



CFPAEUROPE®

Guidelines

Protection of Business Intelligence

~~Company heads, the~~The sustainability and development of ~~your~~ business requires s the management and protection- of ~~your~~ critical information



CFPA-E®-Guidelines xxx : 2016/S



Foreword

The Security Commission of the Confederation of Fire Protection Association Europe (CFPA-E) ~~has developed~~ develops common guidelines in order to achieve similar interpretation in the European countries and to give examples of acceptable solutions, concepts and models. The CFPA-E ~~has the aims~~ aim to facilitate and support fire protection and security aspects across Europe.

The market imposes new demands for quality and safety. Today fire protection and security aspects form an integral part of a modern strategy for survival and competitiveness.

The guidelines are ~~primarily~~ intended for all for the interested parties as well as the general public. ~~They are also aimed at~~ Interested parties include the rescue services, consultants, safety companies and the like so that, in the course of their work, they may be able to help increase fire safety and security in society.

These guidelines have been compiled by the Guidelines Commission and are adopted by all fire associations in the CFPA-E.

These guidelines reflect best practice developed by the countries of CFPA-E. Where the guidelines and national requirements conflict, national requirements must apply.

This document is based on xxx xxx xxx xxx xxx xxx x xxx xxx xxx xx xxx and was kindly supported by xxx xxx xxx xxx xxx xxx xxx xxx xxx.

~~Company heads~~ Chief Executives and Managers, Entrepreneurs



In a world where competition is heightened, competitiveness determines the survival of a company. The protection of know-how and information then becomes a vital issue for its sustainability.

nes the survival of a company. The protection of know-how and information then becomes a vital issue for its sustainability.

From company head to ~~workman employee, from senior executive to foreman~~, everyone is affected by what is commonly called "business intelligence".

This means shedding fresh light on the company, its critical information, and its environment, to anticipate challenges and adapt its behaviour accordingly.

More than a public policy, business intelligence is an approach to help you identify opportunities and

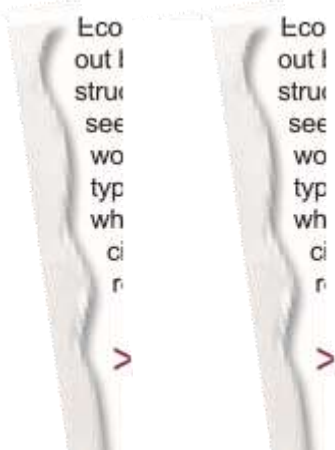
~~deciding-critical~~ factors for success, anticipate threats, prevent risks, secure information, and act on and influence the outside world to preserve the competitiveness of your business. We propose you implement this method with the help of this guide.

In it, you will find help in diagnosing the vulnerabilities of your business, as well as the critical actions to take to protect and defend its interests and ensure its future development.

Don't forget that

THE BUSINESS SECURITY
of your business
is YOUR FUTURE!

2 It could happen to you!



Economic Business interference is frequently carried out by people authorised to enter research structures or businesses. It is common to see motivated trainees going back to the workplace outside normal hours.

These types of behaviour can be a warning sign which should attract the attention of officials in the establishment. They must be reported to the service.

>>> **What to do in case of an incident?**

If the trainee's behaviour **conflicts with national is against the rules of law**, particularly in the case of a computer intrusion attempt or a theft of samples, a **complaint should** be made to the relevant services.

Dishonest trainee

A foreign national working toward a PhD in a laboratory specialising in nanomaterials sent data relating to the research work carried out by the host organisation to his home university over the Internet.

This transfer of information was done informally outside of any cooperative work and without his superiors' knowledge.

Once informed of this situation, the laboratory decided not to make a complaint, but asked the person concerned to leave the facility.

Document monitoring is being performed to claim authorship of any work that is published by the university with which he interacted.

Inserting this key into a company computer would have made it possible to hack into the data, including administrator and user passwords.

>>> What to do?

Strictly control all company computer access by outside staff, ~~especially those of foreign nationality.~~

Only use storage methods (CD, USB keys) that have been checked by the IT department, especially if they were supplied to the company by visitors.

A seemingly "ordinary" crime might have an economic objective.

More than half of economic interference cases through attacks on computer systems consist of thefts of computers containing very sensitive information.

>>> What to do?

Do not leave your equipment unattended in an uncontrolled environment.

