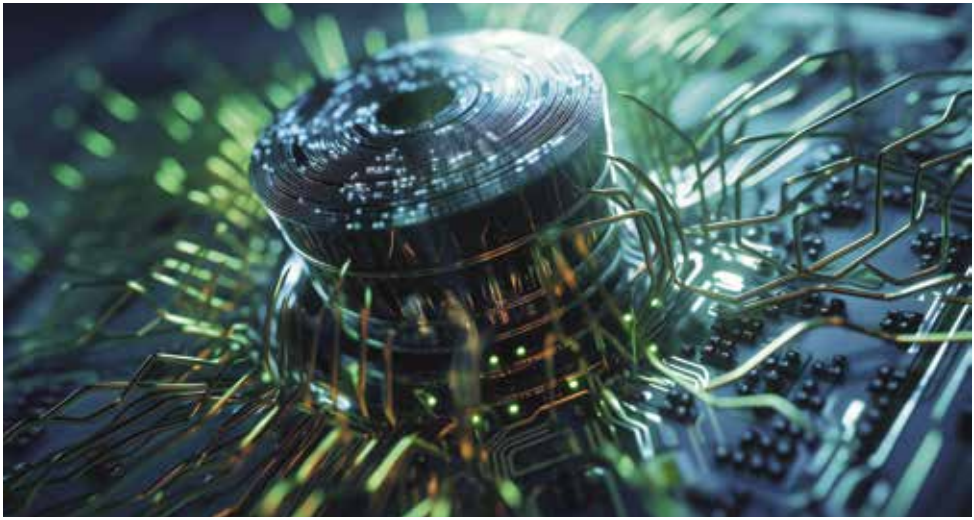


Is your research at risk?

Good advice on espionage prevention to researchers and other staff

CONTENT

Introduction

Denmark is a global leader within a number of areas relating to technology, innovation and research. This world leadership is a major revenue source to Danish economy, and it often contributes to solving global challenges in areas such as green transition and health, but it also makes Danish research institutions and companies attractive espionage targets.

Danish research is facing fierce competition, and Danish research institutions and companies are active in international cooperation. In by far the majority of cases, this is an advantage for Denmark, but the Danish Security and Intelligence Service (PET) has seen examples of research falling into the wrong hands. This may harm Danish research and have financial and security policy implications for Denmark. Consequently, it is essential to achieve the right balance in order for Danish universities and companies to work as openly as possible – and as securely as necessary.

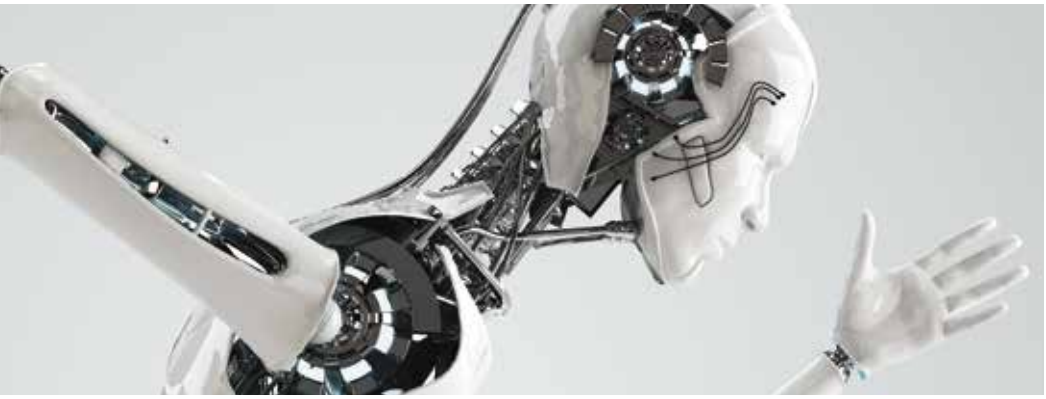
In cooperation with the Danish Agency for Higher Education and Science and the Danish Business Authority, PET has prepared recommendations on how to prevent and handle espionage to staff working for research institutions and research-intensive companies. This is the second edition of this folder – as the threat to Danish research remains significant and complex, and therefore a number of protection initiatives have been launched in recent years.

