



Funded by the  
Erasmus+ Programme  
of the European Union



**IO 1**

**Annex 2 – DP-IS OFFICER IN SME'S**

**“Data Protection & Information Security Officer in SME's”**

v.3. 28.01.2020

Report on Identification of Competence Profiles



Funded by the  
Erasmus+ Programme  
of the European Union



This document is licensed under CC BY-SA 4.0.

This document was produced within the scope of the ERASMUS+ Project “Teilzertifizierung im Berufsfeld Informationssicherheit – TeBeiSi”, Project ID: 2018-1-EN02-KA202-005218

The European Commission support for the production of this publication does not constitute endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



**This first draft of the Job Profile “Data Protection & Information Security Officer in SME’s” (DP-IS Officer in SME’s) is based on the results described in detail in the sections above in the Report on Identification of Competence Profiles.**

**Main outcomes of Field Research:** The partnership interviewed more than 60 experts in the fields of Data protection and Data security, Information security management and IT security in small and medium-sized enterprises (SMEs). It was important to us to gather personal opinions and experiences on these topics, either individually or in focus groups. **All partners collected at least 10 cases from their field research.** Based on these findings we created a first ‘**List of Competences needed in SMEs**’: We have considered different questions to find out how the experts assess the required competencies of employees. Then we presented a short summary of competences identified by our experts for SMEs in fields, Data protection and Information Security.

In the section ‘TeBelSi Requirements matched with ESCO Profiles’ we presented our first mapping of our TeBelSi outcomes (results from interviews with experts, case studies & desk research) with the identified ESCO profiles. We drafted 4 different fictitious sample profiles: Information Security Manager, Information Security Administrator, Data Protection Manager and Data Protection Administrator. This step was important to first time apply the results of desk and field research to concrete job profiles.

The project partners, as well as external partners, concluded that this breakdown into four profiles was far too extensive for the majority of SMEs. We also examined how we could better address the needs of micro and small enterprises in particular and agreed to go one step further:

We drafted one concrete job profile of a "**DATA PROTECTION & INFORMATION SECURITY OFFICER IN SME'S**" (DP-IS OFFICER IN SME'S). We have divided the requirements into the following thematic areas in order to find a clearer presentation for a DP-IS Officer in SME’s:

- Legal Aspects - basic knowledge
- Personality
- Technical Skills
- Social Skills
- Methodologies



## Typical Tasks & Activities of a DP-IS Officer in SME's: a selection

<b>Typical Tasks &amp; Activities:</b>		
<b>No.:</b>	<b>Typical Tasks &amp; Activities:</b>	<b>Short Description</b>
<b>1</b>	<b>EVALUATING SOFTWARE FOR DEFENCE AGAINST CYBER ATTACKS</b>	There are thousands of anti-virus products and software on the market. Therefore, a careful assessment must be made of the cost benefit ratio, ease of use, frequency of updates and level of support and training.
<b>2</b>	<b>DEFINE SECURITY LEVELS</b>	The levels of IT security are an important aspect of business management. They must therefore be defined and agreed with management. And it must be established which employees have access to certain types of information and under which conditions.
<b>3</b>	<b>MANAGE ACCESS VIA PASSWORD</b>	A typical problem, of a management type but also related to computer security, concerns password management. Often there are too many, with the risk of forgetting accesses or, vice versa, creating unsecure passwords.
<b>4</b>	<b>CHECK THE USE OF PASSWORDS</b>	With reference to the previous point, it is important to define password control procedures, and not only manage access to them. This in order to increase the level of computer security.
<b>5</b>	<b>ESTABLISH BACK UP LEVELS AND METHODS OF DISASTER RECOVERY</b>	Still on the IT security front, back up management is crucial. Together with management, the levels of backups must therefore be defined, applying the various methods of disaster recovery.
<b>6</b>	<b>PREVENT ATTACKS ON SOFTWARE BY UPDATING MANUALS AND DEFENSE PACKAGES</b>	The main cause that puts cyber security at risk is external attacks. It is therefore essential to prevent such cyberattacks by constantly updating manuals and anti-virus packages.



