

Video Surveillance

MC Approval: *December 2001*
Policy Responsibility: Director, Corp. Comm. & PA
Contact name: FOI Coordinator

Purpose

- To ensure that all applications of video surveillance in BCBC-administered buildings are authorized and are compliant with the Freedom of Information and Protection of Privacy Act (FOI/POP Act); and,
- To establish standards for security and privacy.

Policy

1. Video surveillance shall be used only for the protection of the safety of employees, customer occupants, and assets and property of BCBC and its clientele.
2. Video surveillance will not occur in staff lunchrooms, nor in areas where there is an expectation of privacy, e.g., washrooms, change rooms, etc. Note, cameras in correctional facility cells must have signage displayed advising of cameras.
3. Covert surveillance (i.e., hidden cameras without signage) should only be used when it is determined to be the only available option. See Item 2 under Application.
4. All areas subject to surveillance will be identified to those in the area by way of signage. See Appendix 1 for recommended wording. Roof-top cameras also require signage that is visible to the public.
5. Surveillance applications will be monitored by authorized personnel only.
6. Any records (videotapes, still photographs, digital images, etc.) produced by surveillance systems shall be kept in a secure, locked facility or manner and managed appropriately by the customer to protect legal obligations and evidentiary values.
7. Each video surveillance application will document procedures for achieving these principles and position(s) responsible (e.g., times that cameras are operational, where signage will be located, etc.). Note: One site is an application if all cameras are being used for the same purpose. If different cameras are being used for different purposes, then they are different applications.
8. "Dummy" (intentionally non-operational) cameras shall NOT employ signage indicating surveillance is taking place.

Application

1. This policy applies to all buildings owned, leased or administered by BCBC. If a building is occupied by BCBC, BCBC is considered the “customer” for the purposes of this policy.
2. This policy does not apply to surveillance activities of law enforcement agencies engaged in a lawful investigation. However, routine video surveillance in court or correctional facilities is subject to the same rules regarding privacy as any other public body. Each application, therefore, still requires that a privacy impact assessment be completed and that requirements of the FOI/POP Act have been addressed.

For covert surveillance, a detailed and comprehensive assessment must be conducted and authorized by a senior level of corporate management and the FOI Coordinator prior to the decision to implement. This is to ensure that it is the only available option and that benefits derived from the material obtained far outweigh the violation to the privacy rights of the subjects being observed.

3. Appropriate signage will be created and installed as part of BCBC’s usual customer service following a signed Request for Service form or minor client request. See Appendix 1 for suggested wording.
4. There are certain mandatory requirements that must be fulfilled prior to the installation of video surveillance. See Appendix 2 - Procedures for listed requirements.

Responsibility

- Customers requesting the installation of video surveillance will assume all responsibility for the justification, compliance and on-going administration of surveillance systems, including any recorded material produced. See Policy Items 5 through 7 for a specific listing of these customer responsibilities.
- Customers are responsible for designating a contact person to ensure compliance with this policy and related procedures. This person will be responsible for:
 - Communication with appropriate staff and employee representatives (i.e., Unions) will be the responsibility of the customer contact person.
 - Any training required for surveillance purposes will also be the responsibility of the customer.

Responsibility (continued)

- Prior to the installation of a surveillance system, BCBC's appropriate contact person shall be responsible for communicating this corporate policy to their customer.
- In support of their customers, BCBC, through district office staff, will assume responsibility for the installation and on-going maintenance for such systems, as negotiated with the customer, as they would for other tenant improvements. BCBC will ensure that all installations of video surveillance completed by BCBC will conform to this policy.
- The Director, Corporate Communications and Public Affairs, is responsible for review of the policy and any future revisions.
- The Vice President, Property Management, will be responsible for the application of this Policy.

Appendix 1

Video Surveillance Signage

Clearly visible signage, identifying the use of video surveillance cameras, must be installed in the building entrance and/or parking garage, and wherever else there are cameras.

