UNDERSTANDING INFORMATION SENSITIVITY

The inappropriate disclosure of sensitive information can place the UN, its operations, and its personnel at risk. In order to mitigate these risks, the UN has developed a formal classification process for identifying levels of information sensitivity. The sensitivity classifications identified in the UN Secretary-General's Bulletin (ST/SGB/2007/6) are defined below.

STRICTLY CONFIDENTIAL: information or material whose unauthorized disclosure could reasonably be expected to cause EXCEPTIONALLY GRAVE DAMAGE TO or IMPEDE THE CONDUCT OF THE WORK of the United Nations.

> Inappropriate disclosure of strictly confidential information might: endanger the safety or security of any individual; violate individual rights; invade individual privacy; endanger the security of Member States; prejudice the security or proper conduct of any operation or activity of the United Nations; or long-lasting and/or far-reaching impairment of a United Nations mission, operation, or programme.
>
> The results of disclosing strictly confidential information might include: the death or physical injury of a United Nations employee or third party; the violation of an employee's right to medical privacy; danger to troop movements within a mission area; sabotage resulting in significant damage to a peacekeeping mission's communication channels; or the collapse of a local population's confidence in a peacekeeping operation.

CONFIDENTIAL: information or material whose unauthorized disclosure could reasonably be expected to cause DAMAGE TO THE WORK of the United Nations.

> Inappropriate disclosure of confidential information might: harm the United Nations, Member States, or individuals, where the damages incurred could potentially be repaired through negotiation, good offices or other means.
>
> The results of disclosing confidential information might include: strained relations between the United Nations and a non-governmental organization; or lack of confidence between the UN and a vendor.

UNCLASSIFIED: information or material whose unauthorized disclosure could reasonably be expected NOT TO CAUSE DAMAGE TO THE WORK of the United Nations.

> The disclosure of unclassified information will not result in any damage to the United Nations, Member States, or individuals.
>
> The results of the disclosure of unclassified information might include: the media's knowledge of a principal's participation in a conference; or a Member State's knowledge of how its contributions to a trust fund have been used.

PROTECTING DOCUMENTS AND RECORDS

All the documents and records under your control should be identified according to one of these three sensitivity classifications. These documents must be stored and handled so that the information in them is not inappropriately disclosed, regardless of whether the information is in paper or electronic form. All documents should be classified according to information security requirements, even if some of them will not be "declared" as records. Even those documents needed for only a few minutes can contain critical and sensitive information that needs to be protected!

The following steps must be followed to ensure all UN documents and records are protected at all times.

1. Manage all documents according to assigned UN sensitivity classifications: strictly confidential, confidential, and unclassified.
2. Declare and store all records, including sensitive records, as soon as possible, so that they are safe.
3. Remove superseded versions, obsolete documents, or other documents that are not deemed official records from office systems as soon as possible, so the risk of inappropriate disclosure is reduced.
4. Always store physical (i.e., paper) records in secure cabinets or locked records storage areas and keep those areas locked and protected at all times.
5. Always store sensitive records in formally established electronic record-keeping systems or secured network drives only. Do not keep them in unsecure locations, such as computer hard drives or C: drives that do not have security controls.
6. Always use approved records classification schemes and file plans to ensure physical and electronic records are stored in the right place.
7. Contact the specialists at IT specialists at UN OICT and the records specialists at UN ARMS for support to delete electronic records are permanently removed from network drives or other storage locations.
8. Work with IT specialists at UN OICT to ensure computer systems are configured with appropriate security systems, anti-virus software, and other security features.
9. Transfer records with ongoing value to UN ARMS according to records retention schedules.
10. Always document the disposal of records, whether they are destroyed or sent to UN ARMS for permanent preservation, so there is clear proof of how records have been managed over time.

Protecting the sensitivity of all UN records requires managing information, documents, and records effectively for as long as they need to be kept, and then disposing of them appropriately and securely.