Canadian Judicial Council
Conseil canadien de la magistrature

Model Policy for the Classification of Court Information

First edition, September 2022

Prepared by Martin Felsky, PhD, JD – Special Advisor to the CJC on Information Technology

TABLE OF CONTENTS

TABLE OF CONTENTS **2**

BACKGROUND **4**

CLASSIFICATION IS ONLY PART OF ACCESS CONTROL 5

CHALLENGES **5**

JUDICIAL INDEPENDENCE **6**

POLICY STATEMENT **7**

1. PURPOSE 7
Commentary *7*
2. SCOPE 7
3. GLOSSARY 8
4. ROLES AND RESPONSIBILITIES 9
5. TRANSITION 10
Commentary *10*
6. INFORMATION ASSET REGISTER 10
Commentary *10*
7. RISK ASSESSMENT 12
Commentary *12*
8. CLASSIFICATION OF INFORMATION ASSETS 13
Public *13*
Confidential *13*
Restricted *13*
Secret *14*
Commentary *14*
9. INFORMATION ALREADY CLASSIFIED 15
Commentary *15*
10. DOWNGRADING CLASSIFICATIONS 15
Commentary *16*
11. LABELING CLASSIFIED INFORMATION – BANNERS 16
Commentary *16*
12. LABELING CLASSIFIED INFORMATION – BLOCK 17
Commentary *17*
13. HANDLING CLASSIFIED ASSETS 18

APPENDIX 1: CLASSIFICATION GUIDE 19

TABLE 1: MAP OF RISK AND ACCESS 19
TABLE 2: SAMPLE CONTROLS 20
TABLE 3: MARKING CLASSIFIED INFORMATION 22
TABLE 4: EXAMPLES OF CLASSIFIED COURT INFORMATION 23

BACKGROUND

This Model Policy follows upon the Council's earlier initiatives concerning court information. All courts, and the Council, recognized that the modern concept of "court information" was no longer merely a matter of official or administrative court records acquired or created intermittently, with limited bespoke content, and with practical obscurity arising from its documentary character and its ease of destruction.

A decade on, it is even more obvious and pressing that courts must recognize that "court information" is a far more encompassing concept and is far more accessible and far more durable than it once was. Accordingly, and in addition to its other responsibilities as to court information, each court needs to create, maintain, and review a systematic approach to the protection of sensitive court information throughout its life cycle. This Model Policy proposes a framework for courts to consider in that effort, and elaborates on policy 16 from the Council's *Blueprint for the Security of Court Information*:[1]

Policy 16a: Courts should adopt a classification scheme so that sensitive court information may be designated for special protection. Classification schemes as adopted should be consistent across all courts to ensure a common understanding of asset sensitivity and protection requirements.

Policy 16b: Classified information may be made available to a person only when the originator establishes that the person has a valid "need to know," appropriate personnel security controls are in place, and the access is necessary to the accomplishment of official court duties.

Classification is a perpetual balancing act that must protect sensitive information without unduly restricting access. The purpose of classification is to ensure that the risk of harm from a security or privacy breach is kept at a level acceptable to the court, corresponding to the court's risk tolerance, through proper designation, labeling and handling of sensitive information.

[1] *Blueprint for the Security of Court Information* (6th edition, CJC 2021). In French: *Plan directeur pour la sécurité de l'information judiciaire*. Henceforth, Blueprint.

CLASSIFICATION IS ONLY PART OF ACCESS CONTROL

The classification of an information asset guides holders with respect to its safe handling and dissemination, but classification is not the only safeguard that limits access. Classified information should be made available to a person only when the originator establishes that the person has a valid "need to know," such that access is necessary to the accomplishment of their official court duties.

There are other potential restrictions on accessing classified information, including personnel security clearances, and non-disclosure agreements.

CHALLENGES

The protection of sensitive information relies largely upon its originators - judicial officers, court officials and staff - to make the right classification decisions with respect to every email or file they draft or receive. This responsibility can be overwhelming, especially in light of the volume of digital information courts handle, and the velocity at which it moves.