Suggested wording:

This area is monitored by video camera.
For further information, please contact the Manager, Central
Services, 555-1234.

Each ministry/agency will designate a contact person for each application.

Appendix 2

Procedures

1. Completion and approval of a **Request for Services form**, which covers both surveillance equipment and installation as well as appropriate signage.
2. Approval from building owner (if other than BCBC).
3. Completion and approval of a **Privacy Impact Assessment form** by customer. See Appendix 3.

For your information and use, blank forms of the Privacy Impact Assessment are available at http://www.mser.gov.bc.ca/FOI_POP/Index.htm. (Select the Privacy Impact Assessment Process button.)

Appendix 3

PRIVACY IMPACT ASSESSMENT FORM

(revised November 1, 2001)

CONSULTATIONS WITH PRIVACY EXPERTS ON SPECIFIC QUESTIONS

Even though the revised PIA has been designed with a view to being completed, at least in part, by program staff, **there are a number of questions in the PIA where consultations with privacy experts are recommended if not required.** These questions have been designated with an asterisk in the margin.

(I) BASIC INFORMATION

1. Ministry/Public Body and Program Area.

2. Contact Position and/or Name, Telephone Number and E-Mail Address (this should be the name of the individual most qualified to respond to questions regarding the PIA).

3. Description of the Program/System/Legislation/Other (Initiative) being assessed. (Note here if the initiative does not collect, use or disclose personal information). If this is a change to an existing legislation, system or program, describe the current system or program and the proposed changes.

(II) DESCRIPTIVE INFORMATION

1. Describe the elements of personal information that will be collected, used or disclosed and the nature and sensitivity of the personal information.

2. Purpose/Objectives of the Initiative (if statutory, provide citation).

* 3. What are the potential impacts of this proposal? (Include privacy impacts in this description)

4. Provide details of any previous PIA or other form of personal information assessment done on this Initiative (in whole or in part).

5. Provide a description (either a narrative or flowchart) of the linkages and flows of personal information collected, used and/or disclosed.

(III) PERSONAL INFORMATION COLLECTION (Sections 26 and 27 of the *Freedom of Information and Protection of Privacy Act* (FOIPP Act))

1. Authorization for Collection:

No personal information may be collected by or for a public body unless authorized under the FOIPP Act (as covered by numbers i, ii, or iii below).

Definition: "Collect" means to bring or come together; assemble; accumulate; obtain (taxes, contributions, etc.) from a number of people; receive money.

- (i). Has the collection of personal information been specifically authorized by, or under, an Act? Yes ___ No ___

If Yes, please specify the name of the Act and relevant section.

- (ii). Has the personal information been collected for law enforcement purposes? Yes ___ No ___

Definition: "Law enforcement" means
(a) *policing, including criminal intelligence operations;*
(b) *investigations that lead or could lead to a penalty or sanction being imposed; or,*
(c) *proceedings that lead or could lead to a penalty or sanction being imposed.*

- * (iii). Is the personal information directly related to, and necessary for, an operating program or activity of the public body? Yes ___ No ___

If none of the above questions have been answered "Yes," your office does not have the authority under the FOIPP Act to collect the personal information in question. Please contact your Director/Manager of Information and Privacy (DMIP) for ministries or the position responsible for FOI and Privacy Coordination (FOIPP Coordinator) for other public bodies.

2. How will the personal information be collected?

A public body must collect personal information directly from the individual the information is about, with certain specific exceptions.

Direct Collection

(i). Will the personal information be collected directly from the individual that the information is about? Yes ___ No ___

If you are only collecting personal information directly as noted above, you will not need to do the next section on indirect collection.

Indirect Collection

If the personal information has not been collected directly from the individual it is about, check which of the following authorizes the indirect collection:

(i). Did the individual the information is about authorize another method of collection? _____

(ii). Has indirect collection been authorized by the Information and Privacy Commissioner? _____

(iii). Has indirect collection been authorized by another enactment? _____

Specify name of Act and relevant section(s).