<b>7</b>	<b>PREVENT HARDWARE DAMAGE</b>	The hardware contains all of the company's information; any damage to it risks blocking many of the company's activities. Therefore, a careful preventive activity (controls, maintenance, training, etc.) must be carried out.
<b>8</b>	<b>ANALYSE THE LEVEL OF EFFICIENCY OF THE INFORMATION SYSTEM</b>	The information system is the "heart" of companies: from here all the information, internal and external, to be managed in order to properly organize business activities, passes through. It is therefore important to understand the basic functioning and the minimum level of efficiency.
<b>9</b>	<b>ANALYSE CRISIS REPORTS</b>	Very often spam messages and procedural errors put the employee in trouble. It is therefore important to understand the meaning of crisis and error reports, sometimes with the support of an external consultant.
<b>10</b>	<b>VERIFICATION OF SUPPLY CONTRACTS</b>	It is very important to deepen the supply contracts, especially in the field of software and hardware (not forgetting the level of support and basic training). As the supply can affect the quality of the information system and the level of security.
<b>11</b>	<b>BASIC EMPLOYEE TRAINING</b>	Training activities, organized within the company, or at an external training institution. It can be proposed with different levels: from basic notions to more specialized ones.
<b>12</b>	<b>ASSISTANCE TO EMPLOYEES IN MALFUNCTIONING</b>	An internal or external expert can support employees in managing and solving IT problems. This also serves as a model for "training trainers", in the sense that over time the employee should become more autonomous.



### Requirements for a DP-IS Officer in SME's:

- Legal Aspects - basic knowledge
- Personality
- Technical Skills
- Social Skills
- Methodologies

DP-IS OFFICER IN SME'S		
Legal Aspects - basic knowledge:		
No.:	Requirements:	Short Description:
1	<b>To have a comprehensive knowledge in GDPR field of regulations.</b>	The DP-IS officer should be familiar with the basic guidelines of the GDPR and know where further information can be found. These basics should be included in the TeBeSi curriculum.
2	<b>To have comprehensive knowledge in national legal documents, regulating information security and data protection.</b>	<p>Suitable persons should have basic knowledge and understanding in the areas of</p> <ul style="list-style-type: none"> <li>▪ national legal documents</li> <li>▪ regulating information security and</li> <li>▪ regulating data protection</li> </ul> <p>These basics should be included in the TeBeSi curriculum.</p>
3	<b>To be able to practically apply national legal documents in the field of information and data security.</b>	The DP-IS officer should be able to create an internal document, regulating information security and data protection procedures at organizational scale.
4	<b>To be able to identify operations related</b>	Risk assessment begins when organization determines the volume and purpose of personal data that



	<b>to personal data protection, and evaluate their context.</b>	<p>are being stored/processed within the organization. Evaluation of the context allows identifying main risk areas where personal data protection procedures might be violated. In order to identify personal data storage/processing operation within organization, it is recommended to follow these guideline questions:</p> <ol style="list-style-type: none"> <li>1. What are the key operations with personal data that are being performed within organization?</li> <li>2. What categories of personal data are being stored/processed?</li> <li>3. What is the purpose of personal data storage/processing?</li> <li>4. What measures are being used during personal data storage/processing operations?</li> <li>5. Where does the storage/processing of personal data is taking place?</li> <li>6. What are the categories of data subjects?</li> <li>7. Who are the receivers of personal data?</li> </ol>
5	<b>Ability to evaluate possible impact of personal data protection violations to fundamental human rights and freedoms.</b>	<p>Personal data violation impact on fundamental rights and freedoms:</p> <ul style="list-style-type: none"> <li>▪ <b>Low.</b> Physical person can experience minor inconveniences (E.g.: time losses for information renewal, frustration, discomfort, etc.).</li> <li>▪ <b>Moderate.</b> Physical person can experience moderate difficulties that can be resolved with reasonable investments of additional effort and resources (E.g.: additional costs, loss access to resources, stress, minor health problems.).</li> <li>▪ <b>High.</b> Physical person experiences significant difficulties that require intense involvement and high resource cost (E.g.: loss of capital, blacklisting, job loss, serious health risks, etc.).</li> </ul>
6	<b>Ability to determine possible threats and their risk probabilities to information security and personal data protection.</b>	<p>These sample questions help determining threats and risks to information security and personal data protection in organizational scale:</p> <ol style="list-style-type: none"> <li>1. Are internal information systems that store/process personal data connected with other external information systems or services?</li> <li>2. Can unauthorized persons gain access to personal data management environment?</li> <li>3. Are access clearances and responsibilities in organizational information systems clearly defined?</li> <li>4. Are employees allowed to transfer, save, or modify personal data, stored in information</li> </ol>



