Terra Firma
Risk Management

Business Travel and Personal Security Guidelines

About us

Terra Firma provides crisis management, security advice and support to businesses, individuals, governments and aid organizations worldwide.

Our advisers are seasoned professionals who combine knowledge and experience with the ability to think critically and deliver clear, coherent guidance to our clients.

Terra Firma can help you prevent and prepare for risk events, respond appropriately to critical incidents and ensure a swift recovery.

Our dedicated international team is available 24 hours a day, seven days a week.

See our website at
www.terrafirma-rm.com
or email us on
info@terrafirma-rm.com

This booklet reviews very briefly some principles of personal security. They are worth keeping in mind and practising.

Then, in Part I, we provide guidance on security for business travellers, followed in Part II by advice on security at home and in the office.

The advice that is given here is, of course, generic. It should not be followed slavishly and should be adapted to each situation.

If you would like more advice, please talk to a Terra Firma Risk Management adviser. Email us at info@terrafirma-rm.com

This booklet accompanies another Terra Firma document, What if … This is a pocket book that gives advice on what to do in a number of risk situations. Access this by contacting us on the same email address.

Contents

The golden rule and principles of personal security

The golden rule - stay safe

Protecting yourself, or those you love, from violent attack is natural and sometimes necessary. But remember that protecting your possessions – your car or money, for instance - is never worth serious injury or death. If violent robbers want something badly enough to attack you for it, let them have it.

Principles of security

There are broadly six principles of personal security:

1. **Preparation**
2. **Awareness**
3. **Profile and image**
4. **Routine**
5. **Communication**
6. **Totality**

1. Preparation

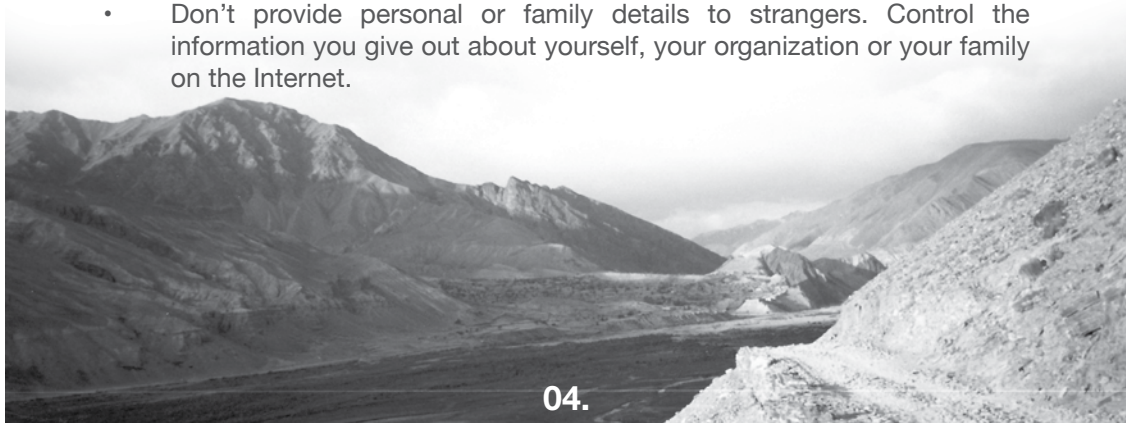
- Make yourself aware of the general threats. There is nothing more dangerous than someone who is so preoccupied with his or her own work or their own personal situation that they don't take the time to understand the political, social and economic environment.
- Take sensible precautions.
- Take responsibility for your own security and for that of your family and colleagues – be pro-active and don't simply rely on others to look after you.

2. Awareness

- Be aware of your environment. Keep your mind focused on the present – what is going on around you - rather than on the past or the future.
- Find out which places or activities you should avoid.
- Be particularly alert at the beginnings and ends of journeys.
- Make sure your family, particularly children, are also alert and aware.

