NSM

POLITIET

Næringslivets sikkerhetsråd

PST
POLITIETS SIKKERHETSTJENESTE

Personnel security

– before, during and after termination of employment

Published by the Police Security Service, the National Security Authority, the Police and the Business and Industry Security Council

Preface

For several years and in a number of threat assessments and reports, the Police Security Service (PSS), the National Security Authority (NSA), the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) and the National Criminal Investigation Service (NCIS) have warned against the threat represented by malicious insiders as a challenge for both public and private sector organisations. Both in Norway and elsewhere, established organisations and strategic employees are being corrupted and vulnerabilities exploited for criminal purposes – with great risk of financial loss and other damage as a result. Corrupt and disloyal employees represent a serious threat to society – a threat that demands increased attention.

In collaboration with the Norwegian Business and Industry Security Council, national security agencies have prepared this guide which hopefully will result in increased awareness about insider threat. In addition, we hope that the guide will enable organisations to make better decisions and adopt sound procedures and practices before, during and after termination of employment and in connection with the hiring of external services.

Table of contents

1 Background and purpose

The purpose of this guide is to provide a tool for public and private sector organisations to use in planning and implementing measures to reduce the threat from malicious insiders.

The guide takes a comprehensive approach and proposes a number of measures to be implemented in a systematic manner and in sequence. The recommendation is that organisations should focus on personnel security in all phases of employment, from before hiring to after termination.

The guide is meant for both private and public sector organisations. We emphasise, however, that the guide should not be used for posts where the Security Act sets out required security measures for employees. In these cases, the provisions of the act and its regulations apply.

We emphasise that organisations must ensure that all personnel security measures comply with current privacy and labour rights legislation.

The guide is divided into sections that follow the employment process from a post is advertised until the employee leaves. It then goes on to discuss security issues in hiring consultants and other temporary personnel.

The guide also briefly discusses how organisations should go about using third parties to carry out background checks and how the resulting information should be assessed.

Despite the guide's comprehensive approach, the list of recommendations should not be taken to be exhaustive. However, organisations that implement these measures will reduce their personnel security risk. The guide recommends that personnel security be made an integral part of the organisation's overall security measures.

It is important that all measures comply with current legislation. Some public sector organisations have special statutory authority to conduct background checks of applicants. They can probably dig deeper than organisations without such authority. It is also important that employers distinguish between measures that can be taken before hiring and measures that can be applied to current employees.

1.1 The threat

An employer–employee relationship requires a high level of mutual trust, as the employee is given access to the organisation's assets. And when they leave, employees take with them all skills and knowledge they have acquired.

In the current job market, use of temporary workers is widespread, either as temps, consultants or contractors, and they often have to be shown the same trust as the organisation's regular employees. They also take with them all the skills and knowledge they have acquired when their contracts end. The same applies to short term employees.

This combination of inside knowledge and trust means that current and former employees have wide opportunity to harm the organisation by misusing the trust placed in them. In some cases employees harm the organisation on purpose, while in others they do harm unintentionally because they do not understand or are unable to follow procedures established to safeguard the organisation's assets. The consequences may be financial loss, business secrets and sensitive information falling into the wrong hands, and reputational damage.

This guide defines a malicious insider as *«a current or former employee, consultant or contractor who has or has had legitimate access to the organisation's information systems, procedures, techniques, technology, equipment and premises, and who misuse their knowledge and access to commit acts that causes harm or financial loss to the organisation». (See also the Australian government guide [1])*

At worst, a malicious insider can commit or act as an accomplice to acts of espionage, sabotage or terrorism that can disable functions critical to society or endanger life and health.

Individuals who act against the organisation's interests can potentially do great damage. Employees are therefore not only a resource, they also represent a potential security risk and, in some cases, a threat to the organisation itself. This also applies to former employees, consultants and contractors.

1 Australian Government – Managing the insider threat to your business – A personnel security handbook

Third parties who may want to make use of malicious insiders include other countries' intelligence services, competing companies, and criminal and terrorist organisations. But a malicious insider can also act alone. Malicious insiders can threaten anything from national security to the money in the till. It is important to emphasise that personnel security measures must be implemented in combination with other measures, and that it is the interaction of the various measures that result in a high level of protection. The Security Act lists a number of required measures for the organisations that fall within its scope.

