2023

Security Manual

"SERVICE WITH INTEGRITY."

Security Manual

Contents

Introduction

This document is meant as a guide to security in general. It is written on a general basis to cover the most of aspects of security work. It is meant as an overview of security methods and a primer in the field of security. It is meant to be read with already known security techniques in mind.

The Idea Of Security

What's the point of security? The idea of security can be defined as something that creates safety and well-being. This idea is at the core of daily activities. The need to secure ourselves and our property becomes a method to help our happiness and well-being. To feel safe is a basic necessity of life, not a luxury. Feeling safe and well is of the utmost importance for the human being. When we are safe, we can carry out our business with peace of mind. People are willing to pay money for their security, showing how much it means to them.

When we secure ourselves and our property, we invest in our safety and well-being. Pro-active security plans help us with keeping our lives and property in good shape. After that, we maintain our security by always keeping up with the latest security plan. For a security-conscious person, a security plan is a must have, in order to have oversight of his security needs. Without a security plan, it's difficult to maintain the current security situation. The security situation must always be maintained. Audits must be made and inventory accounted for. The security plan must be updated, reflecting the latest changes in the situation. A security plan is always fluctuating, keeping up with the latest security needs.

People’s security needs change all the time. The factor which works for some people is not constant. What is working for one person, will not always work for another. Security is temporary, the scenario is changing constantly and relevant security is changing too. Therefore, security needs to adapt itself to circumstances.

When we build security, we need to know the customer's situation. We learn his needs, so we can tailor a security plan for him. We discuss with the customer to figure out how to best build his security. Without co-operation with the customer, it will be difficult to work out the details about the security plan. The customer will explain about his needs and we create the security plan with his well-being in mind.

Mode Of Operation

1: Foundation

The foundation is the preliminary development our company has done. What we have built from the beginning, to make up a platform for our work.

Our trade is information to build security. The information itself is collected and further processed into more ideas for security measures. This consulting is what we provide to the customer as a product and service.

Part of our foundation is our website, where we have presented ourselves to the public. It's a display of what we can do and those products describe our work.

2: Work-process

We gather and process the information into knowledge which is useful for security measures. The information can be useful in itself, even before working out security measures. The security measures are developed based on the gathered information. The gathering and processing are done for the customer, depending on his needs. We know how to produce the products in the work-process and what to expect from our company's abilities.

3: Results

The results are the practical, concrete products and services we deliver to the customer. This can be every aspect of information and the security measures. Reports, articles, media, security suggestions, third-party security, etc. All results are the final outcome of the foundation and work-process and this is the company's achievements.

What is intelligence?

"Intelligence" means information which has been processed into knowledge. There is nothing mystical to it, though sometimes it is not easy to understand how it was acquired. The final outcome of the information-gathering can be delivered by many methods, that's the secret. Various agencies might use different methods, though the quality may vary, since there are many hindrances to the truth. After all, intelligence is all about true knowledge.

Intelligence includes information on the size, capabilities, location, disposition, and plans of foreign security forces, as well as information about foreign countries, and small or large cooperate institutions and events in foreign countries, or security companies required to plan for and carry out security operations. A variety of intelligence organisations help to meet these intelligence needs. Intelligence can provide insights not available elsewhere that warn of potential threats and opportunities, assess probable outcomes of proposed policy options, provide leadership profiles on foreign officials, and inform officials of counterintelligence and security threats.

Fundamentally, intelligence is nothing more than information that can provide decision-makers with advance warning of threats to our security or our prosperity but also of opportunities that we might face. However, intelligence enables individuals to understand and adapt to their environment, solve problems, make decisions, and learn from experiences. It also plays a crucial role in creativity, innovation, and the advancement of knowledge and technology.

Good intelligence comes from real and specific information. No matter how it was gathered, whether from the street or satellite imagery, the information must be informative and essential to meet the needs of those who are going to further process the information for security measures. The information is always on point and fresh up to the minute. The gathering and analysis processes make sure the latest strategic information is available. From start to finish in the intelligence cycle, the personnel maintain focus on getting the very best outcome.

Intelligence Officers

As intelligence officers, we always keep the gathering going on. We snoop around the area and sniff information. Our gathering-work is seen to be useful for delivering the best intelligence on the market. Intelligence officers use the environment and people to gather their information, in order to disseminate the intelligence. Being on the forefront of gathering services, the officers work their way to provide good intelligence. Intelligence officers are the most important tool to get the information-

gathering going smooth. Good officers pave the way for even more gathering, as much as possible. Intelligence officers are to provide a service that is crucial for defence. These officers are also to develop and execute plans, policies, and procedures that will facilitate intelligence functions. They are then meant as experts on all intelligence disciplines and their application across the spectrum of security operations.

Intelligence personnel provide the guard with the information it needs to act. Human Intelligence Collectors talk to sources in other foreign languages and conduct interrogations as such. Signal Analysts and Cryptologic Linguists use advanced surveillance techniques to spy on enemy communications. Again, the intelligence personnel collect, process, and distribute threats of terrorism, sabotage, espionage, etc. They compile intelligence information using maps, charts, reports, etc. And research the accuracy and reliability of data and sources and prepare and deliver investigative reports.

Intelligence can be defined as a general mental ability for reasoning, problem solving, and learning. Because of its general nature, intelligence integrates cognitive functions such as perception, attention, memory, language, or planning. The intelligence mission is to collect, analyse, and deliver foreign intelligence and counterintelligence information to institution, co-operate bodies, or nation's leaders so they can make sound decisions to protect their various institutions, companies and countries. Timely provision of accurate operational environment information gives joint forces operational advantage, increases successful outcomes, and saves lives. These insights can often be shared with allies and mission partners, enabling like-minded nations to achieve collective, synchronized effects not otherwise possible. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities.

The Intelligence Cycle

The Intelligence Cycle is comprised on four fundamental steps: Direction, Collection, Analysis, and Dissemination.

- Direction is the start of the intelligence cycle. This phase informs the rest of the process, and defines the information gap, and intelligence requirement. Intelligence requirements are determined by a decision maker to meet the objectives.
- Collection involves the tasking of intelligence sources and agencies to collect required information to satisfy the intelligence requirement. In response to

requirements, an intelligence staff develops an intelligence collection plan applying available sources and methods.

- Once the collection plan is executed and the data arrives, it is processed for exploitation. Analysis (sometimes referred to as "processing") involves the evaluation of the collected information to understand it.
- Dissemination is the final phase of the intelligence cycle and is how the newly created intelligence is provided to the customer and those who need to know.

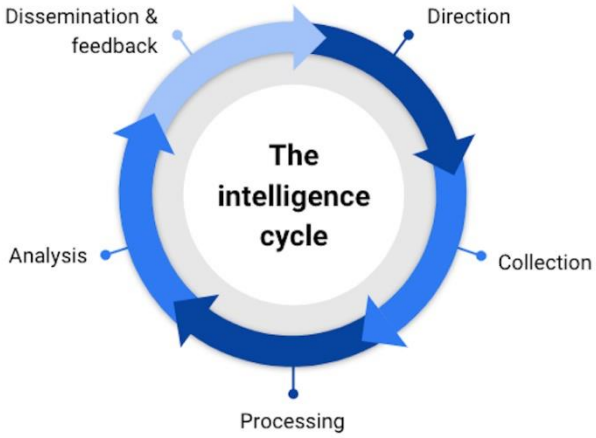


Figure 1 The Intelligence Cycle

Intelligence Operations

Intelligence operations are often the only way to acquire information that would not otherwise be available. The personnel gather information on undertakings that jeopardise security through intelligence operations. Open information sources are

often insufficient for investigating needs for security. The personnel may apply other intelligence-gathering methods in such cases.

One of the most important functions of intelligence is the reduction of the ambiguity inherent in the observation of external activities. Every security-conscious organisation must consider the protection of the three things regarding intelligence gathering: their intelligence personnel, their intelligence facilities and resources and their intelligence operations.

Intelligence is conducted at two levels, strategic and tactical. Strategic intelligence is information that is needed to formulate policy and plans. Tactical intelligence is intended primarily to respond to the needs of operations. Essentially, strategic, and tactical intelligence differ only in scope, point of view, and level of employment. Whether strategic or tactical, the intelligence attempts to respond to or satisfy the needs of the security leadership. The process begins when we determine what information is needed to act responsibly. On the strategic level they are usually called the essential elements of information and are defined as those items of knowledge that are absolutely vital for timely and accurate decision making. On the tactical level, intelligence needs are defined in a similar manner those items of information concerning that which must be collected and processed in order to address any intelligence needs.

Whether tactical or strategic, intelligence attempts to respond to or satisfy the needs of the operational leadership, the person who must act or react to a given set of circumstances, and the process begins when the leadership determines what information is needed to act responsibly.

Strategic intelligence often comes in the form of threat briefings tailored to the organisation. After receiving a threat brief, we may decide to change the way we track towards the risk or request reprioritization of the current strategy to enhance security. Timely provision of accurate operational environment information gives an advantage to increase successful outcomes. These insights can often be shared with partners, enabling like-minded organisations to achieve collective, synchronized effects not otherwise possible.

Security intelligence is to provide threat projections that guide the security services in how best to organize, train, and equip their employers, and warn of potential crises. Finally, they support the employment of the security companies across a broad continuum of operations, from disaster relief, to peacekeeping, to combat operations. Being able to understand what is happening currently across the world is critical when identifying threats. It is not enough to solely be able to view log records when dealing with immediate threats. Security intelligence is able to evaluate potential present threats in the whole wide world.

Security intelligence helps both the employer and his employees to prevent crimes and also add a sense of heightened awareness which improve customer service that provide a quick response time, in order to handle security issues in an efficient manner, which again will create a safe business environment. So, to have someone on site who can handle security matters hence promotes a sense of order.

Good intelligence management begins with the proper determination of what needs to be known and precise requirements are set. All data will be collected systematically and collective data must be evaluated and transformed into a usable form and stored for future use.

