Canadian Judicial Council
Conseil canadien de la magistrature

Model Policy for the Classification of Court Information

Second edition, September 2023

Prepared by Martin Felsky, PhD, JD

TABLE OF CONTENTS

TABLE OF CONTENTS **2**

BACKGROUND AND PURPOSE **3**

CLASSIFICATION IS ONLY PART OF ACCESS CONTROL 4

CHALLENGES **4**

JUDICIAL INDEPENDENCE **5**

POLICY STATEMENTS **7**

POLICY 1 – PURPOSE 7
Commentary 7
POLICY 2 – APPOINT A SENIOR COURT OFFICIAL 7
Commentary: 8
POLICY 3 – SCOPE 8
POLICY 4 – TRANSITION 8
POLICY 5 – INFORMATION ASSET REGISTER 9
Commentary 9
POLICY 6 – RISK ASSESSMENT 11
Commentary 11
POLICY 7 – CLASSIFICATION OF INFORMATION ASSETS 12
Public 12
Confidential 12
Restricted 12
Secret 13
Commentary 13
POLICY 8 – INFORMATION ALREADY CLASSIFIED 14
Commentary 14
POLICY 9 – DOWNGRADING CLASSIFICATIONS 14
Commentary 14
POLICY 10 – LABELING CLASSIFIED INFORMATION – BANNERS 15
Commentary 15
POLICY 11 – LABELING CLASSIFIED INFORMATION – BLOCK 16
Commentary 16
POLICY 12 – HANDLING CLASSIFIED ASSETS 16

GLOSSARY **17**

ANNEX 1: CLASSIFICATION GUIDE **18**

TABLE 1: MAP OF RISK AND ACCESS 18
TABLE 2: SAMPLE CONTROLS 19
TABLE 3: MARKING CLASSIFIED INFORMATION 21
TABLE 4: EXAMPLES OF CLASSIFIED COURT INFORMATION 22

BACKGROUND AND PURPOSE

This Model Policy follows upon the Council's 2013 initiatives concerning Court Information[1], including the *Blueprint for the Security of Court Information* (Blueprint)[2] and *Guidelines for Migration of Judicial Information to a Cloud Service Provider*. All courts, and the Council, recognized that the modern concept of "Court Information" was no longer merely a matter of administrative court records acquired or created intermittently, with limited customized content, and with practical obscurity arising from its documentary character.

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 audit and regulation of the life cycle of Court Information. It is recommended that courts also consider policies for the creation, capture, maintenance, retention and disposition of Court Information in conjunction with conceptual agreement on classification.

This second edition adheres closely to the first but has been prepared to better align with Council's views on the principles of information governance and judicial independence. Some editorial changes have also been made for clarification.

This Model Policy uses certain terms as defined in Council's *Model Definition of Judicial Information* (Model Definition)[3] and it should not be read to alter the distinctions made in the Blueprint. It elaborates on Blueprint Policy 16:

[1] Court Information is information that is received, collected, stored, used or produced by a court in relation to its mission (Model Definition).
[2] In French: *Plan directeur pour la sécurité de l'information judiciaire*.
[3] In French: *Définition modèle des renseignements de la magistrature*.

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 helps 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 Court Information.

CLASSIFICATION IS ONLY PART OF ACCESS CONTROL

The classification of an information asset guides users with respect to its safe handling and dissemination, but 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, non-disclosure agreements, and the individual's function or assigned work, which determines their need to know.

Classified information should be made available to a person only when the classification authority establishes that the person has a valid "need to know," such that access is necessary to the accomplishment of their official court duties.

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 individual users. 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.[4]

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.[5]

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. As part of its institutional independence, the judiciary has exclusive control over Judicial Information. Control includes the inherent authority to govern the access to, use, retention and disposition of Judicial Information. Control

[4] See Azure Information Protection

[5] 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.

is in this sense is divorced from the concepts of physical control, custody or possession,[6] which do not override the court's supervisory power over Judicial Information. Nothing in this Model Policy reduces or eliminates the need for appropriate segregation and protection of Judicial Information.

The judicial and executive branches administer Canadian courts jointly. For example, information in the Case File is the responsibility of both branches. Consultation, coordination and collaboration of efforts on the retention of Court Information are essential.