Insiders who pose a threat can be divided into three categories: The first is the infiltrator. Infiltrators are placed inside the organisation by a third party wanting to exploit the access awarded to the infiltrator to harm the organisation. The second is the self-motivated malicious insider who acts on his or her own initiative and who is not in contact with or controlled by a third party. The third category is the recruited insider working voluntarily or under pressure for a third party. Recruitment normally takes place after the insider has been given access to the organisation's assets. In addition, there is the unintentional insider who inadvertently does something that results in increased vulnerability, damage or loss to the organisation. The unintentional insider may have been manipulated or duped or does not have sufficient insight or knowledge to understand the consequences of his or her act.

It is not possible to make an exhaustive list of what motivates malicious insiders. Some motivating factors include: dissatisfaction with their employer, financial gain, personal problems, desire for revenge, work related problems, divided loyalties, thrill-seeking, vulnerabilities that can be exploited for blackmail, and lack of training, security procedures and personal judgement.

2 Security management system

Security management requires a systematic approach, both in gaining a general overview of the current situation and in maintaining a satisfactory level of security over time. The system should include structured and permanent processes for planning, implementing, operating, evaluating and improving a comprehensive security environment. The security system must also function in interaction with the organisation's regular activities and other control functions.

For the organisation to handle the potential risks posed by employees, it is important that personnel security play a prominent role in the organisation's security management system.

Consider:

- Does the organisation have a well-functioning security management system?
- Is personnel security a prominent component of that system?
- Have we identified key personnel and posts?
- Have we assessed the potential risk associated with any given employee?
- Is senior management aware of this risk?

Successfully implementing a comprehensive security management system chiefly relies on the following four elements:

- management buy-in
- a structured approach to security work
- organisation and roles
- necessary documentation and written procedures

2.1 Security culture

Organisations should strive to establish a working security culture, including:

- management and employee buy-in
- security-conscious conduct from both management and employees
- that management communicates the need for security measures and why
- acceptance and understanding for, and awareness of, personnel security measures among employees
- buy-in to the measures from the employees, preferably through good training and information
- that security measures are adhered to and integrated into the organisation's daily operations
- access to sensitive information given only to persons with a documented need

The National Security Agency's security management guide

Norwegian Standard – Security Risk Analysis 5832: 14

- that the individual employees are aware of how his or her conduct affects security
- adherence to personnel security rules and procedures
- that security breaches are reported
- that proposals for improvement from employees are encouraged and facilitated

2.2 Risk assessment

Organisations should map and identify their assets in a systematic manner. Information, equipment and premises are of great importance to an organisation, and their value will form the basis for deciding what assets need protection from malicious insiders. This should be followed by a risk assessment to identify what risks the organisation faces. The risk assessment will in turn form the basis for the organisation's personnel security measures.

- Map the organisation's assets.
- Make a simple assessment of the risk that hiring the wrong person entails.
- Identify what posts and tasks are particularly vulnerable.
- Prepare guidelines for background checks of applicants to these posts.
- Decide who in the organisation has ultimate responsibility for background checks.
- Make sure that information and the necessary forms are available to those who need them.

An assessment should also be made of whether a standard background check should be applied to all applicants, or whether some posts warrant a more (or less) thorough check. The organisation should also decide whether internal job changes warrant a new check. A separate background check may be devised for this type of job changes. A good plan based on a thorough evaluation of need, opportunity and limitations before measures are introduced, will be key to success.

2.3 Procedures and guidelines

Like other security measures, personnel security must be rooted in the senior management. Organisations should have a procedure and guidelines in place for conducting background checks. The procedure should be in writing to ensure documentation, and must comply with current legislation on discrimination, equal rights, HES, transparency and data protection. In addition, all employees and applicants should be made aware that background checks will be performed and why.

This will underpin background checks as part of the organisation's recruitment process and security culture.

The items below highlight what the procedures and guidelines should include.

2.3.1 Internal assignment of responsibilities

- Who is ultimately responsible for the background check?
- Who is responsible for performing the background check?
- Who makes the final assessment?

2.3.2 Collecting information

- Who collects the information?
- How will the information be collected?
- What information will be collected?
- What information should be verified?
- How should the information be verified – through documentation, search of electronic sources or by contacting people?
- What information cannot be verified?

