Directive - Information security

Responsible: Chief Information Security Officer (CISO)

Note: This document is a deeple.com translation of version 4.1 of the leading document Richtlinie - Informationssicherheit. Therefore, approval by the responsible person is not necessary. Approval is granted by the Managementsysteme (MGA-MS) department.

This policy serves to raise employee awareness of information security issues.
All FP Group employees are responsible for implementing this policy. Violations may result in disciplinary action.

FP Security Information

Information security means protecting information from a variety of threats. It plays a key role in:

- maintaining business operations,
- complying with legal requirements,
- protecting the company's reputation,
- protecting personal data.

Any occurrence of malware or suspicion of a phishing email must be reported immediately. Do not forward the untrustworthy email, but send it as an attachment to a new email to the IT Service Desk (servicedesk@francotyp.com) so that it can be analysed. The IT Service Desk will then decide on how to proceed.
Would you like to report irregularities/problems or do you have questions about information security or the protection of personal data? Please contact **iso@francotyp.com.**

HANDLING DOCUMENTS AND DATA

CONFIDENTIALITY:

Ensure that information only ends up in authorised hands AND is only used for the purpose for which it was collected.

Francotyp-Postalia

AVAILABILITY:

Ensure that equipment, data and processing methods (electronic, manual) are provided in a functioning and timely manner.

INTEGRITY:

Ensure that data requiring protection remains intact and complete AND cannot be distorted during processing.

AUTHENTICITY:

Ensure that the originator (individuals and echnology/programmes) and genuineness of information can be reliably identified and reviewed.

Information must be handled in line with its need to be protected throughout its life cycle (until it is securely destroyed). A secrecy obligation exists beyond the contractual relationship.

SAVING AND TRANSFERRING DATA

In general, all company data must be stored on centrally managed and secured servers. If mobile data carriers are used for specific purposes, they must be kept in an access-protected manner. Data may only be transferred to third parties if they are authorised to access the data. The transmission path must be protected.

COPYING, SCANNING AND PRINTING

Printouts sent to the printer must be collected immediately. Uncollected documents that cannot be assigned to an employee must be disposed of in the locked paper containers or document shredders provided in the copy rooms.

ACCESS CONTROL

Access to all rooms is regulated by a control system. Each employee may only enter the areas for which they have the appropriate access authorisation.
Be alert:
Close doors and speak to people you do not know. Accompany guests in the building and report any unusual occurrences or violations immediately!
Lock rooms and windows and always lock screens when you are the last person to leave a room, even if only for a very short period of time.

Francotyp-Postalia

ACCESS AND ADMISSION CONTROL

Whether in your own office or outside, make sure that only you have access to your data, computers, IT applications, storage locations and storage media. A user account is required to work with IT resources. This is set up by the IT department at the request of the supervisor. User accounts are protected by a password.
Passwords are strictly confidential and must be kept secret.
The user is responsible for all activities carried out with their user account!
To ensure that unauthorised persons **cannot access IT applications or data**, **lock** your screen even if you are only leaving your desk for a short time (**Windows key + L**).
Keep your workplace tidy and your surroundings clean. Only keep information at your workplace that is needed to complete the respective tasks. **Use the storage and locking systems provided** to prevent the availability, confidentiality and integrity of data from being negatively affected. If you plan to be absent (e.g. for long meetings, business trips, holidays, training courses), leave your workstation in such a way that no data carriers or documents requiring protection are left unlocked at your workstation. If you require additional storage space for this purpose, please contact your supervisor. **Every employee is obliged to leave their workstation tidy.**
Passwords must not be stored in plain view (e.g. on sticky notes on the monitor or in an easily guessable location). Use an encrypted password safe to store passwords.

INTERNET USE

Only the access routes provided for this purpose and equipped with appropriate protective devices (e.g. firewall) may be used to access the Internet.

INFORMATION IN CONVERSATION

Ensure that both direct and telephone conversations with business content take place without the involvement of unauthorised third parties.
Organisers of a meeting may classify it as strictly confidential and prohibit the use of mobile phones and tablets or any devices that can record or transmit conversations. This prohibition shall be explicitly stated in the meeting invitation. All employees must comply with this prohibition.

USE OF E-MAIL

- The email function may only be used for business purposes.

Francotyp-Postalia
Francotyp-Postalia

- Requests to forward warnings or calls to friends, acquaintances or colleagues must not be complied with under any circumstances.
- Before sending emails, always check the email addresses on the recipient list to ensure that the email will actually be received by the intended recipients.
- Emails that are no longer needed should be deleted regularly, unless there are retention periods.
- If you plan to be absent for a longer period of time, set up an automated email with an out-of-office message.
- Only file attachments that are expected and plausible may be opened.
- No FP emails may be forwarded to private or third-party email accounts.
- If it is possible to send and receive encrypted emails, this option should be used.
- When sending sensitive content (including content classified as confidential or strictly confidential) to external parties, suitable encryption must be used.
- Please pay special attention to emails with the note ATTENTION: This mail comes from an EXTERNAL sender - please take care when opening attachments and when dealing with LINKS.

CONTROL OF INFORMATION

The creator of information is responsible for ensuring that it is only made available to persons relevant to the purpose of the information.
They are responsible for classifying their information and must determine whether and how it must be labelled and treated accordingly.
Classification attributes: public, internal, confidential, strictly confidential.
If no classification is specified, the classification 'internal' automatically applies, i.e. internally available without restriction and may not be distributed publicly.

ON THE GO

The most common risk is still data loss via mobile phones, smartphones, USB sticks and notebooks.
Always keep an eye on the devices and documents entrusted to you and do not leave them unattended (even during customs checks). Use a privacy screen (notebook) when working outside the business premises.

Mobile data must be stored in encrypted form wherever possible. **A secure VPN connection must always be used outside the FP network.**
In the event of theft or suspected unauthorised access (including of the VPN token), the FP IT Service Desk must be informed immediately.

BUSINESS USE

IT systems provided by the employer (PC, notebook, smartphone, etc.) may only be used in accordance with the terms of use provided with the equipment.

PROTECTION OF PERSONAL DATA

You must:

- processed lawfully and in a manner that is understandable to the data subject (**lawfulness, good faith, transparency**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (**purpose limitation**);
- be adequate and relevant for the purpose and limited to what is necessary for the purposes of processing (**data minimisation**);
- be accurate and kept up to date (**accuracy**);
- be stored in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data are processed (**storage limitation**);
- processed in a manner that ensures appropriate **security of the data**.

PROTECTION AGAINST MALWARE

- The protective measures installed on each IT system (e.g. virus protection) must not be changed or deactivated by the user.
- Do not open email attachments
  - that seem strange to you
  - if the message does not explicitly refer to the attachments
  - Do not click on dubious links
  - with the extensions *.exe, *.msi, as well as *.zip and *.rar archives, if they do not come from a trusted source
- Be sceptical of unexpected invoices, job applications, letters from lawyers, etc.
- If in doubt, check with the sender.
- If you notice that something is wrong with your PC or you realise that you have actually caught an encryption Trojan:
  - If in doubt, pull the plug.
  - Shut down your PC as quickly as possible.
  - Inform the service desk.

email: servicedesk@francotyp.com

HARDWARE, SOFTWARE & NETWORKING

IT systems and other technical equipment may only be used if they have been approved for use by the IT department. Unauthorised or private devices must not be connected to the company's infrastructure. Devices must not be passed on to other people.
Installing software on workstation systems or other IT systems provided for business purposes is strictly prohibited unless it has been explicitly provided for this purpose.