A world map in shades of blue with several glowing orange lines representing global connections or data paths. The lines originate from Europe and spread out to other continents like North America, South America, Africa, and Asia.

**Going on an
assignment abroad,
with your mobile
phone, your
personal assistant
device or your
laptop**

PASSPORT ADVICE TO TRAVELLERS



The use of mobile phones, laptops and personal assistant devices has favoured data carrying and data exchange.

Some of this information could be highly sensitive, both for us and for the administration or the private company we belong to. Its loss, interception or theft would have significant consequences on our activities or on their durability.

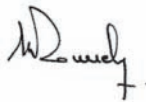
In this context of nomadism, we must protect them against risks and threats, especially during our travels abroad.

This guide presents easy rules to implement in order to reduce risks, or to limit their impact.

We hope that it will contribute to help travellers assure the best level of protection that their sensitive information deserves.



Patrick PAILLOUX
Directeur général de l'agence
nationale de la sécurité des
systèmes d'information



François ROUSSELY
Président du club des directeurs
de sécurité des entreprises

Going on an assignment abroad, with your mobile phone, your personal assistant device or your laptop.

When travelling abroad, make sure your information is secure!

Indeed, additional risks and threats threaten the security of the data you transport or exchange, and notably on their confidentiality.

Your equipment and your data could become objects of desire, and you must remain watchful, in spite of the change in the environment and the resulting loss of reference points.

Cyber-café, hotels, public places and sometimes even temporary offices do not offer guaranteed confidentiality. In many countries, business centres and phone networks are under surveillance. In some countries, hotel rooms can be searched.



In order to cover all these potential threats you can face, you are invited to follow the advice presented in this passport.

Going on an assignment abroad, with your mobile phone, your personal assistant device or your laptop.

Before going abroad :

1) Carefully reread and respect the security rules enacted by your organization.

Technical recommendations are available, for IT services and informed users, on the ANSSI website^[1].

2) Be informed about local law.

Information on border controls and on import or use of cryptography is available on the ANSSI website^[1].

Moreover, the Ministry of Foreign and European Affairs website provides general recommendations :

www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs_909/

3) Preferably use equipment dedicated to assignments (computers, mobile-phones, removable media, etc.).

This equipment must not contain any other information^[2] other than what you need for your assignment.

[1] www.securite-informatique.gouv.fr/partirenmission/

[2] Including pictures, videos, or any other digital work that could put you in a difficult position with the local law or the local customs.

Going on an assignment aboard, with your mobile phone, your personal assistant device or your laptop.

4) Save the data you carry.

That way, you will recover your data upon return if your equipment has been lost, stolen or seized.

5) Avoid going abroad with sensitive data.

Favour, if possible, retrieving encrypted files on the assignment spot, accessing :

- your organization's network through a secure link^[3] or ;
- an online webmail^[4], specially created and reserved for the transfer of encrypted data and deleting this webmail information once read.

6) Bring a screen-protection filter for your laptop if you are planning to work on your files during your journeys. This will discourage bystanders from looking at your documents.

7) Identify your equipment with a distinguishing feature (such as a coloured sticker).

This will give you the possibility to watch your equipment and to make sure that it has not been swapped, during the trip for instance. Also, remember to put a distinguishing feature on the cover.

[3] For instance with a VPN client, installed and configured by your computing department.

[4] If possible define your e-mail in order to use HTTPS protocol.

Going on an assignment aboard, with your mobile phone, your personal assistant device or your laptop.

During the assignment :

1) Keep your belongings (equipment and files) with you!

Take them in the cabin while travelling. Do not leave them in an office or in the hotel room (even in a safe).

2) If you are obliged to leave your mobile phone or your PDA, take the SIM card and the battery out and keep them with you.

3) Use encryption software during your trip.

Do not communicate confidential information in clear on your mobile phone or any other voice transmission systems.

4) Delete your calls and browsing history (data in cache-storage, cookies, passwords to access websites and temporary files).

Going on an assignment aboard, with your mobile phone,
your personal assistant device or your laptop.

5) In case of inspection or seizure by local authorities, please inform your organization.

Give passwords and encryption keys, if requested by the local authorities.

6) If equipment or information is lost or stolen, please immediately inform your organization and ask your Consulate for advice before approaching the local authorities.

7) Do not use equipment given to you before having it checked by your security service. It can contain malicious code.

8) Avoid connecting your equipment to computers or digital peripherals that are not trustworthy.

Beware of document exchanges (for instance through USB keys during business presentations or conferences). Bring a special key reserved for these exchanges and erase the files, preferably with a secure erasing software.

Going on an assignment aboard, with your mobile phone,
your personal assistant device or your laptop.

Before returning home :

1) Transfer your data

- on your organization network with your secure link ;
- or on an online webmail reserved for receiving your **encrypted files** (which will be deleted as soon as you are back). Then erase them from your computer, if possible in a secure manner, with a specific software.

2) Delete your calls and browsing history

Going on an assignment aboard, with your mobile phone, your personal assistant device or your laptop.

After your assignment, and especially if your equipment has not been always under your watch :

1) Change all passwords used during your trip.

2) Analyse or have your equipment analyzed^[5].

Do not connect your equipment to the network before having it at least tested with an anti-virus or an anti-spyware.

[5] A technical note, for informed users and for system managers, is available on the computing security webpage, at the following address :

www.securite-informatique.gouv.fr/gp_article636.html

Going on an assignment aboard, with your mobile phone,
your personal assistant device or your laptop.

You now have all the necessary knowledge to travel safely...

Have a safe trip !

The latest version of this passport is available on ANSSI
website :

<http://www.securite-informatique.gouv.fr/partirenmission/>

This passport “advice to travellers” was written by the Agence nationale de la sécurité des systèmes d’information (ANSSI), in partnership with

- le club des directeurs de sécurité d’entreprise (CDSE) ;

and with the participation of the following ministries :

- ministère de l’écologie, de l’énergie, du développement durable et de la mer ;

- ministère des affaires étrangères et européennes ;

- ministère de l’économie, de l’industrie et de l’emploi ;

- ministère de l’intérieur, de l’outre-mer et des collectivités territoriales ;

- ministère de l’enseignement supérieur et de la recherche ;

- ministère de la défense ;

and the following private companies and organizations :



March 2010

Agence nationale de la sécurité des systèmes d'information

ANSSI, SGDSN, 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP

Website : www.ssi.gouv.fr and www.securite-informatique.gouv.fr

Email : [communication \[at\] ssi.gouv.fr](mailto:communication@ssi.gouv.fr)