Index

- Viewing in Public
- Network Transmission
- Transfer to another PC
- Speaker Phones
- Telephone Conversation

Overview

Information and Classification Procedures
Information classification is a critical process that needs to be adhered to ensure OLG meets it's regulatory and legal commitments for information protection and privacy. This document provides the Procedures to use in the classification and handling of information in compliance with the **Information Classification & Handling policy CP-04-05-009.**

The Information Classification & Handling policy CP-04-05-009 identifies the ownership of the information and the classifications to be used for OLG, when the information has to be classified, how the classification label can be changed, and information handling Procedures.

Employees Responsibility - Every employee who has access to OLG information or information systems has an important information security role in the organization. Each OLG employee is personally responsible for the protection of information that has been entrusted to their care. All employees who come into contact with sensitive OLG internal information are expected to familiarize themselves with the OLG Information Classification & Handling policy CP-04-05-009 and to consistently use these same ideas in their daily OLG business activities. Although this document provides overall guidance, to achieve consistent information protection, employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a model for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

Consistent Approach required - Consistent use of this Information Classification and Handling system is essential if sensitive information is to be adequately protected. Without the consistent use of this Information Classification system, OLG unduly risks loss of customer relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage. These Procedures will protect sensitive information no matter what form it takes, what technology is used to process it, who handles it, where the information may be located, and in what stage of its life cycle the information may be. A single lapse in the security of the information can have significant long-term consequences.

Addresses Major Risks - The OLG information classification system, as defined in this document, is based on the need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect OLG information from unauthorized disclosure, use, modification, and deletion.

Applicable Information - This Information Classification document is applicable to all information in the possession or under the control of OLG. Confidential information entrusted to OLG by customers, business partners, suppliers, and other third parties must be protected. Employees are expected to protect third-party information with the same care that they protect OLG information.

Classification Labels

Owners and Production Information - All production information types possessed by or used by a particular organizational unit within OLG must have a designated Owner. Production information is information routinely used to accomplish business objectives. Examples include payroll summaries, shipping schedules, and managerial cost accounting reports. Information Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are designated members of the OLG management team who act as stewards, and who supervise the ways in which certain types of information are used and protected. All reference to sensitive information refers to Restricted and Confidential information.

INTERNAL - This will be the default classification label which will apply to all information that does not clearly fit into the two higher classifications of Restricted or Confidential. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact OLG or its employees, suppliers, business partners, or its customers. Examples include the OLG telephone directory, dial-up computer access numbers, new employee training materials, internal policies, procedures and manuals.

RESTRICTED - This classification label applies to the most sensitive business information that is intended for use strictly within OLG. Its unauthorized disclosure could seriously and adversely impact OLG, its customers, its business partners, and its suppliers. Examples include merger and acquisition documents, corporate level strategic plans, litigation strategy memos, and reports on breakthrough new product research, and Trade Restricted such as certain computer programs.

CONFIDENTIAL - This classification label applies to less-sensitive business information that is intended for use within OLG. Its unauthorized disclosure could adversely impact OLG or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is included in this classification. Examples include employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally-generated market research, computer passwords, identity token personal identification numbers, and internal audit reports.

PUBLIC - This classification applies to information that has been approved by OLG management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Other Labels - OLG department or division-specific information classification labels are permissible, but must be consistent with and supplemental to the OLG information classification system.

Owners and Access Decisions - Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. Owners must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

Labeling

Information Collections - Employees who create or update a collection of information are responsible for choosing an appropriate information classification label for the new collection. This label must be consistent with the decisions made by the relevant Owners and generally should be the most restricted classification level found in the collection.

Consistent Classification Labeling - If information is sensitive, from the time it is created until the time it is destroyed or declassified, it must be labeled with an appropriate information classification designation. Such markings must appear on all manifestations of the information, such as documents, reports, hard copies, photo copies, Approved Storage Devices. Employees must not remove or change information classification system labels for sensitive information unless the permission of the Owner has been obtained.

Labels believed to be incorrect - If the recipient of OLG internal information believes that the information classification label accompanying this information is incorrect, the recipient must protect the information in a manner consistent with the more stringent of the two possible classification labels. Before using this information or distributing it to any other party, such a recipient must check with the Information Owner to ensure that the label currently applied to the information is correct.

Labeling Computer Storage Media - All Approved Storage Devices and other computer storage media containing sensitive information must be externally labeled with the appropriate sensitivity classification. Unless it would adversely affect the operation of an application program, computer files containing sensitive information must also clearly indicate the relevant classification label in the first two data lines.

Storage Media - If information recorded on computer storage media with a higher sensitivity classification is moved to media with a lower sensitivity classification, then the media with the lower sensitivity classification must be upgraded so that its classification reflects the highest sensitivity classification. For example, if information labeled Restricted were to be placed on a Approved Storage Device containing information with no label, then the Approved Storage Devices must immediately be reclassified as Restricted.