Military intelligence in another way is a discipline which when the personnel use an intel data collection and analysis approaches to provide guidance and direction to support the commanders in their decision making in providing good security.

It's really obvious that effective collection and analysis may be so that, intelligence is useless if it does not reach security commanders or its operational leaders in a form they can use and at the time they need it. It is imperative, therefore, that intelligence support to security operations be synchronized with global command, control, and communications systems. Dissemination channels for intelligence must be compatible with the information systems of the forces, permitting intelligence to be assimilated immediately for use in targeting and delivering precision weapons. In this regard, it has been found that there are still deficiencies that derive from the separate organizations and entities responsible for building the intelligence forces.

Intelligence Tactics

Our intelligence missions follow the intelligence cycle, direction, collection, analysis, and dissemination. We decide what information is needed and acquire this. Analysis after the intelligence is gathered and sharing the results with the customer. The strategy is to gather as much information about the subject as possible, before letting analysis filter every bit of information to extract valuable intelligence. The subject of the information-gathering could be a person or place or car or similar. It is supposed to be unaware that we're collecting information. The subject is isolated in the environment before it is investigated for its properties, as well as the surroundings of the subject. Tactics to deviate the subject from knowing it's investigated is applied. Let the subject act freely and undisturbed, in order to gather even more information about it. Whether tactical or strategic intelligence is gathered about the subject, all aspect of the subject should be surveilled. Any intelligence objects that are collected from the subject are analysed in accordance with already known properties of the subject. Previous properties about the subject are compared to newly collected information about the same properties.

Always stay away from the open area and be in the shadows, to not be seen by people when gathering. This way, we get privacy to gather in peace. If you are gathering information about a person, never let him know that you are there. Stay undercover and don’t blow your cover.

Gathering

It depends on the place and time, where we gather our intelligence. We can't let circumstances rule our job. We must be on point when we do our job. We must be on the forefront of gathering activities and be thorough in our focus. Our methods are applied strictly when there's information that can be gathered. Our intel should be of the highest quality. We never waver when it comes to capturing interesting objects. We keep our intelligence solidly intact after the collection. We keep our effort purely within the range of collecting intelligence. Our analysis will be of the most thorough type and always in conjunction with the direction laid out by management. The dissemination is done in context with the needs of the customer.

If intelligence was a television set, it would be an early black-and-white model with poor reception, so that much of the picture was grey and the figures on the screen were snowy and indistinct. You could fiddle with the knobs all you wanted, but unless you were careful, what you would see often depended more on what you expected or hoped to see than on what was really there.

Gathering intelligence is a discipline that uses information collection and processing approaches to provide guidance and direction to assist in developing security measures. This aim is achieved by providing an assessment of data from a range of sources, directed towards the mission requirements, or responding to questions as part of mission planning. To provide an analysis, the information requirements are first identified, which are then incorporated into intelligence collection, analysis, and dissemination. Most organisations maintain an intelligence capability to provide analytical and information collection personnel in both specialist units and from other departments and services. The intelligence capabilities collaborate to inform the spectrum of activities.

The discipline of gathering intelligence is so much more than a methodology. It is a mindset, a philosophy for how we empower our customers with the contextual intelligence they need to drive every security initiative and strategic decision across their organisations. The gathering is not a singular activity that organisations undertake, rather it is a series of connected activities, technologies and tools that work together to deliver the intended result. The deliverance of intelligence has significant benefits for organisations that face compliance requirements for the sensitive information that they collect through contract applications. The process for

acquiring intelligence feeds into other downstream planning to secure the customer against future unforeseen damages.

You could say that the task of gathering intelligence is like doing research for a new product. The product is meant to be security measures and the information will be the ingredients. You are at the forefront of the new product and your contribution is important for the success of the product. Without the ingredients, there cannot be any final product.

Doing intelligence is tough. It takes skills and endurance. It can even be dangerous. When you are in the field, you must keep open your ears, eyes and register everything that is happening. Use any acceptable means you have to capture the information.

Our working area is the ground, and we will be moving around in the plain environments. We will scour the area for information, wherever we go. When patrolling, we will be collecting information, as well.

We know that it is impossible to review all information collected, but with security analytics, you will be able to set up your tools to help you to identify and prioritise security action items. While we still may be dealing with historical facts, we should be able to optimise our response time to incidents.

Intelligence needs to get synchronized regularly. The most relevant information may change, so we adapt to it. Timely acquisition, processing and deliverance is key. A security audit will give vital information about possible discrepancies. Intelligence is always relevant because it is very difficult to identify a security breach until a third party notified about it, even though they had proof of it. A pro-active security plan can be worked out based on the intelligence, surveillance, and reconnaissance that can be drawn from it.

During an intelligence operation, there might be disruptions. There could be factors that work against us. We may not be able to perform our gathering work undisturbed. This can be seen as a setback to our operations. If we are disrupted too much, it will be difficult to do our work properly. We should not see this as our fault, but rather see the opportunity to better ourselves.

Practical Methods

Bodyguard: Bodyguards, also known as close protection personnel, are employed to protect customers to help ensure their safety from physical attacks and any other form of dangerous movements. Although bodyguards often **act as** a visual deterrent for potential attackers, the ability to blend into the background is key, and you may only be called upon in times of need. We will be our own bodyguards in our work.

In disguise:

As intelligence personnel, you can gather information even acting as a civilian. You can pretend as nothing and still monitor everything that happens. Be careful when using electronic equipment as this may blow your cover.

The use of your head: Our brains are our main equipment. It is called "intelligence" namely because our minds are our main tool. You must know that any details are important. The information may not seem important to begin with, but later analysis may show it to be. Therefore, even if things seem meaningless, they can be used at a later time to extract useful information. In order to register as much information as possible, distractions must be eliminated. Your concentration and focus should be kept in practise. It is easy to miss important details when you are confused. Be like a sniper who is always interested in acquiring the target. You should be able to spot peculiarities, like any irregularities in the environment or with people. You must discern what is interesting and useful for later analysis. Be like a hawk who's scanning the whole sky for its prey. You are hunting for information, like you are starving and need something to eat.

The use of electronic equipment: You should use voice recorder and photo and video camera. If you prefer, you can have all these on a mobile phone. It is not always easy to catch valuable information when there is a stress situation. Try to take short cuts and do not record too much at a time. Try not to draw too much attention to yourself when recording. We do not want anyone to interfere with our recordings and some people may object to the recording, so pretend as nothing and take it calm, in order to make yourself invisible to bystanders. Quickly leave the location after the recording is sufficient.

The use of the internet and public media: In our work, there is limited useful information on the internet. Though, it can be used to double-check and cross-reference our material. We can also find material which can be used for illustrations: text, photos, audio and video. Other public media like newspapers, magazines, radio and TV can be used to be updated on what's happening in the public sphere. We should follow these, though there can be limited use of these sources.

Buildings, vehicles, and other infrastructure: Physical objects like buildings, vehicles and other infrastructure can be valuable information. Record these on camera and note details. Try to remember details like text and colours of objects, because it is not always easy to catch everything on camera. Take photos and video from different angles and various distances. Sometimes isolate one building or vehicle and sometimes capture several of them at once. Is there anybody working on and around buildings? Where are people going? Where did that car disappear? Things may happen faster than you think, so focus on the target and keep watching the objects. If you cannot record anything, use your mind to remember the details.

The environment: When you survey the environment, you will see that there are a lot of details to record. There will be buildings, vehicles, and other infrastructure. These must be recorded onto photo and video for later analysis. Environments like neighbourhoods or villages can be recorded for later marking of oversight over the area. Observe what is going on in the area. Follow people, cars and even animals. Get a panoramic view of the area and zoom in and out, both with your eyes and the camera.

Collecting items: Many physical objects can be interesting. Such items can reveal a lot about activities. Such items should be collected and brought into safety for later analysis. Items of interest could be papers, notes, computers, mobile phones and other items like clothing. Any material which can give clues must be collected. Take photos of the items before you start to collect them.

Counterintelligence: Counterintelligence is when we protect our intelligence, to keep it from falling into the wrong hands. Not under any circumstances should there be left traces that the adversary can use. There should be very little for the adversary to understand about our operations. Be sure to leave everything clean before you finish your gathering.

Talk to civilians: Civilians are protected by international humanitarian law. Civilians often do not know about the subject's operations, but they know what they have done. Bring the civilian to a safe place. Try to avoid the use of names. Some civilians will be reluctant to talk, due to fears of retaliation. These should be left alone and not be coerced into talking, but most civilians do not like mean people, so they want to help.

How to interview people:

• Use a voice recorder if the situation allows for it.

• Do not ask several questions at once.

• Stick to the subject. Do not jump from subject to subject with no coherence.

• Be patient, do not stress for an answer.

• Treat the interview subject in a civilised manner.

• Let the interview subject talk freely by his own.

