

GUIDELINES FOR AUDITS OF AUTOMATED PERSONAL INFORMATION SYSTEMS

OIPC GUIDELINE 01-01

October 10, 2001
(Replaces: new document)

Any changes from the immediately preceding version of this document are italicized.

1.0 PURPOSE OF THESE GUIDELINES

As automated systems for personal information become more common, it is especially important that they be designed, and operated, in accordance with the requirements of the *Freedom of Information and Protection of Privacy Act* ("Act"). Public bodies covered by the Act are permitted to collect, use, disclose and store personal information (as defined in Schedule 1 to the Act) only in accordance with Part 3 of the Act. This document contains guidelines for public bodies to refer to in designing, and auditing the performance of any automated system that contains, processes, transmits or otherwise deals with personal information.

The OIPC may conduct an audit of a public body's automated systems under the authority of s. 42(1)(a) of the Act. The Act gives the Information and Privacy Commissioner the power to order a public body to change its personal information practices if they do not comply with Part 3. Public bodies are, however, responsible for ensuring, in each instance, that they are in compliance with the Act.

Each case differs, of course. A variety of circumstances – including the nature of the personal information involved and the uses for that information – will determine which measures are necessary in each case to protect personal privacy and ensure the security of personal information. For example, a self-governing body need not, in creating and using a list of members' names and addresses, take the same measures for the privacy and security of that limited personal information, as a hospital would have to take respecting patients' personal medical information. These guidelines are, therefore, to be used as a common sense guide in light of the circumstances of each case.

Public bodies should consider the requirements of Part 3 as minimum standards regarding the collection, use, disclosure and storage of British Columbians' personal information. The Information and Privacy Commissioner urges public bodies to collect and use only personal information that it is *absolutely necessary* for a public body to collect and use in order to fulfill its functions, even if legal authority to collect more extensive personal information technically exists.

Before designing and implementing an automated system, a public body should complete a privacy impact assessment, to assess the actual or potential effects on privacy and on the ways in which any adverse effects may be mitigated. The OIPC has developed a model privacy impact assessment and a blank assessment form for use by public bodies. These documents are available on our website at <http://www.oipcbc.org/publications/pia>. A copy of the completed privacy impact assessment, together with the public body's case for the necessity of collection of personal information, should be sent to the OIPC, to the attention of the Executive Director, for review and comment before any final decision is made to proceed.

These guidelines have benefitted from work done by the Organization for Economic Co-operation and Development, the University of British Columbia and various health organizations. The contents of this document, however, are solely the responsibility of the Office of the Information and Privacy Commissioner for British Columbia ("OIPC").

These guidelines do not constitute a decision or finding by the OIPC respecting any matter within the jurisdiction of the Information and Privacy Commissioner under the Act (including any act, decision, failure to act, or the exercise or performance of any power, duty or function, by any public body). These guidelines do not fetter or otherwise affect the powers, duties or functions of the Information and Privacy Commissioner respecting any complaint, investigation or other matter under or connected with the Act and the matters addressed in this document.

2.0 OVERALL DESIGN AND ADMINISTRATION

2.1 Accountability System	Practice	Assessment
1. A comprehensive written security/privacy policy for the system exists, setting out fair information practices that comply with Part 3 of the Act.		
2. The policy designates an individual public body employee at management level (and management level contractor representative, where a contract is in place) as responsible for security and privacy practices.		
3. The individual responsible for security and privacy is consulted when changes are made in information systems, to ensure security requirements are addressed.		
4. Risk assessments for security and privacy are conducted on an annual basis.		
5. Procedures for dealing with security or privacy incidents are in place.		
6. Conditions and procedures for the access and release of personal data to data subjects and third parties are in place.		
7. Reasonable steps are taken to correct confidential personal information that is inaccurate or incomplete.		
8. All unsuccessful system access attempts are recorded and reviewed routinely, with immediate appropriate follow-up.		
<p>9. An auditing system is used to ensure compliance with the policy's fair information practices and Part 3 of the Act, with the auditing system incorporating:</p> <ul style="list-style-type: none"> ○ the power to construct a data trail to follow all instances of access to a database for particular information; and ○ the capacity to conduct site investigations which can delve more deeply into the reasons for a particular request 		
10. Compliance with the rules for the confidentiality & security of confidential personal records is required and enforced, using agreements with employees wherever practicable.		

