BASF
We create chemistry

Be Secure

Information Protection and Cyber Security

Third Party Guide

Checklist: Aid for third parties when working with BASF

Checklist
for information protection and cyber security

This checklist will help third parties working with BASF take precautions and implement measures that will prevent loss and unauthorized access to information deemed worthy of protecting.

Experience has shown that the questions addressed in this checklist constitute essential elements that play a vital part in the practical implementation of information protection that is effective at all times.

This checklist is not exclusive. It is the responsibility of the third party to act responsibly and determine which specific measures and precautions get applied in each case. Instead of relying purely on technical solutions, common sense must always occur.

Information protection and cyber security
E-mail: be-secure@basf.com
Issue date: October 2019

Fundamental questions

- Is the group of persons who should be authorized to handle information deemed worthy of protection („authorized persons“) defined?
- Have the authorized persons been properly committed to confidentiality?
- Have the authorized persons been instructed in information protection and cybersecurity?
- Do regular checks take place to ensure that the specifications regarding information protection remain adequately observed?
- Are the type and extent of the measures implemented for information protection documented in a verifiable manner?
- When handling personal data, are you compliant with GDPR and the Data Protection Regulations in your state/region?
- Are standards observed for software and hardware?

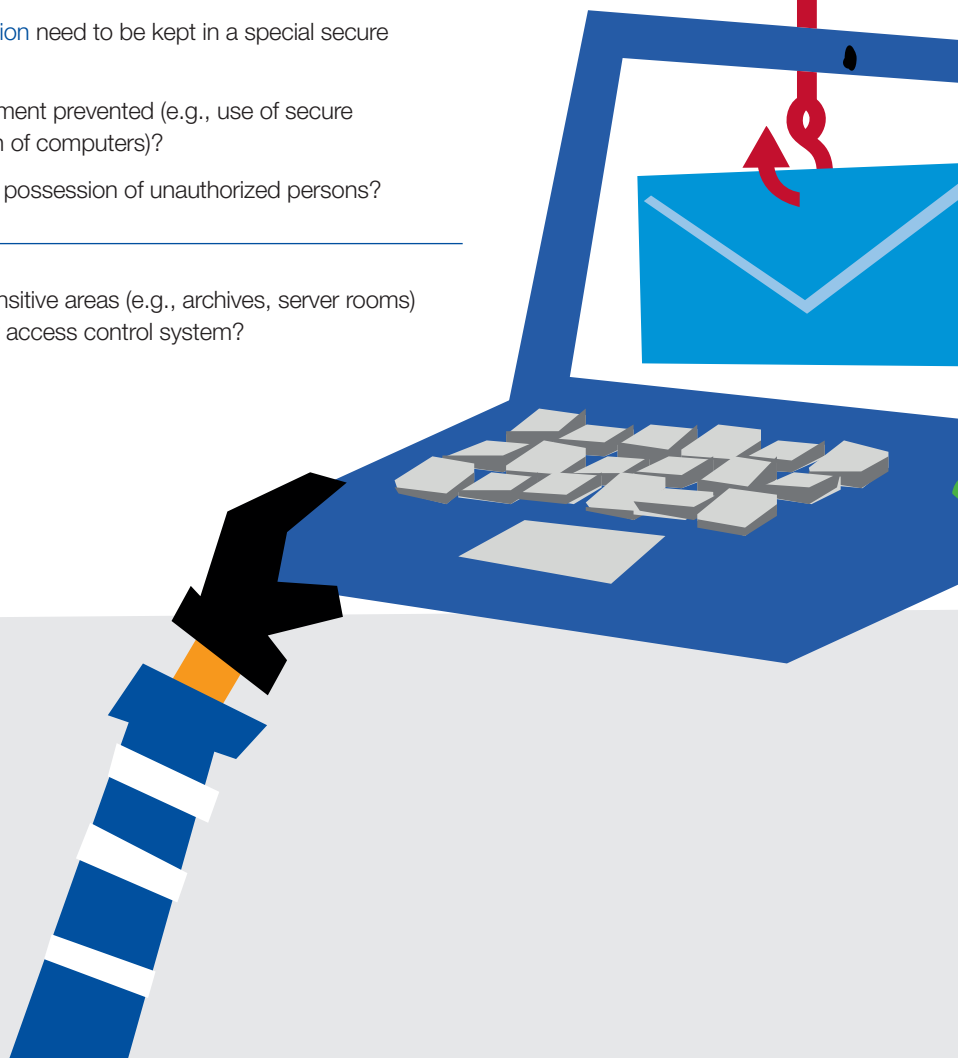
Measures to protect against unauthorized access to information deemed worthy of protection

Is access to information deemed worthy of protection effectively restricted to the authorized persons at all times, and are the access rights regularly checked and - where required - adapted?