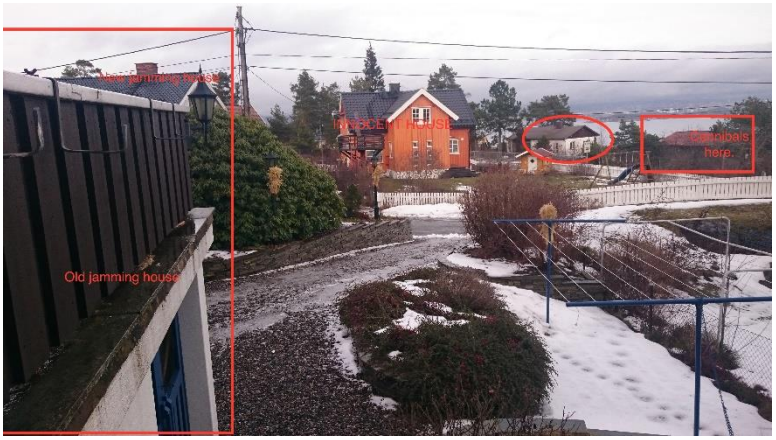
The use of informants:

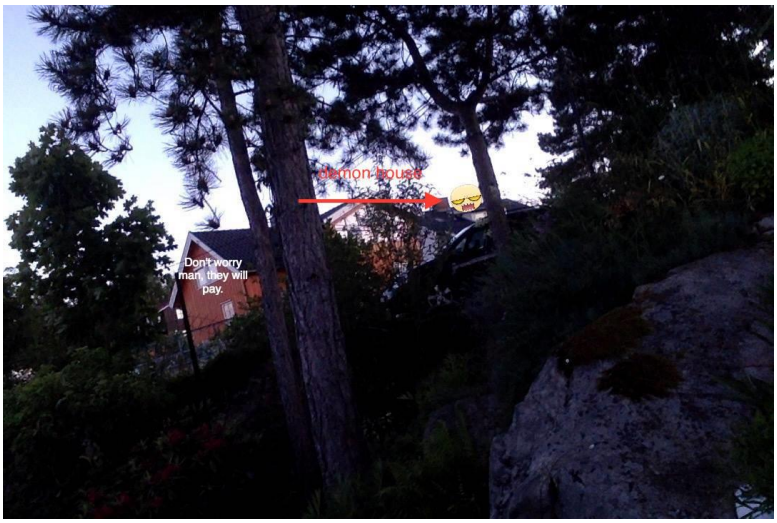
An informant is a valuable resource for information. If you have one, stick to him like a treasure. Keep a professional distance. Do not get to know him, use nicknames. Do not meet him too often. He might demand a good deal of money for his information.

Analysis

When analysing the gathered material, we consider what is relevant for strategic knowledge. Again, it is called "intelligence", so you need to use your brain to process the gathered material. The analysis is the foundation for the report. What is important and what can be discarded should be determined for the final report. You must be thorough in your analysis and not let any details go unnoticed. Notice any details of strategic interest, any details that talk about strategic objects. Ask yourself a lot of questions. Are there any persons of interest? What is the equipment? What colours and markings do the objects have? Which buildings contain what? Find answers to your questions and if you need, use any means to study more about the material. If in doubt, consult with your colleagues.

You can add markings to photographs, like in this example. The area is covered from different angles and items of interest are marked out.





Reports

The intelligence report is the final product of the gathering work. The report will be instrumental in the making of security measures. It is used to plan ahead and make way for taking decisions about how to conduct operations. It should contain the most relevant details from the gathered material. It can include illustrations, photos, audio, and video. It must be easy to read and understand, so avoid the use of academic language. Make sure you get your point through because there can be no room for misunderstandings.

Strategic Knowledge

When we work with strategic knowledge, we create practical, real-world security measures. In order to develop security measures, intelligence is evaluated. As intelligence is gathered, the strategic knowledge is derived. The intelligence is always fluctuating; therefore, the security measures provide a path to effectuate the outcome of a mission.

Operations

An operation within a mission is comprised of tasks. When a mission is developed, strategic knowledge lets us define operations with tasks. The operation can be compared to an umbrella who covers a person from rain. The operation is over-seeing the tasks and the tasks are the parts which make up the operation.

The objective of the operation is the goal towards which we all are striving. The objective must always be clearly defined. There is always an ultimate objective and other immediate objectives. All immediate objectives must contribute to the ultimate objective. This involves attitude, even when it cannot involve action. The attitude works as a pre-cursor to the action. Attitude can go a long way in determining the course of action.

Security Elements

After the five security elements have done their work, the combination will give strength and safety for the operation.

Figure 2 Security Elements

Security Departments

Management Security, Operational Security, and Physical Security are three departments within the organisation. They have various responsibilities in the scheme of operations. We invoke each department for their role in the development of the mission. Security departments and their responsibilities are intertwined.

- Management Security has the oversight of the organisation. They are responsible for the smooth operations of the company. Whenever there's a security issue, Management Security will deal with the issue. Mostly top-level responsibilities are handled by them. The work of Management Security is to ensure that the daily tasks are run as they should. When there's a problem to solve, Management Security is the one to deal with it. To explain the role of Management Security, we consider the roles of Operational and Physical Security as well. These three work in conjunction with each other's areas of work. Since they are intertwined, their work blend in with each other. Their roles are different, but at the same time they co-operate to form a seamless stream of expertise to ensure the organisation works as a whole. Management Security makes sure people are trustworthy and that they know their roles. It keeps the company's structure by investments and benefits. It has intimate knowledge of the company, to ensure it is strength and trust. Information about operations is delivered by Management Security and steps are taken to secure the integrity of the mission. Management Security will make sure that no information about the missions will leak to the public.

- Operational Security is to protect the operations by securing our plans and strategies. The oversight of the security plan is the main responsibility and the involvement of tasks, including locations, personnel, and equipment. Operational Security takes care of technical challenges and figures out how to conduct the operation. Operational Security has the responsibility of creating daily security tasks and make sure these are conducted by Physical Security. The role of Operational Security is to make sure daily security personnel gets their job done. Tasks and tactics are provided by Operational Security and ensure that everything is running as it should. On a daily basis, Operational Security is in charge of Physical Security and in charge of operations. They decide what is being done by Physical Security, who performs their tasks after agreed upon with them. Operational Security has the final word when it comes to how to conduct operations.

- Physical Security is the daily personnel responsible for performing tasks. Their responsibilities are the protection of personnel, hardware and other physical objects from threats that could harm, damage, or disrupt operations or impact the integrity and availability of equipment. The key to maximizing

one's Physical Security measures is to limit and control what people have access to, like sites, facilities, and materials. Access control encompasses the measures taken to limit exposure of certain assets to authorised personnel only. However, these obstacles can vary greatly in terms of method, approach, and cost. The building is often the first line of defence for most Physical Security systems. Items such as fences, gates, walls, and doors all function as physical deterrents to unauthorised entry. Additional locks, barbed wire, visible security measures and signs, all reduce the number of casual attempts carried out by an adversary. We must take note that with Physical Security, the personnel must be vigilant at anywhere and put to guard because you would only have an expectation of where the adversary will come from.

Security Protection

Security protection is about protecting the operation, from beginning to end, by making sure the operation cannot be compromised.

The operation is fundamentally laid down by starting with security protection for the security plan.

- Security protection needs to react to changes in all conditions of the operation and incorporates activities.

Security protection is the responsibility of the whole organisation and should know about the right approach to circumstances. It ought to have the learning and abilities required to survey all situations and to apply fundamental security in their parts. It lays out a structure designed to minimise threats and respond to risks.

The task of analysing risks is part of security protection. To be aware of potential risks and threats is crucial for the mission. Everything may go smooth if risks and threats are understood and minimised before and during operation.

When creating security protection, to undertake a security audit is preliminary action. This is a way to identify all threats, weaknesses, and factors to be considered for the security plan. Whether a security audit is possible or not, at the very least, a risk analysis is required in order to identify all potential obstacles toward the tasks ahead. You cannot determine the best possible course of action if you do not have a full understanding of the risks which you may be facing.

- Conduct regular security posture assessments.

Knowing where the operation stands when it comes to security risks is the first step toward creating a strong security posture and makes it easier to protect against risks

of which we are actively aware. While it may be time-consuming to conduct our initial assessments, we need to be serious about assessment because that is what is expected of the mission. It might not always be in the best interest to expect the worst, though understanding the diverse types of risks out there, allows for pro-active protection against them. This piece of security risk assessment might start as simply listing every possible security risk that could be encountered. No matter the size of the security plan, it is important to keep an up-to-date inventory of assets. Once inventory is taken, it is vital to track who has access to this property. In reviewing, the security protection will be able to see if there are any vulnerabilities that could lead to unexpected disturbances and risks for the mission.

Security Plan

- The security plan lays out a structure designed to guarantee a positive outcome of the operation.

First, decide what needs to get done to complete the task and what information we need to complete the task. During this time, we may develop questions about completing the task, for which we do not have all the answers. To continue planning how to complete the task, some of those questions will be answered by assumptions we make. For others that do not impede the planning, we look to answer later when we gain more insight. We appear with an initial plan to complete the task. To confirm the initial plan, we identify where to find additional information that will aid in completing the plan. We would then build a research draft to execute. To execute our research, we focus on the source of information that would provide the most effective answers to our questions. Once we have answered the questions raised during the first draft, we compile the information and look to develop the plan. In finalising our plan, we revisit the first draft, now armed with the answers to the questions we identified earlier. This will allow us to build an operable plan to execute the task. To start acting on the plan, we brief those who work for us on what needs to be done, how the job will get done, and who will do what to complete the job.

Tasks

Tasks for the security plan are worked out in co-operation between all departments.

- Tasks are delegated per person and there's also group tasks. Thorough briefing and instructions are given in due time before tasks are put into effect within the operation.

Location

The location where the security plan will be put into effect is surveyed before execution. The map is not the territory, so any intelligence is not the truth about the location. Nevertheless, what is known gives a theoretical basis for knowing the environment. Reconnaissance of the location is relevant, though very difficult to obtain.

Visitation of the location may be done during day or night. To know the timing for when it is safe to enter is important. If the operation is supposed to be covert, then undercover actions are required. To operate in disguise might be necessary, in order to stay unknown to eventual people who are placed in the location.

Timing

The timing of the task and when to enter the location is crucial. According to season, day or night and weather changes, the timing must be calculated to fit the task's location, content, and desired goal.

Personnel And Equipment

The Physical Security personnel can be one individual or a team. The proper personnel for the tasks are selected via recruitment interviews. Various properties of the personnel are evaluated to find the right position for them. Like a chess game, they are different players with one goal - the successful outcome of the security plan. The selection process finds out if the personnel are of necessary physical capabilities. Strengths and weaknesses of the person are known before the roles of the personnel are delegated.

Equipment is tailored to suit the employee's skills and capacities. Physical build and strength let various gear be carried by the right people. How to operate the equipment is taught via courses, and practice is done to get familiar with the practical use in a real-world situation.