GUIDELINES FOR INTERNATIONAL RESEARCH AND INNOVATION COOPERATION

In 2020, the Danish Ministry of Higher Education and Science set up the Committee on Guidelines for International Research and Innovation Cooperation (URIS). In May 2022, URIS published a report containing a number of new guidelines aimed at protecting Danish research against financial, security and ethical risks in connection with research and innovation cooperation.

URIS recommends that you identify and protect your critical research, carry out checks on your international partners, and limit the cooperation to specified areas. These guidelines resonate with the recommendations in this publication. You can find URIS' guidelines on the website of the Danish Ministry of Higher Education and Science: *https://ufm.dk/publikationer/2022/filer/uris-guidelines_english-version.pdf*

As a follow-up to the publication of the guidelines, the Danish Ministry of Higher Education and Science has established a permanent forum for international coordination and cooperation. The purpose of the forum is to support the implementation of the new guidelines by research institutions and funds as well as knowledge-sharing and coordinated efforts with a view to protecting Danish research against abuse and foreign interference.



Danish research is an attractive target

Denmark is a global leader within technology and research, which renders the country an attractive espionage target. Foreign states attempt to acquire the most recent knowledge and technology via state-funded industrial espionage and illegal procurement.

For instance, PET has uncovered that foreign intelligence services continuously attempt to establish contact with students, researchers and companies that could provide access to products and specific knowledge about the most recent Danish technology and research.

Foreign students and researchers in Denmark may contribute to transferring sensitive information to foreign states. They may be under heavy pressure from the intelligence services of their native countries, and it should be an attention point that some authoritarian states require by law that their citizens assist their intelligence services in acquiring information of interest to the state.

ESPIONAGE is, among other things, collecting or passing on information on matters which should be kept secret for reasons of state or public interests in Denmark. Espionage includes the disclosure of data that may jeopardize national security, Danish public interests or the security of any individual residing in Denmark. Espionage also includes activities enabling a foreign intelligence service to operate on Danish soil.

INFLUENCE OPERATIONS are carried out when the intelligence service of a foreign state is enabled to influence decision-makers or the general opinion in relation to Danish state matters. The purpose of influence operations may be to influence public debate, international cooperation or foreign opinion of Denmark in order to further own interests.

ILLEGAL PROCUREMENT denotes activities whereby foreign states illegally acquire export-controlled products, technology and knowledge which they can use to build military programmes.

Illegal procurement may for instance take place if Danish companies or universities export products or transfer knowledge which fall into the wrong hands through intermediaries. The foreign states often use intricate networks consisting of many actors in different countries in an attempt to hide the final end use of the products, thus avoiding export control.

PROBLEMATIC ACTIVITIES IN THE GREY ZONE – Espionage, influence operations and illegal procurement are criminal offences as defined in the Danish Criminal Code, Chapter 12, ss. 107-109 and s. 110 c, and Chapter 13, s. 114 h. However, these legal provisions do not necessarily apply to all covert and problematic activities carried out by, or on behalf of, a foreign state.

For instance, it may be problematic if critical Danish infrastructure is owned by companies from a state that is at odds with Denmark. Another example is foreign PhD students bringing knowledge that may be used for unethical purposes with them when returning to their native countries.

It is important to keep in mind that the modus operandi of certain states, including China, is to activate the entire society. In other words, they use not only government agencies, but also private companies, academic environments, media houses, voluntary organizations etc. to reach a common goal – a goal which may consist in acquiring technological leadership within an area of priority.

Exposed research areas

PET knows that foreign intelligence services have a permanent focus on high-tech and defence-related areas. This applies most to energy technology, biotechnology, quantum technology, space technology, robotics, defence products and products subject to export control. In step with global developments, the research areas that are particularly at risk continuously change, and some research areas and products that can have both a civilian and military use, so-called dual-use, make the issue even more complex.

Espionage against Danish research may be both commercially and politically motivated. States may seek to derive a competitive and commercial advantage from knowing researchers' work and Danish research results prior to publication. Areas of particular political focus may give foreign states insight into the research and advice on which the Danish government and parliament base important decisions.

All research institutions and research-intensive companies may potentially become the targets of foreign intelligence services.

