Protection against extreme violence

1. Scope

This plan has an internal focus: it is intended for the organization and its employees.

2. Target

This document attempts to summarize a set of guidelines upon which a BCP approach can be generated by implementing it. Thus, it is both a vision to BCP for terror, extreme violence and bomb-threat, and a listing of measures that can be included and developed in a BCP.

3. Definition

Extreme violence is any act of violence, reminiscent of an act of terror. In doing so, we temporarily shift the question to what is terrorism.

The Judicial Code defines terrorism as the use of violence against persons or material interests for ideological, religious or political reasons with the aim of achieving its objectives through terror, intimidation or threats. This definition is also found in the Law regulating intelligence and security services.
Possible actions that terrorists can carry out include arson, detonating rigs, hijacking means of transportation, releasing hazardous materials, disrupting water and electricity supplies, threatening, kidnapping and taking personnel hostage, ...
Since not only terrorists can commit these acts, but also mafia or gang members, people who are temporarily upset, or mentally disturbed, we prefer to speak of extreme violence in this paper.

Beyond the purely criminological aspect, there are other important reasons for this:

- the employee has a subjective sense of security. After the September 11, 2001 attack in New York, people have come to realize more than ever that "the human side" of work must also be protected. Thinking about security, also makes one think about personnel and their mental needs.
- "Being concerned with safety," likewise gives the employee, visitors and customers a "*safe*" feeling.
- Developing a proper risk assessment in the event of a threat or potential attack is very important for two main reasons: first, it can limit negative impacts on production and service delivery by the organization. In addition, a proper threat assessment will also prevent the organization from "overacting" in terms of protection provisions and not interfering too much with working conditions.

4. Impact of extreme violence

Overall, we can classify the consequences into six categories:

- consequences for the population and personnel (fatalities, injuries, illnesses, secondary victimization[1] , evacuation problems, psychological factors such as traumatization, dramatization of events, ...);
- environmental impact;
- decline in the quality of services and their continuity;
- political implications;
- property damage.
- effects that combine with one or more aspects from the previous categories;

Examples of consequences include:

- Building damage
- Loss of IT systems, data, communication systems and other facilities
- Unavailability of staff due to disruption of transportation to work or they no longer want to travel to work (unwillingness)
- Dead or injured personnel
- Negative psychological effects on staff such as stress and poor morale
- Disruption of other organizations on which one's own organization depends
- Reputation damage
- Financial costs of repair, cleanup,
- ...

5. Preventive measures regarding extreme violence in the context of BC planning

Ideally, the emphasis in the security plan should rather be on quality and organizational aspects such as employee involvement, accountability, communication and motivation. These often have greater effectiveness than expensive technical and electronic facilities.

The measures that can be used to ensure better prevention in the face of terrorist or extremist actions can be distinguished by *nature* into five different categories:

- *Organizational measures,*
- *(Construction) technical* interventions,
- *Electronic measures*,
- *IT Measure*s
- *Measures at the level of individual staff members*

.

Category 1: Organizational measures

Employee awareness and training

Clear arrangements for the reporting and centralization of security incidents are important. Instructions to and from personnel are best stated concisely and clearly. Important telephone numbers should be prominently displayed. Staff must have the confidence to report anything

[1] "Secondary victimization, means that victims actually become victims of the same crime a second time, by facing negative social reactions, (unwilling) officials and agencies that are unwilling or unable to help them, and grueling lengthy, bureaucratic, and expensive court proceedings. Mobbing and stalking victims suffer more from this than other victims." (http://www.sasam.be/secundaire.html)

suspicious all the time; they must know that their report will always be taken seriously even if it is a false alarm. Staff should know to whom they can report, and have the necessary contact information to do so.
The practice and testing aspect is very important here.
This is part of the BCP of the organizational units, and the BCP of each building.

Checks

If terrorists are aware that the company conducts regular spot checks on the quality of services at different stages of the process, some may be less inclined to manipulate this process

Clear business design and orderly housekeeping (see also category 2)

- Good lighting is recommended in order to avoid dark places and corners.
- Keep the reception area, entrances, exits, stairwells, restrooms... neat and clean at all times
- Make sure these places have only minimal furniture, so there are no or few opportunities to hide anything there.
- Lock unused offices, rooms and halls.
- Make sure each object has its (storage) place and that they are always stored there.
- Do not use trash cans at elevated threats, only plastic bags, and remove them regularly.
- Seal the maintenance hatches
- Prune trees and shrubs, especially near entrances.