→Gh, bitte den roten Stempel in den Ausschnitten überall entfernen.

INDUSTRIAL ESPIONAGE ATTEMPT

During a visit to a manufacturing company in the aerospace sector, a member of a delegation from a foreign country asked to print a presentation which was on his USB key.

The representative of the manufacturing company visited asked his IT department to print it. The head of the IT department tested the key before authorising its connection to a company computer.

During the analysis of the USB key, a malware application was detected that automatically recovers data.

The IT manager informed the foreign delegate that it was impossible to print because there was a virus on the key. At the same time, the manufacturing company warned other companies due to be visited by the delegation of the incident.

ILLUSTRATION OF ECONOMIC INTERFERENCE DETECTED BY THE DCRI

PROTECTION OF SENSITIVE DATA

An SME specialised in the creation of software to help with decision-making for the management of industrial risks sent a geophysical engineer to represent it at an international seminar. He presented his company's activities, and underlined their expertise in the very sensitive area of industrial environmental risk management. Forgetting all basic security rules, he left his laptop in the conference room during the lunch break. The room contained many laptops, but only geophysicist's was stolen. The device contained strategic information for the company: client files, confidential business contracts, carbon audits and audit reports from several client companies, and confidential information on the management of industrial risks in the energy and transport sectors.

ILLUSTRATION OF ECONOMIC INTERFERENCE DETECTED BY THE DCRI

2 It

could happen to you!

3



Protection of your sensitive and strategic information **GET ORGANISED**

Define the company's business security policy.

Get organised

Appoint a security officer, whose tasks include:

- ↪ report to a member of the management or executive committee so that his/her activities are effective.
- ↪ define and ensure the proper implementation of the company's security policies.
- ↪ play a role that is: < →Gh, von "preventive" bis "instructive" bitte einrücken>
- ↪ preventive - they must therefore be consulted ahead of major projects,
- ↪ advisory - they contribute to business development by helping in management decision-making and securing operations,
- ↪ informational,
- ↪ instructive,
- ↪ be the contact person for authorities.

Identify and classify items to be protected to avoid intentional or unintentional leaks:

*Intentional or unintentional leaks of sensitive information often lead to market losses or damage to the company image. **THIS AFFECTS THE SUSTAINABILITY OF THE***

- Sensitive data,
- Strategic information,
- Sensitive equipment and facilities.

COMPANY.

Regularly educate staff:

- Through the security officer,
- Through national authorities
- Through internal/external experts (e.g. insurance companies) <-> Gh Leerzeichen hinter "Access:"
Bild tauschen -> Bedien-Paneel >



Access **SECURE IT**

The site, sensitive facilities:

- Secure the site passively (walls, fences) and actively (access codes, deterrent lighting),
- Install surveillance products and services (e.g. alarms, remote surveillance, security guards), adapted to your company.
- Always report any intrusion, theft or attempted break-ing and entering to the relevant forces (police).

~~Moving around inside the~~ Controlling access site:

- Implement a policy for the management of visitors (e.g. should they be accompanied)
- Ensure that sensitive information and similar material is available only to authorised personal.
- Put in place a controlled access system to offices and premises containing sensitive information and materials,
- Differentiate employees from external visitors with badges (trainees, temporary workers, contractors, visitors, etc.)
- ~~Implement an policy for the management of visitors (e.g. should they be accompanied)~~

4

Secure your IT system

RISK: Theft, loss of sensitive information, contamination by computer viruses, unavailability of the IT system



IT organisation **DETAIL IT**

•

- Designate a network administrator responsible for computer security.
- Establish an IT ~~charter~~ policy to which all staff are committed. Annually ~~educate~~ reinforce with users ~~the~~ about computer security rules (security policy compliance, always locking the computer when it is not in use, etc.).
- Define a software update policy.
- ~~Create~~ Establish procedures for ~~change of users~~ the arrival and departure of users (staff, trainees...), e.g. joining or leaving the company.



Internal network: **PROTECT IT FROM INTERNET RISKS**

•

- Use a ~~regularly~~ continuously updated anti-virus software and a firewall.
- When ~~never~~ possible, ~~deactivate~~ exclude from the shared network ~~from~~ computers ~~used to~~ capable of ~~accessing~~ the Internet.
- Avoid the use of wireless technologies (Wifi). If its use is essential, separate Wifi network access from the rest of the IT system and use Wifi security ~~systems~~ measures as ~~an~~ encryption, strong passwords, virtual private networks (VPN), etc.

