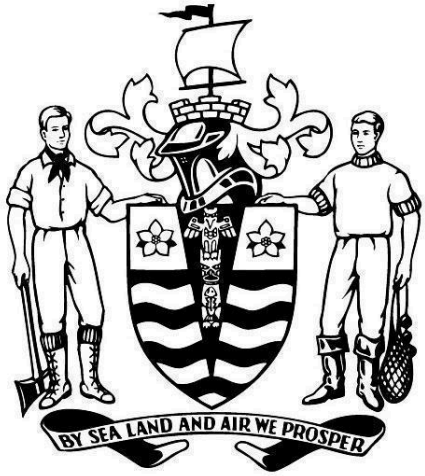
CITY OF VANCOUVER
BRITISH COLUMBIA



C.B 133

This by-law is printed under and by authority of the Council of the City of Vancouver

January 18, 2024

TABLE OF CONTENTS

C.B 133

Security of Information Act

The Council of the City of Vancouver, in open meeting assembled, enacts as follows:

INTERPRETATION

Short title

1. This by-law may be cited as the Security of Information Act or as the Security of Information (Revised) Act.

Definitions

2. In this by-law, unless the context otherwise requires–

"sensitivity" or "sensitive" means relating to classification or protection or, in relation to information or assets, the characteristic of being classified or protected;

"sensitive information" means information that is classified or protected;

"sensitivity level" means the precise level of classification or protection;

"tactical" means relating to–

the Emergency Response Team of either the Vancouver Police Department or Royal Canadian Mounted Police, or

the Protective Operations Unit of the British Columbia Sheriff Service;

"defence" means relating to the Canadian Armed Forces or Department of National Defence;

"armed forces" means the Canadian Armed Forces;

"intelligence" means relating to the Vancouver Police Department's Criminal Intelligence Unit, British Columbia Sheriff Service' Special Investigations Division, or an intelligence capability of the Canadian Armed Forces;

"official" means an employee of a government organisation;

"communicate" includes to make available;

"Mayor" includes the Acting Mayor;

"compromised", in relation to information or assets, means the unauthorised access, loss, or irrecoverable modification or destruction;

"release", in relation to sensitive information or assets, means the removal of any sensitivity level by an authorised official, so that the information or asset is no-longer subject to classification or protection.

3. For the purposes of Schedule C, "marking" means something clearly stating or referring to the precise level of sensitivity in a place where a reasonable person who would be authorised to access the information would automatically find it and understand it as being a sensitivity marking at that precise level.

CLASSIFICATION AND PROTECTION

Issue, modification and release of classification or protection

4. An official (the "authorising official") designated in Schedule A may authorise for the classification, protection, modification of sensitivity level, or release of classification or protection of information or assets where said information or asset is relevant to the official's organisation or work.

5. An official (the "authorising official") designated in Schedule B may authorise for the protection, modification of protection level, or release of protection of information or assets where said information or asset is relevant to the official's organisation or work.

6. The authorising official must have probable cause that the classification or protection is appropriate under this by-law for the classification or protection to carry force.

7. References in sections 4 and 5 to "authorise" may include authorisation for a class of information to be classified or protected (for example, completed web form submissions or automatically generated report documents) even if the authorising official does not have sight of these prior to the classification or protection taking effect so long as the authorising official has genuine reason to believe that most information falling within the class would qualify for the decided sensitivity level.

8. A classification or protection is null unless it carries force under this by-law.

Levels of classification

9. Top Secret, the highest level of classification, applies to information or assets which, if compromised, could cause exceptionally grave injury to the national interest. Further, Top Secret is only to be used on information or assets which, if compromised, could cause exceptionally grave, long-term, or systemic impairment or damage to–

(a) security or prosperity;

(b) relations with friendly nations;

(c) the ability to address (deter, respond to, investigate, or prosecute) serious or organised crime, espionage, sabotage, terrorism, or other actions which undermine security or prosperity;

(d) the effectiveness of or public confidence in the armed forces and intelligence services; or

(e) the social, political, and economic security and stability of British Columbia and of friendly states

or information or assets that would be expected to raise international tension if compromised.