Inputs and outputs

- It is best to keep the number of inputs and outputs to a minimum.
- Side entrances and rear entrances should only be used by authorized personnel.

Access roads

- Visitors should always feel that they can be seen.
- One must check that the appointment or delivery was due, only then can one give permission to enter the premises (preferably with a badge).
- For in-house staff, it is easy to have a computerized badge with photo developed.
- It may be opted to film visitors at the entrance.
- Visitors are best accompanied by someone from the organization[2] , or by someone from internal security and ideally only in areas accessible to all employees.
- One must check the baggage or goods to be delivered before providing entrance to the organization.

Visible performance in the building

- *Cameras* are best in both visible and invisible places.
- Supervision by (*uniformed)* individuals (possibly from outside security firms) deters "less trustworthy" customers and suppliers.

[2] Organization: Headquarters, Business Unit, Department,....

- Customers, suppliers and visitors should clearly notice that the building is secured. In this way, visitors realize that the chance of being caught when noticing suspicious situations is real.

Contact with customers, visitors, passersby and suppliers

- It is highly inadvisable to give customers sensitive information about money transactions, security measures or certain security procedures used.
- Visitors must be accompanied and must wear temporary badges, or some other form of identification, which they must turn in upon departure
- "Random" baggage screening can be implemented as an effective deterrent. Those who do not want to have their luggage checked should be denied entry.
- Keep non-emergency vehicles at least 30 meters away from the building.
- Keep an eye on passersby, whether they keep drifting, whether their faces return often.
- Use cameras to monitor activity on the street or around the building.
- Use cameras to spot individuals.
- Record camera footage for possible later investigation.

Key plan and key management

The organization must prepare a *key plan*. This key plan may include:
Level organizational unit

- Who is authorized to enter certain areas;
- Who is the person responsible for locking down specifically secured areas;
- Who keeps the keys in what places;

Level building

- Which windows, doors and closets have locks;
- At what times to close;
- What type of lock will be used (key or code);
- What the exact procedure is for shutting down.

Key management includes the set of procedures to keep keys efficiently and securely. Situations where keys are left unattended or in the possession of too many different people should be avoided. Some recommended measures are:

Level organizational unit

- the number of persons holding keys should be limited to a strict minimum;
- no labels are put on the keys: after all, this way everyone can know which key fits which lock. An alternative is to number the keys or color code them;
- persons who have received (a) key(s) may be signed upon receipt;
- in case of theft or loss of a key, it is mandatory to report it immediately;
- keys will not be given to temporary employees;

Level building

- spare keys should be kept in a secure place where unauthorized persons cannot access them;
- security cylinders have security keys; no keys can be duplicated without submission of a certificate because the profile is protected;

- A person responsible should be designated for locking the building and regularly checking the hardware (operation, damage, etc.) when leaving the building;
- if there is an alarm system, the staff can be informed of it. How the alarm is activated should also be communicated to staff members, while deactivation is better limited to the person(s) responsible for opening and closing (building manager, janitor,...).

The entrance should provide adequate visibility of the surroundings and is best well lit. Before total closure, the entire building should be checked for any "stragglers" .

Bomb threat

General: do not use cell phones, portable radios or the like.

Car Bombs

- Make sure an identified person is responsible for security and that the police and fire departments know your plans and have the layout of your building.
- Use as a basis good practices such as access control to vehicles and parking lots
- Consider using physical barriers, such as barriers, to keep foreign vehicles at bay. Ask the police for advice.
- Whenever possible, vehicles allowed to approach the building should be known and authorized in advance. The driver must be known and authorized in advance.
- Make the building more explosion-resistant. Have the building reviewed by specialists for this purpose. Get advice on communication and warning systems.
- Conduct training for bomb threats and evacuations. Keep in mind the danger of windows and glass walls and doors in doing so.
- Train and practice your staff in recognizing suspicious vehicles. Contact information for security people should be available everywhere.

