Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

National Cyber Security Centre NCSC

October 2024

Recommendations for conducting security checks on employees in companies

1 Introduction

In today's workplace, the integrity and trustworthiness of employees is critical. By conducting thorough security checks, organisations can minimise potential risks and ensure that only trusted individuals have access to sensitive data, financial resources or critical systems.

A security check should remove any doubts about the employee's integrity, reliability or trustworthiness, and confirm that they are not susceptible to blackmail or bribery because of their lifestyle or circumstances.

The requirement to carry out such a check and the consequences of a negative result should be firmly anchored in both the recruitment process and the employment contract. Compliance with the Federal Data Protection Act[1] must also be ensured.

These recommendations explain what needs to be taken into account when carrying out a security check. In particular, they will help companies that have to carry out security checks due to compliance requirements, including companies in the electricity and gas sectors that have to comply with the ICT Minimum Standard.[2]

2 Items to check and what to look for

A security check includes items such as confirming the persons' identity and checking information against various registers. It can also include a person's social environment to give a full picture of their trustworthiness. A good security check will include the following:

[1] Data Protection Act; FADP; SR 235.1.

[2] The Electricity Supply Ordinance (ESO; SR 734.71) requires companies with an A or B profile in the electricity and gas sectors to comply with certain requirements set out in the ICT Minimum Standard of the Federal Office for National Economic Supply (FONES). Among other things, this includes mandatory security checks for certain roles (see also ICT Minimum Standard, version 1.1, process: PR.IP-11 or GV.PR-04 according to NIST Cyber Security Framework 2.0).

Item to check	What to look for
Criminal records extract	Ideally, the criminal records extract should not contain any information that could affect the person's trustworthiness. If there is information in the criminal records that could be problematic, you can ask the subject of the security check to provide (voluntarily) more information about their criminal judgments or summary penalty orders to help you better assess the situation.
Extract from the debt enforcement register	Ideally, the extract from the debt enforcement register should not contain any information that could indicate corruptibility. If the subject of the security check self-declares that they have taken out personal loans to repay their debts, this may be helpful in evaluating the information. You should inform the subject of the security check that if they have been wrongly accused of non-payment of a debt and have an entry in the debt enforcement register for this reason, they can (voluntarily) provide additional information.
Social media and the internet	By searching public sources, such as the internet or social media, you can see if they have attended inappropriate events or shared content that may call into question their integrity, loyalty or make them vulnerable to corruption.
Diplomas and certificates	To verify the legitimacy of the diplomas or certificates presented by the person vetted, contact the relevant issuing body.
International connections	If the person has connections abroad because of their background or because they have spent a lot of time there, this may indicate problematic influence by a foreign state or vulnerability to blackmail (e.g. by threatening family members) and require an assessment of their trustworthiness. If a foreign national cannot be vetted due to a lack of international agreements or time constraints, your company can assume the risk and document it as part of the risk management process.
Job references and former employers	Incorrect information about previous employers or reasons for dismissal can call into question a person's integrity and trustworthiness. For this reason, it may be helpful to confirm employment information, references and, where appropriate, any reasons for dismissal with previous employers.
Interviews	Interviews are a good way to further verify information.

3 Security checks as part of organisational processes

- **Job application**: The application process must include a requirement to consent to a security check. The job candidate must be informed of this.

- **Security checks for existing employees**: If new obligations require an employee to undergo a security check, their contract may need to be amended.
- **Follow-up security checks**: Security checks should be repeated on a regular basis, every two to five years depending on the level of sensitivity, and whenever there is a change in an employee's role. We recommend that employers obtain the statements they need to carry out these checks directly; this will simplify the process.
- **Criteria**: Your organisation will need to define what types of criminal or debt enforcement records it considers relevant, and develop its own assessment and decision-making process. Wherever possible, ensuring that at least two people are involved in conducting the interview and making decisions will improve the quality of the assessment ('four eyes principle').
- **Storing security check results and data protection**: The results of the security check must be stored in accordance with data protection regulations. Any information that is no longer relevant after the decision has been made should be deleted immediately. If the security check is carried out externally, data protection compliance for the way in which data is exchanged and stored must be confirmed and documented.
- **Employee directory:** An employee directory should identify who needs to be vetted based on their job duties, access rights and roles, and whether they have already been cleared. Whether a security check is required depends primarily on the sensitivity of the job and the damage that the person could do to the company.
- **External suppliers:** Employees of external suppliers must be involved and contractually required to undergo security checks (if there is no obligation to undergo such checks, this should be documented in the risk management system).

4 Abbreviations

NCSC	National Cyber Security Centre
SFOE	Swiss Federal Office of Energy
FONES	Federal Office for National Economic Supply
CSF	Cyber Security Framework
ISA	Information Security Act
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
DDPS	Federal Department of Defence, Civil Protection and Sport