10. Secret, the middle level of classification, applies to information or assets which, if compromised, could cause serious injury to the national interest. Further, Secret is only to be used on information or assets which, if compromised, could–

(a) cause serious injury to security or prosperity;

(b) cause widespread threat to life;

(c) majorly impair the ability to address serious or organised crime, espionage, sabotage, terrorism, or other activities which undermine democracy, security or prosperity;

(d) undermine or impair international relations, trade, or diplomatic efforts or negotiations;

(e) undermine or impair the effectiveness of or public confidence in the armed forces and intelligence services;

(f) undermine the social, political, and economic security and stability of British Columbia and of friendly states; or

(g) raise international tension.

11. Confidential, the lowest level of classification, applies to information or assets which, if compromised, could cause injury to the national interest.

Levels of protection

12. Protected C, the highest level of protection, applies to information or assets which, if compromised, could cause exceptionally grave injury to the public interest or any information which relates to the national interest. When information is protected owing to risk of injury to the public interest, Protected C is only to be used on information or assets which, if compromised, could–

(a) unduly cause major or systemic impairment to the reputation or effectiveness of a government organisation and the information or asset in question is not an operations procedure, policy, handbook, or general chat room; or

(b) undermine or cause impairment to an ongoing criminal or administrative investigation.

13. Protected B, the middle level of protection, applies to information or assets which, if compromised, could cause serious injury to the public interest.

14. Protected A, the lowest level of protection, applies to information or assets which, if compromised, could cause injury to the public interest.

Additional context

15. Information is “unclassified” if it is not actively classified or protected.

16. Information is “declassified” if it was previously classified or protected but no-longer is.

17. Information which is unclassified or declassified is not necessarily public information.

18. Classified and protected are separate schemes of sensitivity relating to different interests. However, for reference use only–

Protected A has no equivalent in the classification scheme;

Protected B is generally slightly less than Confidential;

Protected C is generally equivalent to Confidential or slightly less than Secret; and

Top Secret has no equivalent in the protection scheme.

Meaning of interest

19. The following is considered to be in the national interest:

(a) The success and efficiency of ongoing tactical operations.

(b) Maintaining the confidentiality of the procedures, policies, handbooks, training curricula, and operational communications of tactical teams, intelligence services, and the armed forces.

(c) The maintenance of international relations, including the reputations of British Columbia and friendly states.

(d) The success of diplomatic efforts and trade negotiations.

(e) The success, efficiency, and discretion of the armed forces and intelligence services.

(f) The protection of sensitive and strategic facilities.

(g) The secrecy and effectiveness of defence and intelligence capabilities or strategic advantages.

(h) For the intelligence services to ensure the continued success of and protect the identities of active and former confidential human intelligence sources, agents or other clandestine actors, who–

(1) provide information which relates to threats that could compromise or undermine the national interest; or

(2) engage in subterfuge against persons or groups which seek to compromise or undermine the national interest.

(i) The continued ability to address serious or organised crime, espionage, sabotage, or terrorism.

(j) For government organisations to be able to effectively plan for serious incidents which could compromise or undermine the national interest.

(k) The continued security and prosperity of British Columbia and of friendly states.

(l) The maintenance of the social, political, and economic security and stability of British Columbia and of friendly states.

(m) The maintenance of and protection from threats to democracy.

(n) The continued function of and protection from threats to critical infrastructure.

(o) The continued integrity of and public confidence in the armed forces and intelligence services, including the effective and confidential investigation of misconduct or indiscretions by employees, agents, partners, and contractors of the aforementioned.

(p) Maintaining the confidentiality of any information provided under terms of confidence from a foreign state or international organisation.

20. The following is continued to be in the public interest:

(a) Maintaining the confidentiality of law enforcement procedures, policies, handbooks, training curricula, recruitment systems, and communications.

(b) The ability of law enforcement to successfully and efficiently address crime.