2.3.3 Assessment

- How should the information obtained through background checks be assessed?
- What is an acceptable risk to the organisation (viewed in light of the risk assessment)?

2.3.4 Information handling

- The provisions of the Personal Data Act must be complied with.
- What is the legal basis for handling the collected information?
- What is the purpose of the information handling?
- Who will be given access to the information?
- How will the information be secured?
- How long will the information be stored?
- How will the information be destroyed?

2.3.5 Other issues

- What posts require a background check?
- Will all or part of the check be performed by a third party?
- The procedure should be subject to version control to ensure all changes are documented.
- Procedures and guidelines must be approved, dated and signed by the board or senior manager of the organisation, or by a person authorised to do so by the senior management.

Overall responsibility for background checks should lie with one person only to ensure equal treatment, efficiency and confidentiality, and the organisation should ensure that this person possesses the necessary skills and knowledge.

The organisation may require that applicants provide all information necessary to perform a background check.

A form for this purpose may include:

- full name – including previous name(s)
- date of birth
- current and previous addresses, including dates
- résumé of education and previous employment, including dates
- information that a background check will be performed and the consequences of providing wrong information
- the applicant's consent to a background check
- consent to collecting information from previous employers, finance institutions and others
- a field for the applicant to provide additional information

3 Background checks prior to hiring

3.1 What is a background check?

Organisations should check applicants' backgrounds before hiring. The process involves collecting, checking and documenting information about a person to verify information provided by an applicant. This may include search of open sources, e.g. credit checks, checks of business interests etc.

The purpose is twofold: First, to ensure that the information provided by the candidates is correct, whether they be simple misunderstandings or deliberate lies. Second, to prevent hiring the wrong person. Done right, background checks will reduce the probability of hiring a person whose vulnerabilities make him or her a potential threat to the organisation's assets.

This requires that the results of the background check be held up against the organisation's risk assessment to ensure that the candidate does not constitute an unacceptable risk. If there is uncertainty about a candidate and this uncertainty pertains to assets that the organisation wishes to protect, this must have consequences for the further hiring process. The organisation must then decide whether the risk is too large or whether compensating measures can be taken to mitigate it. That background checks will be performed and have consequences for the hiring process, must be made clear to the candidates early in the hiring process.

Background checks should be completed before new employees are given access to the organisation's premises, procedures and information systems. Because background checks can be both invasive and costly, the extent of the check must be adjusted to the value of the assets that the person who is hired will be given access to.

3.2 Content of a background check

Use the applicant's résumé as basis for deciding what to examine and how.

A background check can be divided into four main parts:

- identity check
- verification of educational background and previous employment
- credit check and check of business interests
- search of open sources

These four parts are the focus of this guide, but organisations should adopt and implement procedures and guidelines adapted to their specific needs.

3.2.1 During the hiring process

During the hiring process, the organisation's priority will be finding the best candidate for the job, but it is also important to have security in mind already at this stage – particularly if the post is exposed to risk.

Make it clear when advertising the post that applicants may be required to undergo a relevant background check. The check should be carried out before the candidate is invited to an interview.

3.2.1.1 Consent from the candidate

Applicants must give their consent before a background check can be performed, cf. the Personal Data Act section 2 no. 7. Remember that consent is voluntary. If the applicant denies consent, a background check as described in this guide cannot be performed.

Consent must be given in writing, and is often a requirement for universities, schools and previous employers to disclose information. This is particularly the case for state registries and agencies.

The consent form should contain information about:

- who will perform the check
- what the purpose of the check is and what the results will be used for
- what information will be verified
- what sources will be contacted
- relevant data protection legislation and the applicant's rights
- where and how the information will be stored

3.2.2 *Verification of identities and residence permits*

The use of false identities is a big problem, also in Norway. It is challenging to keep a check on who lives and works in the country at all times. False, fictitious, stolen and borrowed identities have all been used to get a job in both the private and public sectors.

3.2.2.1 *Verification of ID documents*

- Always ask candidates, independent of nationality, to bring their passports with them to job interviews and the first day of work.
- Check the passport carefully. It is vital to verify that candidates provide their true identities.
- Use simple equipment, e.g. UV light and magnifying glasses, to check ID documents.
- Compare them to open reference databases like Edison TD, www.edisontd.net, and Prado, www.consilium.europa.eu/prado.