3. Profile

- Do your best not to come to the attention of criminals. If you are seen to be particularly rich, or of particular importance, you are more likely to be a target. Maintain as low a profile as you can.
- If you can't avoid a high profile, take appropriate precautions.
- Be conscious of the image you project. Your dress, behaviour, language, ethnicity, nationality, gender – all these factors may affect the image you project in different societies or situations. Be aware of your image, and the effect it might have on your security.
- Don't provide personal or family details to strangers. Control the information you give out about yourself, your organization or your family on the Internet.



4. Routine

- In a low-risk security environment, routine can be a useful security tool: a certain amount of routine can help you identify unusual changes (risk indicators) around you.
- In medium- and high-risk environments, it is advisable to avoid establishing routines that are predictable.
- In medium- and high-risk environments, vary timings and routes. Try to vary, in particular, the approach to and exit from places you often visit, such as your home, workplace, clubs, etc.
- Identify any unavoidable routines and be particularly alert at these times.

5. Communication

- Establish a network. Talk to local people and neighbours. Talk to people from different strata of society so you are not just receiving one viewpoint.
- Listen to the radio, read the newspapers, consult embassy and other relevant websites.
- Make an effort to learn local languages, if only so you can use them in an emergency.
- Always be in a position to communicate with others in case you need to. Keep the necessary contact details (family, colleagues, police, ambulance) to hand.

6. Totality

- Security management needs to be constant. Criminals will try to find gaps in your security that they can exploit. Close the gaps.
- Ensuring your security in one place, e.g., the office, but not in another, e.g., at home, is unworkable. Similarly, you need to consider your security whatever you are doing, whether you are driving or relaxing at home or working.
- Protecting yourself, your colleagues and your family is a continuous, 24 hours a day, 365 days a year process. If you neglect your security at certain times, criminals may notice this and exploit it.

Lastly, anyone exposed to risk should take good, practical first aid training, and this training should be ‘refreshed’ frequently.

Part I - Travel Security

Before you go - preparation and prevention

Analyse

Before travelling anywhere, you should find out as much as you can about the country to which you are going. Consult knowledgeable local people from all walks of life, government websites*, country advice services and relevant academic institutes.

Assess the threat

Be as clear as you can about the threat, and your vulnerability and exposure to it. This will then help you select your accommodation, transport, places you visit, people you meet, clothes you wear, etc.

Take appropriate precautions

Once you understand the threat, you can decide the sort of security support, if any, that you will need when you arrive.

Travel Monitoring

Decide what support you need from home: who will track your travel and raise the alarm if an incident happens? How often and when will you report back home to say that all is well?

What do you need to take with you?

It is of course important to know what weather to expect, what illnesses you should protect yourself from and what medicines you should carry.

Important information should be given to someone at home or in the office – your passport details, blood group, allergies, medications, next of kin or emergency contact person details, etc. Take a photocopy of your passport and visas with you or, better still, keep scanned copies in your computer or telephone.

Your family and employer must be made aware of your blood group and of any significant medical requirements (for instance, if you take vital medicines). You should always carry on your person (e.g., in your wallet or purse) information on your blood group and any medical conditions.

Think carefully about your financial arrangements. Take the minimum number of credit or debit cards that you need. If you can, get some relevant foreign currency either before you leave your home airport or in an ATM in the baggage retrieval area of your destination airport – this means that you will not have to go to the ATM in full view of everybody in the arrivals area.

Think of how you will disperse your money and cards in your belongings, so that you do not 'put all your eggs in one basket'. You may need to take a 'dummy' wallet or purse which you can carry with you on the street or in higher-risk areas. The dummy wallet/purse should contain a little bit of money and a card with a very low limit – this can be given to robbers if they demand money.

*For example:

https://www.gov.uk/government/organisations/foreign-commonwealth-office
http://travel.state.gov/content/passports/english/alertswarnings.html
http://www.smartraveller.gov.au

In some countries, credit card fraud is common and it is safer to use only cash. If you are staying for a long time it may not be possible to carry sufficient cash safely – in this case, try to make arrangements for your host to make cash advances to you throughout your stay and pay your accommodation bill for you. Alternatively, pre-paid cards or traveller's cheques may be an option if local facilities support these methods and they are safe to use. If you must take/use a credit card, do not let it out of your sight.