(c) The protection of key figures from physical harm or threat.

(d) Maintaining the due and fair course of justice.

(e) The detention of prisoners and prevention of either escape from lawful custody or breach of a prison.

(f) The protection of individuals, organisations, and governments from physical, reputational, psychological, or financial harm.

(g) The protection of rights and freedoms.

(h) The successful and efficient development and delivery of government policy.

(i) The protection of the identities of active and former human intelligence sources and anonymous complainants or witnesses.

(j) For government organisations to be able to effectively plan for serious incidents which could compromise or undermine the public interest.

21. Anything which relates to or is in the national interest is also seen as relating to or being in the public interest.

Marking of sensitive information

22. Sensitive information must be clearly marked as outlined in Schedule C for the classification or protection to carry force.

23. Where it is not possible or practical to mark sensitive information, the authorising official must be fully aware of this and must reconsider the classification or protection.

24. Where it is not possible to mark sensitive information and the authorising official has decided to continue with classification or protection, the classification or protection carries force. However, any reasonable or expected steps must be taken to ensure persons who come across the information are plausibly aware of its sensitivity.

25. Sensitive assets which are not information (such as facilities or radio channels) do not need to be marked and there is not necessarily an expectation to ensure persons who come across the asset are aware of its sensitivity.

26. Good faith errors in marking or deciding a sensitivity level made unknowingly does not void the classification or protection. However, a relevant authorising official made aware of an error must correct it or notify another relevant authorising official as soon as practical for the sensitivity level to continue carrying force.

Regulation on sensitive information

27. The head of a government organisation or their principal deputy may set regulations for their organisation relating to classification or protection, for example narrowing (but not expanding) criteria or implementing requirements or restrictions on the sharing of sensitive information.

(a) The Mayor may set regulations in relation to this section but relating either to all or specific government organisation(s). Regulations set by the Mayor in relation to this subsection may not be countermanded or contradicted by other regulations set by the head of a government organisation or their principal deputy.

Authorised sharing or distribution of sensitive information

28. Relevant authorised officials may, within any applicable regulations set in accordance with this by-law, authorise any person to access sensitive information and may authorise their subordinates to do the same subject to any conditions they set.

29. Any sharing of classified information is done exclusively under terms of confidence. All persons to whom classified information is provided have a lifelong duty of secrecy to the Crown.

Internationally classified information

30. Any information, document or other asset or article which was obtained from a foreign state or international organisation and provided under terms of confidence may, where the Mayor approves the foreign state or international organisation for this section and a relevant authorising official declares for the precise information, asset, article, class, bulk data source, or similar, enjoy classification under this by-law without needing to be marked under Schedule C. The relevant authorising official(s) will decide the precise classification level for each type of information.

31. A relevant authorising official may release a classification made under section 30. The Mayor un-recognising a foreign state for the purposes of section 30 voids all classifications made under it unless a relevant authorising official reclassifies or protects the material.

Classification or protection of bulk data

32. Bulk data means any type of information set which contains a large amount of information, of which some but not all may qualify for classification or protection. Bulk data includes, but is not limited to, Discord channels and very large databases.

33. Bulk data may be classified or protected as usual providing the relevant authorising official has suitable cause, under this by-law, that the sensitivity level is appropriate for the intended purpose and typical content of the bulk data source. Entries created within a bulk data source (records, messages, etc.) are viewed as derivative information of the bulk data source.

Classification or protection of facilities

34. Facilities may be subject to classification or protection where the authorising official has probable cause to believe that the facility relates to the relevant interests and that there is a need to control information pertaining to the facility.

35. Photographs (screenshots), video (recordings), or other information obtained by way of being inside of a sensitive facility is derivative information and therefore sensitive at the same level as the facility unless the sensitivity level is modified or released.

Information derivative of sensitive information

36. Information that is derivative of sensitive information automatically retains that original sensitivity level without necessarily needing to be marked. For example, a message sent in a Protected B Discord text channel is automatically Protected B even if that message does not necessarily qualify for protection under this by-law. Similarly, a conversation between two officials where they paraphrase Confidential information is – insofar as the conversation is derivative from the classified information – classified as Confidential.