Delivered (postal) packages / Suspicious shipments

A *suspicious mail package and suspicious letters* can be detected by:

- odd shape and/or unusual weight; Most envelopes weigh up to 30gr, while the more common bomb letters weigh 50gr to 100gr and are 5mm thick or more.
- manipulation gives a different impression than would be the case with paper;
- unusual amounts of adhesive tape were used;
- grease stains or discoloration on the mail package (possibly due to powder);
- the sender's address is not listed, illegible or unverifiable;
- the letter is unexpected and/or from a totally unknown/unusual sender;
- the country/city of origin of the sender of the correspondence does not match the postmark;
- there are errors in the address;
- strange handwriting or poorly typed address (possibly with spelling errors) has been used;
- greatly exaggerated franking: there are too many stamps on the letter;
- the package is directed specifically to a particular person;
- the message "personal" or "confidential" is located on the cover;
- unusual method of delivery;
- Use of foreign material such as cords, tape;

- electrical/metal wires are visible, aluminum paper has been used, and/or there are holes in the envelope (possibly caused by the metal wires);
- the letter leaves a strange odor;
- soft "tap branch" sounds may be heard.
- There is no return address, or it cannot be verified.
- It is incorrectly addressed, misspelled, or with the wrong title. Or addressed to someone who no longer works there.
- The envelope was reused (there are earlier cancellations)
- A bag or envelope with inner lining was used
- There is a sealed envelope inside the outer envelope. (Although this may be the procedure for confidential material in the organization to be sent).

Although most alarms based on these types of criteria are false, it is important that they are always taken seriously. Make sure the procedures made do not interfere too much with normal operation.

- Do not touch the package, try to memorize as many details as possible;
- Vibrations must be avoided, the place must be left and any colleagues present must be taken with them;
- The place should be locked; this ensures that it cannot be accessed by other colleagues;
- A perimeter must be deployed in the area so that there is remote "surveillance."
- Seek advice from your local police security specialist about the threat and possible measures.
- Consider handling incoming shipments only at one point, best in a separate building, or at least in a lockable room.
- Train staff who handle correspondence. Involve the reception staff. Ask your correspondents to always include the return address on the envelope.
- Make sure all mail undergoes the screening process.
- Consider separate air conditioning, alarms, x-ray scanning devices Also own laundry facilities, showers, soap and detergents.
- Train postal personnel in the normal procedures of receiving mail, opening envelopes with letter opener with minimal hand movements, and keeping hands away from nose and mouth. They should not blow into the envelope or shake it. They should wash their hands after opening a suspicious letter. CBR materials are put away in a double plastic bag.
- Consider using latex gloves and masks. Provide overalls and footwear in case contaminated clothing must be disposed of.
- Ensure that post treatment rooms can be promptly evacuated. Provide rooms with wash accommodations where contaminated personnel can be isolated and treated. Provide training on this.
- Provide appropriate signage that can be used in the event of a suspected or actual suspicious shipment.

Personally delivered IEDs (improvised explosive devices).

- Provide strict access control for staff and visitors in the buildings and grounds.
- At times of alarm, the only deterrent may be a systematic check of luggage at the counter.
- If a suspicious object is found, it should not be touched or moved. One should immediately notify the police (112)
- Consider a full-height barrier behind the reception desk to the rest of the building.

Suicide bombers with bomb on body

The most likely targets are symbolic locations, important installations, VIPs or large groups of people for mass casualties.
Consider the following possible measures:

- Deny access to anything and anyone who has not been thoroughly verified. Thoroughly verify identity.
- Form your search location away from the protected building. Have the front desk look out for people with suspicious behavior. Many bomb attacks are preceded by reconnaissance and test attacks. Report these incidents to the police.
- Install working cameras with good quality images. This often helps prevent an attack and can provide needed evidence at trial.
- There is no definitive physical profile of a suicide bomber. So keep staff on alert and have anything suspicious reported to the police.

Firebombs

The attacker will already declare the attack a success if the sprinkler system kicks into action. This can damage supplies and furniture. Fire bombs are easy to make and do not require explosives.

