processed by an ICT System shall ensure that his/her information security requirements are identified and made known to the Information Custodian. Information security requirements may restrict the number of solutions that can be implemented and may impact development, operation and maintenance, personnel and costs.

Note: ICT provides a generic level of security to the applications it manages for the Court. In the event that applications need a different type of management (for instance a higher availability that normally afforded, this must be made known to ICTS.

19.5. The Information Owner accountable for the Information processed by an ICT System shall ensure that sufficient resources are available and allocated to the Information Custodian for the security aspects of the system, at the appropriate stages.

19.6. Information security requirements may impact the development, operation and maintenance, personnel requirements and costs.

19.7. The security requirements for ICT Systems shall take into account that:

(a) Any Information may be vulnerable to access by unauthorized Staff or other individuals, to denial of access to authorized Staff, and to corruption, unauthorized modification and unauthorized deletion in general; and

(b) ICT System equipment is in general complex, fragile, expensive and difficult to repair or replace rapidly; and

(c) Not all individuals with access to the ICT Systems have a common need-to-know for all of the information stored, processed or transmitted within the ICT systems.

Note: The above statements with regards to ICT Systems are not specific to the ICC, they are words of cautions aiming to ensure continuous awareness for the special risks that come with the Court's dependency on ICT System.

19.8. A formal method shall be used as the guiding model for identifying information security vulnerabilities, risks and requirements.

19.9. The ISO/IEC17799:2005 ("Code of Practice for Information Security Management") shall be used as the guiding model for selecting information security requirements and matching controls (ICC/Presd/G/2005/001 paragraph 3.9).

Section 20

Colour scheme

20.1. When colours are used for identifying protection levels, the colour scheme shall avoid any possible confusion with the colour scheme in use for Information provided as State Secrets as defined in subsection 15.1 of the A.I. on "Information Classification and the Handling of Classified Information Provided by States and International Organisations".

Subsection 15.1 of the A.I. on "Information Classification and the Handling of Classified Information Provided by Governmental and Intergovernmental Organisations" reads:

15.1	When indicating security classification levels through the use of colours, the following colour scheme shall be applied:
(a)	IPASS TOP SECRET – Purple;
(b)	IPASS SECRET – Red;
(c)	IPASS CONFIDENTIAL – Yellow;

Note: there are no colours codes foreseen for the type of Information to which the present A.I. pertains. Organizational Units are free to establish colour codes, provide coloured document wallets and stickers and oversee their correct and consistent usage. However, if this turns out to be a valuable addition, it will be incorporated in a later stage.

Section 21

Abbreviation scheme

21.1. When abbreviations are used for identifying protection levels, the following abbreviation scheme shall be applied:

(a) "IS" is the designated abbreviation for [ICC] SECRET;

(b) "US" is the designated abbreviation for UNDER SEAL;

(c) "IC" is the designated abbreviation for [ICC] CONFIDENTIAL;

(d) "IR" is the designated abbreviation for [ICC] RESTRICTED;

(e) "UC" is the designated abbreviation for UNCLASSIFIED.

(f) "PB" is the designated abbreviation for PUBLIC.

Section 22

Exterior marking

22.1. Information shall be marked with its protection level.

22.2. Documents shall be marked with their protection level (by stamp, print, or permanently affixed with a sticker, tape or seal) in the centre of its face and back cover.

22.3. If marking is not possible, the Documents shall be accompanied by a letter stating the protection level.

22.4. Markings may be, in the alternative and in addition, applied to envelopes, folders, boxes or any other mechanism used for carrying, holding or keeping Documents.

22.5. Caveats shall be set out in their entirety on the face of Documents.

22.6. Endorsement Codes shall be set out in their entirety on the face of Documents.

22.7. Markings shall be applied in a conspicuous manner in order to alert the holder of Documents on the actual classification.