37. Duplicate information, for example a screenshot containing no sensitive information sent by the creator of the image in both an unclassified and Top Secret channel, can be seen as holding dual sensitivity as those who come by the message or the information within it from the Top Secret channel would be mishandling information if they shared it without authorisation unless they had also came by it from the unclassified channel prior to or at the time of the sharing. Those who came by the message from the unclassified channel would not be mishandling information by sharing the message.

38. A relevant authorising official may modify or release the sensitivity level of derivative information without also modifying the sensitivity level of the original (source or parent) sensitive information.

39. It is at the discretion of the relevant authorising official if the modification of sensitivity level (including release of classification or protection) of the original sensitive information affects derivative information. This may be decided on a case-by-case basis, for example, the release of classification on a document template, of which some completed documents may still require classification.

Protection of sensitive information

40. If officials become aware that information is or could have been compromised, the head of a relevant government organisation or their principal deputy must be notified as soon as possible.

41. An authorised official who knowingly or recklessly classifies or protects information in a fashion which disregards this by-law may be redeployed or dismissed from their position or employment without the employer committing a violation of rights.

42. Where an employee is within a job that requires routine access to information which is classified or Protected C and there is probable cause that the employee has or intends to mishandle information they obtain by way of their job, the employee may be redeployed or dismissed from their position or employment without the employer committing a violation of rights.

INTERACTION WITH JUDICIAL SYSTEM

Use of sensitive information as evidence

43. Information which is classified as Top Secret shall not be admitted or used as evidence in any administrative, employment, civil matter or other legal proceeding without the written consent of the head of a relevant government organisation or their principal deputy or the Mayor.

> (a) This section does not apply in a criminal proceeding if that evidence is exculpatory and there is no alternative evidence which is not classified as Top Secret.

(b) A witness shall be allowed to refuse to answer a question, if answering said question would cause them to communicate or otherwise compromise or mishandle Top Secret information, without the witness suffering any adverse action.

44. The head of a government organisation or their principal deputy or the Mayor may issue an order for Secret or Top Secret information to be withheld in a response to a subpoena or other request for information. No person can be subject to any adverse action – civil, criminal, or administrative – because of compliance with such an order or because of the issuance of such an order.

(a) An order under this section may only be issued when it is evident to the official issuing the order that the disclosure of the information would cause the national interest to be gravely harmed and such harm is not justifiable or proportionate compared to the aims of disclosure.

45. All reasonable steps must be taken by the relevant parties to ensure that a relevant authorising official is notified in the event that any sensitive information is to be admitted or used or intended to be admitted or used as evidence in a warrant, other court proceeding, or administrative or employment matter.

46. Any admitted evidence which is classified or Protected C can only be heard or substantively referred to in a closed or sealed hearing of a proceeding. Those present at the proceeding must be aware of the sensitivity of the information.

(a) A witness, speaking in open court, shall be allowed to refuse to answer a question, if answering said question would cause them to communicate or otherwise compromise or mishandle sensitive information, without the witness suffering any adverse action.

(b) A witness, speaking in closed court, and who references or divulges sensitive information, must communicate in their testimony the sensitivity of said sensitive information.

47. Parties who wish to present information in court which is sensitive must inform the judge prior. The evidence will be considered for admission only in a sealed or closed hearing. If the information is successfully admitted and is Protected A or Protected B then the facsimile admitted shall be released from protection; the case may then continue in open court.

48. Information classified under section 30 can only be admitted or used as evidence in any administrative, employment, civil matter or other legal proceeding with the consent of the originating foreign state or international organisation.

(a) For greater clarity, this section does not extend to information which was formerly classified under section 30.

Presumption

49. A classification or protection decision is presumed to have been made under probable cause and presumed to meet the requirements for the classification or protection and any special requirements for the precise sensitivity level unless preponderance of evidence confirms otherwise.

