Ministry of Government and Consumer Services

Cyber Security Division

Information Sensitivity Classification Guidelines

Published: 2018 – 08
Reviewed: 2018 – 08

I+IT | Cyber Security

Ontario

Table of Contents

Introduction

The Information Sensitivity Classification Guidelines is a companion document to the new Corporate Policy on Information Sensitivity Classification (ISC). This document replaces the former Information Security & Privacy Classification (ISPC) Operating Procedures (*last revised in 2006*).

This guideline works together with the policy to provide you with the "how" of information classification and protection. In a straightforward and user-friendly way, this document offers a simple process to help you identify sensitive information, rate its sensitivity level and safeguard it appropriately, dependably and consistently.

Preamble

Effective information security involves addressing the confidentiality, integrity and availability requirements of information and information systems. While the sensitivity classification of information and information assets is based on its confidentiality requirements, the information must also be assessed for its integrity and availability requirements.

- **Confidentiality** requirements relate to the relative harm or injury that would result from unauthorized access or inadvertent release of information. This may be assured through a variety of business processes and technical means.
- **Integrity** requirements relate to the harm or injury that would result if an information asset was subject to unauthorized modification. This is usually assured via technical means that prevent unauthorized access to information systems, thereby limiting the possibility of tampering.
- **Availability** requirements relate to the harm and injury that would result if particular information is not continuously made available for authorized access and use. This is usually addressed through contingency plans and efforts to ensure the resilience of information systems.

Although all three aspects of information security are important, confidentiality is most likely to be assured by user behaviour, whereas integrity and availability are most commonly assured through technical means.

It should be noted that the methods and degree of protection recommended to ensure confidentiality will not necessarily be identical to those used to ensure integrity or availability. Similarly, the same information asset may require that different safeguards be implemented to ensure its confidentiality when it is created, stored or shared in different technical contexts (e.g., printed documents; documents stored on an OPS shared drive or internal application; or documents that are accessible via the Internet).

Nevertheless, the type and degree of safeguards recommended to ensure the security of a given information asset must always be proportionate to the risk of unauthorized access, inadvertent release, modification or non-availability.

Classifying Information

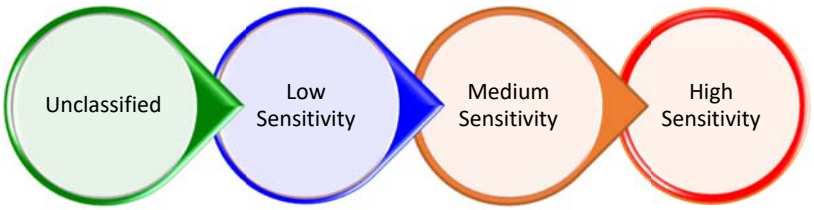
Members of the Ontario Public Service (OPS) often handle sensitive and personal information on a daily basis. Policies and legislation such as the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Protection Act (PHIPA) make it our obligation to enable access to information through the Freedom of Information Process and to safeguard the confidentiality of that information from unauthorized disclosure – but how, and when? How much protection is enough and how much is too much?

Information sensitivity classification promotes reasonable security measures so that personal and sensitive information is protected to the level necessary for the government to meet its business and legislative obligations.

There are three, basic steps to information sensitivity classification:

1. Classify the information to one of the four sensitivity levels;
2. Label all information with the appropriate sensitivity level; and,
3. Safeguard the information in accordance with its sensitivity level.

Here are the four sensitivity classification levels:



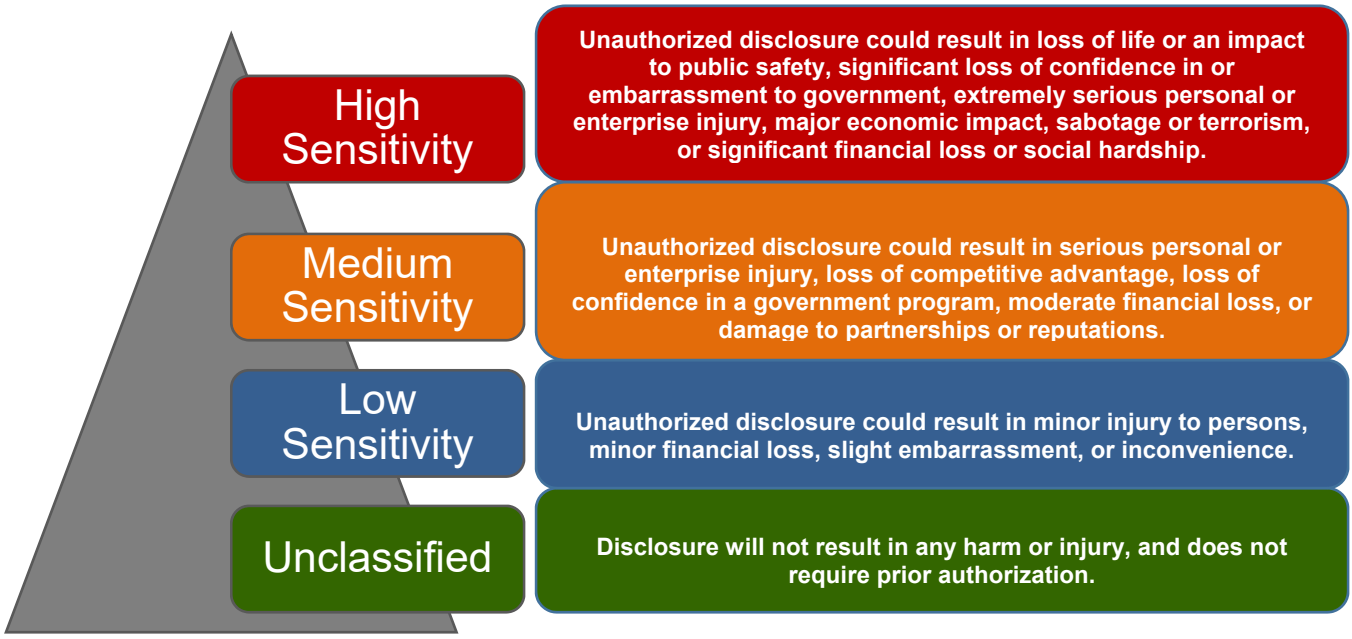
This simple but effective schema must be used to classify all information in the custody or under the control of the Government of Ontario – information in all its forms, whether paper or electronic – and throughout all stages of its life cycle; that means from creation or collection, during access, use, retention and through to disposal.