ESPIONAGE AGAINST GREEN TECHNOLOGY

In the summer of 2020, a Russian citizen, who had lived in Denmark for twelve years, was arrested. In the following year, the court of Aalborg sentenced him to three years' imprisonment for espionage and deportation from Denmark. The defendant was charged with espionage against the Technical University of Denmark (DTU), where he had passed his PhD exam, and a green technology company in Northern Jutland.

For a number of years, he had provided a Russian intelligence service with information against payment. The sentence was upheld by the Western High Court in November 2021, which sentenced him to deportation from Denmark with a permanent ban on re-entry and confiscated the proceeds.

EXPORT CONTROL AND INVESTMENT SCREENING

One of the purposes of export control and investment screening is to protect Danish research and development.

EXPORT CONTROL

Export control is to ensure that products that may be potentially harmful do not fall into the wrong hands. There may be several reasons why a specific product attracts attention and requires an export licence.

A product may be a specific item, technology or knowledge. It may also be a service such as technical assistance or counselling. The function and applications of a product may determine whether you have to apply for an export licence. Basic research not intended for application and technology already available in public spaces are exempted from export control.

Danish export control is based on international rules and lists of materials and technologies that could be misused for the development of weapons of mass destruction, violation of human rights or surveillance.

It is important to know export legislation if your research institution or company works with products within areas such as communications, surveillance, software, space technology, pharmaceuticals, biotechnology or chemistry.

Some products may have both civilian and military applications (dual-use). Examples are sensors, lasers, programs and software. If the product is on the EU list of dual-use items, you will need a licence to export it out of the EU. The rules are more lenient within EU borders, as only the most harmful products require an export licence.

Products that are not on the EU list of dual-use items may also be subject to the rules if covered by so-called catch-all provisions, which are an extra export control safety net. For instance, it is important to whom you export and in which country your buyer is located.

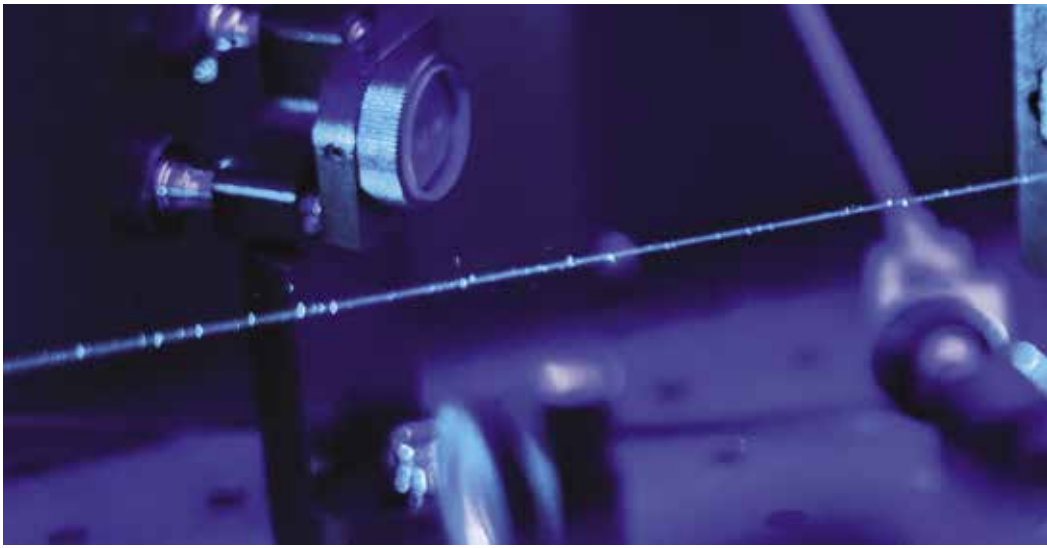
Research institutions are responsible for observing export control rules, which includes applying for an export licence, but the Danish Business Authority can guide you and assist you with customer checks.

INVESTMENT SCREENING

Whereas the purpose of export control is to protect Danish research and development in connection with export of products, investment screening applies to investments in Denmark by a foreign entity. Research and development activities may be subject to investment screening legislation if they are carried out within particularly sensitive sectors and may thus be a threat to Danish security.