50. Where there is doubt about the probable cause of a classification or protection, the authorising official is granted a presumption of good faith.

Extraterritorial application

51. A person who commits, outside of British Columbia, an act that if it were committed in British Columbia would be offence under this by-law or an offence of Espionage under C.B. 128 is deemed to have committed it in British Columbia if the person is–

(a) a resident of British Columbia;

(b) a person who owes allegiance to His Majesty in right of Canada;

(c) a person who is engaged by a foreign state to perform functions within British Columbia, including – but not limited to – a diplomat under C.B. 111 (Diplomacy Act 2023);

(d) a person otherwise subject to the judicial system of British Columbia; or

(e) a person who, after the time the act is alleged to have been committed, is liable under subsections (a-d).

52. For the purposes of section 5 of C.B. 111, a diplomat who, if not for diplomatic immunity, would commit an offence under this by-law or an offence of Espionage under C.B. 128 is deemed to be undermining the government of the City of Vancouver and therefore has their diplomatic immunity revoked.

Limitation

53. The limitation period applied by section 28 of C.B. 116 does not apply to an offence under this by-law or an offence of Espionage under C.B. 128.

54. Prosecution for offences under this by-law or an offence of Espionage under C.B. 128 must commence within 180 days of the offence, unless the offender is not liable per section 51(a–d).

55. For offenders not liable per section 51(a–d) at the time of their offence but who are later liable to an offence by virtue of section 51(e), prosecution for offences under this by-law or an offence of Espionage under C.B. 128 must commence within 180 days of the offender becoming liable.

Prosecution and warrant

56. No person may be arrested for an offence under this by-law except when such an arrest has been authorised and ordered by a warrant.

57. No prosecution may be commenced for an offence under this by-law or for an offence of Espionage under C.B. 128 without the consent of the Attorney General or Mayor.

58. No warrant may be issued for an offence under this by-law or for an offence of Espionage under C.B. 128 without the consent of–

(a) the Attorney General or Mayor;

(b) the Commander or Deputy Commander of the 3rd Canadian Division;

(c) a service member (within the meaning of C.B. 128) designated for the purposes of this section by the Commander or Deputy Commander of the 3rd Canadian Division; or

(d) the director of the Special Investigations Division or of the Criminal Intelligence Unit or one of their superiors.

OFFENCES RELATING TO SENSITIVE INFORMATION

Mishandling information

59. Every person mishandles information who, having in his possession or control any photograph, record, document, article, note, or other information or asset that is actively classified or protected under this by-law–

(a) communicates it or agrees to communicate it, directly or indirectly, to a person not authorised to receive said information;

(b) reproduces, shares, or distributes it, or agrees to reproduce, share or distribute it, without lawful authority;

(c) causes it to be or agrees to cause it to be communicated to a person not authorised to receive said information; or

(d) causes it to be or agrees to cause it to be irrecoverably altered or destroyed without authorisation.

60. It is a defence for a person accused of mishandling information to demonstrate that they were participating in a closed or sealed court proceeding and genuinely believed their actions were lawful.

61. Every person who mishandles classified or Protected C information, where–

(a) the mishandling is mostly attributed to recklessness;

(b) the mishandling was wilful; or

(c) the information mishandled was classified at the Top Secret level

is guilty of an indictable offence, aggravated mishandling information and liable to the punishment prescribed in Schedule A of C.B. 116.

62. Schedule A of C.B. 116 is amended to reflect the punishment for aggravated mishandling information as 900 seconds imprisonment.

63. Every person who mishandles information where–

(a) the information was Protected A or Protected B and either the mishandling is mostly attributed to recklessness or the mishandling was wilful; or

(b) the information was classified or Protected C and the mishandling is mostly attributed to negligence or a lack of due diligence

is guilty of a hybrid offence, mishandling information and is liable to the punishment prescribed in Schedule B of C.B. 116.

64. Schedule B of C.B. 116 is amended to reflect the punishment for mishandling information as 660 seconds imprisonment or a 3200 dollar fine.

