INFORMATION SECURITY

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.

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 technology/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 saved on centrally administered and secured servers. If specific mobile data carriers are used, these must be stored in an access-protected manner.

Data may only be transferred to third parties if they are authorised to access this data. The transmission path must be protected.

COPYING, SCANNING AND PRINTING

Items sent to the printer for printing must be collected without delay. Unclaimed documents that cannot be assigned to any employee are to be disposed of in the locked paper containers or document shredders in the copying rooms.

INFORMATION SECURITY

PROTECTION AGAINST MALWARE

- the user may not deactivate or change the configuration of the protective measures installed on every IT system (e.g. virus protection)
- do not open any e-mail attachments,
  - that seem unusual
  - if the message does not specifically refer to the attachments
  - that are accessed via dubious links
  - that end with *.exe, *.msi or *.zip and *.rar archives if they don't come from a trustworthy source
- be sceptical if you receive any unexpected invoices, applications, correspondence from lawyers etc.
- ask the sender in case of doubt
- if you see that something is not right with your PC or you realise that you have actually received ransomware:
  - Pull out the plug in case of doubt
  - Shut down the PC as quickly as possible
  - Inform the service desk

e-mail: 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.
Networks may not be established between non-approved or private devices and the company's infrastructure. Devices may not be passed on to other individuals.
It is fundamentally forbidden to install software on the workplace system or another IT system provided for business purposes if it was not explicitly provided for that purpose.

INFORMATION SECURITY

FP Security Information

Information security means protecting information against a number of threats.
It makes a significant contribution to:

- maintaining business operations,
- complying with statutory regulations,
- protecting the company's image and
- protecting personal data.

Any actual or suspected malware or a corresponding suspicion of a phishing e-mail must be reported immediately to the IT Security Team. Do not forward the untrustworthy e-mail, but send it to the IT Security Team as an attachment to a new e-mail so that an analysis is possible to the IT Security Team so that an analysis is possible. A decision will then be made there about how to proceed.

e-mail: it-security@francotyp.com

If you have any questions about information security or the protection of personal data or want to report any irregularities/problems, please contact us.

e-mail: iso@francotyp.com

Be alert

Don't let people look over your shoulder

Choose clever passwords

Raise the alarm

Be cautious of external content

Take care when passing on information

Guideline 127e, Rev. 2.5
information security class: public

ACCESS CONTROL

Access to all rooms is governed by a control system. Employees may only enter areas for which they have access authorisation.

Be alert:

Close doors and question unknown individuals. Accompany guests in the building and report any abnormalities or breaches!

ACCESS AND ADMISSION CONTROL

Whether in your own office or elsewhere - ensure that only you have access to your data, computers, filing 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 superior. User accounts are password-protected. Passwords are strictly confidential and must be kept secret.

The user is responsible for all activities conducted from their user account!

Lock your screen even if you will only be absent for a short period (**Windows key + L**).

Keep your workstation and environment tidy. Only keep information available at your workstation that you need to perform the relevant tasks. Use any filing and locking systems provided.

INTERNET USE

Only the intended access paths equipped with corresponding protective systems (e.g. firewalls) are to be used when accessing the internet.

INFORMATION IN CONVERSATION

Ensure that both direct and telephone conversations with a business content are held without the presence of any unauthorised third parties.

USE OF E-MAIL

- The e-mail function may only be used for business purposes.
- Do not comply with any request to forward warnings or calls to friends, acquaintances or colleagues.
- The e-mail addresses on the recipient list must be checked before sending an e-mail to ensure that it is actually being sent to the desired individuals.
- E-mails that are not or are no longer required must be regularly deleted if there are no retention periods.
- Automated e-mails with an out of office signature must be set for planned absences of longer than one day.
- Only expected and plausible attachments may be opened.
- No FP e-mails may be forwarded to private or third party e-mail accounts.
- E-mails should be sent and received in an encrypted form if it is possible to do so.
- Suitable encryption must be used when sending sensitive content externally (including content classified as confidential or strictly confidential).
- Please pay special attention to e-mails 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 originator of any information is responsible for ensuring that it is only received by people for whom the purpose of the information is relevant.

The originator is responsible for classifying the information and must specify whether and how it is to be categorised and handled.

Attributes for information classification policy: public, internal, confidential, strictly confidential.

If no classification is specified for the information, it will automatically be categorised as “internal” - i.e. it is available internally without restrictions but may not be distributed to the public.

ON THE GO

The most common risk is still the loss of data on mobile phones, smartphones, USB sticks and laptops.

Always keep an eye on the devices and documents entrusted to you and don’t leave them unattended (not even during customs controls). Use a privacy screen protector (laptop) when working outside of the business premises.

Mobile data should be saved in an encrypted manner if possible.

The FP IT service desk is to be informed without delay in the event of theft or suspected unauthorised access.

BUSINESS USE

IT systems provided by the employer (PC, laptop, smartphone etc.) are only to be used in line with the conditions of use handed over with the equipment.

PROTECTION OF PERSONAL DATA

It must be:

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