(iv). Is the personal information being collected for the purpose of determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary? _____

(v). Is the personal information being collected for the purpose of a proceeding before a court or a judicial or quasi judicial tribunal? _____

(vi). Is the personal information being collected for the purpose of collecting a debt or fine or making a payment? _____

(vii). Is the personal information being collected for the purpose of law enforcement? _____

* (viii). Is a public body collecting personal information disclosed to it under sections 33 to 36 of the FOIPP Act? _____

Specify relevant section(s) or subsections that apply.

Additional details as required (e.g., explanation of method of collection).

If none of the above authorities have been checked, your office does not have the authority under the FOIPP Act to collect the personal information in question. Please contact your DMIP or FOIPP Coordinator.

3. Notification to collect information

A public body must not collect personal information from an individual without notifying them of the collection as outlined below.

- (i). Has the individual whose personal information is being collected, been informed of:
- | | | |
|--|-----------|----------|
| (a) the purpose for collection? | Yes _____ | No _____ |
| (b) the legal authority for collecting it? | Yes _____ | No _____ |
| (c) the contact information of the person who can answer questions regarding the collection? | Yes _____ | No _____ |

Notification is not required if the answer is "yes" to either of the following:

- (ii). Is the personal information about law Enforcement or anything referred to in Section 15(1) or (2) of the FOIPP Act? Yes _____ No _____
- (iii). Has the minister responsible for the FOIPP Act excused your public body from complying because it would:
- | | | |
|--|-----------|----------|
| (a) result in the collection of inaccurate information, or | | |
| (b) defeat the purpose or prejudice the use for which the personal information is collected? | Yes _____ | No _____ |

Additional details as required (e.g., method of notification).

If you have not provided the required notification as outlined in Section (i) above, please contact your DMIP or FOIPP Coordinator.

(IV) USE OF PERSONAL INFORMATION (Section 32 of the FOIPP Act)

Under the FOIPP Act, personal information held by public bodies may only be used for certain specified purposes as outlined below.

Definition: "use" of personal information means employing it to accomplish the public body's objectives; for example, to administer a program or activity, to provide a service or to determine someone's eligibility for a benefit or suitability for a job.

Definition: "consistent" means for the purposes for which the information was obtained or compiled if the use (a) has a reasonable and direct connection to that purpose, and (b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

The public body must check one or more of the authorities listed below.

- 1) Has the individual the personal information is about consented to the use? _____

Note: Supporting documentation must be on file.

- 2) Will the information be used only for the purpose for which it was obtained or compiled or for a use consistent with the original purpose? _____

Please provide details of the original purpose for which the personal information was obtained or compiled. Please also provide, if applicable, details of the consistent/secondary use.

- * 3) If the personal information was disclosed to the public body under sections 33 to 36, is the information being used for that same purpose? _____

Specify subsection(s) that are being applied.

If you have not checked one of the above, you do not have the authority to use the information. Please contact your DMIP or FOIPP Coordinator.

(V) DISCLOSURE OF PERSONAL INFORMATION (Sections 33, 35, 36 of the FOIPP Act)

A public body may disclose personal information only as authorized under the FOIPP Act (as noted below). It should be noted that section 33 of the FOIPP Act also authorizes the disclosure of personal information in responding to FOI requests.

Definition: "Disclose/disclosure" means to reveal, show, expose, provide copies of, sell, give or tell (personal or non-personal information or records).

1. Disclosure of Personal Information (Section 33)

Section 33 of the FOIPP Act provides the legislative authority to disclose personal information; i.e., personal information cannot be disclosed unless authorized by section 33.

Please check the main authorization(s) for disclosure below.

- (i). If the individual the information is about has identified the information and consented to its disclosure, _____
(Note: Supporting documentation must be on file)

- (ii). For the purpose for which it was obtained or compiled or for a use consistent with that purpose (see section 34), _____

Please provide details of the original purpose for which the personal information was obtained or compiled. Please also provide, if applicable, details of the consistent/secondary use.