Travel with a mobile telephone that works in the country you are visiting. Switch on the telephone straight after landing. Check it is working, as well as for any messages that might alert you to changed pick-up arrangements. Always double check any new arrangements by phoning your key contact back home or in-country.

Ensure you have important contact details with you before you leave: you should have the details of the person(s) meeting you; details of your contact point in your home office; and contact details of the offices or organizations that you are visiting.

Reception arrangements

Make sure that your pick-up arrangements at your destination airport are clear. If possible, plan to be met either by someone you recognise or by someone whose photograph was sent to you before departure. As a minimum, know the name of the person collecting you and check their ID when you meet them. If the name or the picture does not match the person meeting you or if any of the arrangements are not what you expected, call the office to confirm. Do not be afraid or embarrassed to question the driver or cause delay.

While you travel

Departures

- Dress casually on the day you travel. Try not to look 'valuable'.
- Luggage tags should contain only the traveller's name and contact number and should not be easily visible to the casual observer. Don't put addresses and company logos on your luggage, even briefcases.
- Keep a careful eye on your belongings at airports. 'Airside' – the part of the airport that is within its passport, customs control and security checks – is safer than 'the outside', but criminals still manage to operate there, particularly in big airports.

- As noted above, be sure that the right person picks you up when you arrive at your destination. Do not take a taxi in cities that you do not know well, or if the taxi has not been pre-arranged with a reputable company.
- In higher-risk countries, you should register with your Embassy. Ensure you have the Embassy contact details to hand should you need to contact them in an emergency.

At the hotel

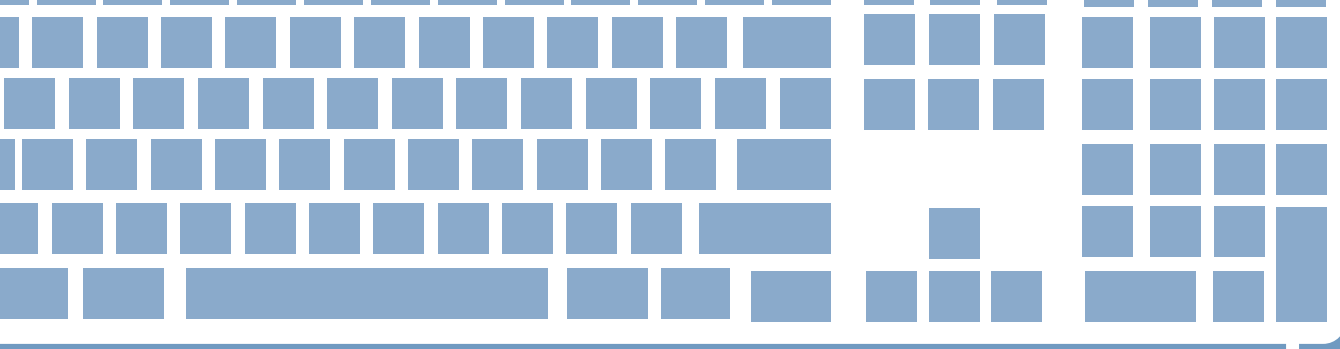
- Provide only the minimum amount of information at Reception – do not give your company affiliation unless it has already been given.
- Request a room above the second floor and preferably below the seventh floor in high-rise buildings.
- First thing, check out fire escape routes. Locate the fire escape doors, and check that they will open and the routes are clear of obstruction.
- Check the room door locks. If they do not function correctly, you should request immediate repairs or a change to a properly secured room.
- Windows and doors should be kept closed and locked. At night, double-lock the door and use the chain lock, if one is available.
- Don't open the room door without positively identifying the visitor. Call the hotel management if you are unsure about unexpected members of hotel staff attempting to gain entry. Remember that you can use the chain lock when opening the door.
- When travelling locally, valuables and cash should be placed in the hotel or room safe, if you consider them to be secure. Think about the relative risk of carrying valuables versus using a hotel safe and take the appropriate course of action.
- Take care with documents left in the room. Ensure any sensitive documents that give information regarding the company and the purpose of your visit are locked away in a safe place before you leave the room.
- Be cautious about what you discuss over hotel telephones.
- When moving around the hotel, be alert to the movements of other people. If you think you are being followed or watched, do not go to your room - return to Reception, if safe to do so, and explain your concerns. If it's safer to return to your room, call Reception immediately and explain your concerns.