The act of classifying information is not just a one-time activity. Security classifications are dynamic and must be revisited periodically, as the court's risk profile changes; as its system capabilities or architecture changes, or as the nature of the information assets themselves changes over time.

Remote work, virtual hearings and cloud computing are now a routine part of court operations, expanding the scope of cyber threats well beyond the premises of the courthouse.

Courts should address these issues by promoting a modern approach to classification. Until artificial intelligence can be trusted to make reliable security classification decisions on our behalf, there are steps available to take the burden of classification, but not control, away from members of the court. Hybrid solutions are available that combine automated and manual classification processes. Systems that parse information can be configured in various ways to suggest appropriate classifications based on the content or context of the information.

For example, Microsoft 365 provides a resource tagging feature with sensitivity labels that can be pre-configured by the court. This makes it easier for users to apply (or simply confirm) labels as they prepare emails and documents.[2]

Data loss prevention (DLP) systems are automated programs that can act as a backstop for classification lapses. They work by parsing outgoing communications and blocking unauthorized communications or warning senders.[3]

Ultimately, the goal of a modern classification scheme should be to establish the groundwork for fully automatic, artificially intelligent classification software.

JUDICIAL INDEPENDENCE

The judiciary is conferred with institutional and individual independence, which adds an important layer of cooperation to court information governance. The judiciary and executive, or other non-judicial administrators, involved with facilities management, human resources, infrastructure, or supply, administer Canadian courts jointly. At the same time, any form of court business intelligence that the court finds appropriate to its mandate or capacity, falls into the category of judicial administration. Chief Justices are looking at matters like judgment delay, load balancing, judicial education, judicial conduct, wellness, public outreach, and many other issues that are common to courts but not covered by business processes like "human resources." Thus, while court information is subject to broad-based legislation[4] and established government policies, it is also subject to individually negotiated MOUs, judicial discretion and the court's jurisdiction over its process and its records.

[2] See Azure Information Protection

[3] DLP systems must always be configured with the principles of judicial independence in mind, but judicial officers should not be exempt from the court's classification rules and security controls.

[4] Examples of relevant legislation include Official Secrets, Archives and Public Records, *Criminal Code* and Provincial Offences, Judicature acts, Evidence, Electronic Commerce and Privacy, Freedom of Information or Access to Information.

This document should not be read to alter the distinction between court information that is exclusively owned and controlled by the court, and any court information which by its nature can be delegated to or acquired by the executive branch directly or indirectly.

POLICY STATEMENT

1. PURPOSE

This policy establishes a formal process for classifying information assets to ensure that the baseline security controls used to protect court information are proportional to the risks of unauthorized access. It sets out clearly defined classification levels that can be efficiently and consistently applied to all court information assets.

COMMENTARY

Ultimately, the classification of court information is designed to prevent harm to individuals (including loss of life); to the court or other organizations; to financial markets, or to the justice system. It protects privacy, legal privileges, and judicial deliberative secrecy, or any type of sensitive information.

A classification scheme ensures clear lines of accountability for proper securing of court information. It helps prioritize budget allocations for security measures, makes it easier to comply with laws, court orders, non-disclosure agreements, licensing, and other obligations. It is an important means of identifying information that can be safely migrated to a cloud service provider or shared with justice partners.

2. SCOPE

This policy applies to all court information assets, wherever those assets may be located and in whatever format or medium they may be transmitted or stored.

Court information that contains personally identifiable information (for example about litigants, witnesses, judges, and staff) is to be classified accordingly.

Personal papers unrelated to the business of the court are private and do not form part of the court's information assets.

3. GLOSSARY

Case File

A Case File contains the Information that relates directly to a single court proceeding or to a number of related court proceedings that have all been assigned the same case file number. It includes the Information that comprises the Court Record and any other Information that has been captured or placed in the Case File.[5]

Court Record

Information and other tangible items filed in proceedings and the information about those proceedings stored by the court.[6]

Information asset

"An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited efficiently. Information assets have recognizable and manageable value, risk, content, and lifecycles."[7]

Information assets include physical information assets (such as paper documents, film, photographic prints) or digital assets stored electronically. An information asset can be a hardcopy document or a box of documents, a spreadsheet, or the contents of a shared network drive; a database, an operating system, an e-filing system, or a PDF file uploaded to such a system; a Case File, a Court Record, an email or an entire email account.