MORE INFORMATION

For more information on export control, see the EU list of items and the catch-all provisions and read about investment screening at the website: *https://danish-businessauthority.dk/export-controls*



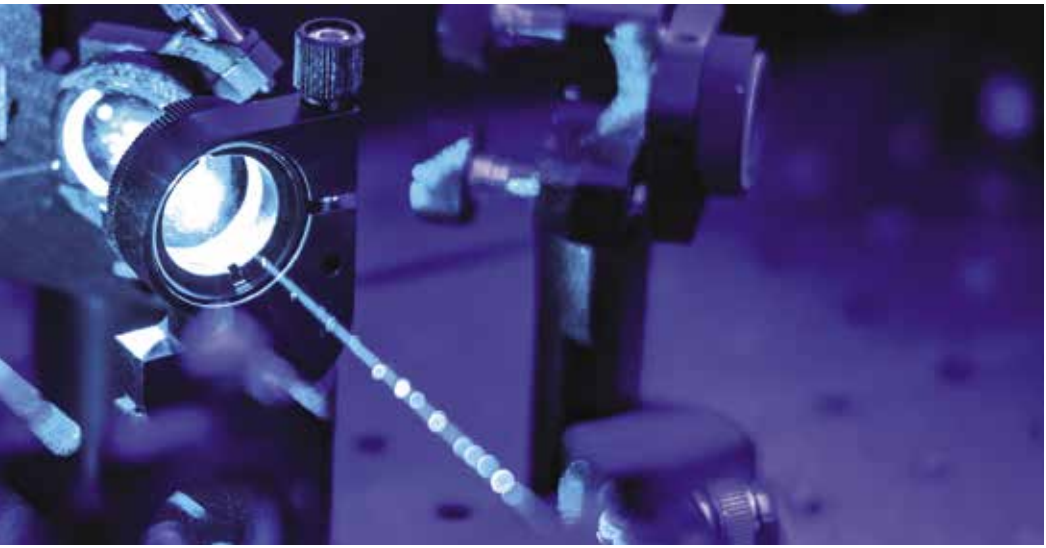
Significant consequences

– for individuals and for Denmark

It may have significant consequences for Denmark if other countries gain unauthorized access to your research. It may also harm the reputation of Danish research institutions and companies, causing difficulty in terms of future finance, recruitment and international cooperation.

Espionage poses a risk of loss of:

• **Confidence and reputation**
Confidence in your research institution, company or yourself may disappear and your reputation may be harmed if the sensitive data and products that you have access to are misused, stolen or fall into the wrong hands in another way.



• Possibilities
The possibility of being credited for your work or of publishing or patenting your research will diminish if, for instance, research results are lost.

• Independence and freedom
Financial dependence involves the risk of financial pressure. Direct or indirect threats of withdrawal of project finance may put pressure on staff to lower ethical standards or to compromise on academic independence or freedom of speech and communication.

• Financing
It may be more difficult to obtain future finance if it becomes known that your research, technology or products have unintentionally ended up with a foreign state. You may also suffer financial losses if somebody accesses data or information owned by your sources of finance.

How exposed are you?

Together with your research institution or company, you should consider how exposed you are to espionage and illegal procurement. Every single organization should assess both vulnerability and risk, for instance on the basis of the URIS guidelines (see page 4). But staff members of research institutions or companies also play a crucial role in assessing the potential interest in and the wider scope for applying your knowledge, technologies and products.

Research projects may be exposed if:

- They are likely to lead to commercial or patentable results.
- They contain sensitive data or personally identifiable information such as genetic information or commercial test data.
- They may be used for foreign military purposes or have both military and civilian (dual-use) applications.
- They may form the basis for international strategic political negotiations or decisions.
- They require sensitive laboratory equipment.

Products and technologies may be exposed if:

- They are subject to export control.
- They may be used for foreign military purposes or have both military and civilian (dual-use) applications.
- The technology is ground-breaking or state-of-the-art. The fewer manufacturers that can match the properties of the product, the higher the risk.

THE ”BRAZILIAN” RESEARCHER

In October 2022, Norwegian police arrested a researcher with Brazilian citizenship at Tromsø University, where he had attended studies in Norway's northern region and hybrid threats since 2021.

According to Norwegian police, the identity of the researcher was false as he was actually a Russian citizen working for a Russian intelligence service. Today, the researcher is remanded in custody, while the Norwegian security service PST investigates whether the researcher has established a network of individuals with access to information that he may have passed on to a Russian intelligence service.