There is also a need to ensure that proper agreements are in place with the executive branch to ensure Court Information classification decisions are understood and respected by all who interact with the information.

British Columbia has developed a responsibility assignment matrix[7] which other courts may find helpful. It clarifies the different levels of participation involved where information governance matters are a joint responsibility. Below is an example borrowed from the British Columbia Court of Appeal:

Who is accountable? – The Chief Justice, Court of Appeal Registrar, and Deputy Attorney General have approval authority

Who is responsible? – Court of Appeal Records Officer (Archivist) or Court of Appeal Legal Counsel (and provide recommendations)

Who is consulted? – Court Services Branch, BC Government Records Service, The British Columbia Archives, The Royal British Columbia Museum

Who is informed? – Members of the Public, Superior Courts Judiciary Staff, Court Services Branch Staff

[6] This distinction is explained 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 court 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."

[7] Also called a RACI chart, which is an acronym for Responsible, Accountable, Consulted and Informed.

Consultation between the judiciary and the executive is required to manage the significant hard and soft costs related to information governance, including classification. There may be costs associated with staffing, software, and training that are not currently budgeted in many courts.

POLICY STATEMENTS

POLICY 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.

POLICY 2 – APPOINT A SENIOR COURT OFFICIAL

The court should consider appointing or designating a senior court official accountable to the court and responsible for implementing and enforcing this Policy. This role can be assigned, for example, to a judicial information technology security officer (JITSO), executive legal officer, or court records manager. The senior court official handles the administrative tasks associated with the implementation and administration of information governance policies, including classification. They periodically

update the Information Asset Register and ensure compliance through regular review and audit functions. Training on the handling of classified information must be provided regularly to all users.

COMMENTARY:

The classification-related duties of this senior official should include:

1. Implementing and administering the Policy;
2. Communicating internally the applicable rules and best practices, through individual interventions, newsletters or other methods;
3. Developing the IAR (see Policy 5) and classification procedures, and updating them periodically;
4. Training users and system administrators, and advising the court on information governance issues;
5. Auditing policy implementation to ensure compliance, and
6. Contributing to systems procurement activities to ensure that court systems are compatible with the needs of classification policy and procedures.

POLICY 3 – 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.

POLICY 4 – TRANSITION

This Policy (or Policy amendment) is effective upon its approval by the court.

POLICY 5 – INFORMATION ASSET REGISTER

The court must prepare and update an information asset register (IAR) that lists, briefly describes, and categorizes at a high level, all Court Information assets.

COMMENTARY

The IAR forms the basis not only for decisions about classification but is also the foundation of a threat and risk assessment, the retention scheduling of Court Information, and business continuity procedures. It is the first step to gaining control over Court Information. The IAR is not a standalone document but forms the core of an asset-based threat and risk assessment (see Policy 6), a retention schedule, and classification protocols. The list is compiled first, then modified for multiple purposes, and updated accordingly. A high-level inventory can serve to identify how information is created and used by the court and by individual groups and users. It can also support the efforts of the court to capture its information flows.

The descriptive elements of the IAR should be determined in accordance with the volume of information in the court, and the state of the court's transition from paper to digital. Key elements to consider for each asset would include:

1. Relevant category
2. Brief description including the asset's purpose and use
3. Date range
4. Individual responsible for ensuring the asset is handled and managed appropriately (with contact information)
5. Custodian (with contact information)
6. Users, including internal and external sharing relationships
7. Location (for example, cloud, on premise, database, repository)
8. Form (for example, paper, digital, other medium)
9. Type of access requests (including bulk access) that this asset might attract

10. Information sensitivity (for example, sealing orders, publication bans, copyright, privacy, confidentiality)

Large, inclusive groupings make sense for digital information, which is voluminous, 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, increasing the burden of management and compliance.

One challenge to any form of register is that as information flows through the court, its custodian, form and location may change. Rules around management, access and use that apply at different points in a record's lifecycle should be considered.