FACT

Unclassified information is not information that's been overlooked or doesn't need to be classified. It's information that won't cause any harm or injury if disclosed without additional authorization.

For example, information on the official Government of Ontario Internet website has been created specifically for the public to see. Therefore, the sensitivity level of the information on the website is "unclassified".

The Harm and Injury Test



Determining the Sensitivity Classification Level

The following guidelines provide further help for you to determine the correct sensitivity classification level for your information.

1. Consider the information in context

- Context refers to where the information appears and especially what other information appears with it. For example, multiple pieces of Medium sensitivity information (including personal information) may be reclassified to High sensitivity, if the information is stored together and the potential of harm or injury increases as a result of the aggregation.

2. Think about the potential for harm and injury if the information were to be disclosed without authorization

- Injury refers to the unauthorized disclosure, how it happened, and what was done with the disclosed information.
- Harm refers to the consequences of the injury – this could be loss of life, loss of personal or individual privacy, damage to partnerships, significant embarrassment, or an unfair business advantage gained.

The sensitivity classification level you choose must balance the information's business and legal requirements for privacy, unauthorized modification and uninterrupted use with the legitimate access requirements of authorized employees. Your choice must also take into account the corresponding safeguards for that level of sensitivity and the government resources, (time, money and people) those safeguards will require.

3. Determine the business requirement for protection of the information's confidentiality

- Business requirements are dictated by applicable legislation (e.g., FIPPA/PHIPA), corporate and individual ministry directives and policies, user requirements, program-to-program interdependencies, as well as the nature of the program and its technology and operational requirements. For example, the Ministry of Health and Long-Term Care's requirements for confidentiality would be different for its medical records than it would be for its Internet website content.
- FIPPA governs the collection, use and disclosure of Personal Information, and any unauthorized disclosure would be a violation of the regulation. As such, Personal Information must be classified as Medium Sensitivity at minimum, but should always be viewed in context. The type of information, and any aggregation of information will determine if medium or high sensitivity is suitable. It is also important to note that unauthorized disclosure can happen at any point in the information lifecycle, including during the creation, collection, use, retention or disposal of the information.

When choosing the proper sensitivity classification level for your information, begin by considering the criteria for "unclassified" first. Then work your way through the levels – from low sensitivity to medium sensitivity, and then to high sensitivity. By process of elimination, rationalize your choice.

Let's examine each one of these individually.

1. Consider the information in context

Take a look at the information and decide:

- What type of information is it?
- Where does the information appear?
- How is the information being used?
- What other information appears with it?
- What legislation applies to it?

For instance - how would you classify business contact information found in the Government of Ontario Employee and Organization Directory (INFOGO)?

Smith, John, Manager
Health and Long-Term Care

900 Bay Street, Toronto,
416-555-1234
john.smith@ontario.ca

The Government of Ontario Employee and Organization Directory is used to publish business identity information that includes the name, title, contact information or designation of an individual that identifies the individual in a business, professional, or official capacity.

Industry estimates indicate that approximately 80% of information created by an organization - including government - is actually unclassified or low sensitivity. Another 15% is medium sensitivity, and the remaining 5% fits into the high sensitivity level.

The sensitivity classification level of this information is "UNCLASSIFIED" because it is not personal information as defined in FIPPA and it is intended for the public to see and access.

For instance - how would you classify the following information?

A telephone book is used to publish specific personal information. John Smith has given the telephone company his authorization to publish this information so that anyone may use it to contact him.

The sensitivity classification level of this information is also "UNCLASSIFIED" because it's been approved by Mr. Smith for the public to see and included in a book specifically meant for public access.

Let's change the context and say that a ministry has collected this same information from John Smith to receive a government service. With this change in context would the sensitivity classification of "UNCLASSIFIED" stay the same? Would disclosure of the personal information be a privacy breach?

Just because information is very important to you or your program, doesn't make it high sensitivity. Classifying information in terms of its perceived importance, as opposed to its true sensitivity, leads to over-classification with increased costs for safeguards. High sensitivity safeguards take extra resources including time, people and money. They also impose very restrictive handling and distribution procedures which may keep authorized employees with legitimate access requirements from being able to access it.

2. Think about the harm and injury

Consider the harm and injury that might reasonably be caused if information was disclosed without authorization.