22.8. Staff who electronically create/process/disseminate classified information shall mark the protection level electronically, so that the classification status of electronic objects, e-mails, documents, databases and optical materials such as photo images and film, may be ascertained without opening the object.

Digital information can be provided with a marking through the metadata. Examples are the metadata fields in applications like CMS and TRIM.

Section 23

Interior marking

23.1. For Documents classified as [ICC] CONFIDENTIAL and above, each interior page shall be marked as such at the top or bottom. When pages are printed front and back, both shall be marked.

23.2. The marking of Caveats and Endorsement Codes is not required in the interior of Documents.

23.3. Markings shall be conspicuous enough to alert Staff handling the Information that the Information is classified.

Note: Markings should be a part of the ICC templates that should be made available to staff. Templates aim at preserving the house style of the ICC but facilitate consistent marking in the process.

Section 24

Administration of [ICC] SECRET Documents

24.1. Documents classified as [ICC] SECRET shall be accounted for, individually serialized, and entered into an ICC Classified Information Register (ICIR).

Note: The above provision implements Regulation 16 of the Regulations of the Registry

24.2. An ICIR entry shall identify the document, and at a minimum include (where available) the date originated or received, individual serial numbers, copy number, title, Originator, action (e.g., created, modified, read transferred, destroyed, downgraded and reclassified) and date of each action taken including the person that ordered or authorized the action.

Note: The above provision is mainly implemented through the logging & audit features of application like TRIM, CMS and the ICC network.

24.3. When handling Documents classified [ICC] SECRET, Staff shall forward notification of any manual action referred to in subsection 24.2 to the ICIR.

24.4. Documents to which ICIR entries pertain shall be physically inspected, or accounted for, by an Administrator at least annually, and more frequently as circumstances warrant.

Section 25

Printing, Copying and Faxing

25.1. Staff may print, copy and fax Classified Information for official use only.

25.2. When printing, copying or faxing Classified Information, the number of reproductions shall be kept to a minimum and be linked to the approved scope of access.

25.3. Print-outs of Information classified [ICC] SECRET shall show the identity of the printing Staff and the timestamp of the moment of printing.

25.4. Copies of Documents classified [ICC] SECRET shall be marked with a copy number, total number of copies made and the names of the copying Staff on its cover.

25.5. Information Classified as [ICC] CONFIDENTIAL and above shall be printed using devices that comply with one or more of the following requirements:

(a) The device shall be in the direct proximity or eyesight of the printing Staff;

(b) The device shall be available only to the printing Staff;

(c) The device enforces Secure Printing.

25.6. Every reproduction shall have the same protection level as the original from which it was reproduced.

25.7. Printers, copiers and faxes shall be placed in areas suitable for the highest protection level of Classified Information processed.

25.8. Printers, copiers and faxes shall not be placed in areas shared with visitors, areas inviting to social contacts, areas that are not observable to the Staff that are the principal users of the printers and areas where the placement of such device printer conflicts with safety and health regulations

25.9. Staff shall not leave their print-outs, copies and facsimiles (or the originals) unattended on printers, copiers and faxes.

Section 26

Shredders

26.1. Every area, containing a shared printer, fax, copier or scanner, that is not a room assigned to dedicated staff, shall be equipped with a shredding device, or a paper disposal bin as provided by GSS.

26.2. Staff may use shredders to destruct Information.

26.3. Information classified [ICC] CONFIDENTIAL shall be, when shredded, shredded by a shredding device that shred compliant to the DIN 32757-1 level 3 or higher.

Note: Staff is not expected to be knowledgeable on DIN standards. However, it is important to set these standards to ensure the correct office stationary and equipment is purchased.

26.4. Information classified [ICC] SECRET shall be, when shredded, shredded by a shredding device that shred compliant to the DIN 32757-1 level 4 or higher.

26.5. Shredders shall be marked with the highest protection level for which they are qualified.

26.6. Alternatively to shredding, the paper disposal bins as provided by GSS may be used for Documents of any protection level.