A basic identity check should include:

- comparing the photo with the candidate's face
- posing open questions to the candidate about the document and the information it contains

3.2.2.2 *Verification of residence permits*

Applicants must have legal residence in Norway. Residence permits can be verified by the Norwegian Directorate of Immigration (www.udi.no) or the police.

- Remember that EU and EEA nationals do not need to apply for residence permits in Norway. However, ID documents from any of these countries are prized assets.
- Of particular importance with respect to third country nationals is to find out when any temporary work or study permits expire.

3.2.3 *Verification of education*

Norway

Ask the candidate for access to his or her exam results in the Diploma Registry or contact the college or university directly.

You can obtain information about:

- the duration of courses taken (start and finish dates) and whether they were part or full time studies
- whether the candidate completed the courses or not and whether the candidate passed or not
- whether and what title or degree the candidate achieved
- whether the candidate's printout of exam results is correct

Has the college or school been closed? Information from public schools, colleges and universities end up in municipal, county and government archives, see www.arkivverket.no.

Other countries

The Norwegian Agency for Quality Assurance in Education (NOKUT) approves foreign degrees. An employer can require an applicant to produce documentation of awarded degrees and authorisations.

- NOKUT issues documents of approval to persons who apply to have their foreign degrees approved in Norway. This document provides a comparison of the degree to similar Norwegian degrees with respect to content and length of the studies.
- NOKUT assesses the authenticity of foreign degrees and tries to verify their authenticity in cases of doubt.
- Employers can ask applicants to apply to NOKUT for such documentation when inviting them to job interviews.

More information can be found at www.nokut.no/en.

The Diploma Registry (www. vitnemalsportalen.no) is an online service provided by the Ministry of Education and Research. You can download your college and university results and share them with other colleges and universities, potential employers and other relevant parties. The service is free to use and has been live since January 2017.

Consider: An applicant may have business interests which are in competition with your own and may potentially misuse any information he or she gets access to if hired. Applicants' business interests should be clarified in advance.

3.2.4 *Verification of work experience*

Calling references is a subjective check of an applicant's professional background.

- Check with e.g. the Brønnøysund Register Centre whether a referenced organisation actually exists.
- Check that the referee and the applicant have actually worked together.
- If possible, call a switchboard number, not a mobile phone number.
- Prepare a topics list for the conversation.
- Remember to obtain the candidate's consent.
- If possible, speak with superiors, equally ranked colleagues and subordinates.
- Call the HR department or the department where the candidate worked.

If the purpose is to check work experience, the following questions may be relevant:

- Duration of the employment (start and end dates).
- Full or part time employment.
- Are the titles and functions provided in the résumé correct?

3.2.5 Business interests

Brønnøysund Register Centre and the European Business Register (www.ebr.org), among others, provide information about business interests and roles held by candidates in private and public sector organisations.

Many registries are commercial, and it may pay to sign a subscription to get lower rates per search.

Search for roles, links to companies and other business interests. Such information is offered by all credit check providers and a number of other companies.

3.2.6 Credit check and financial history

Credit checks of applicants can be performed when there are legitimate grounds, cf. the Personal Data Regulations section 4–3. It is a requirement that organisations in their procedures and guidelines have identified when credit checks are relevant and for what posts. The risk assessment should provide guidance on what is an acceptable level of risk and the background check adjusted accordingly.

- It must be assessed whether a background check can and should be performed, and the applicants must give their consent.
- There are many companies offering credit checks in Norway.

Note: The credit report itself cannot be stored, only the score. This means that information about late payments, debt and mortgages cannot be saved in personnel files etc.

3.2.7 Search of open sources

Remember that open sources often contain unverified information. Open source information should therefore not be used to disqualify a candidate, but rather be a topic during the job interview.

- Search for information about the candidate on the internet, e.g. social media sites.
- Services that collate information about individuals from various sources simplify the search.

Note: Not all information on the internet and social media sites is correct or gives a truthful picture of a candidate. Be sceptical and use only information that is relevant for the job.