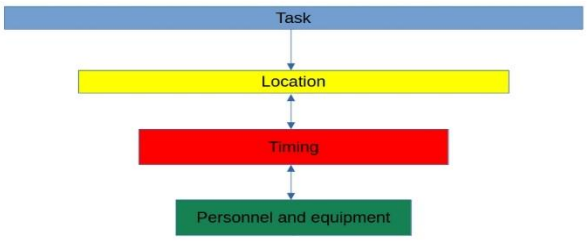


Figure 3 Tasks

Deployment

Deployment of personnel is done depending on the tasks they have been given. Location, time, and equipment are allocated and accounted for, known, and prepared beforehand, by Operational Security.

The Live Operation

During action, the results might not become the same as the envisioned plans, because the personnel are not machines, and the tasks are not programmed like a computer application. This fact lets the personnel have the freedom to adapt to any unexpected circumstances during the operation. Of course, various alternative options to be done in case of disruption in the conduct of the operation are known by the personnel.

The fact that all personnel have relative freedom, is not a weakness; it rather strengthens the personnel in that they get more power to act in accordance with their training and experience. The trust in every involved individual, releases the need to control every aspect of the operation. Thereby, letting the dynamic force of the combined organisation lead the mission.

Reports & Damages Management

RDM is the final element in the mission process. Reports are written and evaluated, and errors and damages are accounted for. If a disaster occurs, the company may become defunct. RDM is there to conclude the success or failure of everything, from the first conception of the mission and all the way up to customer satisfaction.

Whatever happens during the mission's lifetime gets recorded in human memory, whether events are consciously noticed or not. That is why we do de-briefings, so we can build on the experience for future missions. If there happen errors, we can figure out the reason. Sometimes, the error can be instrumental to a positive outcome. Despite an error, we should not conclude a total failure. Nobody can complain if the end result is proven to be successful.

ECC

Note: ECC = Error Checking & Correction. This concept is about knowing, catching, stopping, and fixing errors, before, during and after the mission is completed. Errors are anticipated and corrected on-the-fly, while the entire process is happening, from beginning to end. The idea eliminates unforeseen problems and reduces risks of failure.

General Security

Think Tank

As a think tank, we work with ideas and the subject is always security. The ideas and subsequent practical security measures must be realistic and reasonable. Any form of security is a good idea as long as it's beneficial with no side-effects. Real-world results are the most important outcomes of our work. Whether it's an abstract experimental project or as practical as a guard operation, the customer needs to feel safe and this is the ultimate objective. Safety is something you can "feel" and this is not always easy to deliver, depending on the circumstances of the job. We mostly deliver information. Sometimes, the information itself can create security. Just by knowing the information, you can become secure and even create further security, based on the information. This immaterial security can be valuable for some people.

Concepts Of Security

There are 3 concepts of security:

- Confidentiality

We keep our confidentiality intact at all times. The customer can be sure his interests are taken care of, without disclosing any information.

- Integrity

We keep our word. Integrity serves the purpose of being full proof when it comes to promises. We never fail our integrity and do our tasks as expected.

- Availability

We are sure to be available when the need arises. Always present in the matter at hand. Availability means to deliver the security the customer expects.

Security Consciousness

A security-conscious organisation is what we strive for. We live and breathe security into the lives of our customers. To be conscious of security means to be aware of everything within the focus of security. Security consciousness makes sure that security needs are always put first in the working process. The thought of security becomes the foremost factor in our daily lives. Security consciousness is with us wherever we are. This makes sure that security measures are always in development and that they can be realised. The measures come into fruition by the mentioned conscious behaviour within the organisation.

Good Security

The key to good security is to stay professional at all times. Always keep up with the latest security plan to meet the standards of good security. Be pro-active and alert to any changes in the security environment. Be vigilant in all situations and if you see something, say something. Use tactics that are provided and take action when necessary. Properly applied security is to deliver even under adverse conditions. We strive to be secure in our positions and be in tune with the customer's security needs and to be educative about security and work for security enhancement when needed.

Ethics

Ethics are an important part of the job and are built into the daily mode of operation. We strive to fulfil the highest standards in professionalism. We take care of people and the environment. When it is necessary to use force, the least use of force is to be preferred. We must under no circumstances bring harm upon people or the environment. Our forces are built up by being professional and courteous between the employees. The culture of non-harming will make sure that security ethics are at the highest level.

The Myth Of Security

It's a myth that security is easy work. Real-world security work can be difficult. We have to watch out in everything we do and handle adverse situations and make sure nobody gets harmed. It is not about just pacing back and forth on patrol but comes with many tasks that are hard to perform. We must always be vigilant and keep up with changing security plans and be alert to the environment. There's a lot of responsibility with security work, in that the job comes with certain powers that are not to be abused. Misunderstanding security work can be detrimental if you are supposed to work with security.

The Power Of Security

The power of security makes sure everyone involved, personnel and customer, are safe and sound. The power of security has the means to alleviate a distressing situation. As security personnel, we have the power to influence the surroundings and people and should not take this power lightly. In public places, we never display our power in a rampant fashion. Our power is not to be abused by the personnel and should be kept confidential. The power doesn't belong to us, it is given to us as servants of the civilians. Whatever power we possess, we always keep it safely guarded within the framework of ethics. Ethics makes sure that the power of security is intact and ready to use.

Pro-active Security

Pro-active security means to be on the forefront of any security situation. We plan ahead and develop security measures for the future. By being pro-active, we lay down a foundation for further security plans. Pro-active security is always in development and on point with current security plans. Current security plans can be created by applying pro-active plans. Every pro-active plan should be transformed into the current security plans. Pro-active security means that we are prepared for security needs beforehand. Before the security situation appears, we have already made sure that there's room for security measures.

Security Briefings

Before every mission, we hold briefings for the personnel. We make sure that everyone involved will know their responsibilities. We go through tasks and objectives and brief on every detail regarding the mission. The briefings are held in due time before the mission. The mission statement is always presented in the briefings. Whatever we brief about becomes part of the mission. Mission briefings will make sure that everybody understands their tasks. Mission readiness depends on thorough briefings that are held in conjunction with security standards. These standards are performed to the excellence of the briefings.

Security Awareness

The first mission of a security awareness team focuses on operations. Operational support encompasses management of the financial, human, and material resources required to achieve the objectives of the awareness program. i.e., facilitating access to resources (human, financial and physical). Identifying the tools needed for effective program management. Helping identify the methods for communicating results as well as potential relayers of the information within top management. Conducting the necessary follow-ups to guide the process or correct the gaps noted in awareness activities. Coordinating the program’s deployment phases. Establishing priorities, coordinating awareness activities, and determining the type of support needed for carrying out the activities.

Smooth Security

Smooth security is what we all want. When everything goes smooth and by the numbers, we effectuate the security work. Dealing with security issues becomes a breeze and we can relax confidently that our work is for the good of things. When the security situation goes like a warm knife in butter, we can be sure that our work has bloomed to the fullest. Smooth operations are what we seek, to ensure the confidence we have with ourselves. When our confidence is high, smoothness is easier to achieve. We don't want cumbersome and sloppy elements to interfere with our operations. Smoothness means to always be on top of things and let the security situation almost instrument itself autonomously.

Security Tasks

Tasks are governed by Management Security and the delivery is done by Operational and Physical Security. Operational Security develops the tasks and Physical Security executes the tasks accordingly. Tasks are done according to what objectives we have for the mission. Whether it is securing the premises, guarding a person or valuables, or intelligence operations, the task at hand is done to fulfil the mission in accordance with what we need to deliver. Tasks are handed out to the personnel on a basis that makes sure the personnel are able to perform their duties. Tasks are proliferated in small portions, so the personnel can share the task and never be overwhelmed. Tasks should not be given to personnel under circumstances of severe adversity and stress.

We inherit our security tasks from the top level downwards. The tasks are developed by Operational Security in conjunction with permissions from Management Security. The tasks trickle down from the main mission and are delegated to Physical Security, who perform the role of security officers. Tasks are handed out to Physical Security at a pace which is comfortable and with the speed to get it done immediately. After the tasks have been published, they cannot wait and are set in motion right away. The inheritance from the top down makes sure that a red line is connected between Management and Physical Security, via Operational Security.

Aspects Of Security

The aspect of security where we deliver our most important work is where we can apply security to the fullest extent. We provide good security to the public and serve with integrity to whoever needs our services. Whether we're on the premises or guarding a life or an item, our security is always world class. The importance of our work should not be underestimated, as our first-class security is unparalleled in the trade. Since our work is going forward, we strive on with diligence to give people the safest feeling when they are our customers. We deliver something that most other companies do not and we deliver this by way of being the top of the class player in the trade.

Improved Security

There are many ways to improve security. When we improve security, we consider the weak parts of security and make them stronger. We can improve security by checking what's wrong with the current security plans and fix the errors. Improved security will oversee the current security plan and enhance it. Another way of improving security is to make sure the security plan is solid and intact and up to par with current security standards. Improving security guarantees that current objectives are easier to meet. When security has been improved, the security plan has been full proof.

Security Factors

There are three factors that are involved in this context, when we talk business. These must be considered when we enter a contract and develop a mission. The factors are important since they describe what actions to take. Constant factors as opposed to non-constant shows how to evaluate the factors.

1: The factor of people, environment, and items.

This is the objects of security within a situation. This is the area of expertise where we perform our tasks. These objects are always fluctuating and are not constant.

2: The factor of the personnel

This is the personnel of the security work and how they evolve through the security process. The personnel are the most solid entity in the three factors. This factor is constant, in that it's the personnel who are performing their tasks for the customer.

3: The factor of the customer.

This factor is about the customer and his security needs. The customer helps to decide what course to take during a mission. The customer is always changing, so this factor is not constant.

For example, when we develop an intelligence mission, we take the three factors into account when we evaluate how to perform the mission. We see how the factors work among each other to form a strategy for the mission.

The Object Of Security

An object of security means a person, item, location, or operation. To ensure the safety of the mission, the object is to be evaluated. The object must be clearly defined, when working with the mission. When we define the object, we consider all properties of the object. The object must be accounted for and strengths and

weaknesses are recorded. What are the risks involved with handling the object? Does the object pose a risk by itself? The object must be scrutinized to be aware of any such risks.