2.2 Personnel Training	Practice	Assessment
1. Prospective employees are screened for knowledge of principles and practices related to confidentiality and security of personal information. (References in these guidelines to "employees" include public body employees, contractors, and contractors' employees.)		
2. Employees and contractors sign a confidentiality agreement and are aware of consequences of breaches of privacy rights. Consequences are employment discipline for public body employees and (potentially) contract termination for contractors.		
3. A security awareness program is in place.		
4. On termination, revocation of access privileges and retrieval of keys are done immediately.		

3.0 SYSTEM DESIGN AND OPERATION

3.1 Hardware	Practice	Assessment
1. Up to date detailed inventory is maintained of all system hardware components.		
2. An employee supervises external hardware maintenance personnel whenever maintenance is undertaken.		
3. When maintenance requires equipment containing confidential personal data to be released to an outside service provider or vendor, all data are first erased or encrypted.		
3.2 Software	Practice	Assessment
1. A current inventory is maintained of all software that is used to store or manipulate confidential personal information.		
2. Where a system user is authenticated, the authentication information such as password is not displayed and is protected from unauthorized access.		
3. On initial system access, each user is informed of the date and time of the last valid log-on and any subsequent failed log-on attempts. The user immediately reports any unauthorized access attempts to the individual responsible for security.		

3.3 Computer Operations	Practice	Evaluation
<p>1. Annual physical inventory of all storage media containing confidential personal data is performed and discrepancies are investigated immediately, with correction of any problems.</p>		
<p>2. Each user of a system that processes confidential personal information is uniquely identified, with identification being authenticated before a user is given access to the system.</p>		
<p>3. Where user identification and authentication mechanisms are used to protect confidential personal information, procedures are implemented that :</p> <ul style="list-style-type: none"> ○ Control the issue, change, cancellation and audit of user identifiers and authentication mechanisms; ○ Ensure that authentication codes or passwords: <ul style="list-style-type: none"> ▪ are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code; ▪ are known only to the authorized user of the account; ▪ are pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition; ▪ are no less than 6 characters in length; ▪ are one-way encrypted; ▪ are excluded from unprotected automatic log-on processes; and ▪ are changed at least semi-annually. 		
<p>4. Systems display units and hardcopy production are positioned, or equipped with protective material, such that confidential personal information displayed or processed cannot be viewed by unauthorized persons.</p>		

<p>5. If equipment such as a laptop computer is to be removed from the premises on a temporary basis by staff who would normally have access to the personal data on that equipment, control procedures are implemented that include:</p> <ul style="list-style-type: none"> ○ the approval authority; ○ the identity of the borrower; ○ identification of the equipment; and ○ a signed acknowledgment of acceptance and return of equipment. 		
<p>6. The contents of erasable storage media containing confidential personal information are obscured using an appropriate technique before the media are re-used.</p>		
<p>7. Automated or manual controls, or both, are used to prevent unauthorized copying, transmission, or printing of personal information.</p>		
<p>8. Where data integrity of confidential personal information is a concern, control procedures are implemented to:</p> <ul style="list-style-type: none"> ○ ensure data to be entered or processed have been duly authorized; ○ verify the accuracy of the data; ○ retain the identity of the individuals who authorized and entered the data; and ○ maintain an audit trail of relevant transactions entered on the system. 		
<p>9. The system maintains a log of all security relevant activities on the system (e.g., log-ins & file accesses).</p>		
<p>3.4 Communications Operations</p>	<p>Practice</p>	<p>Assessment</p>
<p>1. Where a local area network containing confidential personal information is connected to a public network, it is protected by a network layer filtering router.</p>		
<p>2. When transmitting confidential personal information where data integrity is a concern, an integrity code is included with the data to verify that the data have not been altered during transmission.</p>		