Depending on the context, some courts may wish to categorize non-documentary physical evidentiary objects (for example forensic samples) as information assets.

---

[5] See Canadian Judicial Council, *Model Definition of Judicial Information* (2020).
[6] See footnote 9.
[7] UK National Archives factsheet.

Custodian

The individual or business unit responsible for maintaining communications and technology systems used for court information.

Provider

External individual or organization that submitted or transferred information assets to the court.

4. ROLES AND RESPONSIBILITIES

Information controller

The information controller has legal control of information assets. This control is divorced from the concept of physical custody or possession.[8] Information controllers (or data owners) define the overarching information policies governing access, use, and retention of information assets.

Controllers are responsible for determining the classification of court information assets in their control and are authorized to approve access or downgrading requests. Controllers may require additional security controls on an *ad hoc* basis or strengthen information handling protocols as needed.

Originator

An originator is an individual or business unit of the court that authors or receives court information. Originators are responsible for considering and applying classification labels to the assets they create or receive, in accordance with this policy and other directions of the court.

[8] It is important to bear in mind the distinctions made in the 2013 CJC report: *Court Information Management Policy Framework to Accommodate the Digital Environment*, at page 6: "In a paper based world possession of a court file is synonymous with control over that file. It was easy for the judiciary to control Case Files in such an environment because an original paper file could only reside in one physical location at a time and those with possession of the physical file could easily control the ways in which information within it could be accessed.
In the digital domain however, it is quite possible to have possession of information without control and conversely, it is possible to have control of information without physical possession."

Judicial Information Technology Security Officer (JITSO)

The JITSO (or other qualified court-appointed officer) is responsible for the administration of this policy. The JITSO periodically updates the Information Asset Register (Policy 6) and ensures compliance through regular review and audit functions. Training on the handling of classified information must be provided regularly to all users.

Users

Anyone with access to court information is a user. Users must attend training and adhere to all policies and procedures relating to the handling of classified court information.

5. TRANSITION

This policy is effective upon its approval by the court.

COMMENTARY

This policy may be implemented progressively, on a day-forward basis. Existing assets can be classified over time, in priority based on the length of their retention period.

6. INFORMATION ASSET REGISTER

The court must prepare and update an Information Asset Register (IAR) that lists, briefly describes, and categorizes all court information assets.

COMMENTARY

The IAR is the first step to gaining control over court information. Key elements to consider recording for each asset category include:

1. Brief description including the purpose and use of the assets
2. Date range
3. Controller (with contact information)
4. Custodian (with contact information)
5. Users, including internal and external sharing relationships

6. Location – cloud, on premise, database, repository, domain
7. Form – paper, electronic, or other format or medium
8. Sensitivities - for example, copyright, private, privileged, confidential
9. Should this be a designated asset?[9]

Current thinking in the information governance profession is that larger, more inclusive categories make more sense for digital information, which is dynamic and often stored in unstructured repositories rather than filed in discrete folders. The more detailed or granular the IAR – for example a listing by document title, the more assets need to be listed and tracked individually.

While the establishment of high-level groupings simplifies the process of assigning classifications, some assets will require classification on a granular level. For example, a single field or record in a database, or particular form or file may contain information requiring classification that differs from its assigned group. Creative design may be required to assign classifications on a granular level, for example within a database, where certain groups of records or fields in the same database may require different classifications. These designs are constrained by the security features and controls built into each system.

Assets can be grouped in various ways. How depends on the court's mandate, size, and technology environment. Typically, the following methods are used:

- ***Content***, which groups information by meaning or purpose
- ***Context***, which groups information by business unit, function, system or platform
- ***User***, which groups information by individual, position or role in the court.