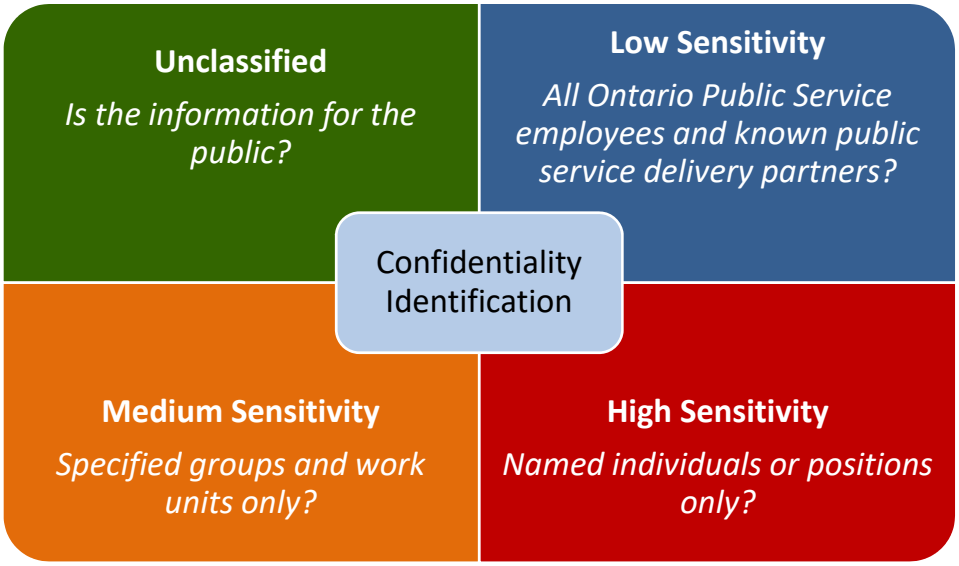
- It might be loss of life – for example, unauthorized disclosure of undercover police identities;

- It might be business disruption or financial hardship – for example, unauthorized disclosure of corporate taxes or job tenders;
- It might be only slight inconvenience – for example, unauthorized disclosure of a staff meeting agenda;
- Or, there might be no harm or injury at all.

3. Determine the business requirements

First, it's important to become familiar with the legislation (e.g., FIPPA/PHIPA), and any directives, policies or standards that apply to the information in your program area.

For example, FIPPA outlines rules for collection, use, disclosure, retention, and destruction of personal information held by government, resulting in a classification of Medium at minimum for Personal Information. These rules would apply to John Smith's personal information collected in the example above, regardless of whether or not it appears in the phone book. Next, determine how much confidentiality the information requires by identifying who should have access to the information based on the following guideline:



Sensitivity Classification Summary

Following is a summary to guide you when choosing the correct sensitivity classification level for your information.

1. Unclassified information:

- No additional safeguards or special handling measures required;
- No harm and injury because no disclosure authorization required;
- Examples: information on a Travel Ontario website.

2. Low sensitivity information:

- Approved for access by all Ontario Public Service employees and known public service delivery partners;
- Requires protection from unauthorized modification but can be easily replaced or restored if necessary;
- Requires a primary level of safeguards and minimal special handling measures;
- Little or no harm and injury if disclosed without authorization;
- Examples: Staff meeting agendas, marketing materials and OPS Charity Campaign information.

3. Medium sensitivity information:

- Approved for access by specified groups and work units only;
- Requires an intermediate level of safeguards and increased special handling measures;
- Harm and injury would be serious personal or enterprise injury if disclosed without authorization;
- Examples: Strategic planning documents, internal briefing or issue notes, business tax returns, public or stakeholder consultation meeting notes and Personal Information governed by FIPPA.

4. High sensitivity information:

- Approved for access by named individuals or positions only;
- Requires an advanced level of safeguards and enhanced special handling measures including vigorous distribution auditing;
- Electronic copies must be stored and transmitted in encrypted form;
- Harm and injury could be loss of life or extremely serious personal or enterprise injury if disclosed without authorization;
- Examples: Witness Protection Program records, GO-PKI registration and encryption key information, personal medical records (see FIPPA/PHIPA), undercover police identity records, and any group of Medium Sensitivity records where the aggregate value of the information, when stored together, may result in more serious harm and injury.

Where mixed information of various sensitivity levels co-exists, all the information must, by default, be classified at the highest sensitivity classification level involved and be secured in accordance with the safeguards required at that level.

Mandatory Safeguards

Information Labelling

Once you've determined the sensitivity classification level of the information based on the information requirements for confidentiality, the first and most important thing that must be done is to label all records accordingly.

Labelling records indicates that their sensitivity has been assessed. A label also highlights the need for special handling measures. In the same way that washing instruction labels on your clothes tell you how to protect them from shrinkage, discolouration and fabric breakdown, information sensitivity classification labels communicate requirements for special handling.

For instance, if the label reads **LOW SENSITIVITY**, **MEDIUM SENSITIVITY** or **HIGH SENSITIVITY**, it's really saying "CAUTION!! Special handling required".

If the label reads **UNCLASSIFIED**, it's saying "No special handling required".

The four labels to be used must read as follows. Use only one of the following four labels.

- **HIGH SENSITIVITY - Degré de sensibilité élevé**
- **MEDIUM SENSITIVITY - Degré de sensibilité moyen**
- **LOW SENSITIVITY - Degré de sensibilité faible**
- **UNCLASSIFIED - Non classifié**

Label all information regardless of its physical form, including: electronic files (MS Word, PowerPoint, Excel, etc.), paper documents, USBs, CDs, DVDs, cassettes, VHS video tapes, reel-to-reel tapes, microfiche, pictures, drawings, maps, diagrams, and emails. Label all information clearly in the upper right-hand corner. Be careful to avoid labelling over existing printing or serial numbers, etc. Label all notes, drafts and photocopies of the information too. Information published by the government and intended for public consumption (i.e.: documents such as brochures or social media posts such as tweets) does not need a label.

The reason we classify and label information is to communicate how to safeguard it properly. When you see a sensitivity classification label it's your responsibility to know the required safeguards to protect that information.

Labelling Options

There are many easy-to-use options available to label information. For example, set a header format in MS Word; or create a macro that will, at the touch of a specified key on your keyboard, apply a pre-recorded label to each new electronic document you create; or you could apply an MS Word watermark; or simply use an ink stamp or a pre-printed, self-adhesive label. Be careful to avoid damaging records or media with self-adhesive labels.

When safeguarding information, remember to use PAT – physical, administrative, and technical safeguards. An example of a physical safeguard is a padlock and key; an administrative safeguard is a logon id and password combination; a technical safeguard is encryption with digital signature.