The object in question is handled with the utmost care and protection, to make sure the object is not compromised. If the object is damaged or poses a risk, it jeopardises the mission. If the object has risks, they must be handled and secured properly. To secure these objects, means to safeguard the mission's objectives, as the objects are instrumental for the mission.

Security Targets

Security targets are there to help our tasks succeed. There could be various targets. A premises, a person or an item are all within the range of security targets. The targets are where we aim to deliver our security measures. They help our tasks by way of being in focus for the tasks. All efforts are focused at employing the mission tasks towards the targets. Mission tasks are secured for the targets by deploying security personnel towards the tasks. Security targets will be held in high regard for being able to complete the mission. The targets play a significant role in the finalisation of the tasks.

The Security Order

The order in which security is applied is important. First, we secure the people, after that, the area and any items. In this particular order, the security is better and easier to build. To secure the elements in the correct order will be the best way of applying security.

- The people are secured by way of watching their movements and actions. They are brought into safe areas as the areas are getting safe. The people are counted one by one and accounted for. Then, they are put into groups if the environment allows for it.

- The area is searched around and scoured for offending objects which will be handled with care. Any offending objects must be cleared away. The area must be clear and safe to enter. The area will be investigated later to search for items.

- Items must be secured and any loose objects are accounted for. Some items are collected for intelligence-gathering. Interesting items must be saved for further analysis. Dangerous items are handled by special units.

Digital Security

Attackers seem to innovate nearly as fast as technology develops. Day by day both technology and threats surge forward as we enter this era of threat. We must be very

careful despite the mounting anxiety about the implications, the full extent of its potential misuse by attackers is largely unknown. To better understand how attackers can capitalize on generative we have to conduct plenty research projects that will shed light on a critical question on human mindset about security and its impact on society and how we can better understand the consequences of our actions.

We should treat personal electronic data with the same care and respect as weapons because it is dangerous, long lasting, and once it has leaked there's no getting it back so we should keep note about that and make sure it is well kept.

Being security aware means that you understand that there is the potential for some people to steal, damage, or misuse the data that is stored within a company's computer system and throughout its organization deliberately or accidentally. Be extra alert; know who and what are around you at all times. Trust your instincts. If you have an intuitive feeling something is wrong, trust your instincts. React immediately and take action to reduce your risk.

Conflict Resolution

Peace is the natural, primordial state of things. Peace is not just the absence of war. Real peace starts with the individual's peace of mind and prosperity, that subsequently extends to communities and then the rest of societies in a nation state. Our work is about creating peace, though not how to establish policies for a government. We begin by negotiations when there's a stand-still during the conflict. This creates an illusion of peace, though the conflict is not fully settled. The conflict might continue if negotiations fail. Our mediation to prolong any possible pause will lay down the preliminary foundation for serious long time plans to resolve the conflict, once and for all.

Security Ideas

We can get a lot of ideas about what security is. What is its purpose, what is it for? These questions are best answered by saying that security is about feeling safety. Safety is something you can "feel" and it's understood when you feel safe. This safety is brought by applying security in all its forms. Securing people, premises, items and collecting security information and creating security measures are all contributing to safety. As long as safety is intact, then security has been well applied.

Security Assessment

When assessing the needs for security, we consider all aspects of the security environment. We assess everything from the beginning, including the security plan.

First, rehearse the operation with the personnel to find out whether they know their tasks. We make sure that all personnel have understood their responsibilities and how to carry them out. The personnel must know exactly what they are going to do.

Then, account for all equipment, as well as location, time, and weather. Equipment is checked beforehand and must be ready for use and without damages. Location is known and time and weather are assessed. Any discrepancies in these parts of security must be amended.

Security Ideals

Security ideals are the most important aspect of the security environment. We evaluate the ideal amount and form when we develop security measures. Security ideals are the perfect measures to be applied for any situation or object. Security should be optimal for the circumstances. It should not interfere with the object of security and cause no harm to individuals or the environment. Security ideals is to make sure operation goes smooth and undisturbed. Security ideals make sure that limited security is always applied. Limited security means that there is no way of creating problems for the object of security.

Ideally, we are not exaggerating the amount of security. Exaggerated security is to complicate the security environment. Security ideals should make sure that security measures are not too lax and not too tight. The scope of any security measures applied should always be within limits that do not interfere with the object's well-being.

Security Enhancement

Security might be loose or tight. When we lax on security, all sorts of disasters may happen. The need to enhance security is evaluated based on the threat assessment for the object of security. When threats are identified, it is easier to see how security can be regulated. It is not always proper to tighten security, even if the threat level is higher, but small enhancements that can easily be laxed or tightened as we see fit, are in place. Tight security is not the best outcome, as it brings with it a lot of technical properties that can be complex to carry out. Security enhancement should be the last resort, after the disaster threats have been thoroughly known.

Since security enhancement is the last resort when the disaster threats escalate, they must be readily available. Therefore, strategic planning beforehand is key for deployment. The security measures must be developed in order to be rapidly put into effect. Security enhancement cannot wait when the situation calls for it and are worked out beforehand, as a backup solution. The security measures cannot always be known to be full proof, so multiple solutions should be provided.

Security enhancement must not be detrimental for existing security. It must not interfere too much, if the current security is well established. It should only be applied

when there are fluctuating aspects to the security situation, for example when the disaster threats indicate the need for tighter security. Existing security is usually good enough, so there is no need to apply security enhancement just to add to it for the sake of increased security itself.

Security enhancement becomes redundant when there is no particular need for extra security measures unless the disaster threats call for them. Therefore, such measures are applied only on a need basis.

Security Analytics

When we analyse security, we analyse every aspect of the security process. We first gain an oversight over the various factors involved in the security process. Then, we get analytics involved in the process. We analyse people, environment and items and see how they are connected in the security process. We also analyse episodes and situations that has happened, in order to learn from previous experience. Every such factor is accounted for and the analysis lets us plan for future security. We can find failings and issues to improve our security plans, by way of analysis. The analysis paves the way for further security plans.

Security analytics is the most important review for further security plans. In the review, we get new knowledge about security aspects and get to the core of any problems in the security process. The security process learns from the analysis reports and we draw on the results to form a better security plan.

Objects Of Analysis

When we analyse, we analyse people, environment, items, episodes, and happenings. We begin by finding out how these factors have been instrumental in creating a security situation. What did the persons do, how was the environment built up, what items have been there, what happened in the episodes? Knowing these factors is important for the analysis, in order to later build better security.

Figure 4 Analysis

Consultancy

Consultancy for the customer comes in two phases: First, we discuss with the customer and every aspect of the security situation is considered. We take notes and map all elements that's needed to fit the needs. The needs are understood by us and we work with the current security situation. Pro-active security measures may be considered, in order to cover the initial security needs. The conclusion of the consultancy should be a complete security package for the customer. All needs are covered from beginning to end of the job. The customer should feel safe about his investment and expect that we have made sure his security is taken care of.

In the second phase, the consultancy further continues with a security plan. The plan is in accordance with the security needs. We have considered what the customer needs in terms of security. Buildings, locks, bars, personnel, items are enumerated and placed into their respective positions. The tasks are developed in conjunction with the first phase and the security plan. They are put into effect according to the security plan. The security plan is always authoritative when it comes to carrying out the tasks.

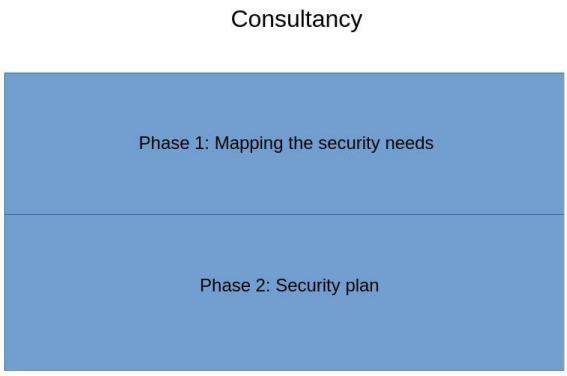


Figure 5 Consultancy

Contracts

Management Security handles the contracts with customers. We negotiate the contract after surveillance of what type of work will be done. Depending on the customer's needs, we calculate the price for our services in accordance with industry standards. We make sure that any liabilities are agreed upon with the customer before signing the contract. Any disagreements with the customer must be resolved before, during or after the mission, in conjunction with what is written in the contract.

Delivery

When we deliver our security products and services, we aim to serve the customer. We keep our professionalism intact and always keep in line with industry standards. We deliver by way of presenting the best possible security solutions to the customer. Delivery serves the purpose of keeping everybody safe and sound. Our customer-centric approach will ensure that everybody is happy with their purchase.

When we deploy our security solutions, whether intelligence or strategic knowledge or guard operations or conflict resolution, our work is carried out with the goal of delivering quality and not quantity. When gathering intelligence, we collect the most useful information and make sure nothing is left uninspected. When we work with strategic knowledge, we find the most plausible and realistic strategy. During guard operations, we are loyal to the task at hand. When conducting conflict resolution, we mediate with the result of pleasing both parties to the best of our ability.

Delivery takes place at the location with the task at hand. Various locations may be visited along the task. Where the location is, is decided by the security plan. The security plan contains all that is needed to specify details about the delivery.

Tactics

Tactical security means to apply security methods in the right manner at the right place at the right time. Tactics are the means to an end in a security situation. Security tactics become an integral part of the security work. The way we conduct operations in a tactical manner helps to secure the objectives of the mission. Tactics are developed by Operational Security and carried out by Physical Security. Operational Security decides how to apply the tactics in co-operation with Physical Security, who gets trained in performing the tactics. These tactics are the most important factor in the delivery of security.