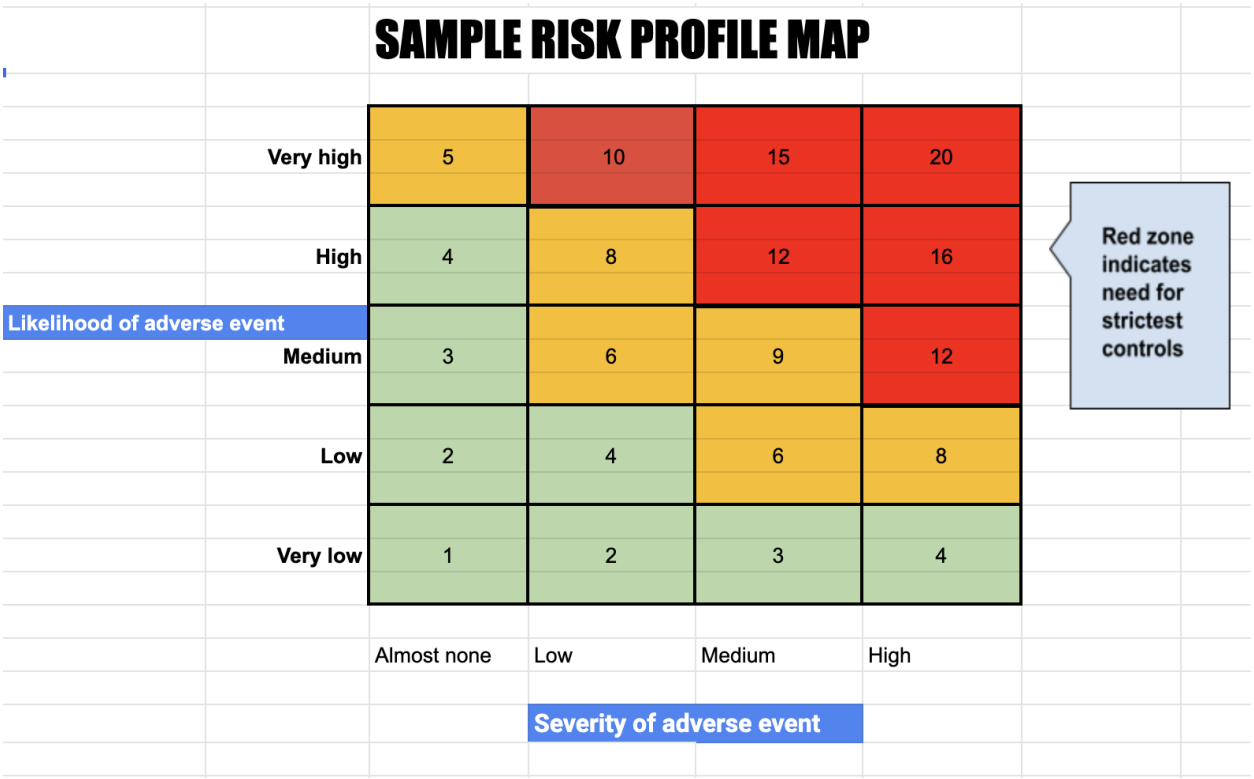
[9] The IAR forms the basis not only for decisions about classification but is also the foundation of a threat and risk assessment, the retention and disposition of court information, and business continuity procedures. The designation of assets in this listing is relevant to retention issues. See Canadian Judicial Council, *Model Policy for the Retention of Court Information* (2022).

7. RISK ASSESSMENT

The court must plan, conduct, and consider the results of a threat and risk assessment (TRA) in order to determine appropriate classifications for each information asset grouping in the IAR.[10]

COMMENTARY

The TRA helps the court assess the degree of harm that could reasonably be expected to result from unauthorized disclosure. A simplified schematic is shown below. Identified risks are assessed in terms of their likelihood and harm. The resulting chart provides decision makers with a basis for determining the court's risk profile, proportionate security controls and classification designations. The TRA report also identifies residual risks which need to be addressed to achieve a level of risk acceptable to the court.



[10] See Blueprint Policy 3b.

8. CLASSIFICATION OF INFORMATION ASSETS

All court information must be classified according to the sensitivity of its content and the risks associated with unauthorized disclosure and access.