Are suitable protection measures for when authorized persons are not present implemented?

- Is it ensured that if no authorized persons are present, nobody who is not authorized to have access to the information deemed worthy of protection („unauthorized persons“) can be present in the room? For example, are rooms always cleaned in the presence of an authorized person?
- Are rooms, cabinets, and other repositories of information deemed worthy of protection locked if no authorized person is present?
- Does information worthy of protection need to be kept in a special secure repository?
- Is unauthorized access to IT equipment prevented (e.g., use of secure passwords, locks, or the shutdown of computers)?
- Is it ensured that no keys enter the possession of unauthorized persons?

Is it necessary to protect particularly sensitive areas (e.g., archives, server rooms) by installing an anti-theft system and/or access control system?



Measures to protect against unauthorized access to information deemed worthy of protection

Secure passwords for systems containing information deemed worthy of protection:

- Are the chosen passwords sufficiently complex (e.g., are they at least eight characters long and contain at least one uppercase letter, one lowercase letter, one special character, and one number), and are they changed regularly?
- Is it ensured that passwords are not passed on to third parties and, if written down, are not kept in a place that is freely accessible (for example, stored in a sealed envelope with the date and a signature on the flap in a safe)?
- Is two-factor authentication used?

Are physical internal mailboxes secured to ensure that unauthorized persons cannot access information deemed worthy of protection that is inside them?

Is information deemed worthy of protection that is saved on data carriers (notebooks, tablets, smartphones, hard drives, servers, CD-ROMs, USB sticks, etc.) adequately secured (e.g., utilizing state-of-the-art encryption)?

Are effective measures implemented for the transmission (e.g., by e-mail, phone, video conference, post) of information deemed worthy of protection? (e.g., encryption of communication connection, distribution of information deemed worthy of protection on different communication carriers)

Measures to protect against unauthorized access to information deemed worthy of protection

Are printers and copiers configured securely? Is it ensured that the reproduction of print and copy jobs that contain information deemed worthy of protection is prevented? Is it ensured that originals, printouts, and copies are removed immediately and not left in the printer/copier/fax machine (using a PIN function if necessary)?

- Are meetings conducted in a way that ensures that the disclosure of information deemed worthy of protection to unauthorized persons is prevented?
- Is it ensured that information outside the room (e.g. signage) does not enable the identification of the confidential content of the meeting?
- Is eavesdropping from outside (corridor, adjoining rooms, windows, doors) effectively prevented?
- Is it ensured that nobody can catch sight of the meeting/presentation materials from outside (e.g. are curtains closed)?
- Is it ensured that no documents, equipment, or presentation media (flipchart sheets, overhead slides, whiteboard texts) are left behind in the room after the end of the meeting?
- Is it ensured that the meeting room cannot be accessed by unauthorized persons when empty (e.g. during breaks)?

Qualified disposal of information deemed worthy of protection

Is the disposal or deletion of information deemed worthy of protection qualified and secure?

- Are paper cross-cut shredders with a maximum particle size of 160mm² used for disposing of such information?
- If collection containers are used: Are the collection containers locked? Are they positioned securely? Is the disposal process sufficiently secure? Is DIN 66399 observed (min. safety level 4)?

Is information deemed worthy of protection on rewritable electronic data carriers (USB sticks, memory cards, CDs/DVDs, hard drives etc.) fully and securely deleted before the data carriers are reused/passed on to third parties?

Information protection aspects during trips and in public

- Before trips, does a check take place to ensure that information deemed worthy of protection is required to be taken along?
- Is it ensured that unauthorized persons are prevented from accessing information deemed worthy of protection during transport (e.g. files and notebooks)?
- Are files and notebooks etc. always kept in sight during transport?
- Are unauthorized persons prevented from listening in on conversations or telephone calls?
- Are notebooks attached to a fixed structure with a suitable cable lock so that they cannot be taken away by unauthorized persons?
- Is information deemed worthy of protection prevented from being published on Internet platforms and social media?
- When rented/leased vehicles are returned, is it ensured that data does not remain in the memory of the telephone/navigation system and that no documents are left behind?

Personal notes

Personal notes

be-secure.basf.net
Issue date: October 2019