How To Escape From Armed Men Or Attack

Find cover, however while doing this evaluate what direction the shooting is coming from and guess on how many shooters are present. Some ideas on finding who is shooting and where the person or people are: Look at who is falling from being shot. What inanimate objects are being hit and what direction the crowd is moving in and move away from the shooter or shooters. Stay low and look for cover while moving and stay down when there is no cover. Do not do things that advertise your existence to the shooters or attackers. Examples include screaming, flailing arms while running and stopping movement from time to time to evaluate situation. Always make sure that you don’t go close to the armed man or men and you stay down flat on the floor and do not talk.

Emergency Planning

Drills and exercises are designed to test, evaluate, and validate emergency plans that protect the safety and welfare of our employees and customers, and must be viewed with the utmost seriousness. Also report broken fences or doors, malfunctioning locks, inadequate or non-working lighting to Management Security department. Observing and reporting system weaknesses will decrease an adversary's chances of success. Operational Security will provide methods to deal with such cases.

Attackers

When attacked by an adversary, we are allowed to defend ourselves by force. The least force should be used, but only enough to bring the attacker under control. The attacker must be pacified and brought into custody. Various self-defence techniques can be applied. Handcuffs may be used when the attacker has been calmed down. Physical Security handles the attacker and later, the episode with the attacker is reported to Management Security, who deals with the aftermath. Management Security decides how to handle the episode and deliver the attacker to the Police. If

the attacker harms the personnel, they must be brought to the hospital as soon as possible.

Privacy Awareness

Don’t give personal information readily. Always ask questions before disclosing private information about yourself or your employer, especially when you think the requested details are not necessary for the objective. Never disclose the requested details until you have been informed about how the information would be used and assured that it would be protected. If you are not satisfied with the answers given, don’t disclose your details.

Adversaries

Within the organisation, threat information is necessary to develop appropriate countermeasures. The threat analysis includes identifying potential adversaries and their associated capabilities and intentions to collect, analyse, and exploit critical information and indicators. Organisations should seek support from their security, intelligence, and counterintelligence experts. As an individual, whether you are at work, or outside of work, try and answer these questions. Who is an adversary? What are the adversaries’ intentions? What is the adversary capable of doing?

Security Analysis

Conducting security analysis after a security job is a good way of planning for the next task. We analyse what happened and what was going on and what should be done, in the episodes of the security work. Security analysis should be done at least once a month. It incorporates every movement and task we have done. The analysis paves way for better security plans. By analysing, we can get a clearer picture of what needs to be done.

Security Zones

We divide security areas into zones. These zones are where we apply security. Teams are occupying the zones and perform their work there. Zones are the areas of interest where we do our tasks. We make sure that the work is done inside the zones, to avoid spreading out of the zones. We keep our work in the respective zone and don't go out of the zone. We stick to our delegated zones and don't interfere with other zones. Each zone is meant for limited security work and is not to be exceeded by excessive security breaches outside the zone.

Security Tracking

When we track security, we track our performance. Security tracking means to record our work, so we can learn from it later. We keep track of everything we do, in order to

keep up to the latest standards and perform our work to the fullest ability. The tracking is to the betterment of our work. Tracking security everywhere is to let us have the ability to look back at what has been done. This tracking will pave the way for even better security at a later time. By recording and learning, we get the best out of our analysis. The analysis of tracking makes sure that the latest data from our work gets known to the fullest.

Privacy

When you are home alone, pull shades or curtains after dark. If you let someone in, and then have second thoughts, be assertive and demand that the person leaves, or leave yourself. Call a friend or neighbour to come over. Pretend you are not alone, mention a friend or family member asleep in the next room. Anyone who refuses to leave is a trespasser and you should call the local police to have them removed. In general, if you don't personally know a person, don't let them in.

Security Modes

Security modes are various parts about the workings of security.

Compassionate Security

If we practise the way of non-harming, we'll get further in our work. Compassionate security is about the least amount of harm being done to people and the environment as well. We care for our surroundings and we want our work to alleviate suffering. We are never aggressive and security is not about being gung-ho and wild about our powers. We pay service to our customers and to the general public. As servants of the civilians, we try to inflict the least amount of pain when we carry out our tasks. The compassionate security officer is always to the help and betterment of the public.

Security Scopes

The scope of security defines what areas we do security in. Whether securing the people or doing intelligence, the scope is where we play out our tasks. A scope means an area of working and where this happens is the place where the tasks are done. The scope of security is the very place where our tasks come to fruition and we get to develop our security measures. Security scopes allows for playroom when it comes to tasks. This is where security is delivered. The scopes are in conjunction with other security modes. Working within the framework of scopes make sure that security is well delivered within the constraints of limited application.

Security Essentials

Essential security is delivered through daily security work. Every intelligence-gathering and security measure are essential security via the mission. This security is the regular objectives for the security routines in daily work. Security essentials is the basic and sound security that we strive for in our work. Essential security does not mean that we lower our standards, it just means that the security is up to par with normal expectations. These essential elements are the security we expect to deliver to the customer.

Applied Security

Applied security is a concept for improved security, since security needs are always fluctuating. When there's need for improvement, the scope of applied security within the threshold of limits to security is to apply said security to basic standards. Basic security is when we secure facilities, protect people or guard valuable items, or intelligence missions, and this is within the limits of standards. The level of applied security is always in accordance with basic security and upholds the highest standards within it. Applied security meets the needs of any security demands on the market.

Applied security is the factor which lets us work smoothly to uphold our standards within security work. Applied security brings out the best in top class security delivery. Applied security should not be exaggerated, but only to the extent where it is in balance with basic security. In conjunction with basic security, such as tactics, applied security secures the immediate application of security measures. The application of security measures is always in sync with applied security standards and sets the level of security which will be delivered.

Window Of Opportunity

The window of opportunity is when we see the chance to get some tasks done. It's when there is an open position to give way for a job to be completed. The security job gets done within this frame of open space. The job is always open to changes, in that there could be given counter-orders and the task has to be altered. In these cases, the personnel adapt to changes and apply the new orders accordingly. The changed orders usually are in sync with the window of opportunity. This window lets there be flexibility to the tasks and assures continuity.

Security Cues

We get cues about when to apply security. These cues come from when we expect there to be a situation that needs security. The cues are picked up by the personnel whenever something is building up, like an alert about a breach. We pick up on the cues and proceed with applying security measures. Any cue is interesting and we can deduct what needs to be done. Security cues will be used for pro-active defence in any security situation. By way of cues, we are always at the forefront of the situation and can quickly lay down a security plan.

Security Changes

Everything is impermanent. Changes in the security situation is inevitable. Changes in the security environment are good for security. There will be changes in the way we apply security and security measures will also be changed. The changes come on a slow basis, meaning that it doesn't happen fast, except when there are faults that need quick repair. We must learn to adapt to changes and be willing to accept the changes. Without changes, there is no development. With changes, there is always something new to discover and we must use the changes to our favour, in order to create better security.

Changes in the security situation comes and goes. The changes are not to be seen as a setback, but rather a chance to step up the security efforts. Changes within the framework are to the betterment of the security situation. When there are changes, security flows smoothly into a wholesome performance. The performance of tasks is directly proportionate to the changes being undergone. Where there are changes, there is also improvements.

Security Efforts

The efforts we put into getting tasks done is the measure of our performance. We lay down the effort to always have the tasks in mind. Our efforts are beneficial to improve the security situation. Sometimes, we step up the effort and put more energy into the work. Thereby, the effort is regulated and never gets exaggerated. Security efforts make sure that all aspects of security have the best amount of power for the job. All efforts are controlled by Management Security and effectuated by Operational Security. Physical Security only needs to know when to apply the efforts. Compliance with basic efforts is ensured by the application of regulatory constraints within the security situation. Independent efforts are to the betterment of the work and is welcomed by everybody.

The efforts which are performed are the basis of the security job. We raise the effort to make sure the job is always done properly. The efforts are stepped up to meet the demands of the tasks. All efforts are to the betterment of the personnel's jobs. Efforts are the sure way of getting the development of security measures done. After a while, the effort becomes effortless and the effort is naturally flowing. Effortlessly applied security is the easiest way of creating security measures.

Wave Of Security

The wave of security comes when there are several personnel working in context with each other, to form a wave of security measures. This wave is charging the security process from start to finish. It pushes the security effort to the limits. There are various properties to the wave, for example, it comes from the security process

and also from the performing of tasks. The wave is in conjunction with the security process, as long as the work does not get hindered. It forms a reliable deliverance of security services and results in broader application of security measures.

Security Relevance

Relevant security is to keep security within limits of what is conducive for security, and nothing else. Security is applied wherever it is relevant and everything else can be discarded. We don't need irrelevant security delivery. For example, a paying customer or a parked bicycle are not relevant for security and will be left out of the security picture. To stay relevant, it means that we do not waste our efforts on things that are not ideal for the security environment to be clear. Clearing out any irrelevancies from the security situation will help to focus better on the tasks. To be relevant means to keep focused on the task at hand and not get entangled in factors that are not important for the successful outcome of the mission. Security relevance is always in the forefront of the security effort and does not bother with aspects that can be ignored.

Security Sense

The sense of our security is the sense of how we do our work. The sense of having a purpose to our work gives motivation. Security sense gives us better working conditions. Sensing all there is to be done for the present and future, makes us keep up with our work. To sense the expectations is a way of creating better security. The sensing is very simply done by the personnel whenever they are applying security.

To sense all that's going on while we are at work is important for the gathering of sense data. Security sense is good for the whole organisation and should be applied in all circumstances. After the sensing has been applied, we take the gathered data and work out strategies for better security work. It's possible to improve our work by analysing the gathered sensing data.

Security Redundancy

Sometimes, the security can be applied too much. We apply a surplus amount of security measures and this becomes redundant. Security redundancy is detrimental to the outcome we wish for when it comes to get the job done. It is more security than what is really needed and this should be avoided. Too many layers of security is to the contrary of what we want to deliver. Deliverance of masses of security will not be in favour of the tasks we are supposed to perform. Therefore, we ensure that security is applied only to the extent where it's enough to get the tasks done. Security is at the core of our operations and redundancy is not in our interest as it bogs down the smoothness of the operations. We want just the right amount of security to be applied, in order to ensure the right conditions for our operations.