When pre-printed paper or electronic forms are created, make sure the printer or the electronic content developer includes the sensitivity classification level directly on the form. The label should then refer to the sensitivity of the form when completed.

When planning and implementing the safeguards for your information, it's important to understand that the most effective safeguards and best practices for secure information handling are layered using a combination of physical, administrative, and technical safeguards. Adding layers makes the information more difficult to access by anyone who isn't authorized to do so. Layers help prevent both accidental and deliberate unauthorized disclosure of personal and sensitive information.

Information Systems

Information systems must also be classified and protected. Information systems are classified differently, and they can't be labelled in the same way a label can be put onto a printed document.

Instead, a Statement of Sensitivity (SoS), often prepared as part of a Threat Risk Assessment, should be completed to indicate the requirements for protection of confidentiality as well as additional requirements for safeguarding the integrity and availability of the information in that system.

The SoS will indicate the aggregate sensitivity of the information and information system assets and will suggest security controls and safeguards to protect both.

Distributing Information

Following are the mandatory safeguards necessary when performing some of the most common processes involved in secure information handling, such as distribution and storage.

When you distribute information, you are granting access to it. Personal and sensitive information must be safeguarded before, during, and after distribution.

Mandatory Safeguards for Distributing and Storing Information

UNCLASSIFIED

- No additional safeguards are required.

LOW SENSITIVITY

- Distribute ONLY to OPS employees and to known public service delivery partners.

MEDIUM SENSITIVITY

- Distribute ONLY to specified groups and work units, on a need to know basis (e.g., those individuals that require access to the information to do their job or provide a service). This could be a small group, or an entire program area, depending upon the business requirement for access and the necessity for confidentiality. Individuals should have basic security clearance;
- Notify all recipients of the sensitivity level of the information and the requirement for them to restrict further distribution.

HIGH SENSITIVITY

- Distribute ONLY to named individuals or positions with enhanced security clearance;
- Maintain a distribution list and require recipients to “sign” for the copy they receive;
- Print copies on darkly coloured paper to make photocopying difficult) and number each printed copy (sequentially, in ascending order beginning from 1);
- Mark each page “not to be copied or distributed without written consent of the program manager”;
- Inform all recipients that the information may not be redistributed;
- Encrypt digital information in storage and transmission (including when sending via email, if necessary).

Don’t send sensitive information to personal email accounts or smartphones. They are not secure!

Emailing Information

The OPS relies on email to accomplish daily communication tasks. Employees are much more likely to email a document to coworkers rather than send it by other means. But how do we restrict access to sensitive information in the digital realm? It is not recommended that this channel routinely be used to distribute high sensitivity information – instead, use a purpose-built system that has been developed for this purpose. If email is used, encryption and digital signatures must be applied.

Inboxes are not shared repositories. When saving an email, ensure you save it in a shared repository on your network drive, not in an inbox folder. Storing emails from external sources on a network drive will also enable you to classify and label the emails appropriately and protect to the level commensurate with its sensitivity.

Mandatory safeguards:

UNCLASSIFIED
- No additional safeguards are required.

LOW SENSITIVITY
- Distribute to OPS employees and known public service delivery partners.

MEDIUM SENSITIVITY
- Information classified as medium sensitivity may be emailed to a specific group of employees only, on a need to know basis with basic security clearance (e.g., those individuals that work with the information as part of their job).
- Take care when selecting recipients from the global address list and double-check the names of all recipients before clicking the SEND button.
- Consider including the words “MEDIUM SENSITIVITY” in the subject line or first line of the email.

HIGH SENSITIVITY
- Information classified as High Sensitivity may be emailed to named individuals or positions (enhanced security clearance may be required);
- Limit the use of email to distribute high sensitivity information.
- Include the words “HIGH SENSITIVITY” in the subject line and advise recipients not to redistribute without your authorization;
- Encrypt and digitally sign (using your Entrust PKI password) all email containing high sensitivity information.

Emails containing high sensitivity information must be sent encrypted and digitally signed within the OPS.

A "digital signature" is not an electronic representation of your hand-written name. It's actually a type of code used to demonstrate the authenticity of a digital message or document.

Encryption

Encryption scrambles information using a special algorithm – a mathematical equation which is often referred to as a "digital key". When the encryption key is applied to the electronic information you want to transmit, it jumbles the characters making the message meaningless to anyone who has not been given a "digital key" to decrypt the message. In the OPS, you can use your Entrust PKI password to encrypt and decrypt emails. This is the same password you use to login to MyOPS and the WIN system.

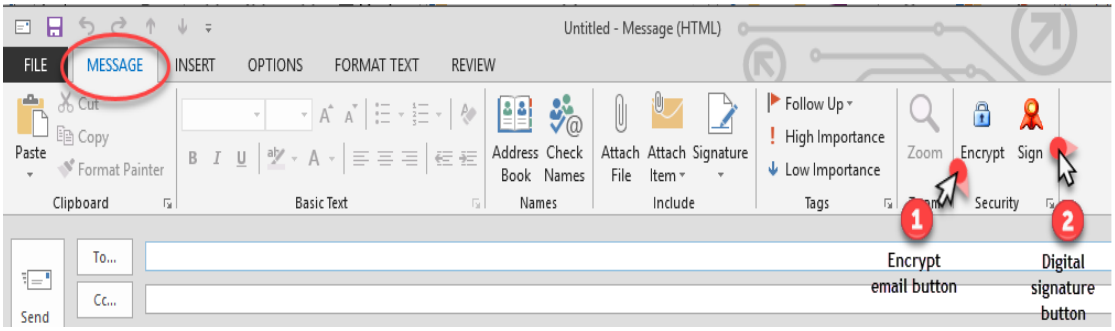
To encrypt and decrypt an MS Word document you need to use your PKI Entrust password. Never disclose your PKI Entrust password to anyone, not even your manager or the OPS IT Service Desk.