Teleconferences - Teleconferences and telephone conference calls where sensitive information will be discussed must be preceded by a statement about the sensitivity of the information involved. Teleconferences and telephone calls where sensitive information is discussed must be preceded by a determination that all parties to the discussion are authorized to receive the sensitive information. Persons other than those specifically invited must not attend meetings where sensitive information will be discussed.

.

Third-Party Interactions

Third Party - Contractors, consultants, temporaries, volunteers and every other type of individual or entity that is not an OLG employee, is by definition a third party.

Third Parties and the Need to Know-Unless it has been specifically designated as Public, all OLG internal information must be protected from disclosure to third parties. Third parties may be given access to OLG internal information only when a demonstrable need to know exists, and when such a disclosure has been expressly authorized by the relevant OLG information Owner.

Disclosures from Third Parties and Non-Disclosure Agreements-Employees must not sign non-disclosure agreements provided by third parties without the authorization of OLG legal counsel designated to handle intellectual property matters. These forms may contain terms and conditions that unduly restrict the future business directions of OLG. The Non-Disclosure Agreement form can be obtained from by OLG Legal.

Third-Party Requests For OLG Information-Unless an employee has been authorized by the information Owner to make public disclosures, all requests for information about OLG and its business must be referred to Public Relations and Procurement. Such requests include but not limited too questionnaires, surveys, newspaper and TV Interviews.

Owner Notification-If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the Information Owner and the Information Security department must be notified immediately.

Handling

Printing -Printers must not be left unattended if sensitive information is being printed. The persons attending the printer must be authorized to examine the printed information. Unattended printing of sensitive information is permitted only if physical access controls are used to prevent unauthorized persons from entering the area by the printer and viewing the material being printed. Some OLG printers are capable of **Locked Printing** which will prevent unauthorized access of print output. **Contact the ITSC for Locked Printing process.**

Use of Outside Services-Prior to sending any sensitive information to a third party for copying, printing, formatting, or other handling, and the third party must sign an OLG non-disclosure agreement. The Non-Disclosure Agreement form can be obtained from by OLG Contract Management.

Backup Storage Media - All sensitive information recorded on backup computer media and stored outside OLG offices must be in encrypted form. If an encryption system with key escrow is not used for this purpose, all keys used to make these backup copies must be promptly provided to the Information Security department shortly after their initial use. If your department or business requirements dictate the need to encrypt information, **contact the ITSC for assistance**.

Envelopes -If sensitive information is to be sent through internal mail, external mail, or by courier, it must be enclosed in two envelopes or containers. The outside envelope or container must not indicate the classification or the nature of the information contained therein. The inside sealed and opaque envelope or container must be labeled with the appropriate classification label.

Delivery of Computer Output - Where possible, sensitive computer system output must be personally delivered to the designated recipients. Such output must not be delivered to an unattended desk, placed in an uncontrolled computer output receptacle, or left out in the open in an unoccupied office. It may be made available to only the designated recipients through password-protected fax mailboxes, departmental or personal computer output lockers, or other physical security methods.

Removal from Offices - Sensitive OLG information must not be removed from OLG premises unless there has been prior approval from the information's Owner. This includes Approved Storage Devices, hard-copy output, and paper memos.

Locked Containers in the Office - Sensitive information in hardcopy form must be secured in locked containers (desk, file cabinet, etc.) when not actively in use, even if it is within a building to which access is controlled.

Locked Containers Off-Site - Whenever a hardcopy version of sensitive information is removed from OLG premises, it must be carried in a locked briefcase or container when not in use. If such information is transported in a motor vehicle, if viable, should be locked in the trunk. Sensitive Information should not be left in an unattended motor vehicle, even if the vehicle is locked.

Destruction and Disposal

Destruction and Disposal - All OLG information must be destroyed or disposed of when no longer needed for business purposes. To support this, Information Owners must review the continued value and usefulness of information on a periodic basis. Owners also must review the data retention schedule to determine the minimum legal periods that information must be retained. Please contact OLG Document Management Services for retention guidelines.
Reference:
OLG Data Backup, Retention and Restoration Policy CP-04-06-002 and Asset Disposal Policy and Transfer Policy CP-02-03-016.

Destruction and Locked Boxes - All sensitive information no longer being used or no longer needed must be placed in designated locked metal boxes until such time as authorized OLG personnel or a bonded destruction service picks it up. The metal disposal bins are already in place at OLG corporate sites. If no locked disposal boxes are in the immediate vicinity, sensitive information in hardcopy form must be shredded, while sensitive information in all other forms must be delivered to the Corporate Security department for secure destruction. Erasing or reformatting magnetic media such as Approved Storage Device is not an acceptable data destruction method. The use of overwriting programs approved by the Information Security department is permissible as a way to destroy sensitive information on magnetic storage media such as Approved Storage Device as per the **Asset Disposal and Transfer Policy CP-02-03-016.**

Destruction Approval - Employees must not destroy or dispose of potentially important OLG records or information without specific advance management approval. Records and information must be retained if they are likely to be needed in the future, regulation or statute requires their retention, or they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts. Any questions about data destruction must be referred to the Information Owner or the Owner's delegate. Reference: OLG Records Retention Schedules. Document Management Services has been tasked by the corporation as the Records Retention Schedule process owner.