- Prohibit the use of the same password for professional and personal applications.
- Vary passwords between applications.



Risks related to **MANAGE IT**

- Protect user accounts with an individual password (minimum 10 characters

4

Secure your IT system

- of different types) that is secret and changed regularly. Delete default authentication data.
- Use a phonic method or first letters for the passwords.
(e.g. "I bought eight CDs for one hundred euro this afternoon" will become "ibawt8CDdisan"; The quote "a bird in the hand is worth two in the bush" will produce "1bithiw2itb").
- Only use storage methods (CD, USB key) previously checked by the IT service, especially if these storage methods have been provided by visitors to the company.
- Beware of suspicious emails or those from unknown senders. Do not open them. <->gh: nächsten Punkt „Delete...“ hier anhängen>
- Delete them permanently.
- Limit the number of backups to the necessary and store them securely.
- Do not install any software without making a preliminary analysis of its characteristics.
- Prohibit Pay attention to** the connection of personal equipment (smartphones, tablets, etc.) to the company IT system. If remote working is necessary, provide the necessary professional means to do this.
- Extract and store the hard drive of the printer or photocopier in the event of repairs outside the company or in the case of renewation-maintaining or scrapping of the machine.
- Take care of an effective destruction of every hard drive of any device no longer in use.

- Arrange screens-monitors, IT screens, etc. with caution to ensure confidentiality when entry is permitted (visits, traineeships, deliveries, cleaning, etc.).

5

Manage the human

factor

RISK:

Dissemination of information, leakage, poaching, corruption, enticement



Sensitive information ACT

Include a confidentiality clause in all employment contracts.

- List the premises containing strategic information; provide access on a need-to-know basis only.
- Pay particular attention to external service providers (cleaning, maintenance, partner companies, suppliers, etc.).
- Educate your employees as to how to protect strategic information.
- Install good practices: storage of sensitive documents under lock and key (lunch break, evening, during office cleaning), use of the shredder, etc.
- Educate your employees as to the proper use of social networks (Facebook, Twitter, Dailymotion, YouTube, etc.)



Trainees and temporary workers:
MONITOR THEM <change Picture ; 2

Personen am Tisch>

Before the traineeship or temporary work period

5

Manage the human

factor

- Study ~~the individuals'~~ CV. Check with the educational institute or the last training organisation or the last employer.
- Define the contents of the training course or temporary assignment by identifying the critical aspects of the planned work as regards your strategic information, documents, facilities or materials.
- Designate a staff member responsible for overseeing the trainee or temporary worker.
- Draw up a specific ad hoc contract among between the company, the trainee/temporary worker and his/her organisation. This shall specify the IT restrictions, security measures, confidentiality clause, and limits of dissemination of reports written by trainees of the probationary report and documents outside of the company.⁵⁷
- Inform management and, relevant staff and the trainee/temporary worker beforehand of which areas of information and premises are accessible to trainees/temporary workers.
 - ~~-are authorised, which premises are accessible, and what the conditions are for using the photocopier,~~
 - ~~=IT tools, and personal equipment (smartphones, USB keys, etc.)~~
- Inform the trainee/temporary worker beforehand of which areas of information and premises are accessible, and what the conditions are for

use any device for making copies as well as using IT tools, and any personal equipment (smartphones, USB keys, etc.)

During the traineeship or temporary work period



Visitors **ACCOMPANY THEM**

Before the visit

- Do not allow trainees or temporary workers to access sensitive equipment or materials alone, nor any documents or information of a strategic nature, particularly via uncontrolled access to computer systems.
 - Be aware of bonds that may develop between the trainee or the temporary workers and staff members.

After the traineeship or temporary work period

- Retrieve badges at the end of the work period. Change the access codes.
 - Study the trainee's work. Check that no data deemed to be sensitive have been disclosed.
 - Give the traineeship report to the security officer.

~~Find out the~~ Establish the identity and position of the visitors.

Ensure the reason for the visit matches the position of the visitors. **During the visit**

Keep a record of visits. Provide a specific badge.

Make visitors of sensitive areas leave all electronic devices (e.g. mobile phones and photographic equipment) at a designated place (e.g. the reception).