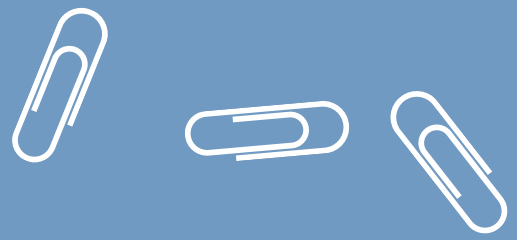
On the street

- Identify high crime areas and avoid them. Ask trusted locals for current information.
- Do not walk alone outside busy shopping streets or at night unless you know the area well and are confident it is safe.
- When walking outside, walk confidently - even if lost. If you must look at a map, try to do so off the street in a discreet location.
- Remain alert to your surroundings. Do not be distracted by telephone calls, texts, etc.
- If you are followed, you should stay on well-lit streets, enter a busy place and ask for assistance. Do not confront your follower.
- While walking, if harassed by persons in a vehicle, you should turn and walk in the direction opposite to the car's direction of travel and head for well-lit areas and people.
- Don't stop to give directions to drivers or pedestrians. If you do, keep your distance to reduce the risk of being assaulted.
- Avoid using ATM machines in the street – it's better to use a machine in a shopping mall or in the hotel. Try to have someone accompany you when withdrawing cash. If you are forced to hand over a bank card and PIN number, do so without resistance and provide the correct number. Failure to do this could lead to physical violence. Ensure you have sensible limits on the card to minimise the amount that can be stolen in a single transaction.

Taxis

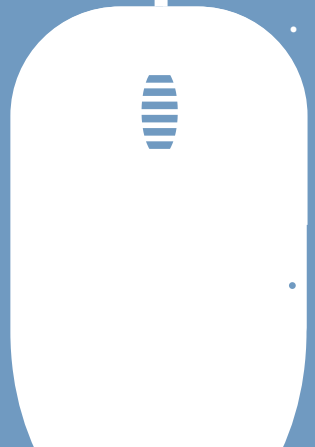
- Reliable local advice should be sought and followed. If in a high-risk country, strongly consider only leaving your hotel when collected by a trusted friend/colleague or their customary driver.
- Where a trusted friend/colleague/driver is not available, use hotel taxis where possible.
- If the hotel calls a commercial taxi company, ensure they note down the registration number of the taxi before you leave.
- Do not use taxis off the street in medium- or high-risk countries.
- If travelling alone, sit behind the driver – it is much more difficult for him to threaten you with a gun or knife. Ensure all doors are locked.
- Refuse to allow the driver to pick up a 'friend' or second passenger at traffic lights or when stopped. If he insists, consider leaving the taxi through the driver's side rear passenger door (if it's safe to do so and it does not put you in a dangerous position).