Information that is copied, extracted, printed, or otherwise derived from classified information inherits the same classification as the source information.

The following classifications are to be used:

PUBLIC

Applies to information that, if compromised, would pose little or no risk to an individual, the court, or another organization. Information may be made public, as release would have no anticipated adverse impact, or is required by law. For example: Records of Proceedings, Annual Reports, Hearing Lists and Court Dockets.

CONFIDENTIAL[11]

Applies to information that, if compromised, could cause injury to an individual, the court, or another organization.[12] Internal and external access is limited to individuals or organizations with a valid need to know. For example: internal policies and directives; routine email, case conference briefs and case conference memoranda.

RESTRICTED

Applies to information that, if compromised, could cause serious injury to an individual, the court, or another organization.[13] Internal access is limited. External access is subject to order of the court, legislation, court policy, court rules, and court-approved security clearance and NDA. Access and actions to be logged. For example: draft judgments and judicial notes; rulings, endorsements and draft jury charges; documents and orders subject to a publication ban, and

[11] This departs from the suggestion in the Blueprint, in which the designation "Official" was proposed. However, as the word "official" could be used to designate certain types of court records for purposes other than security, the term "Confidential" is preferred here.
[12] Corresponds to Canada Protected A.
[13] Corresponds to Canada Protected B.

digital recordings of a closed or sealed proceeding. Restricted court information would be subject to more stringent treatment than Confidential, including special markings, encryption, and storage on designated devices. All such information should be clearly and conspicuously labeled "RESTRICTED."

SECRET

Applies to information that, if compromised, could cause extremely grave injury to an individual, the court, or another organization.[14] Access is restricted to designated, cleared individuals with a need to know, a non-disclosure agreement, or upon order of the court. All access and actions to be logged. For example: government intelligence, sealed Case Files, and information concerning informers. All such information should be clearly and conspicuously labeled "SECRET." (Original source markings should also be left in place.)

COMMENTARY

Each court information asset must be assigned a classification based on the level appropriate to the most sensitive information in its category. Information assets should be classified to the lowest possible level, but as high as necessary. This dynamic represents the critical balance to be achieved between the harm that could be done by unauthorized access and the advantages of accessibility to the court, to parties or the public.

Over-classification leads to increased maintenance costs, restricts legitimate access, and may encourage some users to evade security controls.

Descriptive words like "Confidential" and "Secret" are more meaningful and thus preferred to abstract language such as "Protected A" or "Level 3". Irrespective of their labels, though, the four-level court information classification scheme in this policy aligns with Canadian federal and provincial government classification schemes, reducing confusion for those court staff regularly working with both government and court information. In specialized courts, more classification levels may be required to fine-tune the handling of sensitive data received from providers such as foreign governments.

[14] Corresponds to Canada Protected C.

One way to clarify the differences among the three secure classifications is to train users that disclosure of Secret information would cause about ten times as much damage as disclosure of Restricted information, and disclosure of Restricted information would cause about ten times as much damage as disclosure of Confidential information.[15]

Originators should be aware that the compilation of low-level classified information could in rare cases lead to the compilation requiring a higher classification. This is due to the possibility that the compilation reveals a relationship or a trend that should be classified at a higher level than its components.

9. INFORMATION ALREADY CLASSIFIED

Information that has been classified elsewhere must be classified by the court at a level corresponding to the provider's and handled in accordance with the provider's controls to the extent they are more stringent than the court's.

Information received from external organizations must be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

COMMENTARY

When the court receives information that has been classified by a provider, the court should follow the rules applicable to that classification.

10. DOWNGRADING CLASSIFICATIONS

Information controllers may downgrade information in their control.

Originators (or their successors) may downgrade their own information assets.

Users may not downgrade a court information asset without the approval of its originator or the controller.

[15] See Quist, *Security Classification of Information*, volume 2, chapter 7.

COMMENTARY

Asset classifications may be upgraded or downgraded as necessary, with the proper authority. Over time, classifications of a document or other asset may be modified depending on an expired time frame, a certain event, or a routine re-evaluation.