3.2.8 Other information

Other information of interest in a background check:

- authorisations and accreditations
- certificates of completed apprenticeships and master craftsman's certificates
- other certificates and licences
- concessions and permits
- health certificates – where relevant

3.2.9 Job interview

Job interviews are useful for obtaining a more complete impression of a candidate's opinions and attitudes – including the candidate's attitude to security issues and his or hers own vulnerabilities. Job interviews also give candidates opportunity to demonstrate awareness of these subjects. In addition, they provide an opportunity to clarify any question about the documentation. What topics are relevant is for the organisations to decide.

Information provided during the interview should be taken down and verified.

For example, ask the candidate about his or her:

- upbringing
- family
- social circle
- leisure activities

Skills testing

A good way to verify a candidate's skills is to test them. This can give a clear indication on whether the candidate possesses the skills and knowledge provided in the résumé.

4 After hiring - security management

Both managers and employees are responsible for maintaining security-consciousness at all time.

Security management is an ongoing process that follows the employee from the first day at work until he or she leaves the organisation. It also includes former employees, e.g. through confidentiality declarations.

Fostering security consciousness is an important element of personnel security. This involves training and maintaining the employees' skills and knowledge of the organisation's security policies and guidelines and motivating them to act accordingly.

Possible measures:

- a mandatory introduction course in the organisation's security policies and guidelines
- regular campaigns to increase the employees' awareness of security issues
- dissemination of regular updates and information about the security risks facing the organisation
- mandatory re-training courses in various security issues, e.g. social manipulation and insider threats
- security as topic in newsletters and intranet pages
- holding the individual employees responsible for how they handle and comply with information, systems, procedures and equipment

4.1 Uncovering irregularities

Organisations should have sufficient means of uncovering malicious insider activity and other undesirable conduct from its employees, e.g. have in place procedures for employees and middle managers to report concerns about undesirable conduct and changes in behaviour that may constitute potential vulnerabilities. Reports can also be about conduct that raises suspicions of malicious insider activity.

To uncover potentially harmful conduct, it is important that middle managers and employees are aware of signs of malicious insider activity and social manipulation.

4.2 Following up vulnerabilities

Organisations should have resources to follow up vulnerabilities that arise in employees. Measures must comply with current legislation and must aim at mitigating the risk. Any suspicions of criminal activity should be reported to the police. Suspicions of espionage from foreign countries must be reported to Norwegian authorities, while suspicions of espionage from competitors should be reported to the police. Examples of suspicious conduct that should be followed up are:

- discontent
- changes in behaviour
- contact with criminals
- misuse of alcohol and controlled drugs
- financial problems
- higher spending than what a person's income would allow

Examples of concrete topics:

- What is social manipulation and how is it done?
- What is malicious insider activity and how is it carried out?
- Who represents threats to the organisation?
- Procedures for handling information, systems, procedures and equipment.

5 Termination of employment

Employees' obligations to their employers do not necessarily end they leave the organisation, and all responsibilities and obligations after termination of employment or change of tasks, e.g. as stated in signed confidentiality declarations, should be stated and communicated clearly.

Procedures for termination of employment are an integrall part of personnel security. Checklists and forms are useful for ensuring that all issued equipment is returned. The procedure should also include cancelling access to information, systems, procedures and equipment.

Examples of equipment that should be returned:

- key cards
- code cards
- telephones
- computers
- external hard disks
- documents
- USB memory sticks
- keys

Examples of elements to be deleted electronically:

- passwords
- access and other codes
- external logon accounts

Inform all customers and business partners that the employee has had contact with that he or she is leaving the organisation, and provide them with the details of their future contact.

Carry out termination interviews with all employees before they leave. This is particularly important for employees who do not resign at their own initiative.

6 Use of consultants and subcontractors

From time to time, both private and public sector organisations need to hire the services of consultants and subcontractors. Before selecting a subcontractor, organisations should investigate ownership, corporate structure and historical performance to find out if the subcontractor conducts its business in an ethical manner and is not linked to any criminal or unethical activities.

This includes checking:

- the Brønnøysund Register Centre and other business registries and databases
- StartBANK
- the subcontractor's reference customers

In principle, all personnel security challenges also apply to consultants and subcontractors. Organisations should expect the same level of security from consultants and subcontractors as they practice internally.

To avoid entering into contracts with consultants and subcontractors with sub-standard security, organisations should describe their security requirements in all tender documents, and include them in all contracts.

Before putting assignments out to tender, organisations should identify what information systems, premises and equipment the consultants and subcontractors will have access to and what security risks this may entail. The person responsible for the assignment should ensure that employees skilled in security matters are involved in the acquisition process.