65. Every person who otherwise mishandles information is guilty of a hybrid offence, otherwise mishandling information and liable to the punishment prescribed in Schedule B of C.B. 116.

66. Schedule B of C.B. 116 is amended to reflect the punishment for otherwise mishandling information as 420 seconds imprisonment or a 2500 dollar fine.

Wrongful possession of information

67. Every person wrongfully possess information who has in his possession or control any photograph, record, document, article, note, or other information or asset that–

(a) is actively classified or Protected C under this by-law;

(b) the person is not or was but is no-longer authorised to possess, see, or retain said information; and

(c) the person knows, ought to know, believes, or has reasonable grounds to believe that the person is not authorised to possess, see, or retain said information.

68. A person does not wrongfully possess information who, at the earliest opportunity after coming into wrongful possession of information–

(a) returns the information;

(b) complies with any reasonable requests made by a relevant authorising official, for example to destroy any copies of the information;

(c) does not retain access to the information and does not reproduce it; and

(d) for information not relating to defence or intelligence, notifies the Attorney General or Mayor;

(e) for information relating to defence including defence intelligence, notifies the Commander of the 3rd Canadian Division or their principal deputy; or

(f) for information relating to security intelligence, notifies the director of the Criminal Intelligence Unit or of the Special Investigations Division or one of their superiors.

69. A person who wrongfully possesses information that is classified as Secret or Top Secret is guilty of an indictable offence, aggravated wrongful possession of information, and liable to the punishment prescribed in Schedule A of C.B. 116.

70. Schedule A of C.B. 116 is amended to reflect the punishment for aggravated wrongful possession of information as 600 seconds imprisonment.

71. A person who wrongfully possesses information which is classified as Confidential or Protected C is guilty of a hybrid offence, wrongful possession of information and liable to the punishment prescribed in Schedule B of C.B. 116.

72. Schedule B of C.B. 116 is amended to reflect the punishment for wrongful possession of information as 360 seconds imprisonment or a 1800 dollar fine.

ENACTMENT

Force and extent

73. This by-law is to come into force and take effect fifteen days after the date of its enactment.

74. No aspect of this by-law prohibits any organisation from enforcing non-disclosure agreements or establishing their own protective marking schemes for unclassified information.

75. No aspect of this by-law prohibits a government organisation from implementing codewords, descriptors, caveats, or handling instructions in addition to the classification and protection schemes.

Repeal

76. This by-law repeals C.B. 23 (Security of Information Act).

77. This by-law repeals sections 129 and 130 of C.B. 116 (Offences By-law).

Amendment

78. In C.B. 128 (Defence By-law), create section 23A–

> No person may be arrested for espionage except when such an arrest has been authorised and ordered by a warrant.

79. In section 23(4) of C.B. 128, substitute “or conspires” with “conspires, prepares, or agrees”.

80. In C.B. 116, create section 31.3–

> No person may be arrested for sabotage except when such an arrest has been authorised and ordered by a warrant.

Existing sensitive information

81. Protections and classifications made under C.B. 23 carry force at the original level as though they were implemented under this by-law, even if the criteria set under this by-law is not met, provided the classification or protection was appropriate and lawful under C.B. 23.

> (a) Protections and classifications which remain in force under this section may not be modified. Classification or protections made under C.B. 23 may be reissued under this by-law.
>
> (b) Protections and classifications made under C.B. 23 may be released (in C.B. 23 terms, declassified) by an appropriate authorised person under this by-law.
>
> (c) Sections 43, 44, 46, 47 and 48 do not apply to classifications or protections made under C.B. 23.

82. No later than five days after the coming into force of this by-law, the heads of all government organisations must review (or direct their subordinates to review) any classifications or protections made under C.B. 23.

