Title:	Policy Number:	Pages
Security - General	CP 600-2019	3
Approved by:	**Approval Date:**	Dec 12, 2019
Executive	**Last Review Date:**	N/A
Policy Owner:	**Next Review Date:**	Dec 2020
Chief Security Officer		
Relevant or Related Policies/Legislation/Guidelines:		
The Freedom of Information and Protection of Privacy Act (FOIP) *The Health Information Protection Act* (HIPA) *The Vital Statistics Act, 2009* (VSA)		

SECURITY - GENERAL

PURPOSE STATEMENT

To establish eHealth's security framework.

SCOPE

This policy applies to all of eHealth staff (in and out-of-scope employees, contractors, students and secondments), vendors and agents.

POLICY STATEMENT

eHealth has a duty to secure its information assets (see the Policy Dictionary). Security measures will protect the confidentiality, integrity and availability of all corporate information assets.

eHealth's Enterprise Security Services will support all sections of the privacy policy.

POLICY REQUIREMENTS

General

The cost of safeguards and level of protection will be proportionate to the value of information assets. To ensure this occurs, eHealth will classify information assets according to the following classifications:

- Class A: Breaches of information assets included in this class could result in extremely serious injuries to individuals or enterprises, including, but not limited to, the following:
    - Significant financial loss/economic impact.
    - Loss of life or public safety issues.
    - Social hardship, or
    - Major political impact.
- Class B: Breaches of information assets included in this class could result in serious injuries to individuals or enterprises, including, but not limited to, the following:
    - Loss of competitive advantage.
    - Loss of confidence in an eHealth program.
    - Financial loss.
    - Legal action, or

    - Damage to partnerships, relationships and reputation.

- Class C: Breaches of information assets included in this class could result in significant injuries to individuals or enterprises, including, but not limited to, the following:
    - Limited financial loss.
    - Minor impact in service or performance levels, or
    - Limited damage to reputation.
- Public: Breaches of information assets included in this class will not result in injuries to individuals, eHealth or private sector institutions.

Compliance and disciplinary action

Failure to comply with this policy will result in restricted access to eHealth information assets, or disciplinary action, up to and including, termination of employment, appointment or contract with eHealth.

Exceptions

In certain circumstances, eHealth may allow exceptions to this policy based on a demonstrated business need. All exemptions will be formally documented.

RESPONSIBILITY

Information asset owners are responsible for:

- Performing threat risk assessments (TRA) when there are:
    - New initiatives/projects, or
    - Significant changes.
- Maintaining and annually reviewing a risk register. This will ensure that eHealth keeps its security posture at an acceptable level at all times.
- Protecting information assets from unauthorized access, modification and loss, at a level consistent with their classifications.
- Monitor at a level consistent with their classifications.
- Keeping security patches and software versions up-to-date on all eHealth information systems and other devices that process or store eHealth information.
- Outsourcing all Payment Card Industry Data Security Standard (PCI/DSS) related activities to a PCI/DSS compliant vendor, and
- Maintaining an appropriate disaster recovery posture. This will ensure the availability of critical applications.

Users of eHealth information assets are responsible for:

- Complying with this and all related security policies.
- Protecting information assets according to their classifications.
- Only accessing sensitive information when there is a legitimate business need, and
- Reporting information security incidents immediately to the Service Desk at 1-888-316-7446.

In consultation with Enterprise Security Services, the Vice President of Corporate Services and Chief Financial Officer is responsible for:

- Reviewing and approving exceptions to this policy.

In consultation with Enterprise Security Services, Human resources and the respective health services organization are responsible for:

- Initiating corrective measures (e.g., restricting access to services or initiating disciplinary action) when policy compliance issues arise.

Linked Resources

Policy Dictionary

Appendices

A Guide for Information Protection Classification

A Guide for Information Protection Classification

eHealth Saskatchewan
Enterprise Security Services

Last revised: September 2019

eHealth Saskatchewan

Table of Contents

Revision History

Date (dd/mm/yyyy)	**Version**	**Comments**	**Reviewers Name**
01/09/2019	0.1	New document created	Vivek Verma

1. What is Information Protection Classification?

Information Protection Classification (IPC) is a business tool that enables enhanced security in large organizations. When fully implemented and combined with effective security, in ensures the confidentiality, integrity, availability, and privacy of information.

Good security can be distilled down to two steps: Determining value *and* Applying appropriate security. IPC is a formal process that completes the first step: determining value.