		<p>systems externally (e.g. portable devices, external storage devices, etc.)?</p> <ol style="list-style-type: none"> <li>5. Are there any ambiguous or unclear obligations on the processing of personal data in relation to third parties/persons within the organization?</li> <li>6. Are there employees in the organization involved in the processing of personal data who lack the competence to handle information confidentially for technical or personal integrity reasons?</li> <li>7. Has there been a personal data breach or other security incident in your organization in the last two years?</li> <li>8. Are there activity (activity area) good security practices or standards that your organization does not follow?</li> </ol>
<b>7</b>	<b>General interest in legal issues</b>	The DP-IS officer should be personally interested in legal issues and questions and should also enjoy dealing with the matter professionally.
<b>8</b>	<b>Willingness to familiarise oneself with complex regulations</b>	The DP-IS officer should have an understanding of the fact that a company needs a certain amount of guidelines and would like to help shape them and monitor their compliance.





<b>Personality: The DP-IS officer should have as many of these personality traits as possible</b>		
<b>No.:</b>	<b>Requirements:</b>	<b>Short Description:</b>
<b>1</b>	Being able to act <b>quickly</b>	A person who quickly learns new lessons for new contexts, useful in determining and solving problems, even complex ones.
<b>2</b>	Be <b>flexible</b>	Have a good ability to adapt to different situations; also involving colleagues in finding alternative solutions to complex problems.
<b>3</b>	Try to be <b>precise</b>	Acting accurately, analyzing problems; but also knowing how to make the right decisions to get out of problems, following company procedures.
<b>4</b>	Try to be <b>meticulous</b>	It is important to work punctually, trying to be meticulous in the approaches and choices, also to facilitate the involvement of colleagues.
<b>5</b>	Try to be well <b>organized</b>	Companies, even if small in size, today are complex to manage. It is therefore important to work in an organized and modern way.
<b>6</b>	Be <b>reliable</b> and <b>honest</b>	Acting confidentially, respecting the principles and policies of the company; having a coherent and rigorous logical thought, also following the ethical code of the organization.
<b>7</b>	Have a good <b>maturity</b> and <b>balance</b>	Act in a self-control perspective, consistently (but not rigidly); try not to polemicize, reacting positively to internal and external signals.
<b>8</b>	Have a good capacity for analysis ( <b>problem solving</b> )	Business decisions are always based on a shared process, which then leads to the solution of problems or the identification of alternative ways of acting.
<b>9</b>	Have a good ability to <b>synthesize</b>	In the increasingly complex company choices, after a careful analysis of the situation, a summary of the problem should be made.
<b>10</b>	Being able to apply <b>logic</b> in your actions	Even in stressful situations, one should try to act logically and rationally, dealing with colleagues.



11	Having a <b>dynamic</b> approach	In the management of complex situations and problems you need to be dynamic in your choices, flexible and able to adapt to different conditions, organizational and market.
12	Have a good capacity for <b>imagination</b>	In small companies, one acts with rationality, experience and intelligence. But it is also important to foresee and imagine future situations and contexts.
13	Always be able to act <b>independently</b>	In complex situations always demonstrate balance in actions, and independence of assessment.
14	Having an <b>optimistic</b> and <b>resilient</b> approach	In highly competitive situations, have a good vision of the future, a strong resistance to stress and an optimistic (realistic) approach to business and market conditions.
15	Being able to handle <b>stress</b>	In a dynamic and competitive environment, try to act and work well even in stressful (“under pressure”), personal and professional situations.
16	<b>Result-orientated</b>	In the choices you make, you should always evaluate the expected results and the consequences in terms of business impact.
17	Being able to act in a logic of <b>self-assessment</b> and <b>self-consciousness</b>	In the choices you make, you should always evaluate your own limits and experiences.
18	To be able to act with <b>passion</b> and <b>conviction</b>	In small businesses, people have a crucial role to play: acting with commitment and passion is therefore essential, also to involve all employees in a unified way.
19	To be able to read even medium-term dynamics in a <b>visionary way</b>	The market and the competitive environment are increasingly complex. One should therefore act with at least a medium-term vision in the choices to be made.
20	To be able to achieve results with <b>determination</b>	In SMEs there are many factors, both internal and external, that condition the choices. The choices must therefore be made with determination and conviction, sharing them with all those involved.
<b>Technical Skills: The DP-IS officer should have a basic technical understanding and fulfil a large part of the points listed</b>		