Information and IT security

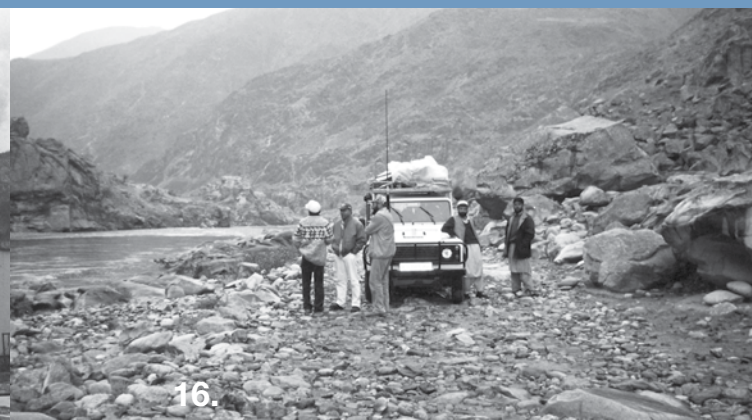
- Make sure your data is kept secure on all your devices. Smart phones often contain as much sensitive material as laptop computers, especially in emails, so take as much care with your phone as with your computer.
- All devices should have password protection enabled and passwords should be changed regularly and contain lower and uppercase letters, numbers and symbols and be a minimum of 8 characters long.
- Software to protect computers from viruses, malware, spyware, etc., is recommended for Macs and necessary for Windows PCs.
- Try to carry as little data on your devices as you can manage. If you must download data, use a trusted access point and only download what you need when you need it, and then remove it from your device.
- Ensure your firewall is turned on and ensure that incoming connections are not automatically allowed for your browser or anything else that looks suspicious.
- If you use an email client (such as Outlook) and have emails containing sensitive or confidential information, it is a sensible precaution in some contexts to travel with a device that does not have your email client software activated and to send/receive email only through a webmail system.
- Any public internet access point (hotel, café, library, etc.) poses an information security risk. Be careful using such places and never leave any email or other accounts open, or download any sensitive or confidential material through these avenues.
- Use only recognized and trusted wifi networks but note that wifi is often less secure than an ethernet connection.



- Always remember that any form of communication is vulnerable to eavesdropping and hacking. If you think you may be a target then avoid sending any sensitive information that is not securely encrypted, or discussing sensitive matters on the telephone. Bear in mind that encryption can be an indicator of having something to hide and this may make you a target for a more determined attempt to hack into your communications. It may also bring you the unwanted attention of the authorities.
- When using webmail, always make sure the website is https://... NOT http://... It is very important that the ‘s’ is part of the web address as this increases the security of data (all data travelling down such a connection is encrypted). Note, however, that a concerted attempt to hack into your communications is likely to be successful particularly if, for example, the hacker has access to the hotel server. This is much less likely to happen in reputable hotels.
- Data should be backed-up regularly and data storage should be protected by industry-standard encryption. Note that, although cloud data storage provides greater security by removing the data from your person, it has some vulnerabilities related to hacking, particularly if you are accessing your cloud storage from an insecure location or access point.
- Be as anonymous as possible and maintain a low public profile. Take particular care with social media networks such as Facebook and Twitter, as well as professional networks such as LinkedIn. If such media are used, the privacy controls should be custom-set to avoid exposure of personal details to those who may conduct research on you with malicious intent. Only allow trusted persons to become part of your network.
- Avoid discussion of work-related subjects on any social or professional media sites, and avoid blogging about matters that relate to work.

Driving security

- If you are in a high-risk area, you should not drive yourself.
- If you have a driver, it is important that he or she is someone you trust, and that you can communicate effectively with him or her.
- Ideally, drivers should be well trained not only in defensive driving (and evasive driving skills in high-risk areas), but should also be discreet and able to negotiate themselves (and you) out of a crisis. Drivers should be trained in first aid, and should be capable of using the first aid kit carried in the car.
- In the car, there should be: a torch (flashlight), relevant maps, first aid kit, fire extinguisher and breakdown kit including spare wheel and tools. Insist on a car that has seat belts, and working locks on doors and windows.
- The car should be as low profile as possible – the sort of car that criminals do not notice.
- If you are going on a longer trip and over rough country, the car will need to be mechanically sound, and carry emergency food and water, and suitable equipment (e.g., snow chains, shovels, extra fuel and lubricants, spare wheels, and sand ladders, etc.). If you are driving to remote areas, ensure that you have some form of communication that works (e.g., satellite phone or HF radio).
- If there is a radio or satellite phone in the car, you as a passenger must know how to use it in case the driver or other passengers are not able to do so.
- The driver should generally travel at moderate speed – this gives the driver time to notice events and react to incidents or suspicious activity ahead. If a driver continually drives too fast, do not be afraid to ask them to slow down or to insist on a change of driver.
- The driver should always leave a gap between your car and the one in front - you should always be able to see tarmac and the rear wheels of the car ahead. In high-risk areas, the driver should drive slightly offset from the car in front, so that you can see what lies ahead
- In high-risk areas, you should generally keep windows and doors closed and locked.
- In areas where the driving or the roads are not good, or in areas of high security risk, do not drive after dark if you can avoid it.
- Only leave the car when you are certain it is safe to do so. Park, if you can, in a secure compound or garage. If you cannot do that, then park as close as you can to the door that you will enter. Don't park on ill-lit streets at a distance from your destination.
- Your car should always be parked either where it can be seen, or where it can be secured. If there is any risk of explosive devices being attached to your car or the car being tampered with in any way, conduct a search of the vehicle before you unlock the doors. Search logically, outside, on top, and underneath (including wheel arches). Conduct a visual search inside (through the windows) and only open the doors when you are sure all is well. If you are at particular risk, conduct a thorough search every time you have left the car unattended.