The best security involves analysis and decision-making done in a structured way. The following "Household Security Grid" shows how we place value on items and make security decisions every day. For each of the four household items, the following table:

- Lists the items;
- Assigns a value;
- Indicates the cost of replacement; and
- Describes security measures.

Example: Information Protection Classification for Household Security Grid

Item	Value	Cost to Replace	Security
Newspapers	Low	Low	None
Household cash	Varies; Usually low	Equal value of cash	Unlocked drawer
Receipts for income tax	No cash value	High; May be impossible to re-create	In file box in a closet
Family wills	High	Irreplaceable	Original in safety deposit box; Copy with lawyer

As you can see, we all make classification and security decisions regarding our possessions automatically. Now, let us introduce a new item into our matrix: Great-grandma's photo album.

Item	Value	Cost to Replace	Security
Great-grandma's photo album	High; A family heirloom.	Irreplaceable	?

If we followed the examples in the "Household Security Grid", we would make a copy of the album for viewing and store the original in our safety deposit box because it is a valued family heirloom *and* irreplaceable.

A Guide for Information Protection Classification applies analysis and a structured decision-making process to determine the security requirements for Government of Saskatchewan Information Assets. Applying IPC is the first part of complete security.

The next step – defining and applying appropriate security measures – is independent of the classification process.

Instead of a dollar amount, the factors which determine security levels in *A Guide for Information Protection Classification* are a combination of the business requirements for confidentiality, integrity, availability, privacy, and the injury that could be caused by unauthorized access, use, or release of the information.

2. History of Information/Data Classification in Canadian Governments

The Government of Canada (GOC) introduced the country's first information classification system during World War II. Its purpose was to protect documents that were important to national security. These documents were stamped with "TOP SECRET" and access was severely restricted.

In 1986, the GOC modified its classification system to accommodate the 1982 Federal Privacy Act. Access and privacy were now important considerations. The changes recognized that many types of government information need to be kept secret and national security is rarely the reason. Consequently, the GOC's corporate culture understands and accepts information classification. Achieving that same understanding and acceptance will take time and effort in the eHealth.

Recently, several provincial governments developed information or data classification systems of their own as part of initiatives to control access and improve security. They were driven by a realization that the Internet and Electronic Service Delivery (ESD) opened them up to new risks as well as new opportunities. They were evolving from department/facility networks to government-wide networks that are potentially accessible via the Internet, by anyone. This potentially raises the risk to government data, much of it about citizens.

In 2001, the National CIO Council Subcommittee for Information Protection (NCSIP), a federal-provincial committee with a focus on IT security, created the Public Sector Security Classification Guideline. It fulfills two purposes. It provides:

- Standard Canadian classification grid for exchanging data between jurisdictions; and
- Generic classification guide for jurisdictions that have not developed their own.

This turned out to be timely for the Government of Saskatchewan and eHealth. Our Security Charter Group, with representation from all departments, had just gone through an intense educational process to support the creation of modern security policies and procedures.

The *Public Sector Security Classification Guideline* and its four levels have been integrated into much of the Government of Saskatchewan's security development work. The Guideline is referred to in department security policies and in the Security portion of the draft Government's Enterprise Architecture – a broad plan for the management of government IT.

A Guide for Information Protection Classification takes the core of the Public Sector Security Classification Guideline and adapts it for use in eHealth.

In 2003, three events led to this version of A Guide for Information Protection Classification, created by the Information Technology Division (ITD):

- In the spring, Cabinet directed the ITD to implement data/information classification within Executive Government.
- In the fall, Cabinet formally adopted *An Overarching Personal Information Privacy Framework for Executive Government* requiring data/information classification.
- Agencies in Executive Government were directed to appoint Privacy Officers. The individuals to lead classification of personal information are now in place.

Release version 1.0 of *A Guide for Information Protection Classification* was produced in the fall of 2003 with the help of Don Herperger, Greg King, Randy Langgard, Verna Mogk, Mike Murray, Roxane Priddel, Randy Schmidt, Duncan Sherwin and Tim Whelan.

3. Three Ways to Classify Information

Classifying information is the first step in adequately protecting it. Information in eHealth is classified in one of three ways:

1. Specific kinds of information that exist in every department or agency are automatically classified. Human Resources (HR) and Cabinet information are two examples.
2. Some general categories of information, like published reports and information web sites, have the same classification regardless of which department/agency/team owns the data.
3. The remaining information is classified at the function level by the department/agency that owns it. The most sensitive information used for a function will determine the classification of all associated information.

The primary purpose of this document is to assist when classifying information at the function level.

