Lesson 1.4
Information Security

Content

- UN Security Policy
- Threats to information
- Classification and handling

Learning Objectives

- Explain the UN security procedures for information security
- Describe the aspects of UN information that threat actors seek to acquire
- Describe the sources exploited by threat actors to acquire information
- Explain key elements of UN policy on information sensitivity, classification and handling

Definitions

Security: Protection against intentional threats

Threat: A potential cause of harm initiated by deliberate actions.

Hazard: A potential cause of harm resulting from non-deliberate actions.

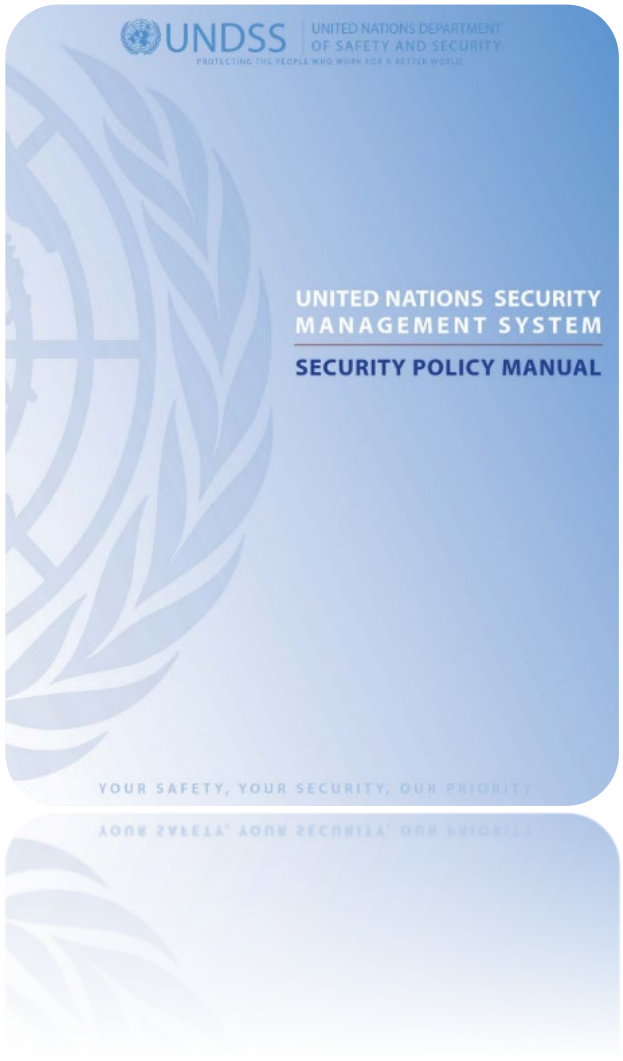
Security foundation

- Pre-requisite for successful UN operations
- Any security breach of official or protectively marked material or information
  - Undermines operational effectiveness
  - Potential risk to life
- All UN personnel responsible

Question: *What entity has primary responsibility for security of UN personnel and property?*

UN Security Policy

- MPKI staff must
  - Be aware of and conform with UN security policy
  - Understand security policies and SOPs
- If doubts, consult your local security officer



Information Security

Question: *At what stage of the intelligence cycle are information security threats likely to manifest?*

Threats to Information Security

Threat actors look to acquire information on aspects of UN activity:

- Future intentions
- Operational plans and activities
- Command, control, and communications
- Strengths and dispositions
- Locations
- Equipment and capabilities

Threats to Information Security

Threat actors exploit UN information:

- Surveillance and reconnaissance
- Radio and line communications
- Loose talk
- Civilians
- Insider threat

Classification & Handling

Information sensitivity, classification, handling

Classification Levels	
UNCLASSIFIED	Unauthorized disclosure could reasonably be expected **not to cause damage** to the work of the UN
CONFIDENTIAL	Unauthorized disclosure could reasonably be expected to **cause damage** to the work of the UN
STRICTLY CONFIDENTIAL	Unauthorized disclosure could reasonably be expected to **cause exceptionally grave damage** to the work of the UN

Classification & Handling

Considerations when classifying:

- Received or sent to third parties
- Endanger safety or security of individual, or violate his or her rights
- Endanger security of Member States
- Prejudice conduct of operation or activity of UN
- Legal privilege / internal investigations
- Internal / draft documents

Classification and Handling

Information handling:

- Accounting and control
- Loss or compromise
- Downgrading of sensitive information
- Storage of sensitive documents and material
- Destruction of sensitive information or material
- Carriage and dispatch of sensitive information

Take Away

- Understand the threat
- Understand your role
- Security policies and manuals provide additional information

Questions