Note: The blue paper disposal bins are disposed of and shredded in a controlled manner.

Section 27

Storing information on ICT Systems, Mobile Devices and Portable Storage Media

27.1. Information classified [ICC] CONFIDENTIAL and above may be stored on, processed by and transmitted via laptops if the information on such laptop is encrypted and accessible only via a token and a password or functional equivalent.

27.2. Information classified up to [ICC] CONFIDENTIAL may be stored on, processed by and transmitted via PDAs if the information on such PDA is encrypted and accessible only via a password or functional equivalent.

27.3. Information classified [ICC] CONFIDENTIAL and above may be stored on Court provided secure USB memory sticks. Information classified [ICC] CONFIDENTIAL and above may be stored on other portable storage media such as floppy disks, DVD and CDs if the information on the media is encrypted and accessible only via a Strong Password or functional equivalent.

27.4. In case Information classified [ICC] CONFIDENTIAL and above is stored on portable storage media not compliant to the condition set out in subsection 27.3, the portable storage media shall be regarded equivalent to hard copy versions of the information they contain and inherit the highest classification of the information stored on them, and shall be protected accordingly.

27.5. Network folders shall only be used for storing Information where the Court's applications like TRIM, CaseMap, RingTail, CMS and SAP do not provide the required functionality.

Note: The above provision addresses the limited capabilities of the network folders to support the Court's accountability requirements and promotes the use of TRIM, CMS etc. However, the use of the network folders is expected to be needed in certain cases as applications may not cater for every need. This has to be assessed and is part of the periodic evaluation of the A.I..

27.6. Documents containing Information classified [ICC] CONFIDENTIAL and above shall be stored under a name that does not divulge sensitive Information by itself.

27.7. Documents containing Information classified [ICC] CONFIDENTIAL and above shall not be stored on local personal computers that are part of the Field Offices unless the Documents are encrypted and accessible only via a Strong Password or functional equivalent. Such Documents may be stored on the central ICT Systems at the seat of the Court.

Note: Experience has shown that field offices are subject to emergency evacuations and that personal computers and media might be checked at customs. For this reason, it is important to enable remote users to take full advantage of the Court's applications while ensuring that information –while accessible remotely-stays at the central ICT Systems of the Court as much as possible.

Note: The above provisions are implemented through the use of the remote access tool 'Citrix' that allows external individuals access to the Court's network and the applications on it.

27.8. Documents containing Information classified [ICC] SECRET shall not be stored on local servers that are part of the Field Offices. Such Documents may be stored on the central ICT Systems at the seat of the Court.

Note: The above provisions are implemented through the use of the remote access tool 'Citrix' that allows external individuals access to the Court's network and the applications on it.

27.9. Documents containing Information classified [ICC] CONFIDENTIAL and above shall not be stored on computers that are not under control of the Court.

Section 28

Electronic transmission

28.1. Classified Information of any protection level may be transmitted within the Court network. This includes the Court web mail facility that enables remote access to its mail facility.

28.2. Documents classified [ICC] SECRET may be transmitted (subject to the provisions of Section 24) outside the Court network only if the information is encrypted independently through a digital certificate.

28.3. Documents classified [ICC] CONFIDENTIAL may be transmitted outside the Court network only if the information is encrypted through a digital certificate or via a Strong Password.

28.4. Documents shall be disseminated where possible through sending a reference (link) to the document (via which the Document can be retrieved) instead of the document itself.

Note: Sending documents increases proliferation and diminishes control as it multiplies the available copies. Furthermore, documents in mails are not subject to the accountability features offered in TRIM, CMS etc. In addition, mail might be forwarded automatically, mailboxes might be shared with staff unknown to the sender, and mail addresses might be misspelled. For these reasons, it is prudent to send references (links) to documents instead of the documents themselves where possible, especially for Classified Information.