No.:	Requirements:	Short Description:
1	<b>Identify system weaknesses and security risks</b>	Apply methods and techniques to identify potential security threats, security breaches and risk factors using tools for surveying ICT systems, analysing risks, vulnerabilities and threats and evaluating contingency plans.
2	<b>Handle data retention and data processing</b>	Identify, locate, retrieve, store organise and analyse digital information, judging its relevance and purpose. Master a wide variety of information security controls in order to pursue maximal database protection. Ensure that access to personal or institutional data conforms to the legal and ethical framework governing such assess.
3	<b>Administrate identity management/password management</b>	Administer identification, authentication and authorisation of individuals within a system and control their access to resources by associating user rights and restrictions within the established identity.
4	<b>Administrate documentation</b>	Develop documentation containing information about IT roll-outs, updates and back-ups.
5	<b>Basic knowledge in data architecture</b>	Oversee regulations and use ICT techniques to define the information systems architecture and to control data gathering, storing, consolidation, arrangement and usage in an organisation.
6	<b>Basic knowledge in encryption</b>	Convert electronic data into a format which is readable only by authorized parties which use key encryption techniques, such as Public Key Infrastructure (PKI) and Secure Socket Layer (SSL).
7	<b>Administrate information and network systems</b>	Plan, realise and monitor system changes and upgrades. Maintain earlier system versions. Revert, if necessary, to a safe older system version. Define set of requirements that describe an information system.
8	<b>Administrate impact evaluation</b>	Evaluate the tangible consequence of the implementation of new ICT systems and functions on the current business structure and organisational procedure. Evaluate scenarios of information security and data protection breaches and develop emergency protocols.



9	<b>Basic knowledge of components of an IT system</b>	Differentiation and knowledge of the functionality of hardware and software
10	<b>Administrate narrow system environment</b>	Understanding of the system administration and the direct environment
11	<b>Basic knowledge of peripheral environment</b>	Understanding and knowledge of the distinction between influenceable peripheral environment and influencing peripheral environment
12	<b>Understanding of programming languages</b>	Knowledge about application areas of different programming languages (e.g. C, C++, Java etc.)
13	<b>Basic knowledge of attack vectors</b>	Knowledge of current threats and common risk sources (Denial of Service, Social Engineering, Spam, Phishing, Vishing, Pharming, Buffer Overflow, Certificate Forgery and Identity Theft)
14	<b>Deal with malicious software/malware</b>	Ability to distinguish between different types of malware (viruses, trojans, worms, spyware, ransomware)
15	<b>Basic knowledge of safety related terms</b>	Knowledge of the meaning of basic concepts (e.g. patch, firewall, bug, domain, backup, cookies, authentication, penetration tests, bot networks etc.)