- Make safety measures part of your anti-crime provisions. Regularly check fire extinguishers, sprinklers, smoke detection and fire blankets.
- At high risk, conduct discreet after-sighting during company operations. Personnel should be trained in what to look for. This requires little knowledge, since most firebombs are not packaged. Most firebombs are hidden in easily accessible places.
- Since the person finding a rig is not qualified to tell whether it is a firebomb or explosives, they should clear the area around it, and call the police. If the rig ignites, it may be useful to try to extinguish the fire, but only with a one-time brief attempt and only if trained to do so. Note that finding one such rig does not rule out the possibility that several more rigs are hidden.

Chemical, Biological and Radiological (CBR) attacks

The dangers are:

- **Chemical**

Poisoning or injury from chemicals, which may be legal or illegal.

- **Organic**

Illness from a voluntary discharge of dangerous bacteria or viruses, biological toxins, fungi ...

- **Radiological**

Illness from exposure to harmful radioactive materials that contaminate the environment.

- Regularly check your air conditioning systems, including the intake and exhaust of them. Improve them where and when possible.
- Limit access to water resources and other key services.
- Check the safety and security of food and beverage facilities.
- Consider whether there are special requirements for the mailroom possibly with its own air conditioning, or possibly at another location.
- Shape staff to use available resources such as cameras, screening visitors, perimeters, ... as appropriate. Shape them to have awareness regarding CBR threats.
- If there is an enclosed area in the building, it can serve as a CBR shelter.
- Prepare safety communications to give staff instructions on how to leave the building. Train them on this form of evacuation.

Chemical, biological and radiological materials in the mail ¨/ Suspicious shipments

Recognize like this:

- Unexpected granular, crystalline or fine powdery material that is loose or in a container
- Unexpected sticky materials, sprays or fumes
- Unexpected pieces of metal or plastic
- Strange smells such as garlic, fish smell, fruit-like smells, mothballs, pepper, meat smell or a rotting smell. If you smell this, stop smelling it further.
- Stains on packaging
- Sudden attack of nausea or sickness, irritation of eyes, skin or nose and mouth.

CBR harnesses that contain a finely ground powder or liquid can be dangerous without opening them.

What you can do:

- The exact nature of the threat may be unprecedented. Always leave specific actions to emergency service experts.
- Regularly review plans for protecting personnel in the event of a threat or attack. Evacuation is not always the best answer. You will need to enlist the help of emergency services.
- Plan to turn off the systems that could cause spread of infection. For example, air conditioning, as well as computers with air cooling.
- Ensure that doors can always be closed quickly when conditions require it.
- Ensure that windows can be closed, if they can be opened. Train staff on this action in response to an alert.
- Test the feasibility of an emergency stop on air conditioning. Test this repeatedly. (e.g., annually)
- If a threat can be isolated by leaving the immediate area, it is appropriate to do so. When doing so, close doors and windows.
- Move infected people to an isolation room to contain the spread of contamination.
- Separate those directly infected by the incident from those not yet infected to prevent further infections.
- Don't ask people to walk away. But you cannot hold them against their will.
- No special first aid facilities are required. Emergency services are responsible for treatment of cases.

If it is believed to be a *powder letter*, the following advice applies:

- do not shake the letter, nor any other form of manipulation; the shipment must not be opened, even partially. Any unnecessary contact with the shipment should be avoided;
- the piece must be placed separately, at least in a plastic bag (ideally store in two hermetically sealed plastic bags) to prevent "dispersal"; in the absence of a plastic bag or any other form of enclosure, ensure that no one else can tamper with the shipment;
- the area must be evacuated and closed off to others;
- ventilation should be avoided and air conditioning should be shut down;
- if powder was spilled, do not clean it up but cover it with a piece of clothing, paper, etc. to avoid further spread;
- persons who came in contact with the product should thoroughly wash body parts that came in contact with the product with soap and water.

In the case of a *threatening letter*:

- threatening letters should be treated with the necessary seriousness. When a person comes into contact with such a letter, it is advisable to immediately put it in a plastic envelope or cardboard envelope. Indeed, it must be avoided that the letter is manipulated by many persons. This complicates the DNA testing that the scientific police can perform on the evidence.
- the recipient decides it is best to notify the local police of the threatening letter, who will notify the specialized services in accordance with the internal procedures of the integrated police.