> (a) This review is to continue indefinitely until the head of the government organisation is satisfied that no classifications or protections made under C.B. 23 remain in their organisation.
>
> (b) Information is considered exempt from review for the purposes of this section if–
>
> > (1) it is not possible to alter the information and therefore the marking could not be updated if the classification or protection is reissued;
> >
> > (2) it would cause harm to the national interest to reissue the classification or protection; or

(3) it would cause grave and exceptional harm to the public interest to reissue the classification or protection.

(c) As part of the review, the head of the government organisation (or their directed subordinates) must evaluate–

For classified information, if the classification is in the national interest

For protected information, if the protection is in the public interest

and either reissue the classification or protection under this by-law (if in the affirmative) or otherwise release the information of classification or protection unless considered exempt from review.

SCHEDULE A

Authorised positions for classification, protection, and release thereof

Relevant government organisation	Description of position(s)
N/A – relevant to all government organisations	The Mayor of the City of Vancouver
Executive Office of the Mayor	The Deputy Mayor
	The Chief of Staff
Office of Foreign Affairs	The Director
Ministry of Justice	The Attorney General
3rd Canadian Division / Canadian Armed Forces / Department of National Defence	The Commander and Deputy Commander
	The Division Sergeant Major
	The commanders of the Royal Westminster Regiment, 1 Military Police Regiment, and Canadian Special Operations Regiment
Royal Canadian Mounted Police	The Commissioner
	The Deputy and Assistant Commissioner
	The director of special operations
	The director of the Emergency Response Team
British Columbia Sheriff Service	The Chief and Deputy Chief Sheriff
	The Chief Superintendent
	The director of special operations
	The directors of the Protective Operations Unit and Special Investigations Division
Vancouver Police Department	The Chief Constable
	The Deputy Chief Constable
	The director of special operations
	The directors of the Emergency Response Team and Criminal Intelligence Unit

SCHEDULE B

Authorised positions for protection and release thereof

Relevant government organisation	Description of position(s)
Parks Canada	The Chief and Deputy Chief Park Warden
Correctional Service Canada	The Warden and Deputy Warden
Ministry of Justice	The Deputy Attorney General

SCHEDULE C

Requirements for marking classified or protected material

Type of information	Requirements (at least one must be met)
Text document	(1) Marking included in every page of document (2) Marking included in first page of document (3) Marking included in file name of document
Spreadsheet document	(1) Marking included in file name of document (2) Marking included in every page/tab/sheet of document
Web form (e.g. survey)	(1) Marking included in name or title of web form (2) Marking visible on or prior to the first data entry element (excluding email address) of webform (3) Marking included prominently on either the first or the final page of webform (4) Marking included in 'description' of webform
File or data storage system (e.g. folder)	(1) Marking included in name or title of storage system (2) Marking included in a file named INDEX or README
Trello workspace	(1) Marking included in name or description of workspace
Trello board	(1) Marking included in name or description of board (2) Marking included in the name of a card on the leftmost or second leftmost list within the board

Discord invite link	(1) Marking included in the name of the server or group DM the invite link leads to, provided the invite link is active
Discord server	(1) Marking included in the name of the server (2) Marking included in a channel accessible to all members of the server (a) The requirement for (2) may be achieved using multiple channels provided all members of the server may view at least one channel including the marking
Discord text channel, including group DM and forum (marking also applies to all sub-channels such as threads)	(1) Marking included in the topic or post guidelines of the channel (2) Marking included in the name of the channel (3) Marking included in a pinned message within the channel
Discord voice channel (marking also applies to all text channels embedded within the voice channel)	(1) Marking included in the name of the channel (2) Marking included in the topic or status of the channel
Individual Discord message	(1) Marking included at the earliest point possible (2) Marking included in the author, title or footer of embed, provided the message is entirely comprised of a singular ‘rich’ embed
Markdown or other text file	(1) Marking included at the earliest point possible
Git repository	(1) Marking included in a file named INDEX or README

ENACTED by Council this #st/nd/th day of Month, Year

Signed "FoxyTheWereFox"

Sponsor

Signed "Shibe_R6"

Co-Sponsor

Signed "Automationeer"

Author

Signed "Name"

Mayor