Information is classified, using the following Information Protection Classification Grid, to establish its correct security level. The objective of classification and security is to protect the confidentiality, integrity and availability of information.

Confidentiality ensures that information can only be accessed by authorized individuals. Integrity ensures that only authorized and accurate changes are made to information. Availability ensures that authorized users have access to the information when required.

While integrity and availability are important considerations at all levels, confidentially becomes increasingly important as you move up the grid.

For the purposes of IPC, a function is defined as: all of the information and information technology associated with a single service/process (or group of closely related services/processes) in a department or agency. This includes files (hard copy and electronic, including e-mail), applications, databases, data storage, hardware, networks, and procedures for the transmission of data.

Examples of functions:

- Collection, storage and retrevial of Health Care Information (PHI);
- Regestation for Births and Deaths;
- Developement and delivery of Snap-Shot FOI Requests; and
- Policy development in the Information Technology Division.

The Information Protection Classification Grid				
Level	**Definition**	**Information Examples**	**Other Information Examples**	**Consequences**
A	Could reasonably be expected to **cause extremely serious personal or enterprise injury**, including: • Significant financial loss; • Loss of life or public safety; • Social hardship; • Major political or economic impact.	• Highly sensitive personal* information that, if compromised, could jeopardize an individual's safety; • Information on a police informant; • Information relating to a sex offender. • All Health information as defined by the Health Information Protection Act;	When ***confidentiality*** is the key consideration: Cabinet documents • Provincial budget information (before public release); • Preliminary investigation files of a major crime; • Legislation under development; • Sealed tenders and request for proposals (RFPs) prior to the closing of a competition. When ***availability*** is the key consideration, information (that when compromised) will result in: • Extended loss of an essential government service; • Loss of crisis communications during emergencies; • Loss of essential police communications and data; • Loss of emergency health services. When ***integrity*** is the key consideration: • Information systems and material used for testing food or water supply that could result in loss of life or severe illness; • Law enforcement information such as that held at the Canadian Police Information Centre (CPIC).	It is difficult, if not impossible, to put a dollar value on the Government's reputation. But as an indicator of the grave consequences of compromising confidentiality, availability or integrity of information in this security level, think of the total impact as being ***over 10 million dollars*** in legal costs, technical problems and loss of reputation

The Information Protection Classification Grid				
Level	**Definition**	**Information Examples**	**Other Information Examples**	**Consequences**
B	Could reasonably be expected to **cause serious personal or enterprise injury**, loss of competitive advantage, loss of confidence in the government program, financial loss, legal action and damage to partnerships, relationships and reputation.	• Most non PHI personal* information; • Information relating to an individual's racial or ethnic origin; • Information describing a citizen's finances; • Case files and information on eligibility for social benefits; • Details of an Employee Family Assistance Plan (EFAP) file; • Human Resources files.	When ***confidentiality*** is the key consideration: • Information compiled as a part of a violation of law; • Ministerial briefing notes; • Information on a company's credit rating; • Disclosure of trade secrets or intellectual property; • Information on competitiveness reviews and investment attraction; • Information/data related to the exploration, mining and production data of mineral/energy resources; • Inaccurate money transfers to a municipality due to loss of integrity; • Information received from another government relative to its position on a particular trade issue; • Drafts of department policy. When ***availability*** is the key consideration: • Payments of benefits or income support to Saskatchewan citizens; • Financial and reporting systems; • Senior management information systems. When ***integrity*** is the key consideration: • Information related to food or water supply that would not meet expected standards of quality but would not cause illness; • Information related to nonemergency health care; • Financial transactions and payments; • Ownership and disposition of Crown minerals, lands, and oil and gas rights; • Information that could be used for criminal purposes.	If it could be measured in dollar terms, the significant consequences of compromising confidentiality, availability or integrity of this information would be ***between one hundred thousand and 10 million dollars*** in legal costs, technical problems and loss of reputation.

The Information Protection Classification Grid				
Level	**Definition**	**Information Examples**	**Other Information Examples**	**Consequences**
C	Could reasonably be expected to **cause significant injury to individuals or enterprises** with limited: • Financial losses; • Impact in service/ performance levels and reputation.	Some limited personal* information like mailing and phone lists not from within PHI Protected sources.	• The availability/integrity of government web sites; • General information databases such as a listing of Saskatchewan manufacturers; • Economic statistics/analysis/ forecasts; • General administrative files.	If it could be measured in dollar terms, the consequences of compromising the confidentiality, availability or integrity of this data would be ***between one thousand and one hundred thousand dollars***.
Public	Will **not result in injury** to individuals, governments or private sector institutions	Personal* information cannot be "Public"	• Information on government web sites; • Job advertisements; • Public reports and policy statements; • Public health information; • Job duties and pay scales.	The type of information, if lost, changed or denied, would not result in injury to an individual or government organization and the financial loss would be ***under one thousand dollars***.