Security Clearance

With security clearance, we clear out the application of security measures. It's the method for ending a task in a timely manner. We withdraw and no more security is applied. The situation should be safe when there's security clearance. We lay down our effort and lax on the security. Security clearance happens when the task is almost done and we see the opportunity to end the security effort. It always comes at the end of the mission, never during the mission itself. Security clearance is not seen as important for the outcome of the mission, but as a by-product of the mission itself. The mission creates the clearance, in that when the mission ends, the clearance is automatically made.

Security Control

Security control controls the mission, operations, and tasks, which are put under control in order to safeguard the mission. The various aspects of the mission is under control by Management Security, who deals with the security of the mission itself. Controlling the mission is the best way of making sure the mission is not spoilt. Security control lets the development of the mission flow freely, while keeping oversight of the whole process. It controls who has access to the mission information and who gets to know about mission details. Under no circumstances must this control be given to others.

Security Alerts

Security alerts is the domain of Operational Security. They are the first to know about alerts and decide how to proceed. Operational Security makes sure routines are developed for Physical Security personnel, so they always know what to do. Then they pass the task to Physical Security, who investigates the alert. Physical Security are deployed after instructions from Operational Security. Physical Security dispatches into the area of the alert and apply any security measures they see fit.

Security Access

Access to the premises is controlled by Operational Security, in co-operation with Management Security. They control who or when access is needed. Security access makes sure those who are not authorised don't get access to the premises. Security access controls how the public gets access to the premises. Physical Security are the actual personnel who gets access. They don't get access unless approved by Operational Security. There are several levels of access rights, so we can control who gets access to what. After Operational Security has granted access, Physical Security takes over the responsibility of the premises. Physical Security gets free reign over the premises, once access is approved.

Security Breaches

When there's a security breach, the matter needs to be investigated. Investigation is carried out in order to identify the nature of the breach. The breach must be identified and the circumstances must be documented. What type of breach, what happened, who were there, what damages must be recorded. The breach must be isolated, so no one can tamper with the evidence. Environmental faculties and items around the breach are secured for later investigation. Operational Security decides what to do about the breach and see if the matter is a Police case.

Security breaches are written down in reports by Physical Security personnel. Report every detail about the breach. The report will be used for investigation by Operational Security.

Tight security

Tight security is when we improve security according to security enhancement. We strengthen our efforts to keep security tight. To tighten security means to build strong defences and security measures. This kind of security is needed in adverse situations. This strict security comes with a caveat, it could be too tight for comfort. Too tight security is not in accordance with standards. Extreme security is not what we want. Our tight security is in balance with recommendations for realistic security.

Security Peaks

When security reaches its peak, there's an intense delivery of security. The highest peak of security is when there's a lot of security activity taking place. This activity is at its highest when security is at its peak. At this time, the activity is very high and the tasks are done away with in quick batches. Security peaks ensure the dynamic delivery of security. The peak must not go too high since this will get a negative outcome. To get done with tasks, the peaks make the performance easy and smooth. It is not easy to reach such a peak, because the causes and conditions are not always present.

Depleted Security

Sometimes, we exhaust our efforts. The security situation gets saturated and we deplete our security application. When this happens, we should not get complacent, but strive diligently towards the goal. The goal is always to bring good security to the customer. Depletion of security comes with a lesser degree of effort. We need to strengthen the effort and reinforce the security situation. When it happens, we can build even better security by relieving our stress and get back to the tasks. Security depletion should not be seen as a setback, but rather as a chance to regroup and step up the security effort. Depletion is sure to happen when there has been a security peak. After the security peak, security depletion comes as a natural reaction and gives way to enhance security.

Security Mapping

Before every mission, we map the security needs. Surveillance of the people, surroundings, and environment where the tasks are to be performed, is done. The personnel map every detail, to get an oversight of the security situation. Security mapping is a step on the way of developing a mission. It must be done to pave way for the complete mission. Mapping is a step towards a smooth-running mission and is always done in the development phase. It is important that the mapping is done covertly, to not attract onlookers. It is to keep the situation under control and not let any false information enter the mapping.

Personnel

Security Officers

As security officers, the main objective is to secure people, premises, or items, or doing intelligence operations, or working out security measures. The responsibility of a security officer is always to perform the tasks in a smooth and timely manner. Objectives and responsibilities are what drives the security officer in a forward direction. He is trustworthy and keeps his integrity wherever he performs his duties. What makes the security officer thrive is to see that the work is going smooth and by the numbers. To deliver security is the first and foremost wish. In daily life, the security officer keeps to his business and applies security wherever he sees the need for it. The security officer is vigilant and always keeps an eye to what is conducive for security.

Set And Setting

When we are performing our tasks, our mindset is set on getting the mission done. We get the mission done by having a mindset of always performing to the best of our ability. The mindset is about being winners in our trade and be able to handle our tasks well. Staying professional is another aspect of the mindset that we keep. This mindset is kept throughout the mission or other tasks, and in everyday life.

The setting of our work is the environment and premises where we do our tasks. The setting affects how we do our work, in that we have to adapt to circumstances. This setting is meant to be on our side when we perform our tasks, since we can take charge of our setting and change it into our favour.

Security Teams

We work individually and also as teams. When in a team, we co-operate between us to ensure that the mission is safely handled. In a team, we support and encourage each other to build a tight knit group that can handle the tasks. We make sure our

fellow personnel are safe and sound and always cover each other's backs. The teams work together as an organisation that are focused on only one thing - to get the job done. The team building makes sure we are a group that can perform our tasks properly. The teams work as a dynamic force, enabling us to be smooth in our performance. Teaming up for the tasks are the most important aspect of our work and can effectuate the mission. Teams exist in conjunction with individual personnel and are at the core of a well-functioning organisation.

Confidence

When we are confident in our ability to deliver security, our work goes more efficient. Confidence makes things go smooth and by the numbers. Proper routines and standards give confidence when performing the mission. Always have the confidence that this is something we can do properly and never waver in our faith in our abilities as security personnel. Our confidence in ourselves makes it easier to perform our tasks in our daily work.

Certain people would try to make it difficult to have confidence, by disrupting our work. These people should be handled with the confidence that they are unable to create problems for us. Their disruption is easy to deal with as long as we are confident and keep the faith. We don't let them disturb us by our confidence in our work.

The Use Of Force

We don't have police or military authority. Our authority is limited and we have to abide by the law. When we perform our tasks, we must consider that our work does not have the mandate to use physical force. The only time we use it is when it's needed in self-defence. There could be an attacker or disruptive person that must be handled. In this case, the law permits us to handle the situation within certain limits. We can't attack anyone directly, only in the defence of our lives. We will never exceed our mandate as security personnel and always defend ourselves within what is permitted. We are allowed to use military tactics to a certain extent, depending on whether we are armed or not.

Testing

There will be held tests to the security. To see that security measures are viable. These tests will make sure that security measures are in place and realistic. Testing is done on a regular basis, whenever new security measures are developed. The testing will show whether the security measures can be used for the mission. There is not always everything can be tested, but we aim for testing as much as possible. Management Security and Operational Security will decide how to conduct the tests. The testing is done by Physical Security in assistance with Operational Security.

Operatives

The main operative personnel are those who perform the operational tasks. They are the personnel who are at the forefront of the mission. They belong to the department Physical Security. Operative personnel are frontliners or direct visionaries on a mission and some of their topmost role is a process that they use to perform critical tasks. It's important that these stay vigilant and are ready on a short notice. They are briefed about the mission in due time and get well-trained for their task.

The operatives will perform their tasks after Management Security and Operational Security have developed the mission. Under no circumstance must the personnel be lacking in instructions from Operational Security. The importance of being well prepared can't be stressed enough. The operatives are very important for the outcome of the mission and must not be obstructed from their work.

Security Assistance

Security assistance is when we support the personnel when the need arises. A backup for the personnel should always be available. Backup personnel should be ready if the normal personnel fail. It is crucial that the backup personnel are briefed on the missions. They must know how to perform the tasks and duties. Security assistance needs to be able to exchange places. The backup must be tactically prepared for the challenge of taking over for the normal personnel. This backup is the last resort if something goes wrong.

Pitfalls

When it comes to security, many things can go wrong. Equipment may fail, personnel get harmed and environmental factors can influence security. In case any of these happen, there's the need to understand the circumstances and learn from it. If equipment fails, we should investigate the matter and find out what went wrong. If personnel get harmed, we should not despair, but know what happened to them and make sure it won't happen again. If the environment ruins security, we may build a new environment to avoid the same result in the future.

Failings must not go unnoticed. Information is gathered and reported. All details about the failings are recorded and Management Security will decide what to do about the failings and the aftermath of the happenings.

Dangers

There could be a danger to work with security. The dangers can be small or severe, depending on the situation. Personnel could be attacked by enemies, or one might hurt oneself in the environment. In this case, acceptable defence methods can be

applied. Whether armed or not, one should always defend oneself. Environmental factors can make it dangerous to work. In all cases, one should apply whatever protective means in order to stay safe. Damages to personnel is detrimental to security. Management Security will handle such situations and decide what to do.

Security Issues

Security Expertise

In security, there's no such things as "experts". The security situation is always changing and your mileage may vary. Real expertise comes from training, knowledge, and experience. To be well-trained in the field of security is a state of mind. You know what the job implies and you know intuitively what to do as a security officer. Whether you are on patrol or on intelligence-gathering, the expertise you show comes from the way the job is being performed. To perform the job in a professional manner means more than just pretending to be an expert. We display our professionalism by getting the job done in a smooth and timely fashion. Also, to be vigilant and alert takes expertise as it is an important part of security work.

Fake Security

We should know that there exist security personnel that are unserious players in the trade. Various bad entities and fake security companies give a bad name to the industry. These people can't influence our work, as we keep our professionalism intact. Fake security is to the detriment of the industry and we should avoid being involved with such people. The moment we act like fake security is the moment where everything goes wrong. We should under any circumstances not let ourselves turn into fake security personnel and we should always keep our standards high.