Photocopies - All waste copies of Restricted information that are generated in the course of copying, printing, or other sensitive information handling must be destroyed. If a copy machine jams or malfunctions when employees are making copies of Restricted information, the involved employees must ensure every attempt is made to ensure all copies of the information are removed from the machine or destroyed beyond recognition.

Equipment Disposal Or Servicing - Before computer or communications equipment is sent to a vendor for trade, servicing, or disposal, all OLG sensitive information must be destroyed or concealed according to methods as per the **OLG Asset Disposal Policy and Transfer CP-02-03-016**. Internal hard drives and other computer storage media may not be donated to charity, disposed of in the trash, or otherwise recycled unless they have been subjected to overwriting processes.

Physical Security

Office Access-Access to every office, computer room, and work area containing sensitive information must be physically restricted. Management responsible for the staff working in these areas must consult the Corporate Security department to determine the appropriate access control method.

Locked When Not In Use-When not in use, sensitive information must be protected from unauthorized disclosure. When left in an unattended room, such information must be locked in appropriate containers.

Unauthorized Screen Viewing-The screens on computers used to handle sensitive information must be positioned such that unauthorized persons cannot readily look over the shoulder of the person using the workstation.

Special Considerations for Restricted Information

Background Checks - All employees who will have access to Restricted information must have passed a standardized background check performed by the Human Resources department. Access to Restricted information must not be provided before this background check is completed.

Storage on Personal Computers - If Restricted information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must support and utilize a system access control list which is controlled by a privilege and held only by OLG system administrators. When these users are not currently accessing or otherwise actively using the Restricted information on such a machine, they must not leave the machine without logging off, invoking a screen saver, or otherwise restricting access to the Restricted information.

Couriers - Restricted information in hardcopy form must be sent by trusted courier or registered mail. Other methods such as regular mail are prohibited.

Transportation with Computers - Employees in the possession of portable, laptop, notebook, handheld, personal digital assistant, and other transportable computers containing Restricted OLG information must not leave these computers unattended at any time unless the Restricted information has been encrypted. If Restricted information is to be transported in computer-readable storage media, it must be in encrypted form. **Contact the ITSC for assistance.**

Viewing in public - Employees should avoid traveling on public transportation when in the possession of Restricted information. Restricted information must not be read, discussed, or otherwise exposed on airplanes, or in restaurants, elevators, restrooms, or other public places. OLG employees must not take Restricted OLG information into another country unless permission has been obtained from the Information Owner.

Transmission over Networks - If OLG Restricted information is to be transmitted over any communication network, it must be sent only in encrypted form. Such networks include internal electronic mail systems, the Internet, and dial-up lines. All such transmissions must use a virtual private network (VPN) or similar software as approved by the Information Security department. **Contact the ITSC for assistance.**

Transfer to another Computer - Before any Restricted information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred. **Contact the ITSC for assistance.**

Speaker Phones – Restricted information must not be discussed on speakerphones unless all participating parties acknowledge that no unauthorized persons are in close proximity such that they might overhear the conversation. Exercise caution as to people within listening area. Employees must refrain from leaving messages containing Restricted information on answering machines or voice mail systems.

Telephone Conversations - Employees must take steps to avoid discussing sensitive information when on the telephone. If discussion of such information is absolutely required, employees must use guarded terms and refrain from mentioning sensitive details beyond those needed to get the job done.

Department / Stakeholder Reviews & Approvals		
Department Approver	**Approve Yes or No**	**Date**
Danny Conte, Security Architect, Information Security Office	YES	Jan 2008
Laurie Laudadio Manager, Information Security Office	YES	Dec 2007
Matthew Power, Manager, Information Security Office	YES	Jan 2008
Dan Borghese, Sr Manager, IT Risk Management and Planning	YES	Jan 2008
Barry Sussman, Document Management Services	YES	June 2008
Carla Fabbro, Finance Manager, New Initiatives Corporate Accounting and Reporting	YES	June 2008
Marty Wright, Director Technology Internal Audit & Risk Mgmt	YES	June 2008

REVISION / REVIEW HISTORY			
Date	**Requested By**	**Updated By**	**Summary of Revision**
Dec 09 2007	External Audit	IT Security Office	• New Procedure
Feb 14 2010	IT Security Office	IT Security Office	• Removed 'draft' watermark
Oct 2019	IT Security Office	IT Security Office	Updated Policy titles: Data Backup, Retention and Restoration Policy CP-04-06-002 Asset Disposal Policy and Transfer Policy CP-02-03-016.