- (iii). For the purpose of complying with an enactment of, or with a treaty, arrangement or agreement made under an enactment of, British Columbia or Canada, _____

Specify name of Act and relevant section(s).

(iv). For the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information, _____

(v). To an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister, _____

(vi). To the Attorney General for use in civil proceedings involving the government, _____

(vii). To the Attorney General or a person referred to in section 36 of the *Coroners Act*, for the purposes of that Act, _____

(viii). For the purpose of collecting a debt or fine owing by an individual to the government of British Columbia or to a public body, or making a payment owing by the government of British Columbia or by a public body to an individual, _____

(ix). To the auditor general or any other prescribed person or body for audit purposes, _____

(x). To a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem, _____

(xi). To a representative of the bargaining agent who has been authorized in writing by the employee whom the information is about, to make an inquiry, _____

(xii). To the British Columbia Archives and Records Service, or the archives of a public body, for archival purposes, _____

(xiii). To a public body or a law enforcement agency in Canada to assist in an investigation (i) undertaken with a view to a law enforcement proceeding, or (ii) from which a law enforcement proceeding is likely to result, _____

(xiv). If the public body is a law enforcement agency and the information is disclosed (i) to another law enforcement agency in Canada, or (ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority, _____

(xv). If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety and if notice of disclosure is mailed to the last known address of the individual the information is about, _____

(xvi). So that the next of kin or a friend of an injured, ill or deceased individual may be contacted. _____

Additional details as required.

If you have not checked any of the above authorizations for disclosure or require clarification, you should contact your DMIP or FOIPP Coordinator.

2. Systematic or Repetitious Disclosures/Exchanges

(i). Do the disclosures of personal information under section 33 occur on a regular basis? Yes ___ No ___

(ii). Has an Information Sharing Agreement been Completed for these disclosures/exchanges? Yes ___ No ___

(iii). Has information related to the Information Sharing Agreements(s) been entered into the Personal Information Directory? Yes ___ No ___

Personal information exchanges within a public body do not normally require an ISA if they are for a consistent purpose as defined under section 33(c) of the Act or are necessary for the performance of an employee of the public body under section 33 (f). However, depending on the nature and sensitivity of the personal information exchanged, the public body might choose to prepare an ISA or similar written statement of understanding.

3. Research or Statistical Purposes (under Section 35 of the FOIPP Act)

(i). Has a researcher requested access to personal information in an identifiable form for research purposes? Yes ___ No ___

If "yes", a research agreement that conforms to the criteria established in section 35(d) must be in place. Contact your DMIP or FOIPP Coordinator for assistance. Please note: research using personal information may only be conducted if it meets all of the terms of section 35.

4. Archival or Research Purposes (under Section 36 of the FOIPP Act)

The British Columbia Archives, or the archives of a public body, may disclose personal information for archival or historical purposes as authorized by Section 36.

Please check the authorization(s) for disclosure listed below.

* (i). the disclosure would not be an unreasonable invasion of personal privacy under Section 22. _____

(ii). the disclosure is for historical research and is in accordance with section 35 (research agreements) _____

(iii). the information is about someone who has been dead for 20 or more years. _____

(iv). the information is in a record that has been in existence for 100 or more years. _____

Additional details as required.

If you have not checked any of the above authorizations for disclosure or require clarification, you should contact your DMIP or FOIPP Coordinator.

(VI) ACCURACY AND CORRECTION OF PERSONAL INFORMATION (Sections 28 and 29 of the FOIPP Act)

If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must make every reasonable effort to ensure that the information is accurate and complete. An individual must also have the ability to access to, or have corrected or annotated their personal information or a period of one year after a decision has been made based upon the personal information.

- (i). Are there procedures in place to enable an individual to request/review a copy of their own personal information? Yes ___ No ___

- (ii). Are there procedures in place to correct or annotate an individual's personal information if requested including what source was used to up-date the file? Yes ___ No ___

- (iii). If personal information is corrected, are there procedures in place to notify other holders of this information? Yes ___ No ___

If yes, please provide the name of the policy and/or procedures, a contact person and phone number.

