HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

Mini MBA Security and Risk Management: protecting teams and maintaining access

Course handout · Week 4 : Security plans, procedures, movements and communications

A programme of exactly 3 months (12 weeks, 144 hours) to manage the security and risks of a humanitarian organisation: duty of care, context analysis, risk assessment, plans and procedures, acceptance and access negotiation, incidents, crisis management and kidnapping, staff health and wellbeing, digital security and data protection, organisational risks and compliance, risk sharing with partners, governance and business continuity. Corrected numerical exercises, three monthly exams with case studies, and a verifiable diploma from the Humanitarian Academy.

https://humanitairejobs.org/en/academy/mini-mba-securite-risques/semaine-4/

Free document from the Humanitarian Academy. It may be printed and shared freely for training purposes, without modification.

Week 4 : Security plans, procedures, movements and communications

Objectives

- Write a country or area security plan, with security levels and associated measures.
- Design realistic standard operating procedures, in particular for movements and sites.
- Set up a communications and movement tracking system that works when everything else fails.

The security plan

The **security plan** translates the risk assessment into rules and responsibilities. It is short, practical, known to everyone and regularly reviewed. Typical contents:

- summary of the context and the main threats;
- strategy (mix of acceptance, protection, deterrence);
- security levels and associated measures;
- standard operating procedures (movements, sites, communications, visitors, cash, incidents);
- contingency plans (medical evacuation, hibernation, relocation, evacuation, kidnapping, attack);
- security organisation chart and emergency contacts;
- annexes: maps, staff lists, inventory of communications equipment.

Every new arrival receives a **security briefing** on arrival and signs to confirm they have read the plan. An 80-page plan that nobody has read protects nobody.

Security levels

Most organisations use 4 or 5 **security levels** per area, each associated with automatic measures, which speeds up decisions in times of tension:

Level	Situation	Typical measures
1. Normal	Low, stable risks	Standard procedures
2. Vigilance	Tensions, isolated incidents	Movements restricted to certain hours, reinforced check-in calls, review of plans
3. Restriction	Rising violence, possible targeted threats	Essential movements only, with authorisation; reduction of non-essential staff; adapted activities
4. Hibernation or relocation	Widespread or targeted violence	Staff gathered in a safe location, or departure of the most exposed staff; activities suspended or managed remotely
5. Evacuation and suspension	Unacceptable risk	Departure from the area or the country according to the plan; contact maintained with staff who remain

Moving from one level to another is decided by the country director, on the basis of **indicators** defined in advance (see week 2), and communicated immediately to everyone.

Movement procedures

Movements are when staff are most exposed. Typical procedure:

- Prior **authorisation** according to the security level, based on a movement plan: route, timings, passengers, vehicles, contacts.
- **Route check** on the morning of travel: security forum, authorities, transporters, local staff.
- **Vehicle** checked and equipped: fuel, spare wheel, first aid kit, communications.
- **Check-in calls** at set intervals and at each key point; a clear procedure if a call is missed.
- **Internal curfew**: arrival before a set time, with a margin.
- **Behaviour** at checkpoints and in the event of a carjacking (no resistance, no photos, calm, cooperation).

Departure calculation. A 180 km journey at a realistic average speed of 40 km/h: 4 hours 30 minutes. Internal curfew 17:00, one-hour margin: planned arrival no later than 16:00. Departure no later than 11:30. With a check-in call every hour and on arrival: 5 calls. If a call is missed, the base tries to make contact again for 15 minutes, then triggers the missing vehicle procedure.

Site security

Offices, residences, warehouses and distribution sites are assessed and given appropriate measures:

- **Site selection**: neighbourhood, surroundings (avoid proximity to potential targets: military buildings, sensitive ministries), two access routes, distance from flood-risk areas.
- **Perimeter**: wall or fence, gate, lighting, trained unarmed guards, visitor control.
- **Building**: solid doors and windows, safe room or shelter depending on the threats (room reinforced against intrusion, shelter against indirect fire).

- **Fire and electrical safety**: extinguishers, detectors, emergency exits.
- **Stocks**: water, food, fuel and medicines for hibernation (often 7 to 14 days).