Espionage methods

– used by foreign states

Foreign states have many different methods for collecting information and products. The methods range from legal to illegal ones, and many are in the difficult grey zone. The methods are generally used in complex combinations.

Traditional academic activity is one of many ways in which a foreign intelligence service may get access to you. One method is to show interest in your research at conferences or on social media such as LinkedIn.

International cooperation provides state actors with a legitimate access to collect research without using traditional espionage or cyberattacks. However, there is a risk that the cooperation may give unwanted access to individuals and IT networks as well as insight into research which may be sensitive.

Trade, investments and supplier agreements are other methods for acquiring the desired knowledge, technology and products. Transactions made via front companies in order to circumvent sanctions and export control are illegal procurement activities. See page 8 about export control.

IRANIAN INSIDER INCIDENT AT NTNU

One of the most recent Iranian espionage incidents took place at the Norwegian University of Science and Technology (NTNU). In November 2022, a professor at NTNU was convicted of multiple violations of Norwegian export control. He had given guest researchers from Iran access to a laboratory with sensitive equipment and to one of the university data systems subject to export control. Here one of the guest researchers installed a program that gave him remote access to data from the system.

METHODS – WHICH ARE GENERALLY COMBINED

Some methods for collection of knowledge, technology and products are illegal, while others are grey-zone methods or even legal. Still, they may potentially be problematic, and therefore they require attention.

FINANCIAL METHODS

- Scholarships and grants that may involve problematic requirements or self-censorship
- Retention of funds or threats to this effect
- Investment in projects with access to knowledge etc.
- Acquisition of products without disclosure of the real end user
- Bribery

METHODS TARGETING INDIVIDUALS

- Recruitment of students and lecturers for posts abroad in order to collect know-how.
- Recruitment of students and lecturers, for instance for espionage purposes.
- Elicitation, which means luring individuals into providing information through psychological manipulation. Generally, the target person is ignorant of the elicitation performed.
- Deployment of intelligence officers who work under cover as, for instance, researchers, students or investors.
- Blackmail, threats and coercion.

DIGITAL METHODS

- Open media searches for information that may pave the way for elicitation.
- Influence campaigns to change viewpoints, for instance in respect of a foreign state.
- Cyberattacks

PHYSICAL METHODS

- Surveillance
- Theft and burglary

Ten security tips

1. Beware of the threat
A precondition for protecting your research is that you are aware of the espionage threat and the methods used. This way, you may consider the threat in the light of the values, for instance data and technologies, that need protection – see the next tip. On this basis, it will be possible for you to ensure that your security procedures and initiatives are at the desired level. Furthermore, it is important to make the espionage threat known, in order to create consensus on joint efforts. We advise you to read the threat assessments published by PET on a regular basis.

2. Assess the value
You, as the staff of, for instance, a research institution or a high-tech company are the best to assess the value and possible applications of a research project, a technology or a product. You should therefore consider whether research results, new technologies etc. are of interest due to their commercial value, are related to security and defence technologies or have a dual-use purpose etc. In short, you should consider whether there are information and data that you cannot "afford" to lose. Based on your assessment of the value, you can decide to whom you will give access, both physically and electronically. Reference is made to the sections "Exposed research areas" and "How exposed are you?" on pages 7 and 12.

3. Know relevant legislation
The EU has classified a high number of products and technologies as critical, and therefore they are subject to export control. It is important to bear in mind that legislation applies to both physical products and knowledge transfer. Further, legislation on foreign direct investments has been laid down to prevent that such investments represent a threat to national security. See page 8.

4. Know your international partners
Make a thorough background check of your international partners. Does the research institution or company appear

legitimate? Is it financed by, or does it cooperate with, the military institutions of the country? Does your partner have a set of values that resonate with your organization? Always weigh the value of a partnership against the potential risk and delimit what you want to share. Sign a partnership agreement in order to have clear guidelines for the cooperation.

5. Take good care of your employees and colleagues

When you recruit new employees, it is a good idea to run a background check to verify that their CVs are legitimate. Check references and assess whether the stated publications are real. Also check whether there are matters of concern in relation to the values and interests of your organization.

Job satisfaction is generally important – also from a security perspective. Work pressure and job dissatisfaction can lead to errors that may result in security vulnerabilities. In a worst-case scenario, job dissatisfaction may cause an otherwise loyal employee or colleague to become the source of a rival or a for-

eign intelligence service. You should also be aware of the risk that foreign employees or colleagues may be under pressure from an intelligence service in their native countries.