When a consultant or subcontractor has been selected, the contract should include the security requirements. A conversation before signing can confirm whether or not the requirements have been understood. The organisation should ensure during the whole engagement that the consultant or subcontractor complies with the security requirements.

If the engagement requires access to classified information, the provisions of the Security Act apply.

The levels of subcontracting should be kept to a minimum, as a long chain of subcontractors will make control difficult.

When the engagement ends, a meeting with the consultant or subcontractor should be held to clarify what obligations they have with respect to the information, skills and knowledge they have acquired during the engagement. See also chapter 5 on termination of employment.

7 Legal framework

There are a number of laws that regulate and influence the relationship between employers and employees. Some laws are sector-specific, while others apply to all. The Working Environment, Civil Service, Gender Equality, Anti-discrimination and Personal Data Acts are all relevant for personnel security. This legislation regulates what measures can be implemented, what employers can ask and make inquiries about, and how the collected information can be handled, stored and used.

Note that the Security Act contains provisions regulating both government agencies and other legal entities whose activities are vital to national security.

As a main rule, employers are not allowed to inquire or collect information about applicants' health, trade union membership, cohabitation arrangements, sexual orientation, pregnancy, adoption, family planning and cultural, political and religious views. The exception is when the information is relevant for assessing whether an applicant is qualified for the job, i.e. is required by the nature of the job in question. The purpose of collecting the information must then be described. Because collection and handling of personal information must be based on informed consent, employers must inform potential applicants of this as soon as possible, including in the advertisement.

7.1 Privacy concerns

Protection of personal data is of fundamental value in a democracy ruled by law like Norway. This means that everyone has a right to privacy and control over their personal information. Modern information technology provides ample opportunity to search for other people's interests, actions and opinions. This will often conflict with the right to privacy.

Organisations must ensure that the information they collect about applicants and employees stays within the limits of the Personal Data Act. The act sets out requirements for statutory authority for collecting information, limitations on what purposes information can be used for, and requirements for the handling and securing of information.

Guidance on privacy can be found on the Norwegian Data Protection Authority's website (www.datatilsynet.no).

7.2 Police certificate of conduct

Police certificates of conduct provide information from the police databases about a person's conduct. A number of jobs require a police certificate, as does some offices in volunteer organisations. Employers can only require police certificates from applicants if they have statutory authority, in law or regulations, to do so. Examples of such employers are security companies, the national mail service and schools and nurseries. This requirement should be made explicit in the advertisement.

All information in police databases is confidential. Only when it falls under the exemptions specified in the Police Databases Act can this information be shared with others, including private and public sector organisations.

The Police Databases Regulations set out for what professions employers can demand police certificates that are not provided for in special acts.

For the purpose of hiring, a police certificate of conduct will represent only one – often incomplete – source of information about a candidate's suitability for a specific job. Both simple and extended police certificates of conduct only contain a person's criminal sanctions history.