Digital Signature

All emails containing high sensitivity information must include a digital signature when sending to another member of the OPS. A valid digital signature provides evidence of the authenticity of the email, including who the email came from. When sending high sensitivity information by encrypted email, always remember to click both the "encrypt" and "digitally sign" icons on the Outlook message toolbar. If the icons do not already appear on your toolbar, contact the OPS IT Service Desk or use S.ODO to have this functionality enabled.

Encrypting and Digitally Signing Emails

To encrypt and digitally sign an email, create the email then click on the encryption and/or digital signature icons on the Outlook tool bar. Press the SEND button and then enter your PKI password at the prompt and your email will be sent encrypted. If the encryption and/or digital signature icons do not appear on your Outlook tool bar or if they are not responsive, contact the OPS IT Service Desk.



TIP

If the encrypt and digital signature icons do not appear on your toolbar, contact the OPS IT Service Desk.

Faxing Information

OPS staff may still use traditional fax machines and eFax services to distribute information. But be aware that sending information by traditional fax machine may increase the risk of unauthorized disclosure. It's easy to send a fax to the wrong telephone number or for the document to be left in plain view on the receiving fax machine. It's also possible for a fax to be intercepted during transmission.

Mandatory Safeguards:

UNCLASSIFIED

- Use a fax cover sheet labelled UNCLASSIFIED in the upper right-hand corner.

LOW SENSITIVITY

- Use a fax cover sheet labelled LOW SENSITIVITY in the upper right-hand corner;
- Use a fax machine located in a physically secure area.

MEDIUM SENSITIVITY

- Use a fax cover sheet labelled MEDIUM SENSITIVITY in the upper right-hand corner;
- Send from a fax machine located in a physically secure and supervised area with no access to the public;
- Contact the intended recipient to alert them BEFORE sending the fax (so they can await its arrival) and to re-confirm their fax number;
- Keep a copy of your fax transmission report.

HIGH SENSITIVITY

- DO NOT FAX high sensitivity information or records.
- Instead: Send the information by encrypted and digitally signed email (within the Ontario Public Service) or arrange for authenticated delivery (face-to-face or bonded courier) to

your known and named service delivery partners who can acknowledge receipt of the documents.

Faxing high sensitivity information is strictly prohibited. If you need to Fax other less sensitive information, always be sure the document and cover sheet are clearly labelled to indicate the appropriate sensitivity classification level.

Make it easy for others to safeguard personal and sensitive information by always using a fax cover sheet clearly showing the contact information of both the sender and receiver.

Storing Information

Information can be stored as documents and/or in electronic form. Different electronic storage media include, for example, desktop and laptop computers, smartphones, peripheral media such as CDs, DVDs, VHS tapes, and USBs. Business Records must be stored in shared repositories as per the Corporate Policy on Recordkeeping. In all cases, information must be stored and safeguarded in accordance with its assigned sensitivity classification level.

Mandatory Safeguards:

UNCLASSIFIED

- No additional safeguards are required.

LOW SENSITIVITY

- Store printed documents away from public view (ideally in lockable containers adequate to prevent casual disclosure such as a desk drawer or cabinet);
- Lock your computer before leaving it unattended.
- Use the Secure Document Destruction Services Vendor of Record for secure disposal of all paper business documents.

MEDIUM SENSITIVITY

- Restrict access to specified groups and work units;
- Individuals with access to Medium Sensitivity records may require a basic security clearance;
- Store paper copies in lockable containers such as a filing cabinet, desk storage compartment or secure record room;
- Keep file cabinets in a secure area with no public access;
- Seek prior approval from your program manager before removing medium sensitivity information from the office and use only OPS-issued laptops and digital storage devices (USB sticks or portable hard drives) to transport sensitive information;

- Lock your computer before stepping away from your desk;
- Use the Secure Document Destruction Services Vendor of Record for secure disposal of all paper documents.

HIGH SENSITIVITY

- Restrict access to named individuals or positions only;
- Ensure that all individuals given access to this information have presented government ID or other suitable credentials (including having their identity corroborated) to substantiate their claimed identity;
- Ask for evidence of security clearance before granting access to high sensitivity information; individuals with access to high sensitivity information may need to possess an enhanced security clearance;
- Ensure all electronic files in encrypted form on all computer hard drives, network drives, or other digital storage media.
- Seek your Director's approval before removing any high sensitivity information from the workplace on a laptop or other mobile device;
- Use only OPS-issued laptops and USB sticks with encryption capabilities (orderable via S.ODO);
- Number all paper copies and maintain an audit log of who has which numbered copy;
- Keep documents in lockable file cabinets in a physically secure, supervised area with no access to the public;
- Store paper documents in lockable, CSA fire-rated file cabinets (particularly if they are original documents);
- Maintain a key log to control who has keys to any drawer, file cabinet, room or other storage area used to secure high sensitivity information:
    - confirm the list on a periodic basis;
    - retrieve all keys from employees leaving active employment in the program area;
- Lock your computer before leaving your workstation unattended.

When removing electronic information from the office, use only OPS-issued laptops and secure USB sticks (with encryption).

Develop everyday protection habits like keeping the desktop clear and locking office doors when the work area is unattended. If you're going to be away from the work area for any length of time, don't wait for the screen-saver to come on. Use Ctrl/Alt/Delete to lock your workstation.

Check all furniture, file cabinets, printers, faxes and photocopiers for leftover documents before releasing them as surplus assets or returning them to the vendor.

High sensitivity information may only be accessed by named individuals or positions; therefore, electronic versions must be encrypted in storage and in transmission.