The IAR can group information assets by function, user group, purpose, or repository. To take one example, a court could divide its information assets into three broad categories corresponding to fundamental concepts as follows:

Concept	**Category**
Open Courts Principle	Case File[8], Court Record, docket
Shared responsibility (judicial and executive)	Court Operations Information[9], administrative and historical records
Judicial independence	Judicial Information

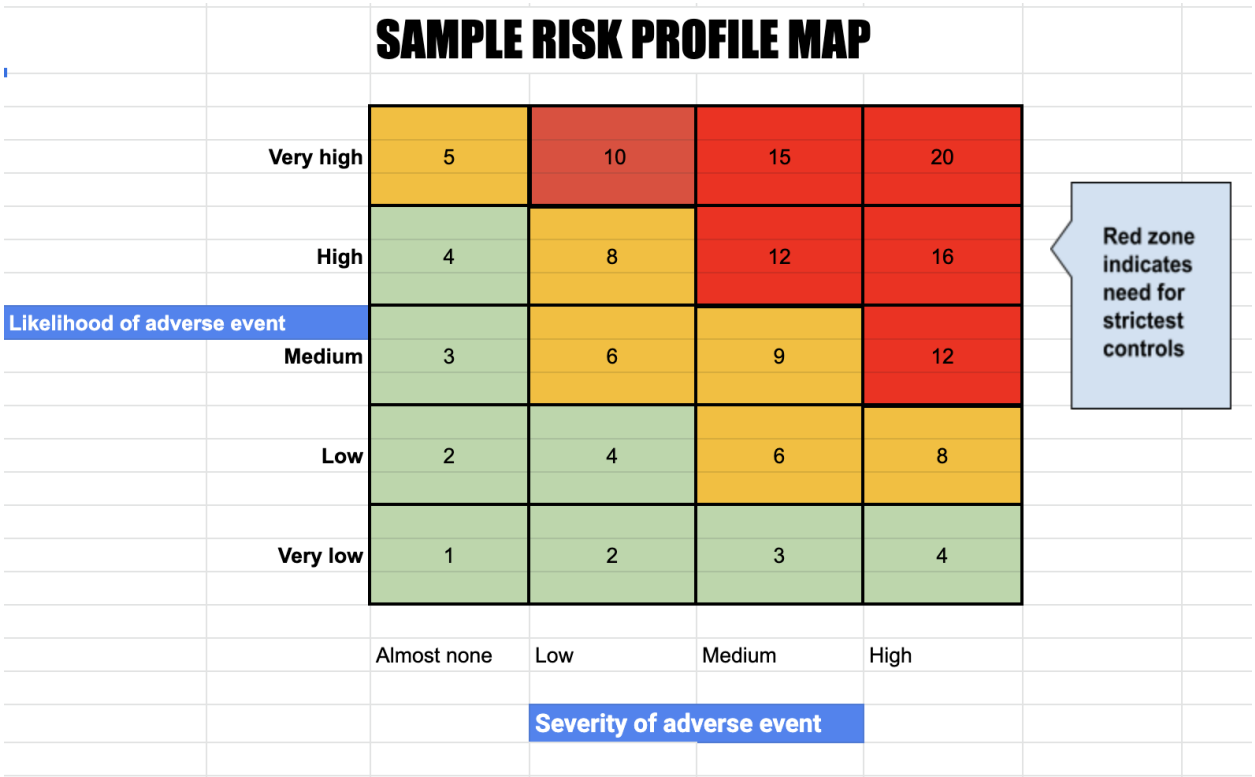
[8] "A Case File contains the Information that relates directly to a single court proceeding or to a number of related court proceedings that have all been assigned the same case file number. It includes the information that comprises the Court Record and any other Information that has been captured or placed in the Case File" (Model Definition).
[9] "Information related to the supervision, management and direction of matters necessary for the operation of the Court or other matters assigned to the Executive by law or agreement (such as a Memorandum of Understanding)" (Model Definition).

POLICY 6 – 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.

POLICY 7 – 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, could reasonably be expected to 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.

CONFIDENTIAL[11]

Applies to information that, if compromised, could reasonably be expected to 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. All such information should be clearly and conspicuously labeled "CONFIDENTIAL."

