UNITED NATIONS

unite
Office of Information and Communications Technology

Sharing United Nations official information with external parties

GUIDELINES

Sharing United Nations official information with external parties

Purpose, Responsibilities, Scope

These guidelines describe the responsibilities of and provide approaches for United Nations personnel who are planning to, and are sharing with external parties United Nations information, data, documents, records and work products and regardless of their format (referred to hereafter as information), or information received by the Organization from third parties with external parties for specified purposes to conduct official business.

ST/SGB/2007/6 governs the classification and handling of United Nations information. Heads of Departments and staff that create or receive information are responsible for ensuring that information classification and handling requirements are met; the Office of Information and Communications Technology is responsible for providing secure electronic information systems for processing, storing, and transmitting information.

The scope of these guidelines is as follows:

What	Where	Who
• All United Nations official information, data, documents records and work products regardless of format • All information originating from an external or third-party that is maintained by the United Nations in the conduct of official business	• All current and future systems for information sharing, including online forums and communities, enterprise information-sharing and collaboration platforms, other tools such as email or direct file transfer and exchange solutions	• All United Nations authorized users • All external parties who are granted access to United Nations official information for specified purposes to conduct official United Nations business

Definitions

Authorized User: UN personnel and other individuals who are authorized to use UN ICT resources; see ST/SGB/2004/15.

External Party: any person who is not an authorized user.

Information Owner: the originator of the information concerned, or its recipient if the information is received from an outside source.

Non-Sensitive Information:

- *Public*: information created with the expectation that it will be shared with the public.
- *Unclassified*: information whose unauthorized disclosure could reasonably be expected not to cause damage to the work of the United Nations.

Sensitive information:

- *Confidential*: information whose unauthorized disclosure could reasonably be expected to cause damage to the work of the United Nations;

- *Strictly confidential*: information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of the work of the United Nations.

- *Personal data*: any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified by reasonable means, directly or indirectly, by reference to an attribute or combination of attributes within the data, or combination of the data with other available information. Attributes that can be used to identify an identifiable individual include, but are not limited to, name, identification number, location data, online identifier, metadata and factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual.

Principle for sharing information with external parties

The United Nations promotes transparency and collaboration with external partners and recognizes that sharing information may be appropriate and necessary to conduct official business. At the same time, it is essential to protect all information whenever it is shared with external partners in a way that upholds the Organization's rights and interests, protects the rights of the Organization's beneficiaries, and maintains public trust and confidence.

Approaches, processes, tools

Authorized users who undertake information sharing initiatives should adopt and adhere to these approaches, processes and tools; they are intended to enable authorized users to share information in keeping with the above principle, while protecting the United Nations' rights and interests. Using these approaches, processes and tools will provide the minimum levels of protection necessary to satisfy the requirements expressed in ST/SGB/2007/6.

- Authorized users of United Nations information systems are expected to protect United Nations information at all times.

- Written authorization by the head of department or office is required in order to share sensitive information with external parties or to provide them with access to it. That authorization should connect the decision to share the information to the conduct of official business. Unauthorized disclosure of sensitive information jeopardizes the effectiveness and credibility of the Organization, erodes public trust and is prohibited. In some cases, it may put the Organization in breach of its legal obligations.

- Strictly confidential information in electronic information systems may be shared with, and access to it may be provided to external parties only on condition that the respective United Nations electronic information system provides the required technical protections. United Nations Information and Communications Technology service providers can confirm to authorized users which systems adequately protect information classified at each security classification level and can identify secure information transmission methods, if required.

- Sensitive information sharing should be covered by a legal instrument or agreement that explains why the information sharing initiative is necessary and that clarifies the objectives of sharing the information. This should be documented in precise terms so that all parties are clear as to the purposes for which information is being shared and that there are limitations as to how shared information may be used, such as non-disclosure clauses. It may also set out the legal status of shared information; for example, that the United Nations retains ownership of all shared information, including intellectual property rights in it.

- Information sharing agreements will address a range of requirements for each circumstance. For instance, they may:

  - identify clearly all the entities that will be involved in the information sharing and contain procedures for including additional entities in the information sharing arrangement and for dealing with cases where an entity needs to be excluded from the sharing;

  - explain the types of information that can be shared with the entities stated above. For example, in some cases it will be appropriate to share certain details held in a file about someone, but not other, more sensitive, material;

  - establish common rules for the access, retention and deletion of shared information items and procedures for dealing with cases where different entities may have different statutory or professional retention or deletion rules;

  - establish common technical and organizational security arrangements, including for the transmission of the information and procedures for dealing with any breach of the agreement.

References

- Staff rules: ST/SGB/2011/1 1.2 (h) and 1.9
- ST/SGB/2007/5 – Record-keeping and the management of United Nations archives
- ST/SGB/2007/6 – Information sensitivity, classification and handling
- ST/SGB/2004/15 – Use of information and communication technology resources and data
- ICSC, standards of Conduct for International Civil Servants, 2013, Para 24, Disclosure of Information; para 39, use and protection of information

For more information

- Contact your UN ICT service provider.