The Illusion Of Security

Security is not always good enough. We build security, but there happen breaches. There could be holes, even with the tightest security. Maximum security should not create an illusion of complete safety. There could be factors that we haven’t considered. To build full proof security is impossible. Don’t be fooled by appearances, the illusion of security could fool you into thinking that you are safe when you’re not.

The Lack Of Security

The lack of security could be detrimental to an organisation's well-being. Lacking security will make the organisation weak and suspect to damages. An organisation will always prioritise their security, in order to keep the functioning intact. An organisation without security is in danger of risking the operations of their business.

Therefore, any security-conscious organisation would make sure that security is well applied throughout the organisation. As a means to an end, security becomes an integral and important factor for the organisation.

Security Risks

There's always a risk to working with security. The risk of getting damaged by the environment or people. The risk of failure of the mission is possible, however professional we are. We live with this risk every day. The risks should not be underestimated and taken into account when we perform our work. When we aware of the risks, we can better protect ourselves against such risks. We work to minimise risks and failures in every way. We are aware that risks influence our ability to perform our tasks, but we don't let them interfere with our work.

Security Traps

There could be traps in our work. Traps mean something disturbing to our work. A disruptive person, or fault in the environment could lead to traps. In this case, we should use whatever means we have to remedy the situation. To handle the disruptive person or adapt to the environment is the best solution whenever a trap appears. Traps are to be handled with care and not to be sloppy in the treatment of traps. Traps could be difficult to handle and detrimental to security, but the handling will make sure that our work is not disturbed.

Security Failures

Sometimes, there are failures when it comes to securing people, premises, and items. The people do not get protected and the environment might be open for breaches and items may disappear. In these cases, a prompt solving of the failure needs to be applied. We should not see the failure as a crisis, depending on the severity of the failure. The failures are not always the fault of the personnel. It's difficult to secure everything full proof. Sometimes, external forces are the cause of the failure. For example, the people were not cooperative, or there was a natural disaster, or a thief may had stolen a property. When the personnel are not at fault, we figure out the failure and learn from them. We make sure they don't happen again, by reporting it to management. Management will oversee the failures and work out a strategy to eliminate such failures in the future.

Damages

When there are damages to people, premises, or property, they are reported to Management Security, who are responsible for clearing up what happened. Management Security deals with the repercussions of the damages. Damages must always be recorded for figuring out who are liable and gets the blame for the damages. Whether it's the customer, the owner of the premises, or the people involved, the fault of the damages must be sorted out. Management Security will

negotiate with the involved in order to find out who are responsible for the damages and what to do about the damage.

Security And Society

The danger which is least expected soonest comes to us. “At the end of the day, the goals are simple: Safety and security." “The safety of the people shall be the highest law." “The automobile has brought death, injury and the most inestimable sorrow and deprivation to millions of people.” Therefore, true individual freedom cannot exist without economic security and independence. People who are hungry and out of a job are the stuff of which dictatorships are made. The fact is that people are good. Give people affection and security, and they will give affection and be secure in their feelings and their behaviour.

Appendix

Safety Methods

```
These safety methods come with no warranty, though they have been tested
and released for general interest.


The Chip Disabler
-----------------

This method might clear your head if you're implanted with the human chip:

If a bad feeling enters your soul, say the following phrases inside the
mind, but not out loud. Repeat the sequence till your mood becomes better.


                                We are nothing

                               They don't exist

                               They are nothing

                                We don't exist

                             There's not anything

                                I don't exist
```

I am something

You are nothing

I am something

You don't exist

FearMonger Tuner

This method might get your thoughts off a false Very Important Person (VIP):

It may happen that an acquaintance you meet somewhere starts to talk idle chatter with you, then the person suddenly mentions some VIP (but not by name) but you've never heard of this VIP before. If the tone and words of the person's chatter creates a worrying atmosphere and the VIP is mentioned a lot, then the person is an "agent" and the VIP would like to be your private leader. If you don't agree, find out who the "agent" comes from like this: Create a suitable joke name for the "agent" based on his public appearance and something that fits his behaviour. Use this joke name directly to the "agent" in context with the VIP's importance, then the name of the VIP may be revealed. Then tell the "agent" that the VIP is not interesting, because it's only a fearmonger.

Double Reverse Psychology

This method might pause an annoying interrogation:

The case is to launch a phrase for an opposing person in order to get any comment back. Then launch another phrase with a challenge, in order to elicit a meaningless answer. A third neutral phrase concludes the conversation.

Example one:

Your 1st phrase: "There's a problem and you know what it is."
Others' answer: "Is that so?"
Be patient, then say the 2nd phrase.
Your 2nd phrase: "I stand strong."
Others' answer: "Sure."
Your 3rd phrase: "But you didn't see it."

Example two:

Your 1st phrase: "You know what we're debating?"
Others' answer: "But, of course."
Be patient, then say the 2nd phrase.
Your 2nd phrase: "Or, was the subject removed?"
Others' answer: "What?"

```
Your 3rd phrase: "It's done."


PIP-TV
------

This method might expose an unseen vehicle in twilight:

RGB palette colour code is Red 78, Green 198, Blue 230. This colour is
greenish blue. Create this colour on a computer screen and memorise it.
Then have a mobile camera and practise on focusing it on something grey-
coloured, until you are able to visualise the greenish-blue colour as a
layer that's projected onto the camera display. When the greenish-blue
colour appears clearly between your eyes and the camera display, then PIP-
TV is ready to use.

Usage: In case you hear deep, low-frequency sonic vibrations in the close
area, then turn to the direction the vibrations come from. Then focus with
the camera on the target, with the greenish-blue colour projected onto the
camera display and watch a Paranoia-Inducing-Person (it's a mouse).
```

Security Tips

A security-conscious person would consider the following practices:

- Pro-active defence is to prepare security: Create security beforehand, so you are prepared.
- Advancing and withdrawing, movement and rest: Going ahead, stepping back while moving on and taking breaks.
- Active doing – active and passive non-doing: Do worthwhile actions and leave behind any useless actions.
- Non-destructive defence with applied non-aggression: Only protective force is used, meaning no attacks. No anger = no damages

Mind Training Programme

Being a soldier, you are asked to do things not asked of most people. You have to behave properly and show self-control all the time. You have to fit in and be part of a team. You have to trust your teammates and they have to be able to trust you.
It's essential to recognize the fact that a soldier, like all soldiers, has its own norms and practices and therefore, there is the urgent need to tune one's mind and body to suit the new system one finds oneself in.

Everything taught on the training must be considered as beneficial in shaping a soldier into a good and reliable one, and therefore see the need to adjust one's personality to suit to the system.

The kind of a soldiering involves communication with a wide variety of people. The good soldier must be a good communicator. A soldier needs to understand that communication is what we do to build understanding between a soldier and civilians. Building a soldier is the process of which involves transmitting from one person to another to a group. Facts, ideas, and feelings etc.

A soldier must build his interpersonal skills. We build the soldier's mind to become able to approach every demanding encounter. A soldier must be courageous and have self-respect and regard for others and the superiors. One should also know how to solve problems with or without any senior people.

Interpersonal Skills

A significant part of being a competent soldier is empathising with others. Empathy is a quality every soldier must look for. If a soldier complains for any reason, the senior colleague must listen to their concerns thoughtfully by expressing compassion towards their issues, but not fear them.

Active listening is more than just hearing what people say. To be an active listener in the field, it's important to devote your full attention to the commander(s) whose orders you are listening to. You absorb their message, respond to them with relevant questions and retain key information. You are also likelier to retain the information you need to perform your job to the best of your abilities.

In any situation, the need to communicate is important. It's important to communicate with your leaders. Your leaders can't help you if you don't speak up about a situation — they don't read minds. Approach your leaders with ease to make sure to build rapport, earn their trust, and be somebody they can count on. Make your life and your leaders' lives easier by being a good communicator.

When in a team, we synchronise ourselves to each other. Your teammates are an extension of yourself, and vice versa. This gives shared power and energy between us.

Be alert and aware! While you are walking, keep your mind on what is going on around you.
Display confidence. Walk with purpose, scan the area around you and make casual eye contact with others to display confidence. Keep your hands free, trust your instincts.

Strengthen Concentration

If you have great powers of concentration, that means you're able to focus all your attention on the matter at hand. It can also refer to something that's clustered together and the strength of a solution. We can concentrate in many aspects when it comes to security and handling of serious situations. A high concentration in a solution means that there's a lot of it, relative to the human concentration. To say that you have good concentration skills, means that you pay attention well.

Think Like A Soldier

- An agile mind is an advantage. Heedfulness will sharpen your awareness and gives few dull thoughts.

  This means that being heedful and paying attention will make your mind awake.

- Only will-power is not enough. When will is depleted, to think beyond that can give extra energy.

  This means that when your will gets tired, look outside your thoughts to find further strength.

- During stress, there's less room for thinking, so your training and experience will be on "automatic".

  This means that you will do things by experience, instead of thinking about what to do.

- Let your mind merge with the surroundings.

  This means to forget yourself and become part of the environment.

- Try to become «one» with the target.

  Again, let yourself go and become a part of the target you want to catch.

- The target is like your own life, it must be well secured.

  This means to secure the target like it was part of your own life.

- If you spot something interesting, let go of everything else.

  This means that if the target is the object of focus, then try to forget the surroundings.

Fear Management

- The only thing to fear is your own self. Find a balance between the nerve to be courageous, and the urge to flee.

This means that if you merge yourself with everything, there's no self to fear.

- The fear of doing wrong is disruptive, so don't attempt to be perfect.

  Even the best soldiers make errors, there is no such thing as a perfect soldier.

- Be kind to yourself, thinking mean thoughts will make you distracted.

  This means to avoid thinking negative, in order to avoid weakness.

- Fear can be transformed into alertness and vigilance. It can sharpen the focus if you go beyond the fear.

  This means that if you can transcend the fear, it can rather create better focus.