<b>Social Skills: The DP-IS officer should have as many of these skills as possible</b>		
<b>No.:</b>	<b>Requirements:</b>	<b>Short Description:</b>
<b>1</b>	<b>Active listening skills</b>	'Active listening' means, as its name suggests, actively listening. That is fully concentrating on what is being said rather than just passively 'hearing' the message of the speaker. Active listening involves listening with all senses. As well as giving full attention to the speaker, it is important that the 'active listener' is also 'seen' to be listening - otherwise the speaker may conclude that what they are talking about is uninteresting to the listener. Interest can be conveyed to the speaker by using both verbal and non-verbal messages such as maintaining eye contact, nodding your head and smiling, agreeing by saying 'Yes' or simply 'Mmm hmm' to encourage them to continue. By providing this 'feedback' the person speaking will usually feel more at ease and therefore communicate more easily, openly and honestly.
<b>2</b>	<b>Paraphrasing skills</b>	Paraphrasing is an effective form of verbal feedback to use when listening, however it is not simply repetition or "parroting," but restating another person's statement in your own words to gain understanding. Paraphrasing enables the listener to clarify the speaker's meaning and it conveys interest in what the speaker is saying and helps create a supportive environment for the conversation.
<b>3</b>	<b>Nonverbal communication skills</b>	Non-verbal communication includes facial expressions, the tone and pitch of the voice, gestures displayed through body language (kinesics) and the physical distance between the communicators (proxemics). These non-verbal signals can give clues and additional information and meaning over and above spoken (verbal) communication. Indeed, some estimates suggest that around 70 to 80% of communication is non-verbal.
<b>4</b>	<b>Effective team-working skills</b>	Working well in a team means: working with a group of people to achieve a shared goal or outcome in an effective way, listening to other members of the team, taking everyone's ideas on board, not just your own, working for the good of the group as a whole, having a say and sharing responsibility. A successful team is one where everyone's unique skills and strengths help the team achieve a shared



		goal in the most effective way.	
5	<b>Self-study skills</b>	Self-studying is a learning method where people direct their own studying— eg. in informal education and without direct supervision. Since people are able to take control of what (and how) they are learning, self-study can be a very valuable way for many people to learn. Self-study and learning in formal education can be used together to help people get the most out of his or her learning experience. Together, these methods help people learn and retain information better, helping boost comprehension and motivation.	
6	<b>Knowledge sharing skills</b>	Knowledge sharing is the act of exchanging information or understanding between individuals, teams, communities or organizations. Knowledge may be explicit (procedures and documents) or tacit (intuitive and experience-based). Sharing knowledge is an intentional process that not only bolsters an individual's understanding, but helps create or enhance an archive of accessible knowledge for others. The concept of knowledge sharing is important because it helps individuals and businesses be more agile and adaptable in the face of change, and helps ensure continued growth and survival.	
7	<b>Coping with stress skills</b>	Coping with stress is the process by which a person consciously attempts to master, minimize, or tolerate stressors and problems in life. Good coping skills prevent stress from getting us down and help us thrive. The most common coping techniques identified in the American Psychological Association's 2014 Stress in America survey are: listening to music, physical activity, reading, meditation, praying, going to church, yoga, getting a massage. All of these strategies were rated as effective by more than half the people who used them.	
8	<b>Mentor team colleagues skills</b>	Mentoring is a formal or informal relationship established between an experienced, knowledgeable employee and an inexperienced or new employee. The purpose of a mentor is to help the new employee quickly absorb the organization's cultural and social norms. The mentor helps the continuing employee grow in their current position and become ready for new jobs and career opportunities. Mentoring can also assist an employee, new to a specific job or area of responsibility, to quickly learn what they need to know to succeed in their job and role.	



9	<b>Taking criticism skills</b>	Taking criticism is the ability of a person to accept constructive criticisms for improvement, and being able to withstand the pressure of unfair or dispiriting criticisms while motivating himself to work harder and better instead of giving up. Taking criticism is not just about accepting what people say. It is also the ability to ignore distractive comments and critics whiles pressing on to achieve an objective. Criticism refers to a thorough examination and review of a person’s actions or work which is aimed at correcting associated faults, defects, and drawbacks. People who criticize are referred to as critiques.
10	<b>Openness to change skills</b>	Openness to change refers to an individual’s level of acceptance and conscious awareness of the possibility that change may be needed across a range of situations and scenarios, together with the appetite or drive to enact that change. The main components of openness to change are: acceptance of the need for change, willingness to support the change, positive affect or emotions towards either the change or the potential consequences of the change, an appetite or drive to enact or be involved in the change.
11	<b>Creativity skills</b>	Creativity means being able to come up with something new. Therefore, creative thinking is the ability to consider something – a conflict between employees, a data set, a group project – in a new way. Creative thinking means looking at something in a new way. It is the very definition of “thinking outside the box.” Often, creativity in this sense involves what is called lateral thinking, or the ability to perceive patterns that are not obvious. Creative people have the ability to devise new ways to carry out tasks, solve problems, and meet challenges. They bring a fresh, and sometimes unorthodox, perspective to their work. This way of thinking can help departments and organizations move in more productive directions.
12	<b>Empathy skills</b>	Empathy is awareness of the feelings and emotions of other people. It is a key element of emotional intelligence, the link between self and others, because it is how we as individuals understand what others are experiencing as if we were feeling it ourselves. Empathy is the ability to accurately put yourself "in someone else's shoes" – to understand the other’s situation, perceptions and feelings from their point of view – and to be able to communicate that understanding back to the other