Accompany visitors at all times in the company, even into the most incongruous places.

Establish a visit program ~~with the~~ clarifying content of presentations and identify ~~ing~~ information that should not to be disclosed. <hochstufen> Define the visit route, avoiding sensitive areas in the company.

Prevent ~~Prohibit~~ contact with employees not previously approached to be their contacts.

Prevent the same questions from being asked ~~of to~~ different employees.

Do not answer any relevant questions outside the originally planned subject of the visit.

Do not allow any photos, sound recordings or sampling to be taken/made except if authorised.



5

Manage the human

factor



Collaboration with partners **BE CAREFUL**

Many developments of new processes, products, services, etc. are the product of collaboration among several complementary companies (co-design) or

between companies and research institutions or technical centres.

The most innovative developments often require the skills of suppliers, complementary businesses, clients, public and private laboratories, technical centres, or competitiveness business development centres, national or international.

When this type of organisation is necessary for the creation of new solutions, it is particularly difficult to ensure satisfactory protection of the interests of each partner.

Before the project:

- Precisely Carefully analyse the objectives, issues and risks related to the collaborative project for the company.
- Clearly identify and define the position of each of the partners in the project:
 - Who does what?
 - Who accesses what type of information? Who is responsible for what?
 - What are the objectives and the expected return of each partner?
 - Are there any potential competitors?
 - Are there any partners who already have close links with some competitors?
- Identify by name the people who will be involved in various parts of the project. Find out their backgrounds, their work and their past or present links with potential competitors.
- Build a partnership agreement or consortium clearly stating the role and operating limits of each of the structures involved in the project and how the intellectual property of the results will be distributed (patents, licenses, scientific publications, etc.).
- Require confidentiality agreements (from the people involved) and exclusivity agreements (from the structures) on the technologies developed. The use of a specialised lawyer is highly recommended.

During the project:

- Use a secure collaborative platform, providing access only for each previously identified person to the information that they are authorised to see.
- Hold regular meetings with the partners involved. Examine the tools and means to ensure the security of the knowledge or information that they hold.
- Thoroughly monitor the information published by the partners on the project in question and/or on related projects (communication campaigns, press articles, scientific publications, etc.).
- Organise, re-evaluate, and secure the distribution of intellectual and industrial property rights for each innovation.
- Equip yourself with tools for the traceability of work carried out (such as laboratory specifications kept individually by each partner). Each person can thus prove their authorship or that they are the inventor of the new elements they have provided to the project.

6

Protect information

outside of the company

RISK:

Dissemination of information through negligence



Public place **ESTABLISH GUIDELINES**

- Avoid bringing up professional topics verbally or at the telephone (train, plane, restaurant, etc.)
- Monitor your work equipment (briefcase, documents, computer, telephone).
- Avoid using the communication equipment (computers, telephone, etc.) available in hotels.
- Be aware of the risks of using internet access available in hotels and other public places without proper security means. <Zeilensprung>
- - Do not leave any media containing sensitive data in hotel rooms (even in the hotel safe).
- If you must work in public places, disable the Wifi and install a filter on your computer screen.



Trips abroad: **FOLLOW CERTAIN BEHAVIOURAL RULES**

Daily life

- Avoid travelling alone to ~~sensitive~~ high risk locations.
- Refuse any valuable gifts.
- Be careful in terms of relations outside work.

Professional life

- Select the information to be transported.
- Report your presence to your official national authorities, if advised.
- Be aware of the risk of giving away confidential information while ~~Avoid~~ reading or working on public transport.
- Never leave a computer, mobile phone or confidential material in a room.
- Do not talk about sensitive matters over the telephone.
- Be careful about photocopying on site.
- Be discreet about your comings and goings.
- On your return inform management on any suspicious incidents.

6

Protect information

outside of the company



TRADE SHOW

Before the show ~~anticipate~~

- Define the objectives of your participation (prospecting, finding partners, launching a product, etc.)
 - Target stands. Prepare a visit plan.
- <"VdS-Bild" mit CFPA-Topic neu erstellen>



- List the information that you want to gather, including the level of detail and the way of obtaining it (brochure, sample, etc.)
- Define the information that can and cannot be given out at the show.
- Prepare answers to sensitive subjects (know-how, innovation, etc.)