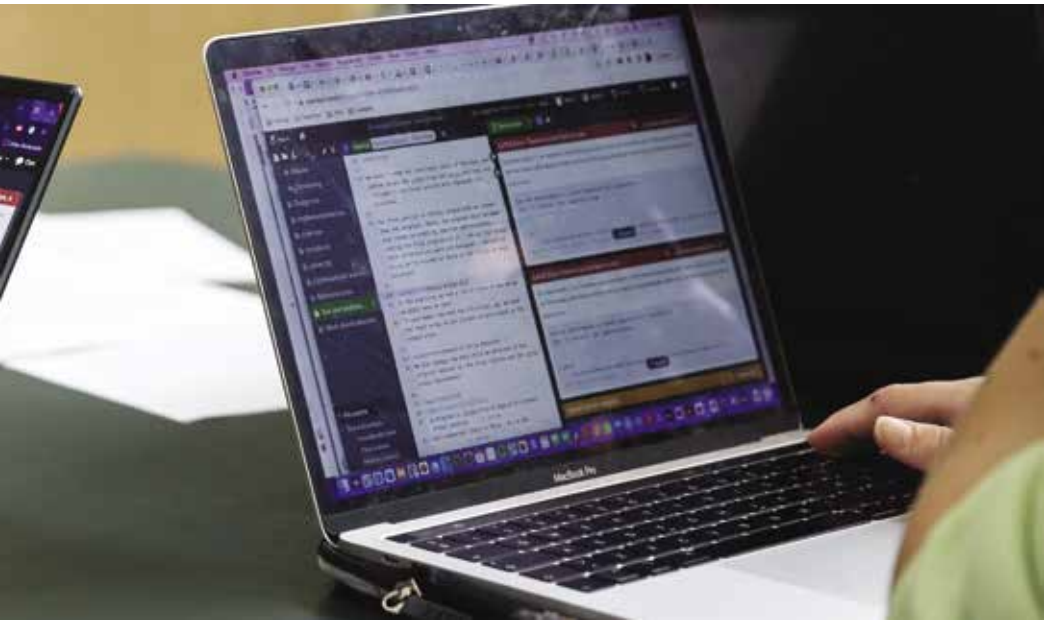
Consider which access each person should have to sensitive knowledge, technology and products – also in the period before and after the expiry of a contract. Reference is made to the PET publication "Take good care of your employees".

6. Focus on IT security

There is both a technical and a human side to IT security. The technical side includes various procedures and initiatives to improve the security level, for instance the installation of an effective security package with an antivirus program, a spam filter and access via VPN. Keep devices and software up to date to ensure you always have the latest security upgrades.

To this should be added the human side, your behaviour. Your protection will be better if:

- You have a clear division between your work and your personal life, which means that you do not use your private email address or mobile



phone at work. You should lock the screen of all equipment when you leave it in order to avoid unauthorized use during a brief moment of inattentiveness.

- You check your privacy settings on social media and consider which personal information you want to display. Social media information may be used against you or your colleagues via spear phishing.

- You never click on attachments or links if you do not know for certain that the source is reliable.

- You do not apply used USB sticks unless you trust the individual or the company providing them. USB sticks may contain malware enabling someone to access your computer.

For further IT security tips, visit the website *www.cfcs.dk/en/*

7. Focus on physical security

Improve your physical security in order to reduce the risk that knowledge, technology and products are stolen. Many measures must be introduced centrally, for example access control, alarms and surveillance.

But every one of you can also make a difference:

- If you use access codes, protect them to prevent others from seeing them.

- Your ID card should be visible when at work. This reduces the risk of tailgating, which means that an individual without an ID card latches on to somebody having one, thus gaining unauthorized access. Do not show your ID card when it is not relevant, for instance when going to and from work.

- Obscure the view into the premises. Set up your workstation so that screens, whiteboards etc. face away from windows, for example. Alternatively, use curtains/blinds as required.

- Be aware of your physical surroundings – are there any indications of attempted forced entry?

- Be aware of compromised physical security measures such as security doors that have been wedged open.

- Implement and observe procedures for secure storage. If you have a cabi-

net with a code, make sure others do not see the code.