Other BCR incidents

In the case of a BCR incident *outside* the building:

- turn off all air conditioning, computers, printers, photocopiers and heaters before leaving the building for evacuation;
- close all windows and doors when leaving the room. It is recommended to leave the key still on the door;
- Leave the building and move as far away from the scene of the incident as possible;
- when in doubt, do not leave the building immediately until express permission from the emergency services;
- Stay as far away from the object as possible. Pay attention to the wind direction, and stand with the wind at your back, looking toward the scene of the incident;
- notify emergency services.

In the case of a CBR incident *within* the building:

- when the item is still intact, do not shake or open it. If you have already grasped the item, or it is still in your hands, place it in a transparent plastic bag, or container. If there is no container available, cover the item with an object within easy reach, for example clothing, paper, ... and do not remove or move this covering;
- Do not touch a suspicious item or move the item to another place;
- Turn off all air conditioning, photocopiers, printers, computers and heaters;
- close all doors and windows but leave the key in the room, evacuate the room;
- if possible, place a visible warning on the door;
- move to an isolated room and at least avoid other people if possible. This is necessary, among other things, when the package is potentially toxic or contains contents that could produce an infectious disease;
- do not rub your eyes, do not touch your face and definitely avoid physical contact with others;
- notify emergency services.

Apply evacuation planning?

- In case of a threat to the building
- A threat elsewhere, with a notification about it by the police.
- Discovery of a suspicious item in the building.
- Discovery of a suspicious item or vehicle outside the building.
- An incident reported by the police.

Whatever the circumstances, tell the police what measures you are taking.

A general rule is to find out if the rig is inside or outside the building. If it is inside the building it is good to evacuate. If it is outside the building it may be safer to stay inside.

Security of secret documents

- Special documents, recordings, photographs, which are no longer needed after a period of time, are best destroyed immediately, stored in safes or kept in rooms accessible only to those with security clearance.

Category 2: (Construction) technical measures

(Building) technical measures refer to all security measures directly related to the building. Examples include impact resistant glazing, fencing, security lighting, mechanical protection of windows, doors, garage doors, unloading docks and hardware.

Doors and windows

- Glass doors deserve attention: on the one hand, they offer the advantage of making it easier for the company to notice suspicious situations due to their transparency, but on the other hand, glass is not the safest and sturdiest raw material for a door.
- In explosions, much damage is often caused by shattered glass from windows and doors. One solution is to choose glazing with an anti-shatter film and also adjust the thickness of the glass to where the risk of terrorist threats is highest.
- Similarly, consider an alarm system on doors that are not used often. Accessible windows should be locked.

Lighting

- Good lighting deters and is also essential for good quality when filming with the camera. (cf supra)

Secured areas

These spaces preferably laid out as follows:

- In places completely surrounded by masonry or the like such as aisles, restrooms, conference rooms, with doors opening inward
- Away from windows, external doors and external walls
- Away from the space between the boundaries of the building and the first line of load-bearing support columns.
- Away from stairwells or locations with access to elevator shafts that face the street on the ground floor because the explosion can climb up them. However, if they are enclosed on all floors, they are good protective locations.
- Avoid the ground or second floor if possible.
- In a space with enough room to get people to safety.

Category 3: Electronic measures

Electronics are prone to failure. Thus, proper maintenance of alarm systems, camera and video surveillance, among others, is a necessity for the effectiveness of these devices.

Alarm system

This is best put together on a custom basis. The nature of the building to be secured, the activities that take place there and the habits of the user(s) all play a role.

Camera Systems

These facilitate, if necessary at a later stage, the identification of perpetrators or of witnesses.