11. LABELING CLASSIFIED INFORMATION – BANNERS

All assets (including copies and printouts) must be labeled with a banner indicating their classification level.

The banner consists of the name (or abbreviation) of the court and the classification level in UPPER CASE. For example:

Sample Classification Banner (options)	
Canadian Judicial Council – CONFIDENTIAL	CJC – CONFIDENTIAL

At the time of original classification, the banner must be clearly and conspicuously displayed on the face and every page of the asset, for example in headers and footers, or if the information is not susceptible to such marking, the classification designation must be clearly associated with its subject in a manner suited to its form. Where it is impractical to apply any marking, users must be made aware of the classification designation and any special handling required.

If portions of a document have different classifications, each portion shall be appropriately labeled to indicate its level of classification.

COMMENTARY

The classification banner is the primary mechanism by which the sensitivity of an information asset is displayed. A key aspect of a classification label is that it is like a passport - an important piece of identification that must accompany it on its travels. Whatever method is used to apply a label, it should be conspicuous, legible, and persistent.

Where classifications are pre-determined, they can be added to document templates. For emails, the classification should be marked in the subject line and optionally in the body of the email. Email signatures can also contain classification marking, which works well when policies are applied by user or user group. Preferably, email systems should be configured to compel users to select a classification before sending, for example in a drop-down menu.

12. LABELING CLASSIFIED INFORMATION – BLOCK

In addition to the banner, classified assets may be marked with an optional information block. The purpose is to provide users with more information about the status of the asset. The block should be displayed on the face of every classified document, or otherwise in a conspicuous manner suited to the form of the asset.

The sample below shows the type of information a block would contain:

> *Classified by*: Hon. Moreau, C.J.
> *Reason*: Sealed evidence
> *Declassification*: On order of the court
> *Additional dissemination restrictions*: None

COMMENTARY

By providing the name of the classifying authority (controller or originator), users know who to contact in the event a reclassification is proposed. Providing a reason for the classification is useful for audit and compliance purposes. If a declassification date or event can be determined when the asset is created, this helps users with making decisions about dissemination. Additional restrictions can be useful in various circumstances, for example when handling assets classified by providers who require more than the established controls.[16]

[16] Access to court information is not determined by classification alone. Rather, access rights are determined by a combination of classification-based controls, individual security screening or clearance, and the individual's function or assigned work, which determines their need to know.

13. HANDLING CLASSIFIED ASSETS

All court information must be handled in accordance with its classification and the procedures set out in the sample Classification Guide. (See Annex 1.)

Where classified court information is transferred to a third party, the court must ensure that the third party's security policies and procedures are sufficiently robust to respect the required classification controls.

APPENDIX 1: CLASSIFICATION GUIDE

The tables below are examples intended as guidance and are neither definitive nor comprehensive. The list of select references below can be consulted if more approaches or examples are needed.

TABLE 1: MAP OF RISK AND ACCESS

Classification	Risk level	Risk Description	Access
Public	Almost none	Applies to information or assets that, if compromised, would pose little or no risk to an individual, the court, or another organization.	Information may be made public.
Confidential	Low	Applies to information or assets that, if compromised, could cause injury to an individual, the court, or another organization.[17]	Information may be shared internally, and to third parties with a valid need to know.
Restricted	Medium	Applies to information or assets that, if compromised, could cause serious injury to an individual, the court, or another organization.[18]	Internal access is limited. External access subject to court-approved security clearance and NDA. Access and actions to be logged.
Secret	High	Applies to information or assets that, if compromised, could cause extremely grave injury to an individual, the court, or another organization.[19]	Access restricted to designated, cleared individuals with a need to know, and NDA. All access and actions to be logged.

[17] Corresponds to federal Protected A. See https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html.
[18] Corresponds to federal Protected B. See https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html.
[19] Corresponds to federal Protected C. See https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html.