Part II - Residential and Office Security

Security at home

Homes are of different types – houses, apartments, condominiums, etc. When you choose your home, you should take the security situation, and any specific threat to you and your family, into consideration.

The security protection required for your home will vary widely. A rich or prominent family living in a place with poor law and order and a background of crime or terrorism will need more robust, and probably more intrusive, security protection than a family with no specific threat in an area with a strong and effective policing and justice system.

This guidance will not inform you how to protect your individual home – you would need an individual risk assessment for that – but it sets out some broad guidelines on how to keep you and your family safe at home.

Physical security

- Make sure that all doors and windows are strong and effective. Look not only at the locks, but also at the hinges and the frames.
- Consider installing a door viewer to the main door, or a video intercom.
- Fit and use a door chain on the front door.
- Always keep external doors locked, even when you are at home.
- Do not advertise your name or any affiliation on external doors and gates.
- Consider fitting an alarm system, connected at least to all external doors and windows, and linked to a competent and reputable security company or to the police. You might install ‘panic buttons’ in various rooms.

- Use external lighting.
- Close curtains or blinds at night.
- In higher-risk areas, you may choose to fit bars to ground-floor and other accessible windows. Ensure, though, that the bars do not obstruct any emergency fire exit.
- Control the number and distribution of keys.
- In higher-risk areas, homes should have at least one safe room. This is a room to which all the occupants of the home can withdraw in the event of a security incident. It should be strongly protected by thick walls and a reinforced door. The safe room should be located so that all those at home have quick access to it (you may need more than one safe room, possibly one on each floor). It should contain a charged phone, a list of emergency contact numbers, food and bottled water, a torch (flashlight), and a first aid kit.

Visitors

Only let people you know, or visitors you are expecting, into your home. Check identification before you open the door, even if the visitor claims to be a policeman or some other official. Make sure that your domestic staff, if you have any, and your children understand and follow these rules.

Information

Try not to provide information that could be useful to criminals, if you can avoid it. Don’t give information about your home or family over the phone or internet to people you don’t know. Avoid telling people when you will be away from the house.

Children

Make sure that your children are aware of potential risks, and that they know what to do in the event of an incident.

Make sure your children are trained in first aid, take frequent 'refresher' training, and know how to use your home first aid kits.

Domestic staff

If you have domestic staff, check their references very carefully. If possible, avoid giving them house keys or alarm codes. If they leave your employment, change the locks and alarm codes. Make sure they understand the need to keep the home secure and not to provide information to others about the house or the family.

Domestic staff should be trained in first aid, and should know how to use your home first aid kits.

Fire

Fit smoke alarms - if not available locally, get some from your home country.

Establish an evacuation procedure and make sure all family members are familiar with it, including children.

Ensure keys are easily accessible to enable a swift exit.