Stock calculation. 12 people, 10-day hibernation: water at 4 litres per person per day for drinking and minimal use = 480 litres; with a 20% margin, about 580 litres. Food: 12 × 10 = 120 daily rations. Fuel for a generator at 2 litres per hour, 8 hours a day: 160 litres.

Communications

The communications system must work **when the mobile network is down**, which often happens just when it is most needed. Principle of redundancy: at least two independent means.

- **Mobile phone**: convenient, but fragile and open to surveillance.
- **HF radio**: long range, independent of networks, but requires trained operators and licences.
- **VHF radio**: short range, ideal in town and in convoys, with repeaters.
- **Satellite phone** and satellite data terminals: independent, but expensive and sometimes regulated or viewed with suspicion by the authorities.
- GPS **tracking devices** with a panic button.

Rules: call signs, plain language but no sensitive information (no names, cash amounts or detailed routes over the radio), call tree (each manager calls a defined number of people), regular tests, chargers and back-up batteries. Communications are also an acceptance issue: using a radio or satellite phone where the authorities forbid it can lead to suspicions of spying.

Procedures that are actually applied

Procedures often fail for simple reasons: too many of them, poorly known, impossible to apply, or bypassed out of habit. Good practice:

- Write **few** procedures, short ones, adapted to the real context, with the staff who will apply them.
- **Explain** them (the why) rather than just imposing them.
- **Practise** them: simulations of a missing vehicle, hibernation, medical evacuation, at least twice a year.
- **Check** them: spot checks of logbooks, check-in calls, visitor registers.
- Treat non-compliance as a **management** issue: a manager who bypasses procedures sets an example for the whole team.

> Complacency is a risk in its own right: after months without incident, procedures slacken precisely when the context may tip over.

Exercise: planning a field mission

Situation. A team of 4 people must travel from the base to a site 210 km away for a distribution. Realistic average speed: 35 km/h. Internal curfew: 17:30, with a one-hour margin. The distribution lasts 3 hours. The site has no mobile network over the last 80 kilometres. The security level of the area is "vigilance". The driver suggests leaving at 09:00 "as usual".

Task. 1) Can the mission be done as a return trip in one day? 2) If not, how should it be organised? 3) What means of communication and what check-in calls?

Answer. 1) Journey: 210 / 35 = 6 hours. Return trip 12 hours + 3 hours of distribution = 15 hours; arrival no later than 16:30: departure at 01:30, which is impossible (no night-time driving). The mission cannot be done in a day. 2) Overnight stay on site or in a safe stopover town, in accommodation assessed in advance; or split it up: day 1 travel (departure at 09:00, arrival around 15:00), day 2 distribution and partial return, or distribution by a local partner with monitoring. Vary the usual departure time, which makes movements predictable. 3) Mobile phone where there is a network, satellite phone or HF radio for the 80 km without network, tracking device; check-in call every hour and at each key point (departure, entry into the area without network, arrival, start and end of distribution); missing vehicle procedure known to the base.

Key takeaways

- A short security plan, known to all, signed on arrival, regularly reviewed.
- Security levels with automatic measures and escalation indicators defined in advance.
- Movements: authorisation, route check, check-in calls, curfew with a margin, non-resistance.
- Redundant, tested communications, with no sensitive information in plain language.
- Few procedures, explained, practised and checked; complacency is a risk.

Quiz

1. A 160 km journey at 40 km/h, arrival no later than 16:00. Latest departure:
   A. 12:00
   B. 10:00
   C. 14:00
   D. 11:00

2. 10 people, 7 days of hibernation, 4 litres of water per person per day. Minimum water:
   A. 70 litres
   B. 400 litres
   C. 40 litres
   D. 280 litres

3. Why require two independent means of communication?
   A. To reduce costs
   B. Because donors require it
   C. Because the mobile network often fails at the critical moment
   D. To communicate with the press

4. On the radio, you avoid mentioning:
   A. Call signs
   B. Names, cash amounts and detailed routes
   C. The time
   D. The security level

5. After six months without incident, the team relaxes check-in calls. This is:
   A. Complacency, a risk to be corrected by management
   B. Normal and risk-free
   C. A good adaptation
   D. A decision for the driver

Quiz answers : 1. A · 2. D · 3. C · 4. B · 5. A