TABLE 2: SAMPLE CONTROLS

Classification	At rest (storage)	In transit	Destruction
Public	May be stored on removable devices and public cloud service	No special controls.	No special deletion requirements.
Confidential	• All baseline Blueprint[20] security policies in place. • On premises, must be stored on the court's network with folder-based access controls (and backed up). • May be stored on a court-approved public cloud service. • May be stored on removable devices only if encrypted with court-approved tools. • Technical controls at this level will be based on assured, commercially available products and services, without need for any customization. • Information at rest will be protected at rest by default. Data must only be transmitted via a secure network. • Data traversing an untrusted (insecure) network must incorporate industry standard cryptography.	Only use approved court email, text and other communication platforms.	Information should be purged using industry standard tools.
Restricted	• Enhanced Blueprint[21] security policies in place. • May be stored on a court-approved public cloud service. • Access requires multi-factor authentication • May be stored on removable devices only if encrypted with court-approved tools.	Information must be encrypted with court-approved tools.	Information should be purged using industry standard tools.
Secret	• Requires the highest level of security controls reasonably available. • All access to be logged and tracked (subject to the Monitoring Guidelines).[22]	Not to be transmitted by email or any means over public networks.	Information must be irretrievably purged; storage devices may need to be physically

[20] Courts should have reference to the Blueprint for details on access control, physical security, and other controls.
[21] Courts should have reference to the Blueprint for details on access control, physical security, and other controls.
[22] Reproduced in the Blueprint.

Classification	At rest (storage)	In transit	Destruction
	• May not be stored on removable devices. • Not suitable for hosting on a public cloud service. • Data stores should be disconnected from the public internet. • Electronic files and/or data must be stored on a court shared directory or stationary device (i.e., desktop computer or server) with controlled physical access and role based logical access controls. • Electronic files and/or data must be encrypted when stored on portable or insecure devices. • Confidential or sensitive information shared with third parties must use file-based encryption. • Portable or insecure devices must be stored in a secure location when not in use.	Exchanged only via appropriately secured mechanisms. This will involve use of appropriately accredited shared services with high-grade encryption. Information will only be shared with designated users.	destroyed. Data and media must be degaussed (magnetically wiped) or rendered unreadable by other means. Devices may be physically destroyed.

TABLE 3: MARKING CLASSIFIED INFORMATION

The days of the rubber stamp are numbered, so to speak, as are the days of manila envelopes and wax seals. Digital information is not always in the form of a word-processed document to which headers and footers can be readily applied. This table provides some sample methods of marking digital information. Any method used must be appropriate to the format of the asset and must make it clear to the end-user that the information has been classified.

Format	Marking
Email or text message	Insert label banner in subject line. If not possible, insert at the top of the body of the email or signature block.
Text or image file	Insert label in metadata, on all images, or in available in header, footer or watermark.
Database	Insert label in header, footer or watermark of reports generated, and in metadata for each record, field or report.
Audio	Insert audible classification information at the beginning of the file.
Video	Insert audible classification information at the beginning of the file. Insert visible classification label on every frame.

TABLE 4: EXAMPLES OF CLASSIFIED COURT INFORMATION

Please note that these listings are drawn from several public and internal resources as examples only and are neither definitive nor comprehensive. They are simply representative of the type of information that might appear on a court's classification framework.

Classification	Examples
Public	• Case listing history • Pleadings • Orders and reasons for judgment • Trial transcripts • List of judicial districts • Annual reports • Forms, rules and practice directions or notes • Names of judges and dates of appointment
Confidential	• Internal policies and directives • Scheduling of judicial officers and hearings • Professional development information • Staff meeting records (other than judicial administration) • Jury charges • Routine email and other communications • Court Record / Case File not subject to a sealing order
Restricted	• Draft judgments, rulings, endorsements • Final court judgments if subject to a publication ban • Digital recording of a closed proceeding • Research memoranda, judicial notes • Outstanding warrants, pardons • Agendas, note and minutes of meetings regarding judicial administration • Personnel administration information • Information concerning judges • Information obtained with judicial authorization (sealed documents, child/youth protection)

Classification	Examples
Secret	• Certain draft judgments • Personnel information of judicial officers • Applications for warrant for search and seizure, electronic surveillance, and corresponding documentation • Information concerning informers • Psychiatric assessments • Personal information of judges • Privileged documents • Information related to national security