Inferior or poor results are due to factors such as:

- a lack of education about the capabilities of camera systems;
- a lack of a clear prior objective regarding camera installation;
- a disproportionate focus on technology rather than functionality;
- the lack of a recording test;
- a lack of proper user instructions;
- a lack of maintenance of the equipment;
- the lack of proper recording management. Attention must be paid to the regular replacement of image carriers. After all, when cameras are not properly maintained, they produce poor (and therefore unusable) footage;
- recordings are best kept for at least one month after filming;
- the time and display must be installed correctly;
- good quality image carriers should be used;
- the cameras should be well placed so that people and vehicles can be filmed clearly;

Category 4: IT measures

General and concrete preventive ICT recommendations

See ISO 27001 and ISO 27002

Recommendations for victims of IT crime

- Disconnect from external systems such as the Internet;
- Evaluate whether the damage is more important than restarting IT connections?
    - if *rebooting* is most important: make a full backup before reinstalling the system
    - if *damage* is most important: stay away from everything and notify police departments;
- Do not exchange emails on your own IT system regarding the incident;
- change all passwords and if possible the names of the users;
- Only restore the Internet connection if you are sure that all security holes have been closed.

Category 5: *Measures at the level of individual staff members.*

Physical security

See ISO 27001 and ISO 27002

Alarms

- Drug or alcohol abuse
- Expressions of extremist view, actions or incidents, specially when violence is preached.
- Major unexplained changes in lifestyle or spending.
- Sudden loss of interest in work, or overreaction to a career turn or disappointment.
- Signs of stress, such as excessive emotional behavior
- Unusual interest in security measures or in another mandate.
- Changes in work patterns, e.g., working alone (in isolation) or at unusual hours and reluctance to take leave.
- Frequent unexplained absences
- Repeatedly failing to follow procedures.
- Sudden or marked change in religion, political view, social commitment or other practice that has a contrarian impact on the individual's performance or attitude toward security.

However, it is important to note that some of these signs have other causes. This should be taken into consideration.

(Sub)Contractors

- Make it a contractual requirement that contractors verify the identity and good intentions of their personnel.
- Regularly check the contractor's compliance with the contract.
- Ensure that each contractor is part of a recognized professional organization that is accredited.
- Ensure that the person presenting is also the person who was hired. E.g. with a photo, along with the full name requested in advance.
- Provide passes. It must be worn prominently at all times.
- Provide a procedure for replacing staff with temporary replacements. Consider whether this person's access rights should be restricted.
- Supervise contractors and subcontractors. Especially if they have to work in sensitive locations.
- Appoint a responsible godfather or godmother for the contractor. This person can guide the contractor through the work, as well as identify security problems early on.
- If a person's work requires sensitive information or large financial transactions, consider tiered assignment of these access rights.

AMOK situation (wild shooter etc.)

An AMOK situation is that situation in which a person or persons at a particular location attacks those present there and attempts to inflict as many casualties as possible, without entrenching themselves or taking hostages. It is obvious that the intent should be to get the perpetrator(s) to stop and end the incident as quickly as possible.

AMOK situations evolve rapidly and unpredictably. Typically, police services must be called to the rescue. Because the AMOK situation often ends within 10 to 15 minutes before the police can intervene, personnel must be prepared both psychologically and physically for this type of situation.

Preventive:

- Make sure the building has at least two evacuation routes.
- Make these evacuation routes known to personnel, train in their use.
- Involve local police and first responders in training sessions
- Maintain a tidy workplace
- Be aware of indications of workplace violence and take remedial action accordingly.
- Screen your staff when hiring
- Create a notification system for signs of potential violence.
- Provide physical access control
- Distribute to appropriate managers:
    - Keys
    - Building layout
    - Phone no. of Facility
- Provide a crisis kit with
    - Radios
    - Building layout
    - Emergency numbers and contact lists
    - First aid kit
    - Flashlight
- First aid training provided to be able to work with tourniquets and hemostats.

Active:

(Good practice for catching a wild shooter)

- Be aware of your surroundings and potential hazards at all times;
- Always make sure you know the two nearest exits in the building you are in;
- If you can flee, flee, and report the alarm (for evacuation)
    - Even when others have doubts.
    - Try to help others flee.
    - Leave your belongings behind.
    - Prevent others from walking toward the shooter if possible.
    - Leave wounded.
    - If you see police, follow their instructions and always keep your hands visible, put down what you have in your hands.
- If you are in a lockable room (not a room with glass walls), lock it, close the blinds, turn off the lights, and stay there;.

