If travelling, you should first follow the advice outlined in the Preparation lesson.

This lesson focuses specifically on how to cross borders if travelling for sensitive work or with sensitive information. In establishing the potential risk and risk mitigation measures for crossing borders, it is important to establish a few basics about the reasons for, and possible sensitivities of, your trip. It is vital to be aware of the nature of the information you will be carrying into and out of the country, and how you will carry it.

Sensitive or revealing information you may carry could include:

* Data on people at risk/HRDs you are meeting
* Travel plansPasswords/ access codes
* Censored/ banned information
* Organisation sensitive information
* Personal information
* Embarrassing/ incriminating information
* Legal - encryption or data not allowed for export
* Receipts
* Reports

This information may be stored in/on notebooks, publications, laptops, phones, USBs, CDs, or SD cards.

Remember:

* Only minimal data should be brought with you
* Bring a ?clean? laptop and phone if possible
* Carry sensitive information and electronic equipment in hand luggage, as at least you know If it has been tampered with
* Small, encrypted USB sticks or Micro SD cards can be useful for security and being able to hide sensitive data if necessary. See the Protecting Files lesson for advice on how to encrypt files.
* Bring a cheap notebook in which you can rip out the pages unnoticed
* Tamper proof Scotch tape can be useful for enhancing the security of your equipment, hotel safe, laptop ports etc.
* Check pockets, wallet, bags everything before travel
* Prepare your story (More in next section)
* Agree in advance with colleagues what you will say. Discuss any red lines you will not cross (e.g. giving information about high risk activists who you intend on meeting)
* In some environments, it is best not to attract attention by travelling in a group, so sit separately and approach immigration separately. (Although bare in mind that authorities often know if big organisations are coming to the country anyway.)
* Say/do nothing sensitive on plane ? many human rights defenders have been arrested because they were overheard speaking about their activities.
* Provide only minimal information to immigration about activities.
* It may not be within the remit of your organisation to lie but neither should you volunteer information unnecessarily.
* Be prepared to be questioned about your activities in other countries/visas marked in your passport.
* Be polite but firm with authorities.
* Decide in advance if you are going to put the actual hotel and location where you are staying on the visa entry form. (Consider risk vs. benefit)
* Do not get separated from your belongings, especially electronic items. If they are taken away from you, you should assume that they have been compromised.
* Keep phones off until well outside airport. Airports are common areas for tracking and viruses.
* Keep Wi-Fi off if not vital ? do not connect to airport Wi-Fi.
* Agree in advance with colleagues a location in the building where you will meet after immigration and a set time to turn on mobile phones if you have not met at this point and need to communicate.
* If using a paper notebook, try to minimise any potential data loss by making up short codes that only you understand. For example, if you are meeting a high-risk activist, give them a different name and refer to them as that in your notes. Don?t mix sensitive information with easily identifiable information.
* Don?t forget about receipts, tickets, bills etc. They can link sensitive activists to your work if not carefully protected.
* Keep sensitive information in another place (e.g. interview notes in a notebook but sensitive names and locations securely emailed to yourself.)
* Type up or take photos of your most sensitive written notes as soon as possible and securely email them to yourself and/or keep them on an encrypted drive. (See the Protecting Files lesson for advice on how to encrypt files.)
* Avoid taking paper reports or other information from the organisations and people that you work with - if your bags are searched they will link you. Instead, ask them to give or email you digital copies if possible.
* Dispose of sensitive paper waste immediately. Avoid doing this in locations like hotel rooms or offices where it might be taken by cleaners or security staff. If necessary, soak paper in water to ensure it is unreadable.
* Minimise the amount of security related information you give to people that you meet. At meetings and during other interactions, avoid giving details of future operational and travel plans.
* Travel by different routes at different times if possible in high-risk areas.
* Avoid walking alone/at night if possible.
* Advise hotel staff not to provide information on your activities; although be aware they could be monitoring you, too.
* Try to memorize emergency phone numbers.
* Agree a simple discreet signal with any colleagues that can alert them to nearby danger. It should be something easy to do but not something that would happen accidentally.
* Always wear seatbelts!
* You should assume that you might be stopped and searched. Assume that anything you have written will be copied or read and prepare accordingly.
* Make sure all sensitive notes are typed up/ photographed and then encrypted. (See the Protecting Files lesson for advice on how to encrypt files.)
* To prepare for the long-term confiscation of your equipment at an exit port, you should backup key files remotely, such as to your secure email.
* Before departure, make sure to remove any sensitive paper waste from your room and dispose of it safely elsewhere. If necessary, soak paper in water to ensure it is unreadable.
* At a suitable time, speak with your colleagues (if travelling with them) about what you will say if stopped and questioned when leaving the country. It might be the case that certain parts of the trip (such as meeting with a high-risk activist) you do not want to mention to the authorities. Any plan of what you agree to say should be:
  + Simple;
  + Easily repeatable;
  + Verifiable.
* When leaving the country, the same principles as entering apply. Keep electronics and sensitive material on you at all times. If necessary, hide a small USB or micro SD card somewhere it is harder to find.

Swipe right for this lesson's checklist

### RELATED LESSONS/TOOLS

* [Preparation lesson](umbrella://lesson/preparation)
* [Protecting Files lesson](umbrella://lesson/protecting-files)
* [Backing Up lesson](umbrella://lesson/backing-up)

### FURTHER READING

* [Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)](www.odihpn.org/download/gpr_8_revised2pdf)
* [ECHO Generic Security Guide for Humanitarian Organisations](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fecho%2Ffiles%2Fevaluation%2Fwatsan2005%2Fannex_files%2FECHO%2FECHO12%20-%20echo_generic_security_guide_en.doc&ei=kLxAVc6LOILuUP2SgbAE&usg=AFQjCNEXEOcbLeV24f3WolHmDwLq7KJzlQ&sig2=hbnI7wfdrGIHS7mmikBRWA)
* [Protection International: New Protection Manual for Human Rights Defenders (3rd Ed.)](protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/)