***** *as defined by The Freedom of Information and Protection of Privacy Act*

4. Applying Information Protection Classification

An organization can classify information once an IPC team has been established. Typically, an IPC team includes a member of senior management, the organization's Privacy Officer, IT staff with knowledge of security issues and an individual responsible for Records Management. Staff from the eHealth's ESS is available to assist departments in the application of IPC.

In order to classify all information held within an organization, including personal information, the IPC team will need to work with program managers. The Privacy Officer will need to be familiar with relevant legislation and policy documents such as *An Overarching Personal Information Privacy Framework for Executive Government*. All people involved in IPC will need a current version of *A Guide for Information Protection Classification* and be familiar with its content.

The first step in classifying information is to do an inventory of all information in an organization. Part 7 of this document contains suggestions on how to do this.

The next step is to determine if an information/records system includes personal data. The legal definition of "personal," for most information, is in section 24 of *The Freedom of Information and Protection of Privacy Act* (the FOIPP Act). The legal definition for health information is in section 2 of the *Health Information Protection Act* (HIPA). (Layman's guides to these definitions are on pages 8-9 of the Privacy Framework.) Agency specific legislation may also apply. If it is determined the information being classified falls within the scope of legislation and is therefore personal, classification should proceed with the assistance of the department Privacy Officer. On the other hand, if information is not protected by legislation and is therefore not personal, classification continues under the lead of administration and security staff.

4.1. Many Types of Information

Some types of information that will be included in classification levels are:

- information received in confidence from other governments or organizations (possibly private sector entities);
- information prepared by or obtained by a federal or provincial investigative body (could be law enforcement);
- personal information as defined in the FOIPP Act;
- business information;
- budget details prior to the delivery of the Budget Address;
- advice and recommendations involving Cabinet or confidences of the public that would affect the operations or integrity of government;
- personal health information as defined in HIPA; and
- information shared between departments.

4.2. Marking or Labelling Information

Information that is deemed to be sensitive should be classified/marked at the time that it is created. This will ensure that the information has appropriate protection as it enters government hands. All individuals who have access to this sensitive material need to be made aware of its classification so they can be part of its security. Additionally, any information that is transferred beyond the organization in which it was created must be appropriately couriered and marked. Information that is exchanged under formal Memorandum of Agreement must be marked and the recipient organization must be able to translate its security classification into appropriate protective measures.

4.3. Downgrading or Declassifying of Sensitive Information

Information should only be classified for the period that it requires protection after which it should be downgraded or declassified. This requirement recognizes that information can lose its sensitivity with the passage of time or the occurrence of specific events. This process contributes to the overall integrity of the security system and will ensure that information can safely be made available to those who need to have it quickly and safely.

4.4. Automatic Downgrading or Declassification

Organizations should, when applicable, provide for automatic downgrading or declassification of information by selecting a specific year or event or, a review period at the time the record is created. When such information is received under a Memorandum of Agreement, the recipient should ask if a declassification or downgrading date has been selected by the originating organization for the information.

It is suggested that a period be identified for all categories of information, along with the date or “event-specific triggers” that will indicate downgrading or declassification. However, it is also suggested that an automatic expiry date not be selected for information classified in level “A”. Downgrading information as appropriate will be a regular part of information handling. This does not mean downgrading the IPC level is synonymous with making it publicly available. The normal FOIPP application review process would still apply.

4.5. Shared Information

The requirement to downgrade or declassify sensitive information applies not only to information within an organization but also to information provided from one department to another, or from one jurisdiction or partner to the government under agreement. Before declassifying or downgrading any such information, the originator must be contacted. If need be, the information can be sent to the “office-of-origin” for downgrading or declassification. In certain

circumstances, it may not be possible to consult the originator. In such cases, consultation with other appropriate officials such as the Freedom of Information or Privacy Officer for that organization should occur.

5. Determination of Security Standards

A Guide for Information Protection Classification supports the process of determining correct safeguards for each classification by clearly indicating potential consequences of loss for each level; however, it will not dictate specific security standards.

6. Limitation of Information Protection Classification

A Guide for Information Protection Classification is limited to identifying the proper indicator to place on information so that it is clear what set of protective standards are required.

