TOOLKIT MODULE

Security to go, Module 12: people management

The manager's part in the security of a team: recruitment, briefing, supervision, conduct, wellbeing and the things that only a line manager can do.

European Interagency Security Forum

Security arrangements are made of documents, equipment and procedures, and none of them functions without a manager who uses them. This module covers the part of a team's security that belongs to the person who supervises it, and it is written on the assumption that the reader is a programme manager rather than a security specialist.

What only the manager can do

- **Decide whether the work happens.** The assessment identifies the risk; the manager decides whether the activity proceeds anyway. That decision is the largest single determinant of the team's exposure and it cannot be delegated to a security adviser, who has no authority over the programme.
- **Set the tone on compliance.** Whether the check-in schedule, the movement procedure and the equipment rules are followed is determined by what the manager does, not by what the plan says. A manager who travels without filing a movement plan has abolished the requirement.
- **Make the concern safe to raise.** Staff test the reporting channel before they use it, by watching what happens to somebody else.
- **Represent the team upward.** When the risk is unacceptable or the mitigation is unfunded, the manager is the person who has to say so to somebody with authority, in writing, and to keep saying it.

Recruitment and deployment

- **State the conditions in the advertisement and the interview.** Where the posting involves a curfew, restricted movement, shared accommodation or a compound, the candidate is told before accepting rather than on arrival. Most disputes about security conditions begin with a person who learned the arrangement after signing.
- **Discuss the individual's profile explicitly.** Ask the candidate what they anticipate, and record the answer. Where a candidate identifies a constraint, the organisation decides what it can accommodate before the contract is issued, rather than discovering the problem in the country.
- **Establish what is not negotiable and what is.** The organisation's procedures, the communication requirements and the movement rules are conditions of the post. What can be adjusted is the arrangement rather than the requirement.
- **Check that the person is equipped for the role.** A driving requirement, a language requirement or a physical requirement stated in the job description but never tested produces an incident on the first field visit.

Induction and briefing

Four conversations, each of which has a purpose and a record.

Conversation	When	What it establishes
Induction	First days in the country	The security plan, the communications tree, who to call, where the medical facilities are, how to report an incident, and the fact that the manager expects the procedures to be used
Deployment briefing	Before each field visit or new location	The current threat picture for that specific place, the movement plan, the check-in schedule, and the point at which the visit is abandoned
Debrief	After the visit, always	What was observed, what nearly went wrong, what the person would do differently, and what the manager needs to change
Check-in conversation	At intervals, not only after incidents	How the person is, whether the arrangements are working for them, and whether anything has changed in their circumstances

The debrief is the most valuable of the four and the one most often skipped when the visit went well. A near miss reported in a debrief is the cheapest security information an organisation can obtain.

Conduct and non-compliance

Where a member of staff does not follow a procedure, the manager's response determines what the rest of the team does next.

- **Establish what happened before deciding what it means.** Most non-compliance is caused by a procedure that does not fit the work, and the procedure is the thing to fix.
- **Treat a security procedure as a work requirement, not a personal preference.** Where the procedure was clear and the risk was real, the response is a management response and it is recorded.
- **Be consistent across the team.** The enforcement of the rules against the newest or most junior member and not against the most senior is noticed immediately and permanently.
- **Do not use the security procedure as a performance instrument.** Where the check-in requirement is used to discipline somebody over an unrelated matter, the reporting channel is damaged for everyone.

Wellbeing and the manager

Managers are not clinicians and are not expected to be. What they are expected to do is recognise a change, ask a direct question, and know where to refer the person.

- **Recognise the ordinary signs:** withdrawal from the team, changed behaviour around movement or accommodation, increased drinking, sleep problems, an unusual reluctance to travel, a sudden request to leave.
- **Ask about the work rather than the person.** "How are the field visits going" opens a conversation that "are you all right" closes.
- **Know the referral route** before it is needed: the organisation's staff support arrangement, the insurer's assistance line, the medical provider, and the person designated to receive a disclosure of harassment or abuse.
- **Do not make the decision for the person.** A manager who removes a member of staff from a location without discussion has made a decision about their career on their behalf. Offer the options and record the choice.
- **Watch the manager.** The person running a difficult programme is the least likely to be asked how they are, and their judgement is the one the team depends on.

Managing a team with different profiles

A team whose members carry different exposure cannot be managed with one set of arrangements applied uniformly. The manager's tasks are specific.

- Know which members of the team face constraints that others do not, and why.
- Decide what the organisation will do about each constraint, and tell the person what was decided rather than leaving them to manage it privately.
- Fund the mitigation. Where a constraint requires a driver, an escort or different accommodation, the cost is the organisation's.
- Review the allocation of the dangerous work. Where the least protected members of the team are consistently given the most exposed tasks, that is a management decision and it should be recorded as one.

- Ask, on a schedule, whether the arrangements are working. The answer changes as the environment changes, and the manager will not be told unless they ask.

Leavers and handover

The end of an assignment is a security event that is usually treated as an administrative one.

- **Recover the equipment** and confirm what was held. An organisation that does not know which devices are in the field cannot assess what it lost when one is taken.
- **Remove access** to premises, to systems, to the communications tree and to distribution lists, on the day.
- **Debrief the leaver.** Departing staff give the most candid assessments the organisation will ever receive, and they are asked nothing on the way out.
- **Manage the transition of relationships.** Where the person held the organisation's contacts with an authority, a community or a local partner, those relationships are the organisation's principal security asset in the location and they do not transfer automatically.

Published by the European Interagency Security Forum as part of its resource library, as a module of the Security to go risk management toolkit.

This module is published for information and training purposes. It is not legal advice and does not replace the organisation's own human resources and security policies, which take precedence where they differ.