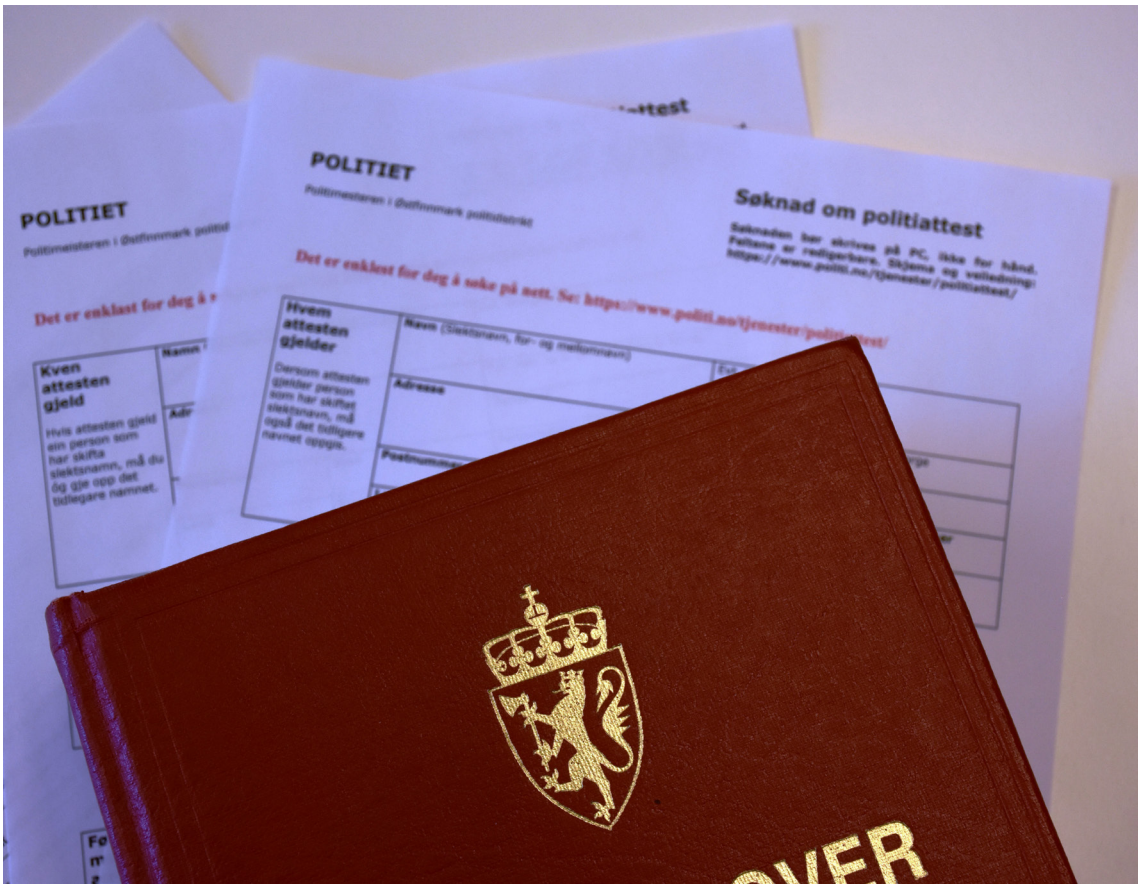
More information about police certificates can be found on the Norwegian police's website www.politi.no and in the Police Databases Act and Regulations.

Consider:

- What information do you as an employer need?
- Can your needs be grounded in the nature of the job?
- Have you made the applicant aware of your information needs?
- Have you obtained the applicant's consent?
- Are your information collection procedures documented?
- Are you in compliance with the requirements for storing and handling information set out in laws and regulations?

Important legislation:

- Act relating to working environment, working hours and employment protection, etc. (the Working Environment Act)
- Act relating to civil servants, etc. (the Civil Service Act)
- Act relating to gender equality (the Gender Equality Act)
- Act on prohibition of discrimination based on ethnicity, religion, etc. (the Anti-discrimination Act)
- Act relating to the processing of personal data (the Personal Data Act)



Preventive security measures: Measures designed to prevent or mitigate the effect of undesired acts, to be implemented before they happen, ideally to prevent them from happening at all. Preventive security includes human, technological and organisational measures.

Personnel security: Preventive security measures against potential and current employees designed to reduce security risk.

Vulnerability: Factors in a person's life that can induce him or her to act contrary to the organisation's interests, either because they are being exploited by outsiders or because they motivate the person to act on his or her own initiative.

Threat actor: An actor who intends to commit an act or induce someone else to commit an act designed to harm Norwegian security interests or an organisation's interests.

Malicious insider: A current or former employee, consultant or contractor who has or has had legitimate access to the organisation's information systems, procedures, techniques, technology, equipment and premises, and who misuse their knowledge and access to commit acts that causes harm or financial loss to the organisation

Value assessment: An analysis to identify and evaluate information and assets of value and what security measures can be implemented to protect them.

Security measures: Planning, implementation and control of preventive security measures designed to remove or mitigate the risk of espionage, sabotage and terrorist acts.

Background check: Collection and verification of information in connection with the hiring of new or posting of current employees.

Published:
March 2018

Printing:
The National Criminal
Investigation Service (NCIS)

Layout and illustrations:
The Norwegian Business and
Industry Security Council (NSR)

Photo:
Adobe Stock/Arne Røed Simonsen

Contact:
Email: nsr@nsr-org.no

Address:
Middelthuns gate 27, Majorstuen

Combat crime – for the protection of business and society