During the show: collect

- Do research. Collect information (customer expectations, discontent regarding a product, etc.).
- Get professionals, not “hostesses”, to present your technical products.
- Listen and have a conversation before launching into your demos.
- Stay aware during your conversations.
 - Be careful of visitors who may seek for confidential information of your company.
 - Monitor at risk materials. Keep the number of sensitive documents or materials to a minimum.



After the show: evaluate

- At closing time, empty the stand and check all materials and documents.
- Study reactions in the press and on the Internet.
- Analyse the documentation collected.
- Organise a debriefing session.
- Draw up a summary document with new contacts, surprising facts and action to be taken.

7

Protect your assets and

your know-how

RISK:



Industrial property **ORGANISE IT**

- Protect your technical or aesthetic creations with industrial property titles (patents, trademarks, designs, models, etc.). They allow you to maintain your legitimate rights, keep a monopoly on to these creations.
- For partnerships, draw up confidentiality agreements. Establish ways to prove the date on which the innovations were implemented.
- Keep absolute secrecy before filing the patent application. Any disclosure is likely to destroy the condition of novelty and thus be an obstacle to filing a patent or a reason for its cancellation.
- Make sure there is maximum awareness within the company of the necessity of protecting your intellectual property rights (IPR) and of the importance of confidentiality.
- Be sure to address invention and creation activities in the employment contracts of the employees who will participate in the development of your innovations. If this is not done, the employee could claim ownership of the invention.



Patent, trademark, logo: **MONITOR YOURS AND YOUR COMPETITORS'**

- Monitor your patents and trademarks and those of your competitors to ensure that no one uses your invention without authorisation.
- In particular, use patent information sources freely accessible on the Internet (www.epo.org) so as, for example, to see what your competitors have filed: have they filed patents on technologies that you have already protected?
- Try to identify signs of counterfeiting as early as possible (reduced activity due to loss of markets, unexplained deterioration of reputation, etc.).

7

Protect your assets and your know-how

Have you identified a counterfeiter?

You should immediately challenge the counterfeiter. Start by negotiating amicably. Presentation of your property title may put an end to any hint of counterfeiting or lead to an agreement between the parties (a license agreement, for example). If the counterfeiter persists, request the intervention of specialised services (customs, industrial property consultants, specialised lawyers, etc.) that will help you enforce your rights.

↳ For any questions, please contact your national patent office or institution in charge of dealing with counterfeiters. <Anstrich streichen>

Links on organisations:

INPI: <https://www.inpi.fr>

OHIM: <https://oami.europa.eu>

European Consumer Center: <http://www.eu-verbraucher.de/en/home/>

European Union Intellectual Property Office: <https://www.euipo.europa.eu>



Specific know-how linked to an employee: **ANTICIPATE**

↳ Organise the departure of any staff member assigned to a strategic post in the company (retirement, resignation, headhunting, illness, etc.) while preserving their know-how (training of another member of staff) and through precautionary measures, so as to prevent disclosure (prior signature of a non-competition clause).

8

Monitor your

environment

RISK:

DisparagementDenigration, defamation, trademark infringement, loss of markets



E-REPUTATION:

Do you know what the Internet says about you?

- Monitor your image on the Internet. Study the information on your company and your products, and any information found by your customers (site, forum, blog, social networks, etc.)
- Answer reviews (positive and negative). Show your interest in questions and comments made by customers. Manage the information provided on your products.
- Protect your online reputation. Establish crisis communication and continuity plans in case of damage to the company image.



STRATEGIC MONITORING Do you know your competitors as well as they know you?

- Define the strategic issues for your company. **Only mFocus oneniter** those who are truly important for your business.
 - Is it better to know your customers, **your partners**, your competitors, or your suppliers?
 - Is it more relevant to detect new technologies or market trends?
- Analyse your strengths and weaknesses.
- Discover development opportunities or threats to your business.

- Develop a culture of information_gathering among your employees (experience feedback, discovery reports, ability for self_criticism, etc.).
- Do not hesitate to contact the consular network (chamber of commerce Enterprise Europe Network, etc.), professional structures (e.g. branch organisations), or technical centres.
 - They organise technology, materials, markets, regulatory monitoring, etc.
 - They will support you in developing your innovation and competitiveness.

9 Further information

Links, additional information, ...

xxxxxx

THE BUSINESS SECURITY
of your business
is YOUR FUTURE!



CFPA EUROPE®