office directive

IGDS Number 456 (Version 1)

International Labour Office

5 January 2016

Classification of ILO Information Assets

Introduction

1. This Directive is issued further to article 8 of the ILO Constitution which delegates overall responsibility to the Director-General for the efficient conduct of the Office.

2. This Directive establishes the policy for classification of information entrusted to, or originating from, the ILO ("ILO Information Assets"), as well as the roles and responsibilities to assist the Office with classifying ILO Information Assets.

3. This Directive supersedes Director-General's Announcement, *ILO policy on public information disclosure*, IGDS No. 8 (version 1), of 11 April 2008, and should be read in conjunction with:

   - Office Directive, *The use of email and Internet in the ILO*, IGDS No. 452 (version 1), of 5 January 2016;
   - Office Directive, *Ethics in the Office*, IGDS No. 76 (version 1), of 17 June 2009;
   - Director-General's Announcement, *ILO accountability framework*, IGDS No. 137 (version 1), of 15 January 2010;
   - Office Procedure, *Security of electronic information*, IGDS No. 164 (version 1), of 25 May 2010; and
   - Office Directive, *Information technology governance*, IGDS No. 333 (version 1), of 31 July 2013.

4. This Directive is effective as of the date of issue.

Scope

5. This Directive applies to classification of all ILO Information Assets as part of a framework to ensure that they are identified, classified and protected throughout their respective life cycles. The appropriate level of protection required corresponds to the sensitivity, value and criticality of these Assets. Classification facilitates determining baseline security controls for the protection of these Assets. Detailed rules concerning the handling and retention of Information Assets will be announced shortly.

6. ILO Information Assets include, but are not limited to, ILO communications, correspondence, databases, documents, electronic messaging, graphics, graphs, images, presentations, publications, repositories, sound, spreadsheets, text, video and web content.

7. This Directive applies irrespective of the medium on which ILO Information Assets reside and regardless of format.

Guiding principles and classification levels

8. The ILO produces and collects a vast amount of information in various forms. The ILO is responsible for the security and safeguarding of information to ensure the integrity, availability and, where required, the confidentiality of this information.

9. The overall approach to classifying and using information is based on the understanding that the work of the ILO and its officials should be open and transparent and that information concerning ILO policies, strategies and operational activities is available to its constituents, partners in the UN system, the development community and the wider public. It follows that there is a presumption in favour of public disclosure of ILO Information Assets.

10. At the same time, strict guidelines on how to produce and classify information are required to ensure that critical assets are protected from internal and external threats, including the unauthorized disclosure, modification or loss of information, and to minimize the impact of financial, reputational and legal risks.

11. To implement security at the appropriate level, as well as identify, handle and facilitate compliance, ILO Information Assets are classified as follows.

Public/unclassified

12. ILO Information Assets available to the public can normally be accessed through the ILO public web page, its libraries or are published by the ILO. Some publications and documents may only be made available on a cost-recovery basis, particularly when the request is from for-profit organizations. The main types of unclassified information include:

- general information about the role and function of the ILO;
- basic and regulatory texts;
- International Labour Conference documents;
- Governing Body documents (other than those related to private sittings);
- agreements concluded between the ILO and intergovernmental organizations under article 12 of the ILO Constitution;
- programme and budget documents;
- audited financial statements;
- reports of the External Auditor;
- Decent Work Country Programmes;
- reports of regional and sectoral meetings and of other official meetings convened by the ILO;

- press releases and other communication material;
- other official documents;
- selected internal governance documents; and
- archives (subject to 30- and 50-year access rules).

Restricted/classified

13. Information not otherwise considered "public" will, by default, be considered to be classified as "restricted".

14. Restricted information is intended only for internal use by ILO officials when carrying out their functions. It includes internal inter-office or intra-office communications, such as draft documents or internal opinions.

15. Restricted information must be protected from unauthorized access, modification, transmission, storage or other use. This includes information that is restricted to ILO officials and third-parties designated by the Office who have a legitimate purpose for accessing such information.

16. Information is considered restricted if its unauthorized disclosure could lead to the disruption in the normal functioning of the ILO, result in reputational damage to itself or its constituents, lead to a loss of public confidence or if it could undermine the Organization's free and independent decision-making.

Confidential/classified

17. Information classified as confidential (e.g. personal, legal, medical, safety, security or employment-related information) is covered by privilege or is related to internal investigations and procedures that are being carried out with respect to either an ILO official or entity engaged either directly or indirectly by the ILO.

18. The unauthorized disclosure of confidential information could be expected to cause grave damage to the confidence placed in the Director-General and the ILO per se, or endanger the safety, privacy, rights or security of an individual. Confidential information therefore requires strict control on access and use, which is limited only to authorized officials on a "need-to-know" basis.

19. The classification of confidential information is controlled and established by the Staff Regulations, CABINET, the ILO's Legal Adviser or other individuals as authorized by the Director-General and is therefore subject to specific rules. These include files of the Z series (CABINET), P series (HRD), M series (HSU), and those in series IAO, JAAB and TRIB.

20. Other information classified as confidential includes:

    - information created by the ILO, as well as information received from, or sent to, third parties, under an expectation or on condition of confidentiality; and
    - information containing commercial information, whose disclosure would harm either the financial interests of the ILO or those of other parties involved.