    - If you are in an open space, go into a room without glass walls and lock it / barricade the door;
    - silence your cell phone.
    - Hide behind a large object if possible.
    - Call 911, and provide the following information
        - The number of shooters, where they are located,
        - Which and how many weapons are used (small arms or larger guns, knives,...),
        - How many victims you have seen.
        - If the shooter is nearby and you cannot speak, keep the line open so the operator can listen in.
- As a last resort, if you cannot run away from the shooter, try to take him out. Become enraged, use improvised weapons, throw things at him. Convince yourself that you want to overpower him and go for it. In doing so, grab his hands.
- Call 911 when you are in safety.

At insecurity:

- If confronted by police, keep your hands above your head, keep them highly visible and do not hold anything.
- Leave the police alone, do not ask for instructions either.
- The building manager will:
    - Follow the orders of the police, and give them the plans of the building, and any necessary keys.
    - Collect information regarding victims and pass it on to the police.
        - Who
        - Where in the building
    - Collect information regarding the perpetrators and pass it on to the police.
        - How many are
        - What weapons do they use
        - Description of the perpetrators
    - Identify and isolate the witnesses from the rest of the fugitives and each other
    - Keeping people away from the crime scene
    - Signal to staff that the crisis is at an end when this is decided by the emergency services and this decision is relayed by the V-CMT.
- The crisis communications officer will:
    - Catching the media
    - Implementing the CCP
- The HR person in charge will:
    - Having the prospective family sheltered and isolated from the victims
    - Provided a list of victims/patients to family members
    - Provide psychosocial care and related facilities.

6. Protective Measures Regarding Extreme Violence in the Context of BC Planning

The HR person in charge will:

- Provide a number of classrooms in which colleagues of the victims/deceased staff members can experience their grief. These classrooms should be large enough for several people. These classrooms are best not on their own floors.
- Provide a listening ear, professional or otherwise, for grief counseling (see framework contract).
- Provide a list of colleagues present at the event to their supervisor.

The supervisor of colleagues will:

- Follow up who has much need to grieve.
- Allow circumstance leave if necessary
- Suppress erroneous rumors about the victims/deceased and ask staff to stick to the facts.
- Let the crisis management team in their own organizational units know which employees appear to be in trouble, especially if they are reluctant to ask for help in the process.
- Must have awareness of how he/she himself/herself is coping with the event and the loss and, if necessary, communicate about it with colleagues.

The deceased employee's supervisor will:

- Empty the deceased's locker after hours, when colleagues are gone, after being released by the police and the court no longer has or lays claim to it.
- Returning the deceased's personal items to the family. He delivers these items personally, not through the mail or through a third party.
- The manager will organize a meeting with the family of the deceased. He/she will be accompanied by a member of the crisis management team.
    - The meeting place for the meeting will be determined by the family. In doing so, they will have a choice between at the family home or at work.
    - If the family requests it, schedule another meeting.
- The organization's crisis management team will engage the professionals following up with colleagues in a comprehensive debriefing after the event.
- Limit long-term active succession to a commemorative moment the following year.
- A letter provided to the family of the deceased. It is signed only by the executive manager of the organizational unit. This letter is non-general but specific and includes the following sections:
    - Part 1: inform about the event. In it, use only factual material and no euphemisms such as "passed away from us" but rather the concrete neutral terms such as "died of his/her injuries"... Also, do not use strong words such as "was murdered" "committed suicide" "was beheaded" etc.
    - Part 2 : Inform what steps the crisis management team will take in the context of this event.

    - Part 3: explain why you are sending this letter of information: the family needs to know what happened in order to help their family member. Possibly provide them with a phone number if they want to call to ask for further help. This may be a sign that this colleague is developing a problem.
    - Part 4: This involves giving the family additional information they may need, e.g., regarding the deceased's personal belongings.
- The building manager will: Prepare a lessons learned document.

7. Specific info

a. Responsibilities of the safety coordinator

- Creating a safety plan based on a risk analysis
- Ensure that security measures are implemented and tested on a regular basis
- Creating BCPs focused on bomb threats, suspicious shipments and the possible need for evacuation.
- Lead the evacuation after emergency services released the building.
- Cooperate with emergency services and other emergency services.
- Organize staff awareness and training, as well as prepare communications and sandbox exercises.

