Executive Office Instruction Ref. EOI.IAIG.2019.02 Information Classification

Authority:

This Executive Office Instruction (EOI) is promulgated by the Director, Internal Audit and Investigations Group (IAIG) under the Executive Office Directive on Privacy and Information Security (Ref. EOD.ED.2019.02) on the basis of a delegation of authority by the Executive Director.

Purpose

The purpose of this EOI is to provide instructions on classifying UNOPS data based on its sensitivity and quantifying the amount of data protection required.

Effective Date:

This EOI shall become effective immediately.

[signature redacted]

Paul Lucas
Director, IAIG

1. Introduction

1.1. UNOPS data is information generated by or for, owned by, or otherwise in the possession of UNOPS that is related to the organization's activities.

1.2. UNOPS data may exist in any format (i.e. electronic, paper) and includes, but is not limited to, all strategic, tactical, operational, administrative, and research data, as well as the computing infrastructure and program code that supports the business of UNOPS.

1.3. In order to effectively secure this data, we must have a vocabulary that we can use to describe the data and quantify the amount of protection required. This EOI defines four categories into which all UNOPS data can be divided:

- Public
- Unclassified
- Confidential
- Strictly Confidential

1.4. UNOPS data that is considered as Public may be disclosed to any person regardless of their affiliation with UNOPS. All other UNOPS data is considered as potentially Sensitive Information and must be protected appropriately and may only be disclosed carefully, in accordance with UNOPS Operational Instruction on Information Disclosure (Ref. OI.LG.2019.02). Section 3 of this document provides definitions for and examples of each of the four categories.

1.5. The various units and departments in UNOPS have a multitude of types of documents and data. While not all documents and data need to be physically marked as Public, Unclassified, Confidential or Strictly Confidential, each business unit or department should consider in which of the above categories its documents and data falls by taking into account the potential for harm to individuals or UNOPS in the event of unintended disclosure, modification, or loss. The Chief Information Security Officer (CISO) will assist with this process to achieve consistency across UNOPS. When considering its data classification, each department should weigh the risk created by an unintended disclosure, modification or loss against the need to encourage open discussion, improve efficiency and further UNOPS' goals of the creation and dissemination of knowledge. Departments should be particularly mindful to protect sensitive personal information, such as national identification numbers, drivers' license numbers and bank account numbers, disclosure of which may create the risk of identity theft.

1.6. Note that some information could be classified differently at different times. For example, information that was once considered to be Confidential data may become Public data once it has been appropriately disclosed. Everyone with access to UNOPS data should exercise good judgment in handling sensitive information and seek guidance from management as needed.

2. A Note About Research

2.1. UNOPS is committed to openness in research – freedom of access by all interested persons to the underlying data, to the processes, and to the final results of research. Research at UNOPS generally should be widely and openly published and made available through broad dissemination or publication of the research results. Research data is generally considered as Public data unless there are specific

requirements to maintain the confidentiality of research data, such as when a researcher is bound to protect the confidential information of a collaborating government, partner organization or when the data relates to human subjects.

3. Classification Levels

Public

3.1. Public data is information that may be disclosed to any person regardless of their affiliation with UNOPS. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the community and no steps need be taken to prevent its distribution.

3.2. Examples of Public data include: press releases, directory information, application forms, and other general information that is openly shared. The type of information a department the organization chooses to post on its website is a good example of Public data.

Unclassified

3.3. Unclassified data is information that is potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of UNOPS without the permission of the person or group that created the data. It is the responsibility of the data owner to designate information as Unclassified where appropriate. If you have questions about whether the information is Unclassified or how to treat Unclassified data, you should talk to Information Security or your department head.

3.4. Examples of Unclassified data include: Some memos, correspondence, and meeting minutes; contact lists that contain information that is not publicly available; and procedural documentation that should remain private.

Confidential

3.5. Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or the business of the UNOPS. This classification also includes data that UNOPS is required to keep confidential, either by law or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or in transit.

3.6. Any unauthorized disclosure or loss of Confidential data must be reported to the appropriate department head. The department head should determine whether to report the unauthorized disclosure or loss of Confidential data to the CISO at ciso@unops.org[1].

3.7. Examples of Confidential data include:

- Information covered by privacy and data protection legal frameworks across UNOPS operations and other jurisdictions (e.g. EU GDPR, HIPAA, etc.).

1. mailto:ciso@unops.org

- Personally identifiable information (PII) entrusted to our care that is not Strictly Confidential data, such as information regarding government officials, existing donors, potential donors, or children of current or former employees.
- The UNOPS ID (CSID), when stored with other identifiable information such as name or email address.
- Financial records.
- Individual employment information, including salary, benefits and performance appraisals for current, former, and prospective employees.
- Legally privileged information.
- Information that is the subject of a confidentiality agreement.

Strictly Confidential

3.8. Strictly Confidential data includes any information that UNOPS has a contractual or fiduciary obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require UNOPS to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.

3.9. UNOPS's obligations will depend on the particular data and the relevant contract or laws. The Minimum Security Standards sets a baseline for all Strictly Confidential data. Systems and processes to protect the following types of data need to meet that baseline:

- Personally identifiable health information.
- Personally Identifiable Information (PII), including an individual's name plus the individual's national identification number, driver's license number, passport information, or bank account number.
- Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens.
- "Criminal Background Data" that might be collected as part of an application form or a background check.

3.10. More stringent requirements exist for some types of Strictly Confidential data. Individuals working with the following types of data must follow UNOPS's policies governing those types of data and consult with Information Security to ensure they meet all of the requirements of their data type:

- Protected health information (PHI). Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage.
- Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored.
- European Union (EU) and the countries of the African, Caribbean and Pacific Group of States (ACP) partnership information.
- U.S. Government Classified Data.

3.11. Strictly Confidential data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of Strictly Confidential data must be reported to the Chief Information Security Officer at ciso@unops.org[2].

2. mailto:ciso@unops.org

4. Resolving Conflicts between this EOI and other Regulations

4.1. Some data may be subject to specific protection requirements under a contract or grant, or according to a law or regulation not described here. In those circumstances, the most restrictive protection requirements should apply. If you have questions, please contact the CISO at ciso@unops.org[3].

3. mailto:ciso@unops.org