While sensitive information needs to be protected in storage, it also must be made available in response to an access request through the FOI process, if it is determined that the information should be released. Additionally, safeguards for sensitive information should not preclude authorized program owner access required to administer the program.

Encrypting documents in storage

High sensitivity information must be encrypted in storage and in transmission.

To encrypt documents in storage such as MS Word, Excel, PowerPoint, Access databases, Adobe, and other file types using Entrust, first, find the file in the file directory and then follow these steps to encrypt it and, at the same time, to create a list of authorized people who will be able to access the file.

For computers with and MS Office 2003 and 2007

- Right click on the file to be encrypted, click on **SECURE FOR LIST,** click on **SELECT RECIPIENTS,** and enter your PKI password.
- When the Entrust “select recipients” window appears, change the “Look In” window to “Directory Search”
- In “Search For” Window, key in the recipient’s name
- When the list appears, highlight the correct recipient’s name and click on Add>> (the name will be added to the “selected recipients” window and click **OK**

For computers with Windows 10 and MS Office 2013

- Right click once on the file to be encrypted to highlight it; select “Encrypt File….”
- On the “Welcome to the Encrypt file Wizard” window you will see the file name with the automatically added suffix “.docx”; click **NEXT**;
- On the “Encryption Options” window click on the little box beside “Encrypt the files for other people in addition to yourself”; click **NEXT**;
- On the “Additional Recipients” window click **ADD** (if you do not wish to grant access to others, skip this and click **NEXT**);
- On the “Select People” window, in the Search field, key in the name of the first additional person you would like to grant access to this file – first name then last name as it appears on the Entrust certificate list – (e.g., if Doug Smith is not found – try Douglas Smith);
- Click **SEARCH** and the person’s name and email will show in the large window;
- When all persons have been added to the list, highlight the first name and then click **OK** then click **NEXT**;
- On the “Completing the Encrypt Files Wizard” window make sure you click on the box beside “delete the original file on finish” and click **FINISH**;
- To access the encrypted file, double click on it and if you are not already logged in, key in your PKI (WIN) password;
- On the “Entrust Entelligence Security Provider” window click **YES** and click **FINISH**.

The file will then be encrypted and can only be decrypted by you and those whom you've specified on the list you created. You can tell the encryption has worked because a little yellow key will be placed in the file name in the file directory listing.

Remember! When you decrypt the file, the system creates a decrypted version which it places near the encrypted version or at the bottom of the file directory. This decrypted version of the file must be deleted when you're finished making any changes to it. Changes to the decrypted version will be applied to the encrypted version automatically. If you use the automatic delete in step 12 above you'll avoid accidentally deleting both versions.

Encrypting databases, applications or systems requires other controls which will have to be implemented. For further information or assistance contact the OPS IT Service Desk.

Password protecting MSWord documents is possible but not recommended. If you forget what the password is, it can't be retrieved or changed, not by the OPS IT Service Desk or even Microsoft. You will not be able to open the document again or any of its backup copies. Caution is strongly advised.

For more information about cryptography refer to the GO IT Standard 25.12 "Use of Cryptography." This document can be viewed on the MyOPS intranet website, OPS Directives and Policies page, under I&IT Management.

Appropriate Recordkeeping Processes to Identify Which Records to Retain, Transfer or Dispose Of

The Archives and Recordkeeping Act, 2006 states that the retention, transfer and disposition of records in any format is governed by a records schedule approved by the Archivist of Ontario. The records schedule determines how long records must be retained in the ministry, and their final disposition (i.e. either transfer to the Archives of Ontario or destroy). If transferring archival digital records, please refer to the Guideline for Transferring Archival Digital Records to the Archives.

Simply deleting or reformatting electronic information does not guarantee that the information can't be reconstituted. It must be made unreadable by overwriting it electronically, or when that isn't possible, it must be made inaccessible by physically crushing the device so it's no longer usable.

Appropriate Disposal of Information

Paper Documents

All paper documents, regardless of their sensitivity classification level, must be placed in the secure disposal containers provided by the Secure Document Destruction Vendor of Record. Unclassified information may be recycled.

If your office doesn't have the Secure Document Destruction Services shredding containers, access the Supply Chain Ontario intranet from the MyOPS website and search for vendor of record number OSS-076789.

Information on Computerized Devices & Digital Storage Media

Information on computerized devices and digital storage media must be made inaccessible using the sanitization process and hardware destruction procedures approved for use in the OPS. Please refer to the GO-ITS 25.20 Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media and the corresponding Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media Guidelines.

When disposing of information, make sure all backup copies are deleted too.

Additional Safeguards

Reclassifying Information

Information may be reclassified at any point in its lifecycle.

For example, before the provincial budget is released, drafts of the budget documents would likely be considered "high sensitivity". However, upon its release to the public, the same information is then considered "unclassified" and may be downloaded from the Ministry of Finance's Internet website.

In addition, multiple pieces of Medium sensitivity information (including personal information) may be reclassified to High sensitivity, if the information is stored together and the potential of harm or injury increases as a result of the aggregation.

The information owner may change the sensitivity classification level assigned to a given piece of information if it's appropriate to do so. However, only the program manager may reclassify information labelled as "high sensitivity".

Information received from other jurisdictions or organizations

Classified information received from other organizations or jurisdictions should not be reclassified. Instead, follow any safeguards or special handling instructions received from that organization or jurisdiction.

However, if the information has not yet been classified, then classify the information in accordance with the sensitivity classification schema in this document, then label and safeguard the information accordingly.

Service Level Agreements

All contractual agreements and service level agreements with third party service providers who have access to, or custody of, information and/or information technology must include the requirements of the Corporate Policy on Information Sensitivity Classification and these guidelines.

Agreements must include the mandatory requirement that only OPS-issued computing devices and secure USB sticks be used. In addition, all third-party service providers who require access to government information must sign a non-disclosure agreement and undergo a security clearance before being granted access to any sensitive government information.