		person. Empathy is sometimes confused with sympathy.





<b>Methodologies: The DP-IS officer should be/become familiar with these methodologies and related techniques</b>		
<b>No.:</b>	<b>Requirements:</b>	<b>Short Description:</b>
<b>1</b>	<b>PROJECT MANAGEMENT</b>	<b>Project managers ensure that a project is completed on time, within budget, and that its objectives are met. They oversee the project, manage the team, ensure the most efficient resources are used and ensure that all parties involved are satisfied.</b>
<b>1.1.</b>	<b>→ Planning and organizing</b>	<p>Establishes a realistic and systematic course of action to accomplish objectives, and determines priorities and allocates resources effectively:</p> <ul style="list-style-type: none"> <li>▪ Foresees risks and obstacles and allows for contingencies when planning.</li> <li>▪ Allocates appropriate time and resources effectively for completing work.</li> <li>▪ Involves and communicates appropriately with others in own planning.</li> <li>▪ Considers the larger picture in developing and implementing plans.</li> <li>▪ Consults with relevant parties to ensure that tasks and time frames are realistic and resources are available.</li> <li>▪ Uses appropriate systems and tools to track and monitor progress.</li> </ul>
<b>1.2.</b>	<b>→ Making quality decisions</b>	<p>Forms sound, evidence-based judgments, makes choices, assesses risks to delivery, and takes accountability for results.</p> <ul style="list-style-type: none"> <li>▪ Proactively seeks relevant information before making decisions.</li> <li>▪ Understands complex information and quickly identifies key issues.</li> <li>▪ Commits to a clear course of action and takes decisions that are consistent with it.</li> <li>▪ Takes decisions that optimize the impact on the Organization and others.</li> <li>▪ Is able to make sound decisions quickly and takes balanced risks associated with them before committing to action.</li> </ul>



1.3.	→ <b>Results focus</b>	<p>Focuses on and assumes accountability for the delivery of agreed results, and demonstrates an understanding of how these contribute to the goals of the Organization.</p> <ul style="list-style-type: none"> <li>▪ Sets quality standards and realistic target dates for activities.</li> <li>▪ Manages time and resources effectively, monitoring progress and making adjustments, when necessary.</li> <li>▪ Consistently maintains focus and perseveres in the face of obstacles, inspiring others to the same.</li> <li>▪ Quickly identifies issues in own work and is able to generate creative and practical solutions.</li> </ul>
1.4.	→ <b>Teamwork &amp; Collaboration Tools</b>	<p>Collaboration is the process of two or more people working together to solve tasks to achieve a common goal. Cooperation requires a certain amount of leadership, although in more modern structures this often takes place within a decentralized and equal group.</p> <p>Project managers are required to adapt to a changing world of work. Digitisation and mobility also require new forms of cooperation or make them possible. People increasingly work together in teams that are not bound to a specific location. People meet in virtual rooms and work together on ideas and documents.</p> <p>Important collaboration tools are for example:</p> <ul style="list-style-type: none"> <li>- Collaboration platforms like Google Docs or</li> <li>- Microsoft Office 365 (Teams)</li> <li>- Trello</li> <li>- Basecamp</li> <li>- Wrike</li> <li>- Redbooth</li> <li>- Slack, etc.</li> </ul>
2	<b>AWARENESS RISING</b>	<b>The DP-IS should have strong communication skills! The first evaluation of our survey showed that</b>