<p>3. When faxing confidential personal information, the following steps are taken:</p> <ul style="list-style-type: none"> ○ the receiver is notified by sender; ○ the receiver stands by to receive the data; ○ the sender takes the utmost care to ensure the accuracy of the fax number dialed; ○ the fax cover sheet includes name, address, and phone number of both sender and receiver; ○ where there is frequent transmission between two points, or where faxes are sent to a fax mail-box: <ul style="list-style-type: none"> ○ the transmission is encrypted; ○ a confidentiality notice is attached; and ○ the purpose for which the confidential personal information is provided is explained. 		
<p>4. Confidential personal information is not transmitted by cellular or radio communications unless encrypted.</p>		
<p>5. Confidential personal information transmitted by electronic mail or Electronic Data Interchange is encrypted.</p>		
<p>6. Regular checks of the accuracy of pre-programmed numbers are made where the transmission of confidential personal information is involved.</p>		

4.0 SYSTEM SECURITY

4.1 Physical Environmental Security	Practice	Assessment
<p>1. A secure physical area is provided for the system's components, ensuring:</p> <ul style="list-style-type: none"> ○ walls extend to floor above; ○ physical access is restricted to authorized personnel; ○ access to hardware and confidential personal information is prevented in the absence of authorized personnel; and ○ motion detectors and alarms are used. 		

2. Removable media used to store confidential personal information are stored in secure containers when not in use.		
3. Printer ribbons and carbon paper are physically secured and disposed of in an appropriate manner.		
4. Hardcopy waste containing confidential personal information is shredded, mulched or burnt.		
5. Confidential personal information on magnetic media is destroyed by overwriting, degaussing or burning.		
6. Physically secure areas are used for storing confidential personal records.		
7. Individual designated in the policy maintains control over the secure storage of confidential personal information.		
8. Access is controlled to fax machines used for transmission of confidential personal information. Security is provided for access keys and passwords.		
9. Access to documentation about computer systems that contain confidential personal information is restricted to authorized personnel.		
10. Terminals and personal computers used for manipulating confidential personal information are positioned so that unauthorized personnel cannot see them.		
11. Software programs are used which automatically blank the screen if a computer remains unused for a set (brief) period.		
4.2 Operational Security	Practice	Assessment
1. Privacy awareness is enhanced within the operations group if any members of the group have access to confidential personal information.		
2. Access to confidential personal information is withheld from manufacturers and maintenance staff.		
3. Records used for educational purposes are made anonymous.		
4. Passwords are changed at frequent and irregular intervals.		

5. Confidential personal records are not removed from the agency 's premises without authorization.		
6. Formal procedures are maintained for dealing with the termination of operations employees who have access to confidential personal information in matters such as identity badges, keys and passwords.		
4.3 Technical Security	Practice	Assessment
1. Automatically validate, where possible, any confidential personal information entered into the system.		
2. Software used for recording, processing, storage and retrieval of confidential personal information is validated through detailed audit and certified as suitable for the uses to which it is put.		
3. Procedures are in place to ensure confidential personal information cannot be passed between computers, or discrete systems within the same computer, without authority		
4. Reasonable steps are taken before a computer interface is established with a system to ensure the arrangement does not increase the risk of unauthorized access to confidential personal information.		
5. Classes of information, which can be sent by fax, are controlled.		
6. Production and distribution of an official and regularly updated list of fax numbers ensures that fax numbers are current and accurate.		
7. Technical safeguards from simple locks to encryption facilities are in place on faxes used for the transmission of confidential personal information.		
8. Fax activity history reports are retained to check for unauthorized transmissions where confidential personal information is involved.		
9. Fax confirmation reports are carefully checked to ensure the correct transmission of confidential personal information.		
10. Fax machines used for the transmission and receipt of confidential personal information are only used by authorized staff.		