28.5. For Documents classified [ICC] SECRET the receipt of a transmission shall be recorded by the sender and confirmed by the recipient.

Note: The records of transmission and receipt are in most cases automatically done through the infrastructure used.

28.6. The protection level of Documents shall be sent with the Documents.

28.7. Documents to be exchanged through electronic transmission shall be stripped from metadata that reveals internal discussions, operations or names unless such metadata should be available to the recipient.

Note: For documents transmitted outside the Court network stripping is necessary as metadata can reveal internal discussions and redactions. The stripping of metadata is foreseen to be done automatically.

Section 29

Faxes and facsimile

29.1. Documents classified [ICC] SECRET shall be faxed outside ICC premises only by cryptographic fax devices.

29.2. Fax devices shall be physically protected to ensure that only authorized Users can access them.

29.3. For Documents classified [ICC] CONFIDENTIAL and above, receipts of incoming and outgoing fax transmissions shall be recorded.

29.4. A facsimile shall have the same protection level as the Document(s) from which it is a copy.

Section 30

Transport within ICC premises

30.1. Documents classified [ICC] CONFIDENTIAL and above that is carried within the Court premises (including any field office) shall be covered in order to prevent observation of its contents.

30.2. Documents classified [ICC] CONFIDENTIAL and above shall, when removed from secure storage, at all times be under surveillance by a Staff.

Section 31

Transport outside and between ICC premises

31.1. Information shall be removed from the Court premises only when there is a reasonable expectation that the Information will be protected in compliance with or equivalent to the provisions of this A.I.

31.2. Information classified [ICC] RESTRICTED and above shall be removed from the Court premises only when required for the conduct of official use.

31.3. Information classified [ICC] CONFIDENTIAL and above shall be under constant surveillance by Staff and kept in a cover sheet.

31.4. Documents classified [ICC] CONFIDENTIAL and above shall not be read and/or discussed in public places where unauthorised access could be gained through overlooking and / or overhearing.

31.5. Information classified [ICC] SECRET that is transported outside ICC premises (including any field office) shall require the use of receipts.

31.6. Only the following means shall be used to transport Classified Information:

(a) National postal service for Information classified up to and including ICC RESTRICTED; or

(b) Registered post via a national postal service or a commercial courier service for Information classified up to and including [ICC] CONFIDENTIAL; or

(c) Diplomatic pouch for Documents up to and including [ICC] SECRET; or

(d) Designated Staff for Documents up to and including [ICC] CONFIDENTIAL if such Documents are not protection against access by customs or local governmental officials.

(e) Designated Staff for Documents up to and including [ICC] SECRET if such Documents are protection against access by customs or local governmental officials.

Note: 31.6.d and 31.6.e address the risk associated with bringing documents through for instance customs or the risk of interference by other local governmental officials that have the authority to inspect material carried by Staff. This could compromise information and might break the chain of custody. In the event such material is stored digitally on a secure USB memory stick or an encrypted laptop, the risk is adequately mitigated. Otherwise, the Pouch is the better solution for sensitive information or artefacts (where available).

31.7. The following conditions shall apply to the carriage of classified Documents by couriers:

(a) Documents shall not leave the possession of the courier unless stored in a secure area, appropriate for its security classification level; and

(b) Documents shall not be left unattended, and shall not be opened en route; and

(c) For Documents classified as [ICC] SECRET, couriers shall be briefed on their security responsibilities and be provided with a formal written authorization for the Documents they carry (see annex B).

31.8. Cryptographic keys, passwords and access tokens shall be transported separately from the Information to which they give access.