21. Although access and use restrictions apply to all confidential information, it should be understood that certain types of confidential information are extremely sensitive. Such information requires very stringent physical and electronic measures to be put in place to ensure it is safeguarded. These measures include restricting access to a minimum number of staff, ensuring complex passwords are enforced, applying encryption where appropriate, and auditing user activity.

Roles and responsibilities

22. Each ILO official is responsible for handling of ILO Information Assets consistent with this Directive.

23. In accordance with the ILO's Accountability Framework, including the *Standards of Conduct for the International Civil Service*, ILO officials have the responsibility to ensure the integrity, availability and, where required, the confidentiality of information, irrespective of the medium on which the information resides and regardless of format.

24. INFOTEC, in consultation with heads of departments and offices, shall ensure that manual processes and automated systems used to manage information have controls in place to prevent access by unauthorized persons and to ensure the integrity and availability of the information.

25. The following roles and responsibilities are established for carrying out this Directive.

Information Owner

26. An Information Owner is the head of a unit or function (usually the author unit or the recipient unit for information received from an external source) with the responsibility to appropriately classify ILO Information Assets and/or authorize user access to such information. Information Owners, within their functional areas of responsibility:

- maintain an inventory of their ILO Information Assets;
- classify their ILO Information Assets in accordance with this Directive;
- establish a disclosure schedule for Information Assets under their responsibility;
- approve decisions regarding controls and access privileges of users to such assets;
- ensure that those with access to information understand their responsibilities for collecting and handling of information appropriately;
- conduct annual, or more frequent, reviews of user access lists so as to ensure that they are up to date;
- participate in periodic reclassification/declassification reviews of ILO Information Assets;
- report actual or suspected vulnerabilities/breaches in the confidentiality, integrity or availability of information to the INFOTEC Information Security and Assurance Services Unit (ISAS@ilo.org);
- report any loss or unauthorized disclosure of ILO Information Assets classified as restricted or confidential to the Information Custodian as described below; and
- take ILO information security awareness training to better understand risks and preventative measures associated with the use of information.

Information User

27. An Information User is any ILO official or other individual who needs and uses ILO Information Assets as part of their assigned duties, tasks or contractual arrangement.

Information Users:

- ensure that they do not put at risk ILO Information Assets for which they have been given access;
- exercise utmost discretion when handling ILO Information Assets of a restricted or confidential nature;
- use ILO Information Assets only for approved ILO purposes;
- follow operating procedures as defined by the Information Custodian;
- report actual or suspected vulnerabilities/breaches in the confidentiality, integrity or availability of information to the INFOTEC Information Security and Assurance Services Unit (ISAS@ilo.org);
- report any loss or unauthorized disclosure of ILO Information Assets classified as restricted or confidential to their Director or Information Custodian as described below; and
- take ILO information security awareness training to better understand risks and preventative measures associated with the use of information.

Information Custodian

28. The direct operational responsibility for ensuring the integrity of ILO Information Assets rests with INFOTEC. INFOTEC Information Custodians are responsible for managing the IT infrastructure and applications used to process ILO Information Assets.

    Information Custodians:

    - implement and administer appropriate levels of controls over information in compliance with Office Procedure, *Security of electronic information*, IGDS No. 164 (version 1), of 25 May 2010, as well as other regulations, rules, directives and procedures;
    - ensure technical controls in physical and electronic systems are in place to safeguard ILO Information Assets;
    - maintain a centralized inventory of ILO Information Assets within their functional area of responsibility;
    - provide expertise and support to Information Owners in carrying out their responsibilities;
    - grant access privileges to users as authorized by Information Owners or their designees;
    - implement a programme to ensure that ILO Information Assets of continuing value are preserved over time and remain accessible and usable;
    - launch periodic reclassification/declassification of ILO Information Assets based upon revisions to regulations, rules, directives and procedures, including compliance to the latest security standards;
    - ensure that changes to ILO Information Assets are captured and can be audited in accordance with related retention policies;

- report actual or suspected vulnerabilities/breaches in the confidentiality, integrity or availability of information to the INFOTEC Information Security and Assurance Services Unit (ISAS@ilo.org);

- report any loss or unauthorized disclosure of ILO Information Assets classified as restricted or confidential to the Chief Internal Auditor and Ethics Officer; and

- take ILO information security awareness training to better understand risks and preventative measures associated with the use of information.

Authority to classify

29. The Information Owner shall decide the appropriate classification of an ILO Information Asset.

30. Where an ILO Information Asset originating from an external source contains classification markings, it shall retain those markings or shall be assigned a classification that provides a degree of protection greater than, or equal to, that of the entity that furnished the item.

Authority to declassify

31. If no date or event for declassification has been specified, ILO Information Assets may be reviewed and declassified at any time by the Information Owner, following consultation and approval by the Information Custodian and JUR, or by such official(s) as the Director-General may authorize.

32. Review for possible declassification shall take place before ILO Information Assets are transferred to the custody of the ILO historical archives (archives@ilo.org).

33. When undertaking a review for declassification in connection with information received from an external source, the ILO shall give due regard to expectations of confidentiality of that external source and, if appropriate, shall seek the prior consent of the external source or, if that is not possible, consult JUR before declassifying an Information Asset.

34. Queries regarding this Directive should be addressed to INFOTEC.

Guy Ryder
Director-General