

















Information security and GDPR

Nr	Question	Score	Advice
1	Are the roles and responsibilities for information classification assigned	3.5 	<i>Roles and responsibilities for information classification should be defined, so that it is clear which information is accessible to which readers. A commonly used classification: intended for public, for internal use, or confidential.</i>
2	All employees are informed and trained about the importance of information security	3.8 	<i>Information security requires a process of awareness. A director or manager should be appointed who takes responsibility for information and training on information security.</i>
3	Our organization has defined preventive measures to avoid unauthorized removal of equipment	5.7 	<i>It is fairly easy to steal a smart phone, laptop, tablet or PC from a desk. Smart phones, laptops and tablets should not be easy to remove. Consider using anti-theft chains in vulnerable places.</i>
4	The user organization informs us in an adequate and timely manner about colleagues joining and leaving the organization	5 	<i>Guarantee that the IT organization receives timely information about personnel mutations, so that access rights can be changed in time.</i>
5	All IT staff have signed a policy for careful and integer use of their IT rights	No 	<i>IT personnel has access to a lot of information on the network. Let them sign a policy to assure awareness of integrity regarding handling of authorization. Also mention a fine in case IT rights are misused.</i>
6	Have NO situations of misuse been revealed during the last 12 months	Yes 	<i>Analyse the misuse of authorizations and implement preventive measures.</i>
7	All wireless networks have a private network segment ('VLAN')	4.3 	<i>Deploy different Wi-Fi network segments to separate traffic types. This gives priority to the main data traffic, and prevents that intrusion into the VLAN enables access to all network traffic.</i>
8	For the safe exchange of data (carriers), procedures have been defined	No 	<i>Define procedures to allow the safe exchange of data on media (such as USB sticks, hard drives) or via data connections.</i>
9	Data carriers are cleared and disabled after disposal	No 	<i>Set up a procedure to erase data carriers and make them unusable after being put out of use. Think of an adequate software program and physical destruction.</i>
10	Storing our data takes place with encryption technology	5.5 	<i>Consider storing (at least the very crucial) data with encryption technology, so that it becomes unreadable for unauthorized persons. Regard data encryption as an addition to physical and software-based access control.</i>
11	Does your organization have a vision on the phasing out of network components based on IPv4	No 	<i>Because the last IPv4 address blocks were issued in 2011, we recommend preparing a vision for a (unfortunately complex) transition to IPv6.</i>
12	All employees in our organization have signed a policy for prevention of information leaks and correct treatment of corporate- and personal data	5.8 	<i>Several studies have shown that security issues are 90% caused by their own staff, who have access to information systems. Having employees sign a policy reduces that risk.</i>
13	The employees in our organization know the disciplinary measures in case they do not correctly handle corporate or personal data	No 	<i>90% of the information leaks are caused by own employees. Therefore, communicating disciplinary measures is crucial.</i>
14	Our employees work according to a 'clean desk' and 'clean screen' policy	5.4 	<i>Set clear rules for clearing desks and blocking screens when the employee leaves the workplace. This reduces the risk of misuse of information.</i>
15	Outgoing email is filtered, to verify what information leaves your organization	No 	<i>Confidential information can be sent unconsciously or deliberately simply by email to an unintended recipient. You can consider technical filtering. It is better to make your employees aware of this and to communicate sanctions.</i>
16	Our organization has rules for the use of removable media (such as USB flash drives)	No 	<i>Make a guideline for sharing removable media so that colleagues become aware of the risk that a medium might come in the hands of third parties.</i>