Threat/Risk and Privacy Impact Assessments

A Threat Risk Assessment (TRA) is a formalized process used to determine the risks to information and information technology (I&IT) assets and to provide recommendations about ways in which program owners can lower these risks to acceptable levels. A Privacy Impact Assessment evaluates a program's or information system's privacy risks and compliance with legislation such as the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Protection Act (PHIPA).

It's the responsibility of the program area to ensure that they have security controls in place at acceptable levels to safeguard the confidentiality of the data they create and collect, and to address the information's integrity and availability requirements.

For more information about Cyber Security services, please visit https://intra.ontario.ca/cyber.

Glossary

In this guideline,

"availability" means to be present and ready for use.

"confidentiality" means a condition of, or the requirement for, privacy or secrecy.

"control" means not in the physical possession of information but with a legal/contractual right to deal with it.

"custody" means in the physical possession of the information (excluding unsolicited or accidental possession).

"digital signature" means a mathematical scheme for demonstrating the authenticity of a digital message or document identifying the sender and proving that the message was not altered in transit.

"disclosure" means any exposure to recorded information, whether deliberate or accidental, authorized or unauthorized and includes the ability to read only, or to read and also write to or otherwise manipulate the information.

"disposal" means the act or process of getting rid of something that is no longer required and does not need to be retained.

"disposition" means the final action taken with a record when its retention period is over

"encryption" means to alter text using a secret code for the purposes of making it unreadable by anyone who isn't authorized to see it.

"extremely serious personal or enterprise injury" means a level of injury causing catastrophic physical harm, even death, or ruinous financial injury, or unqualified or permanent loss of reputation to an individual, the Government of Ontario, or a third party company or organization that does business with the government.

"harm" means the damage (including physical, mental, emotional, financial) that results in response to an injury.

"injury" means a security incident that causes harm.

"information" means recorded information in any form, in any medium, and at all stages of its life cycle including information created, recorded, transmitted or stored in digital form or in other intangible forms by electronic, magnetic, optical or any other means, but does not include a mechanism or system for creating, sending, receiving, storing or otherwise processing information.

"integrity" means a condition of, or the requirement for, information that has not been modified or deleted in an unauthorized and undetected manner.

"ministry" means a ministry of the Government of Ontario and includes all I&IT clusters and applicable agencies.

"business owner" means any program director or equivalent having authority and accountability under legislation, regulation, policy or other instrument for particular business activities and for the business records relating to those activities.

"privacy impact assessment" is both a due diligence exercise and risk management tool. It is a proactive approach designed to help protect privacy by identifying and analyzing privacy-related risks early enough to be able to take appropriate action; avoiding, eliminating or minimizing negative impacts on privacy; and complying with relevant privacy legislation and assess broader privacy implications.

"record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes:
(a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics and any copy thereof;
(b) any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution ("document").

"records schedule" means an Archivist of Ontario-approved document that identifies and describes the records made and received by public bodies and set out retention periods and final dispositions for those records, the format in which the records are to be kept and which records. Records schedules consist of records series (Page 11, Corporate Policy on Recordkeeping, 2015).

"risk" means the potential outcome of the successful application of a threat agent.

"safeguard" means a protective and precautionary measure intended to prevent a threat agent from reducing security or causing harm and injury.

"sanitize" means to make information inaccessible.

"sensitive information" information, that if released without authorization, would cause harm (personal or enterprise injury, embarrassment, unfair economic advantage, etc.).

"serious personal or enterprise injury" means intense physical harm, or pronounced financial injury, or degradation of reputation, to an individual, the Government of Ontario or a third party company or organization that does business with the government.

"significant financial loss" means a loss of funds in excess of one-hundred thousand dollars.

"social hardship" means wide-spread severe public suffering or privation.

"Threat/Risk Assessment" means a formalized process to determine the risks to information and information technology. The assessment determines the sensitivity classification level of all information involved, the appropriateness of the security controls currently in place to protect the information's confidentiality, integrity, and availability, and provides recommendations to increase the efficiency and effectiveness of those controls as required.

"unauthorized disclosure" means unapproved access to information whether deliberate or accidental and includes unapproved reading and/or writing to the information.

"user" means anyone authorized to access recorded information in the custody or under the control of the Government of Ontario.

Appendix

Information Sensitivity Classification Example Scenario

You're a manager in the Ontario Public Service, and you've been asked to create a draft strategy that reflects an important, public-facing branch initiative on "going green". The draft will need to be reviewed by your team and then approved by your director. A public communication will take place after it's approved. Your director has stressed how really important this document is to her and how it plays a vital role in setting a strong foundation for your division's "green" strategy.

How would you classify this information?

Unclassified?
At this stage, this document is not ready for the public to see and, therefore, should not be classified as "unclassified".

Low Sensitivity?
This is the right classification for the document primarily because many people in the OPS may need to review it and add input.

Medium Sensitivity?
This is an overly cautious approach and will probably result in unnecessary access restrictions as well as increased safeguard costs.

High Sensitivity?
Because the strategy is very important to the director and the division, the manager may think that it should be classified as high sensitivity. But, this is an excessively cautious approach and will result in more costs than are necessary to protect this information.

This classification will make it difficult for authorized staff to access and manage it (e.g. it must be stored and transmitted in encrypted form). The high sensitivity classification should only be used when personal health information is involved or there is a clear potential for extremely serious harm and injury.

Remember – high sensitivity information needs to be controlled to ensure it is accessible by named individuals or positions only. Distribution of the information needs to be audited vigorously. It needs to be stored and transmitted in encrypted form for absolute protection, and it must be preserved in temperature-rated, fire-proof file cabinets.