Section 32

Packaging

32.1. Documents classified [ICC] CONFIDENTIAL and above transmitted outside ICC premises shall be packaged as follows in order to prevent unauthorized disclosure:

(a) The Information shall be enclosed in two opaque and strong covers. A locked pouch, locked box or a sealed diplomatic pouch may be considered as the outer cover; and

(b) The inner cover shall be secured, bear the appropriate classification, as well as other prescribed markings and warning terms, and bear the full designation and address of the addressee; and

(c) The outer cover shall bear the designation and address of the addressee and a package number for receipting purposes; and

(d) The outer cover shall not indicate the classification of the contents or reveal that it contains Classified Documents; and

(e) If transmitted by courier, the outer cover shall be clearly marked with the endorsement code "By Courier".

32.2. Documents classified [ICC] RESTRICTED shall, as a minimum, be transmitted in a single opaque envelope or wrapping.

Section 33

Destruction of Documents

33.1. Documents may be destroyed after the relevant retention period has expired.

33.2. Documents may be destroyed before its assigned retention period has expired only after authorization by the Owner responsible for the Information.

33.3. In case no retention period has been assigned to (a type of) Documents, such Documents may be destroyed only after authorization by the Owner responsible for the Information.

33.4. Documents marked as [ICC] CONFIDENTIAL and above including all side products resulting from the preparation of such Documents such as spoiled copies, working drafts and notes, shall be destroyed by burning, pulping, shredding or otherwise reduced into a form that cannot be reconstituted.

Section 34

Destruction and repair of memory and storage media

34.1. Any device (e.g. facsimile machines, printers, copiers, scanners, PDAs and laptops) or medium with memory or digital storage capabilities (e.g. memory sticks, flash cards, floppy disks, DVDs and CDs) used for Information classified [ICC] SECRET shall be sanitized of any classified Information before being released to third parties for repair, maintenance or disposal.

34.2. Maintenance and repair shall be performed in situ where possible.

34.3. Devices used for Information classified as [ICC] SECRET shall be switched off temporary before maintenance is performed.

Note: Switching off equipment aids to clear the internal memory of equipment. It will not affect data stored on internal hard drives and other pervasive types of memory.

34.4. Devices used for Information classified as [ICC] SECRET containing a persistent memory shall be instructed to overwrite stored Information; alternatively the memory shall be removed by hand before maintenance.

Section 35

Physical Security of Documents

35.1. Documents classified [ICC] CONFIDENTIAL and above shall be removed from their place of storage only for the periods when they are actively in use.

35.2. When not in use, Documents classified [ICC] RESTRICTED shall be stored away.

35.3. When not in use, Documents classified [ICC] CONFIDENTIAL and above shall be locked away.

35.4. Staff shall:

(a) operate a locked door policy during and at the end of each working day; or

(b) operate a clear desk policy at the end of each working day.

Note: Locked offices are still accessed by co-workers and other staff and contractors with a legitimate need to be.

Section 36

Requirements for safes, vaults and strong rooms

36.1. Hard copy Information classified as [ICC] SECRET shall be stored outside ICC premises only within safes, vaults and strong rooms. Such safes, vaults and strong rooms shall be CEN II compliant or certified.

Note: Staff is not expected to be knowledgeable on CEN standards. However, it is important to set these standards to ensure the correct office stationary and equipment is purchased.

36.2. Hard copy Information classified as [ICC] SECRET shall be stored inside ICC premises that have limited physical security in place shall be stored only within safes, vaults and strong rooms. Such safes, vaults and strong rooms shall be CEN II compliant or certified.

Note: This provision caters for field offices, parking lots and temporary offices that do not provide the same inner building security as the Arc.

Section 37

Physical protection through areas, rooms and vaults

37.1. All premises, areas, buildings, offices, rooms, communication and Information Systems in which Information is stored and/or handled shall be protected by physical security measures commensurate with the protection level of the Information kept.

37.2. End-of-day security checks shall be performed by the Security and Safety Section to ensure that all areas which (can be expected to) process or hold Documents classified [ICC] CONFIDENTIAL and above are properly secured.