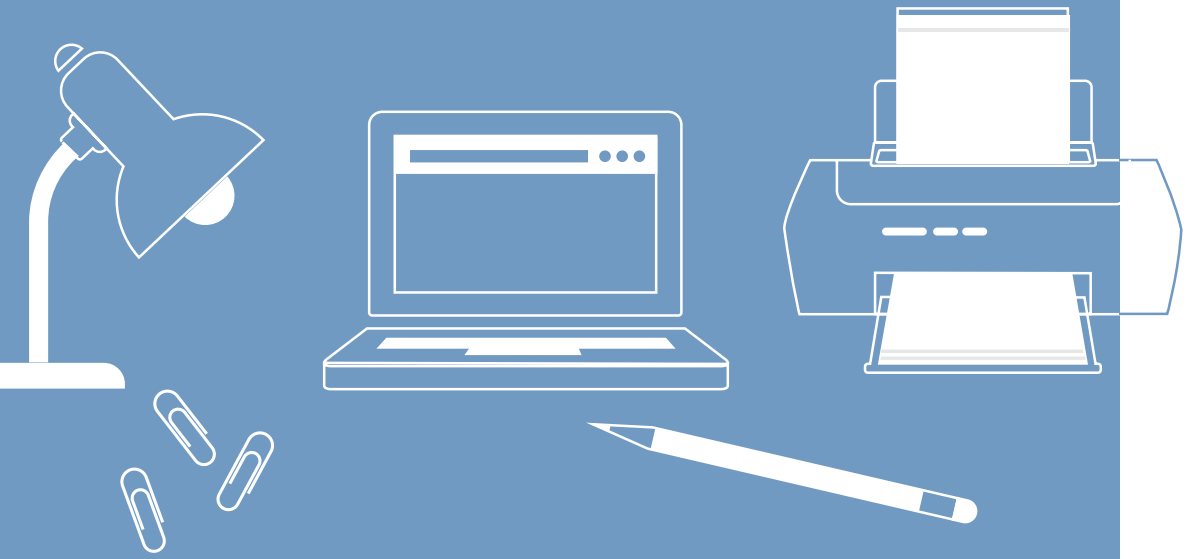
Security guards

Your home may be protected by security guards:

Whether the guards are managed directly by you or by a security company, you should take some responsibility to ensure that they do their work properly and that they are equipped appropriately. If you find that they are asleep or are not behaving as you expect, or that they are not equipped adequately, inform the management immediately and ensure that standards improve.

Do not let the guards into your home. Do not give them your keys or tell them your alarm codes. The security company management should ensure that the guards have access to a bathroom and to water, and are dressed appropriately for the weather.

If there is an incident, you should communicate with the guards without having to open the doors or windows. You should keep the guards' phone numbers or have a radio with which to talk to them from within the house. You should also keep the security company's office numbers with you, so that you can talk to them in an emergency.



Security in the office

All offices are different in terms of location and building type, and the profile and vulnerability of the occupants. This guidance is necessarily very generic, and will focus solely on the principles of office security.

Profile of office

The profile of the office – the extent to which its presence is advertised on the street – will depend upon the situation. In general, offices at risk should assume as low a profile as possible.

Protection

The office should be located so that it is a suitable distance from the road. For some offices, this distance will be minimal, but for offices in areas that are under sophisticated terrorist threat, they should stand back and be protected from the road by a considerable distance.

Protection required for an office will depend on the threat. Most offices in high-risk areas will benefit from blast-resistant window film. Windows should have blinds fitted for use when required.

Access control

All offices will need some degree of access control, if only to check the identity of visitors. Some offices will also need to be able to search bags and people entering the building.

Access control must be effective – only visitors who have been checked should be allowed into the main office space.

Once they have been through the access control, all visitors should be escorted to the office they are visiting.

Other entrances to the office – delivery entrances, for instance – must be secured so that entrance into the main office is impossible.

Car parking must be suitably controlled and secured. If the office has an underground car park, vehicles must be suitably screened before they enter, and occupants of the cars should be directed to Reception, without other means of access to the office space.

In the event of an incident

Office staff should be clearly briefed and rehearsed in a number of security drills in the event of, for example:

- Fire
- Illegal entry into the office
- Assault or attack within the office
- Bomb attack
- Reception of a letter bomb
- Threatening phone calls

In higher-risk environments, the office should have an appropriate number of safe rooms to which staff can withdraw in the event of an incident. The rooms should be strongly protected by thick walls and a reinforced door. The safe rooms should be located so that all those in the office have quick access to at least one. The safe rooms should contain a charged phone, a list of emergency contact numbers, food and bottled water, torches (flashlights), and a first aid kit.

E info@terrafirma-rm.com

www.terrafirma-rm.com