The safety plan must include:

- The details of protection measures physical protection measures, information safety and personnel safety and security
- Instructions on how to respond to a bomb threat.
- Instructions on how to respond to suspicious items and events.
- A search plan for individuals
- Evacuation plans, including details for secure locations in the event of a full evacuation.
- Other BCPs
- A communication plan and media strategy including responding to questioning by concerned friends and family.

b. Upon entering a bomb threat:

Bomb threat

Use a checklist so that no actions are overlooked. The checklist should be in a place where it is immediately available.

1. Staff guidelines:

- Remain calm, composed and courteous,
- Listen carefully, try to gather as much information as possible from the caller (gender, motive,...). Write down everything he says; **ensure that the conversation is recorded**,
- Do not interrupt your interlocutor (bomber),
- Keep him/her on the line as long as possible for any phone tracing,

2. Ask the following questions:

- Precise nature and description of the danger or threat,
- When will the threat be carried out, (When will the bomb explode?,...)
- What does the bomb look like?
- What kind of bomb is it?
- How is the explosion caused?
- Where is the bomb located?
- Did you place the bomb?

- Who are you?
- Where do you live?
- What is your phone number?
- Why was the bomb placed?

3. Internal guidelines:

- Report the bomb threat immediately to the security officer and notify the police immediately. In principle, one is not legally obliged to inform the police of the bomb threat. However, if it is not a "false alarm" and consequently a lot of damage can be done, one can possibly be held responsible for the omission of the bomb threat. It should also be noted that reporting the bomb alarm to the police authorities does not automatically mean that the production process will be shut down.
- Alert internal crisis management team emergency number immediately
- if you have been notified of the bomb threat, do not touch suspicious packages;
- Building manager or senior manager take appropriate action,
- In case the building is evacuated, take the attendance lists and give them to the leader of the external emergency services; when evacuating, never stand in front of a window or a glass door; do not block roads that could serve as escape routes;
- A limited search may be done with the staff who know the area very well. They always do this on a voluntary basis.
- If the suspect gear is found, it should never be touched.
- Immediately verbally communicate location of suspected rig to building manager or outside emergency services.

ATTENTION!!! The use of cell phones and walkie-talkies is PROHIBITED during a bomb scare!

4. Evacuation:

- If necessary, follow the normal evacuation instructions posted on each floor.
- The order for evacuation is given only by the (adj.) building manager or Mayor of xxxxx (fire or police officer), or by the Crisis Management Team or by labor safety.

5. Communication data:	
During office hours: ○ Internal emergency number ○ External emergency number: emergency number 112 ○ CMT:	**Outside office hours:** ○ Emergency number 112 ○ General Permanent Number of the building: e.g. 0800/ xxxxxxxxxxx ○ ○ CMT:
Disaster coordination city xx/xxxxxxxxxxxx	

6. In case of bomb threat:

Please fill out the appropriate form as completely as possible.

Inquiry Form "BOMMELDING"

1. Initial actions

Turn on the recorder

Tell the caller which city you are answering from

Note the exact wording of the threat:

Notify police, crisis management team and building manager

2. Identity of the caller: male OFemale O

3. Spoken language: Presumed accent:

4. Voice:

Strong: O Normal: OSoft: O

Clear: O Hesitant: O Confused: O

5. Way of talking:

Strong: O Normal: OSoft: O

Clear: O Hesitant: O Confused: O

Taped in O OffensiveReading text: O

6. Way of talking:

	YES	NO
Self-assured:	O	O
Calm	O	O
Irritated:	O	O
Emotional:	O	O
Reasonable:	O	O

7. Background noise(s):

O Office	O Airplanes	O Street noise
O Factory:	O Ships	O Children
O Trains	O Cars	O Adults (M/F)
O Animal sounds	O Music	O Domestic sounds

8. Miscellaneous information: (e.g., content of conversation)

9. Time of the call: Date: .... / .... / ....Hour : .... U ....

Duration: ..... min

Number where the call came in: .....