Additional details as required.

If any of the questions above have been answered "No", please contact your DMIP or FOIPP Coordinator for further clarification.

(VII) SECURITY ARRANGEMENTS FOR THE PROTECTION OF PERSONAL INFORMATION (Section 30 of the FOIPP Act)

Note: For PIAs related to new or existing systems, this section should be completed by the branch of the ministry responsible for systems maintenance and security and signed off, by this branch, in the Signatures section.

For PIAs that do not involve systems initiatives, this section should be completed by the Branch or DMIP/FOI Coordinator completing the PIA. In this case, the signature of the systems representative is not required.

A public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. G.M.O.P. Section 8.4.5 requires public bodies to conduct a Security Threat Risk Assessment for information systems.

Definition: "Reasonable security arrangements" are those which a fair, rational person would think were appropriate to the sensitivity of the information and to the medium in which it is stored, transmitted, handled, or transferred. A sliding scale of security arrangements is appropriate, depending on the sensitivity of the personal information that a public body handles.

1) Is there reasonable technical security in place to protect against unauthorized access or disclosure? Yes ___ No ___

Please explain.

2) Is there reasonable physical security in place to protect against unauthorized access or disclosure? Yes ___ No ___

Please explain.

3) Are there branch policies and procedures in place for the security of personal information during routine collection, use and disclosure of the information? Yes ___ No ___

If yes, please provide the name of the policy and/or procedures, a contact person and phone number.

4) Have user access profiles been assigned on a need to know basis? Yes ___ No ___

5) Do controls and procedures exist for the authority to add, change, or delete personal information? Yes ___ No ___

6) Does your system security include an **on-going** audit process that can track use of the system (e.g., when and who accessed and updated the system)? Yes ___ No ___

Please explain the audit process and indicate how frequently audits are undertaken and under what circumstances.

Does the audit identify inappropriate accesses to the system? Yes ___ No ___

Additional details as required.

If any of the questions above have been answered "No", please contact your DMIP or FOIPP Coordinator.

(VIII) RETENTION OF PERSONAL INFORMATION (SECTION 31)

If a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

1) Do you have an approved records retention and disposition schedule? Yes ___ No ___

2) Is there a records retention schedule to ensure information used to make a decision that directly affects an individual is retained for at least one year after use? Yes ___ No ___

If you answered "No" to the above questions, your procedures may need to be revised. Please contact your DMIP or Records Officer.

Note: Records of provincial public bodies and specifically designated organizations/public bodies cannot be destroyed unless approval is granted under the authority of the *Document Disposal Act*. Please consult with a Records Officer to initiate the records scheduling process.

(IX) DIRECTOR/MANAGER OF INFORMATION AND PRIVACY (DMIP) OR FOIPP COORDINATOR REVIEW

1) Have you contacted the individual responsible for the completion of the PIA to discuss the information submitted, in particular those questions identified by an Asterisk? Yes ___ No ___

2) Does the Initiative meet the requirements of the FOIPP Act? Yes ___ No ___

3) Is there a mechanism in place to review this PIA as appropriate to ensure the information remains current? Yes ___ No ___

Are you satisfied that the policies/procedures for correction and/or annotation are adequate?

If there is additional information that would support the intended collection, use or disclosure of the personal information, please either insert in the appropriate text box or append to the PIA.

Comments

X) SIGNATURES:

PUBLIC BODY APPROVAL:

Program Manager (if appropriate)

Date

Director/Manager of Information
Information and Privacy/FOIPP
Coordinator

Date

Ministry Contact Responsible for
Systems Maintenance and Security
[this signature only required for PIAs
on new or existing systems]

Date

Assistant Deputy Minister or
Equivalent

Date

MINISTRY OF MANAGEMENT SERVICES REVIEW:

Corporate Information and
Privacy Advisor

Date

Director, Corporate Privacy and
Information Access

Date