37.3. Documents classified [ICC] RESTRICTED and above shall be processed and stored in areas where:

(a) General access shall be controlled by a pass or personal recognition system;

37.4. Information Classified [ICC] CONFIDENTIAL and above shall be processed and stored in areas where, in addition to subsection 37.3:

(a) Information, when removed from secure storage, shall be under constant surveillance by an authorized person or kept in a cover sheet; and

(b) Visitors shall be escorted; and

(c) Access to rooms is controlled by registered keys; and

(d) Unused keys are administered and controlled; or

37.5. Information classified [ICC] SECRET shall be processed and stored in areas that comply with the following requirements, in addition to subsection 37.4;

(a) Entrance to and exit from the area must be through an electronic lock dedicated to the area involved; and

(b) Perimeter walls, doors, windows, floors and ceiling, including all openings, provide sufficient sound attenuation to preclude inadvertent disclosure of conversation; and

(c) Primary entrance doors are limited to one. Perimeter doors shall be closed when not in use, other than in emergency circumstances; and

(d) Windows which might reasonably afford visual surveillance of Information processed within the area, shall be made opaque or equipped with coverings to preclude such visual surveillance; and

(e) Perimeter windows at ground level shall, unless located within guarded and fenced premises, be covered by an Intrusion Detection System (IDS) that shall detect attempted or actual unauthorized entry; and

(f) The use of non-Court provided reproduction devices shall be prohibited.

Section 38

Breaches and Compromise of information security

38.1. Information classified as [ICC] CONFIDENTIAL and above that is lost, or temporarily lost, (including Documents which cannot be located at periodic inventories) is presumed to be compromised unless evidence to the contrary is presented.

38.2. Suspected Compromise shall be reported to the Court's Information Security Officer in a timely fashion.

38.3. The Information Security Officer shall, in consultation with the Information Owner, investigate suspected Compromise to determine:

(a) Whether Classified Information has been divulged; and

(b) To whom Classified Information has been divulged; and

(c) The potential impact of the Compromise; and

(d) How the Compromise or breach of information security occurred; and

(e) Whether negligence or malicious intent is suspected; and

(f) What corrective and preventive measures are recommended.

38.4. In order to conduct a comprehensive and adequate investigation, the Information Security Officer may access, in consultation with the Information Owner, and the Registrar when Staff privacy is concerned, the sources of information relevant to the investigation and may choose to deploy forensic capabilities on such Information and or its carriers.

38.5. Where an investigation may impact on operational, financial or legal constraints of the Court, the Information Security Officer shall act in consultation with affected Organizational Units.

38.6. The Information Security Officer shall report to the Information Owner and, where applicable, the Registrar and Head accountable for the Staff involved in the suspected Compromise.

Section 39

Evaluation and Assessment

39.1. Periodic checks shall be implemented to ensure that the provisions in this Administrative Instruction are implemented and complied with:

(a) The Head accountable for Information shall establish the compliance with this Administrative Instruction and the recording of records to demonstrate compliance; and

(b) At least annually the Information Security Officer shall determine compliance with this Administrative Instruction.

Section 40

Final Provisions

40.1. The Court may choose to enforce any or all provisions through organisational, administrative, physical and technical controls of a deterring, preventive, detective and corrective nature

40.2. The Court reserves the principle right to record, monitor, review and investigate any and all aspects of the usage and handling of Information for the purpose of verifying compliance with its regulations and guaranteeing the continuous integrity, confidentially and availability of the Information.

40.3. Violation of this Administrative Instruction or Compromise of Information may result in disciplinary action in accordance with applicable Staff Regulations, Staff Rules or any other administrative issuances.

40.4. Staff wishing to request an exception to any provisions of this Administrative Instruction shall make such request in writing through his/her supervisor to Information Security Unit of the Security and Safety Section.

40.5. This Administrative instruction shall be reviewed, and amended when necessary, yearly by the Information Security Officer as part of the Court's information security management process.

40.6. This Administrative instruction shall be applied from the date of its signature.

Bruno Cathala
Registrar