Specific security standards that apply to information in each classification level (A, B, C and Public) are developed independently of this document. While these security standards will change over time, as technology evolves and security practices change, the classification of information should not change.

Establishing "protective profiles" or "minimum baseline strategies" in communities of interest such as the "health area" can be alternative strategies that will provide assurance that information is being protected at a known level.

Similar to the above "community of interest" example, the Canadian Payments Association may also establish minimum protective standards in the area of finance or payments. This will allow the exchange of financial information during ESD given that an "industry best practice" has been established for information safety. This will apply equally to private and public sector organizations.

Generally, access to information is separate from IPC. Granting access is a procedure internal to your agency. When access requests are made from outside government, the existing FOIPP process still applies.

7. Recommended Process for Information Protection Classification

7.1. Establish an IPC Team

Each department/agency should establish an IPC team. Members should include a member of senior management, the department/agency Privacy Officer, IT staff with knowledge of security issues and an individual responsible for Records Management. Program managers are brought in as the information under their stewardship is classified.

Roles of the IPC Team:

- The IPC team leader ensures the classification work gets done and reports back to senior management;
- IT and IT security staff serve as resources on technical and security issues;
- The Privacy Officer helps the IPC understand privacy issues, including what is "personal," and ensures all personal information is classified.

7.2. Complete an Inventory of Information

Here are two ways to get an inventory of your department/agency information. Each method piggybacks on existing work.

If your organization has completed its work on the Administrative Records Management System (ARMS) and the Operational Records Management (OARS), you already have an information inventory.

The Department of Justice is producing a new FOIPP Access Directory in the winter of 2003-04. They will be asking all departments/agencies to create an inventory of their operational information as the basis of the Access Directory. The inventory your organization produces for Justice can also be used as the starting point for your IPC efforts.

7.3. Organize Information into Functional Groupings

All of the information related to a function (or set of related functions) should be grouped. Groups would include:

A. all the information in a branch;
B. all the information connected to a single function/program; or
C. all the information connected to a series of closely related functions.

Examples:

A. all the files in a policy unit;
B. all information related to Labour Standards; or
C. all information concerning consumption taxes.

Once you have created your functional groupings, the most sensitive information in each group will determine the security classification for all information in the group.

7.4. Identify Functional Groups which include Personal Information

"Personal Information" *as defined by The Freedom of Information and Protection of Privacy Act*

You will need to become familiar with:

- *The Freedom of Information and Protection of Privacy Act*;
- *An Overarching Personal Information Privacy Framework for Executive Government*; and
- Other relevant legislation in order to determine what is personal. You may need to consult a lawyer.

Classifying personal information should be your first objective as it has been mandated by Cabinet. While it is a good idea and sound business practice to classify the remaining information (which is not personal) it is not a Cabinet requirement.

7.5. Apply the Information Protection Classification Grid

The IPC team will slot each functional group of information into one of the four levels in the Information Protection Classification Grid. Program managers should be consulted as their information is classified.

There will be a tendency to classify information high. Keep in mind that only personal information that has an impact on the safety of specific individuals belongs in classification "A". Use the examples in the Information Protection

Classification Grid and match each of your functional groups to an example. The examples are there to make classification easier.

In addition to classifying information, indicate any events (triggers) that will automatically change the information's security classification. Examples of triggers:

- An individual's health file is downgraded from "B" to "C", ____ years after the person's death;
- The budget address is downgraded from "A" to "Public" after it is delivered by the Minister of Finance.

It is a good idea to check all your contracts and agreements regarding information sharing, as it will let you know:

- Which organizations handle your information; and
- Which organizations provide you with information.

7.6. Prepare a Report Detailing Classification Results

Prepare a report detailing the classification results for your senior management. Once adopted by senior management, circulate your report to department managers. This is the first step in informing staff of which information in your organization's possession needs high security and which does not. Send a copy of your report to your IT Security Officer (or IT director) and others with a role in security so this new process for adequately protecting information can begin.

8. Implementation Issues

Complete implementation of IPC and the application of appropriate security will take money and time. It may also change the way we store and access information.

If you classify some of your agency's information at a level that requires higher security than your infrastructure currently supports, your department or agency will need to spend money in order to bring security up to standard. Do not let the possibility of this happening detract you from classifying information correctly.

It may take some time for your department or agency to adequately secure all its information. This is a separate issue from the task of IPC. As the government is new to both IPC and standardized security, time will be given for implementation.

It may be the case that information in classification "A" is stored in a few high security facilities (as the cost of creating many such facilities cannot be justified). Fortunately, modern networks and storage technology make this far easier than it was a few years ago.