Take good care of your employees

How to improve security before, during and after employment

INTRODUCTION

If you are involved in recruiting new employees or responsible for managing staff, this folder is for you. We want to convey the message that good information security begins with putting employees first.

When companies, research facilities and educational institutions want to safeguard knowledge, their employees are an essential factor. Whether you have business-critical information, research results, information relating to national security interests, or other sensitive information, you may want to protect it from unauthorized disclosure.

Before employment

A new employee must be more than just professionally competent. They must also be trustworthy.

PET recommends that you perform a background check on the candidate to ensure they are who they say they are. The objective is to prevent you from hiring someone who is concealing facts of potential relevance to their loyalty and integrity. A background check reduces the risk of hiring someone who will subsequently attempt to collect and misuse information.

Background checks are performed with different levels of detail. The check should be adapted to the intended role of the candidate and the need within your organization to protect information. You may for example consider if you need to perform background checks on all new employees or if you should limit the checks to include specific groups or individuals.

Background checks are particularly relevant if the position gives access to sensitive information.

When assessing a candidate, you may want to consider the following:

Professional background:

- Check whether the listed educational institutions and companies even exist.
- Always request permission from the candidate to contact the relevant educational institutions to confirm that they have completed the studies listed in their application.
- Ask the candidate for references from former employers to confirm their professional and personal qualifications.
- If the candidate is from a country such as Russia, China and Iran, it is important to check whether the listed educational institutions or companies are funded by or cooperate with military institutions of those countries. When checking a university, it is also important to check the specific institute or centre.
- Be aware if the research area or field of work is related to a critical technology which may give cause for concern.
- Check whether any cited scientific publications have actually been published and whether the co-authors have any links to military institutions.
- Be inquisitive about gaps in the CV that are not accounted for and ask about them during the interview with the candidate.

CRITICAL TECHNOLOGY

Critical technology is technology with a significant capability to enhance or threaten national interests, including national security, social cohesion and welfare. Critical technology may include quantum technology, artificial intelligence and marine technology.

In this context, technology means the practical, especially industrial, application of scientific discoveries, while application may cover methods, processes, components and platforms, etc.

Personal situation:

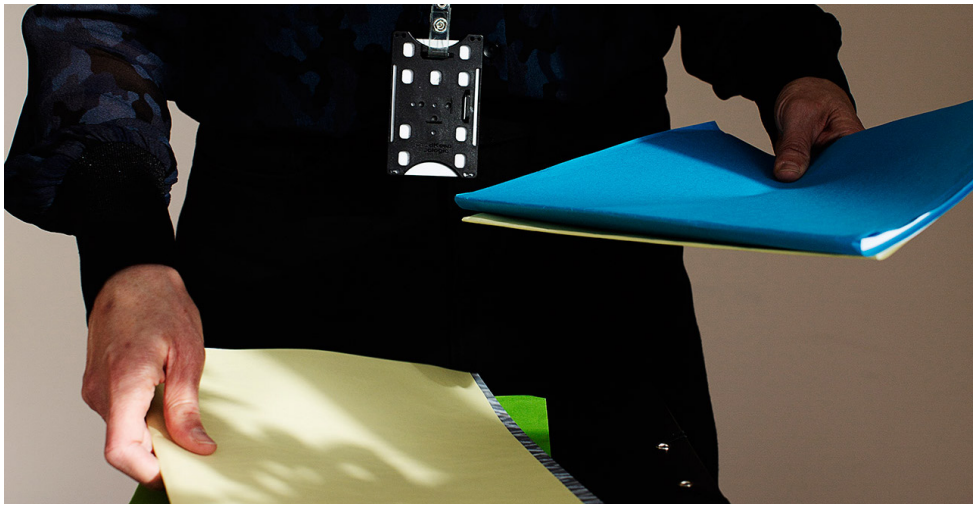
- Check the information available about the candidate online. Does anything give cause for concern in relation to the values and interests of your organization?
- Compare the data stated by the candidate in the CV and application form with the information collected.
- Check the identity of the candidate and compare it with official photo identification.
- During the job interview, tell the candidate about your focus on good security behaviour and take note of their reaction.

Once you have narrowed down the field to one candidate and are ready to employ the person in question, you may consider adding a non-disclosure agreement to the contract.

SECURITY CLEARANCE

If the employee needs access to classified information, a security clearance is required. The clearance is, among other things, based on a vetting procedure performed by PET. A simple background check is not sufficient.

Details on when information should be classified are stated in the so-called Security Circular.



During employment

The risk of a deliberate security breach by an employee is not only prevented during the recruitment phase. Daily life at the workplace also plays a significant role. Dissatisfaction may cause otherwise loyal employees to commit deliberate security breaches, for example by leaking information to competitors or foreign intelligence services. Common causes of dissatisfaction include a perceived lack of recognition, unfulfilled career ambitions or an inappropriate work culture – for example bullying.

Examples of how to increase security in your daily operations:

- Use the trial period actively. Be aware of how long the trial period is, and evaluate the initial employment period.
- Give special attention to the risk of information leaks and have an open dialogue on this matter, including on the espionage threat. Discuss what characterizes good security culture at your workplace. Everyone makes mistakes, and it is important that employees feel comfortable sharing their experiences and concerns.
- Pay attention to your employee satisfaction. You may for example conduct regular job satisfaction interviews, offer support in difficult situations and enquire about work pressure. Also, be aware if the employee may be under pressure from a foreign intelligence service.
- Confront employees who show changed or problematic behaviour. Clarify the underlying reasons objectively and prevent problems from growing. Be aware that any evasive, excessive or other inappropriate response from your organization may worsen the situation.
- Pay special attention to how employees react to organizational changes, as these may create insecurity. For example in connection with job cuts or restructuring.
- Consider what information each employee needs to perform their job. It may be relevant to introduce physical and/or technical solutions ensuring that not all staff have access to the same pool of information.
- Be aware that any change of work/research area or new sideline occupations may bring employees into contact with potentially problematic partners.

After employment

Job changes are bound to occur in the course of a career, and it rarely poses a security risk when employees move on to a new job. However, be aware that most cases of unauthorized knowledge transfer occur within the last 30 days of employment. It is therefore important that you incorporate the question of security into the process from termination of employment to final exit.

You may consider the following:

- What is the risk of unauthorized knowledge transfer when the employee leaves? Did the employee resign or were they dismissed? What information does the employee have access to? What job is the employee moving on to and who is the new employer?
- Is it okay for the employee to carry on working until the last day of employment or should access rights be restricted? In some cases, you may have to terminate all digital and physical access rights to the workplace at once.
- Conduct an exit interview to ensure an open exchange. Incorporate the question of security and remind the employee of any relevant legal aspects resulting from the discontinued employment (non-disclosure agreement, intellectual property rights, etc.).
- Make sure to cancel access rights to electronic systems in connection with the exit. Aside from computer login and email accounts, the employee may have access to community logins for programs or websites, which must therefore be changed or deactivated.
- Make sure that the employee returns all physical objects belonging to the workplace. Including access card, keys, mobile phones, computers and USB sticks, but also documents.

Do not ignore worrying behaviour

If you encounter any worrying behaviour or other deviations in connection with the employment or exit of an employee, it is important that you react. You can for example raise the matter with the head of security or your immediate superior.

If you worry that an incident may be related to espionage or terrorism, you should also request a confidential meeting with PET on *pet@politi.dk*.

For more information concerning advisory services, briefings or courses, please contact PET on *raadgivning@pet.dk*.

Published: August 2022
Graphic design: Permild & Ko
Photos: Ditte Valente