RESTRICTED

Applies to information that, if compromised, could reasonably be expected to cause serious injury to an individual, the court, or another organization.[13] Internal access is limited to individuals or organizations with a valid need to know. External access is subject to order of the court, legislation, court policy, court rules, and court-approved security clearance and non-disclosure agreement. Access and actions to be logged. 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."

[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.

SECRET

Applies to information that, if compromised, could reasonably be expected to cause extremely grave injury to an individual, the court, or another organization.[14] Access is restricted to designated, cleared individuals with a valid need to know, a non-disclosure agreement, or upon order of the court. All access and actions to be logged. 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 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.

One way to clarify the differences among the three non-public 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]

[14] Corresponds to Canada Protected C.
[15] See Quist, *Security Classification of Information*, volume 2, chapter 7.

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.

POLICY 8 – 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 those of the court.

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.

POLICY 9 – DOWNGRADING CLASSIFICATIONS

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.

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.

POLICY 10 – 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 should 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 a 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 from a drop-down menu.

POLICY 11 – 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. If used, 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 could contain:

> *Classified by*: Hon. Moreau, C.J.
> *Date*: 2023-11-25
> *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 minimum established controls.

POLICY 12 – 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 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.

GLOSSARY

Controller

The controller has supervisory power and control of information assets. As classification authorities, controllers define the overarching policies governing access, classification, use, retention and disposition 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.

Custodian

The individual or entity (such as an IT department or cloud services provider) with physical possession of Court Information assets. This role does not confer supervisory control.

Information asset

A grouping of records, defined as a unit so it can be managed efficiently. Use of the word "asset" in this Policy is not meant to imply ownership.

Originator

An originator is a classification authority of Court Information assets it has produced or received from a provider. Note that the controller and the originator can be the same person or entity. 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.

Provider

An external source that submits or transfers information to the court.

ANNEX 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	Information that, if compromised, could reasonably be expected to pose little or no risk to an individual, the court, or another organization.	Information may be made public.
Confidential	Low	Information that, if compromised, could reasonably be expected to cause injury to an individual, the court, or another organization.[16]	Internal and external access is limited to individuals or organizations with a valid need to know.
Restricted	Medium	Information that, if compromised, could reasonably be expected to cause serious injury to an individual, the court, or another organization.[17]	Internal access is limited to individuals or organizations with a valid need to know. External access is subject to order of the Court, legislation, Court policy, Court rules, and Court-approved security clearance and non-disclosure agreement (NDA). Access and actions to be logged. Restricted Court Information would be subject to more stringent treatment than Confidential, including special markings, encryption, and storage on designated devices.

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

Secret	High	Information that, if compromised, could reasonably be expected to cause extremely grave injury to an individual, the court, or another organization.[18]	Access is restricted to designated, cleared individuals with a valid need to know, and NDA, or upon order of the Court. All access and actions to be logged.

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[19] 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[20] security policies in place. • May be stored on a court-approved public cloud service. • Access requires multi-factor authentication.	Information must be encrypted with court-approved tools.	Information should be purged using industry standard tools.

[18] Corresponds to federal Protected C. See https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html.
[19] Courts should have reference to the Blueprint for details on access control, physical security, and other controls.
[20] Courts should have reference to the Blueprint for details on access control, physical security, and other controls.

Classification	At rest (storage)	In transit	Destruction
	• May be stored on removable devices only if encrypted with court-approved tools.		
Secret	• Requires the highest level of security controls reasonably available. • All access to be logged and tracked (subject to the Monitoring Guidelines)[21]. • 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.	Not to be transmitted by email or any means over public networks. 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.	Information must be irretrievably purged; storage devices may need to be physically destroyed. Data and media must be degaussed (magnetically wiped) or rendered unreadable by other means. Devices may be physically destroyed.

[21] Reproduced in the Blueprint.

TABLE 3: MARKING CLASSIFIED INFORMATION

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

Classification	Examples
	• Personnel administration information • Information concerning judges • Information obtained with judicial authorization (sealed documents, child/youth protection)
Secret	• Certain draft judgments • Personnel information of judicial officers • Applications for warrant for search and seizure, electronic surveillance, and corresponding documentation • Information concerning informants • Psychiatric assessments • Personal information of judges • Privileged documents • Information related to national security