		<p><b>Awareness Rising was most frequently mentioned for the topics data protection and information security.</b></p> <p><b>Successful communication within the company is an important basis for Awareness Rising measures in order to be effective for all employees.</b></p>
2.1.	→ Awareness Rising activities	<p><b>Intervene and implement programs or activities that raise awareness of issues relevant for the respective company or clients regarding Data protection and Information Security measures.</b></p> <ul style="list-style-type: none"> <li>▪ Awareness creation – create situations which force employees to familiarize themselves with data protection policies (e.g. leave a USB stick with a specific software lying around, conduct social engineering scenarios etc.)</li> <li>▪ Communicate regularly with employees and make them aware of the importance of the topic under the slogan: Everyone is responsible!</li> <li>▪ Organise regular training: the feedback from the first survey showed that even trained employees often quickly forget what they have learned.</li> <li>▪ Creativity is required: Think about how a rather dry topic can still sell well.</li> <li>▪ Convince the management and all leading persons to lead by example.</li> </ul>
2.2.	→ Effective Information sharing	<p><b>Effectively conveys and shares information and ideas with others, listening carefully, clarifying understanding and taking into consideration different viewpoints.</b></p> <ul style="list-style-type: none"> <li>▪ Adjusts communication style, content and tone to suit the audience/team/client.</li> <li>▪ Is able to process and filter diverse information appropriately.</li> <li>▪ Disseminates information appropriately and in a timely manner.</li> <li>▪ Seeks and encourages two-way communication.</li> <li>▪ Shares relevant information with others.</li> <li>▪ Uses communication channels, tools and options effectively.</li> </ul>



2.3.	→ Inspiring others	<p><b>Inspires others toward a common vision and fosters trust and ethical behavior.</b></p> <ul style="list-style-type: none"> <li>▪ Inspires and motivates others to follow their ideas and vision.</li> <li>▪ Knows team’s strengths and areas for development.</li> <li>▪ Builds upon and nurtures the potential of individuals.</li> <li>▪ Is visible and available to colleagues.</li> <li>▪ Acts as a role model by demonstrating strong leadership skills.</li> <li>▪ Persuades and encourages others to adapt to changes.</li> </ul>
3	<b>CHANGE MANAGEMENT</b>	<p><b>There is a saying that applies very well to our rapidly changing work environment: "The only constant is change".</b></p> <p><b>That's why we need people who can handle these change processes well, involve employees in the changes, reduce existing fears and clearly communicate the benefits.</b></p>
3.1.	→ Dealing with change	<p><b>Show a positive, open attitude towards change.</b></p> <ul style="list-style-type: none"> <li>▪ Takes ownership of the change process.</li> <li>▪ Leads and manages change effectively.</li> <li>▪ Is able to mobilize the team towards change, and encourages and empowers people to implement change.</li> <li>▪ Identifies potential resistance to change and deals with it effectively.</li> <li>▪ Identifies potential opportunities for improving ways of working.</li> </ul>
3.2.	→ Strategic thinking	<p><b>Supports, promotes and ensures alignment with the company’s vision and values.</b></p>



		<ul style="list-style-type: none"><li>▪ Understands the internal and external influences that require organizational changes.</li><li>▪ Considers multiple possible causes and risks and anticipates consequences of situations.</li><li>▪ Is able to translate strategies into action.</li><li>▪ Looks beyond the immediate and considers long-term impact and consequences.</li><li>▪ Places issues in the broader context of the Organization's priorities and plans.</li></ul>
3.3.	→ Knowledge sharing	<p><b>Keeps abreast of new developments in own field of competence and promotes knowledge management and a learning culture.</b></p> <ul style="list-style-type: none"><li>▪ Demonstrates technical competence, job knowledge and ability to add value to the core job function and beyond.</li><li>▪ Draws constructively on own and others' experiences as opportunities to learn.</li><li>▪ Shares knowledge with colleagues and partners to enhance performance and foster knowledge transmission.</li><li>▪ Identifies own development needs and pro-actively seeks new challenges and opportunities to develop.</li><li>▪ Solicits feedback and identifies ways to improve.</li></ul>