- Implement and observe a closing procedure. For example, make sure that all windows, doors and cabinets are closed when leaving a room.

- Implement and observe procedures for the secure disposal of documents etc.; use a shredder, for instance.

8. Set the framework for visitors

Problematic scenarios may arise in connection with foreign visitors. Prior to the visit, you should decide which information you will share with your guests, and in particular which information you will not share. Be aware of any last-minute changes to the list of participants. Check the premises prior to the visit to ensure that there is no sensitive information lying around in the visitors' area.

During the visit, you should observe whether your guests behave in an unusual manner. Do they photograph or film profusely? Are there any participants who do not stay with the group, but instead disappear and show up in unexpected places? Do some participants ask questions that are not related to the purpose of the visit? Do not allow foreign software or hardware to be installed – this also applies in relation to presentations. It is better if visitors connect their own computers to a projector rather than using a USB stick in your computers. In order to avoid critical situations, you should ensure that an adequate number of colleagues accompany and monitor your guests.

You are most welcome to inform PET in advance of a visit which is of national security interest because of the delegation members and the purpose of the visit.

9. Be careful when travelling

It is worthwhile to focus on security in connection with trips, conferences and stays abroad, as you are generally more exposed to theft, cyberthreats etc. abroad. Prior to departure, you should therefore assess how much sensitive information you need to bring with you – and you should of course have a backup. It may also be a good idea to draw up a list of the documents and data you bring with you. This way, you will have an overview of the information that may have been accessed without authorization.

You should be aware of individuals whom you "happen to" meet and who

are particularly interested in your work or in you as a private individual. It may be a method used by a foreign intelligence service to collect information. If you stay at a hotel, you should be aware that staff etc. are likely to be able to access the safe.

Wi-Fi abroad may be monitored, and therefore you should not access sensitive material via this connection. You should use a VPN service or mobile data. Keep an eye on your equipment, do not lend it to anybody and use your own equipment only.

You should also turn off Bluetooth on all your devices. It is very common to receive USB sticks at conferences. You should be aware that they may contain malware – see the tip on IT security on page 18.

The best procedure is to bring borrowed equipment on your trips. Alternatively, it may be a good idea to delete as much as possible, for instance call history, messages etc., from your own equipment. When home again, you may consider changing the passwords you have used on your trip.

10. Report what you see

– do you have any concerns or has the damage already been done?

It is important to have a good security culture allowing employees to discuss security concerns, such as the suspicious behaviour of a partner or a visitor.

Depending on how your institution is organized, you may report your concern or suspicion to your superior, top management, the head of security or the relevant authorities. PET is able to provide specific advice on the implementation of preventive and security-related initiatives or procedures – write to *civ@pet.dk*. If you have any concerns or have observed something you would like to share, please do so using the contact form at the website *www.pet.dk*.

In case of a cyber-related incident, please contact both the Centre for Cyber Security (CFCS) and PET.

See contact details on page 23.

Contact

DANISH SECURITY AND INTELLIGENCE SERVICE (PET)
Klausdalsbrovej 1
DK-2860 Søborg
Tel. +45 45 15 90 07
Email: *pet@politi.dk*
www.pet.dk/en

CENTRE FOR CYBER SECURITY,
DANISH DEFENCE INTELLIGENCE SERVICE
Postal address: Kastellet 30
Visiting address: Holsteinsgade 63
DK-2100 Copenhagen Ø
Tel. +45 33 32 55 80
Email: *cfcs@cfcs.dk*
www.cfcs.dk/en

DANISH AGENCY FOR HIGHER EDUCATION
AND SCIENCE
Haraldsgade 53
DK-2100 Copenhagen Ø
Tel. +45 72 31 78 00
Email: *ufs@ufm.dk*
www.ufm.dk/en

DANISH BUSINESS AUTHORITY
Langelinie Allé 17
DK-2100 Copenhagen Ø
Tel. +45 35 29 10 00
Email: *erst@erst.dk*
www.danishbusinessauthority.dk

Published: August 2023
Graphic design: Permild & Ko
Photos:
Pages 2, 17, 18-19, 20: Ditte Valente
Pages 1, 4-5, 9, 10-11, 13: Adobe Stock

Danish Business Authority

PET

Danish Agency for Higher Education and Science