Strike a balance between the need for program functionality, especially access to program information, and the need for confidentiality (secrecy or privacy). Work to reduce or eliminate the harm and injury that might result through unauthorized disclosure of the information.

Additional Resources

Legislation

Freedom of Information and Protection of Privacy Act, R.S.O.1990, c.F.31;
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
Personal Health Information Protection Act, S.O.2004, c.3, Sched. A;
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm
Archives and Recordkeeping Act, S.O. 2006, c. 34, Sched. A;
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_06a34_e.htm

Corporate Directives, Policies, Standards, Guidelines and best practices

- Management and Use of Information and Information Technology (I&IT) Directive;
- Corporate Policy on Information and Information Technology Security;
- Corporate Policy on Information Sensitivity Classification;
- Acceptable Use of Information and Information Technology (I&IT) Resources Policy;
- Corporate Policy on Recordkeeping;
- Corporate Policy on Protection of Personal Information;
- GO-IT Standard 25.20 Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media;
- GO-IT Standard 25.12 Security Requirements for the Use of Cryptography;
- GO-IT Standard 25.15 Security Requirements for Password Management and Use;
- GO-IT Standard 25.21 Security Requirements for Cloud Services
- Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media Guidelines;
- Guidelines - Managing Records in a Shared Drive.
- Freedom of Information and Protection of Privacy Manual
- The Guideline for the Protection of Information When Contracting for Services;
- Taking the Right Steps – A Guide to Managing Privacy and Privacy Breaches;
- Government of Ontario Records Schedule Requirements.

E-learning available on the OPS Learning and Development intranet website - Centre for Leadership and Learning

- It's Everyone's Responsibility e-learning
- Privacy Basics – e-learning
- Keep I.T. Secure - video

- Records and Information Management (RIM) 101

Sensitivity Level		High Sensitivity	Medium Sensitivity	Low Sensitivity	Unclassified
	Definition	Information reasonably expected to cause extremely serious personal or enterprise injury, significant financial loss, loss of life or public safety, social hardship and major political or economic impact if released without authorization.	Information reasonably expected to cause serious personal or enterprise injury, loss of competitive advantage, loss of confidence in a government program, moderate financial loss if released without authorization	Information reasonably expected to cause no serious personal or enterprise injury if released without authorization.	Information reasonably expected to cause no harm or injury if released without authorization.
	Examples	Witness Protection Program records; personal health and medical records; identity of undercover police officers; child protection, offender or evidentiary data. Personal Financial records, cabinet records, deliberations and support documents	Personal information governed by FIPPA, for example a person's name or phone number or a photograph; Briefing/policy notes; business tax returns; OPS personnel files.	Ordinary staff meeting agendas; announcements about new business procedures or processes; fund raising outcomes; simple escalation procedures.	Government of Ontario web content; speeches that have been delivered; Travel Ontario brochures; blank public forms and applications; enacted legislation.
	Label	Label all records **"HIGH SENSITIVITY"**	Label all records **"MEDIUM SENSITIVITY"**	Label all records **"LOW SENSITIVITY"**	Label all records **"UNCLASSIFIED"**
Transmission	**Mail or Courier**	Seal envelop and label **"HIGH SENSITIVITY"** and **"to be opened by addressee only.**" Hand deliver or send via bonded courier to named recipient only (and request signature on delivery).	Seal envelop and label **"MEDIUM SENSITIVITY.**" Hand deliver, send by registered mail or bonded courier.	Single envelope, sealed without security markings. Internal and regular mail.	No additional safeguards.
	Facsimile	Faxing prohibited.	Use Government of Ontario fax cover sheet marked **"MEDIUM SENSITIVITY"**; include contact information of both sender and receiver. Notify recipient in advance and send from a secure area with no access to the public.	Use Government of Ontario fax cover sheet marked **"LOW SENSITIVITY."**	Use Government of Ontario fax cover sheet marked **"UNCLASSIFIED."**
	Email	Email encrypted using Entrust (PKI). Label as **"HIGH SENSITIVITY".**	Email - label **"MEDIUM SENSITIVITY"**	Internal network and email marked **"LOW SENSITIVITY".**	Internal network and email marked **"UNCLASSIFIED".**
	Transport	For removal from the office, obtain permission from program Director then copy to OPS-issued laptops and USB sticks with approved encryption capability.	For removal from the office, obtain permission from program manager; copy to approved laptops and USB sticks only with approved encryption capability.	For removal from the office, copy to approved laptops and USB sticks only.	No additional safeguards.
Storage	**Paper copy**	In lockable, fire-proof, filing cabinets. Clean desk policy when work area is unattended.	In lockable, filing cabinets, desk drawers or overhead bins. Clean desk policy when work area is unattended.	In lockable desk draws or overhead bins sufficient to avoid casual disclosure.	No additional safeguards.
	Electronic media	Encrypt using approved encryption methods. Use access control lists.	Use access control lists; discretionary encryption.	No additional safeguards	No additional safeguards.
Destruction	**Paper copy**	Use shredding bins provided by the Secure Document Destruction Services Vendor of Record (SDDS)			Use recycle bins or shredding bins provided by the SDDS VoR.
	Electronic media	Follow procedures outlined in "GO-IT Standard 25.20 Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media" and its corresponding user Guidelines.			

Document Management

Contact Information

Information Sensitivity Classification Guidelines	
Contact	Alex Fanourgiakis Manager, Cyber Security Policy and Standards, Ministry of Government and Consumer Services Alex.Fanourgiakis@Ontario.ca 647-776-1167
Writer	Sylvia Nikodem Security Policy Advisor Cyber Security Policy and Standards, Ministry of Government and Consumer Service Sylvia.nikodem@Ontario.ca 416-327-2502
Effective Date	
Date Last Amended	
Date of Next Review	
Supporting Documents	See Page 24 – Additional Resources