IT security instructions for Contractors and their work assignments at Messe Frankfurt

1. General information

Information technology (IT) is a strategic corporate factor for Messe Frankfurt. In addition to protecting against unauthorised third-party access, smooth operation is a key competitive factor. The aim of these security requirements is to heighten information security awareness, while at the same time ensuring that the Contractor's deployment proceeds as smoothly as possible. If problems or atypical events are noticed, the IT ServiceDesk of Messe Frankfurt must be notified without undue delay. It must be taken into account that an IT failure, loss of data or the misuse of data may affect the competitive position and result in financial losses for Messe Frankfurt and its customers as well as partner companies.

In the following, we will define general requirements when handling potentially provided IT resources (hardware, software and data) and the IT infrastructure of Messe Frankfurt. These safety requirements also include recommendations and instructions on how to behave in the event of problems or conspicuous events and how to deal with them. The Contractor must provide instruction for its employees on such IT security information and requirements and have a supervisor or contact person on site to ensure compliance. Proof of such training must be presented at the Client's request.

2. Scope and target group

2.1 The following behavioural and security instructions apply to deployment at Messe Frankfurt, whether on-site or via the connection of IT systems with access to the IT infrastructure of Messe Frankfurt.

2.2 The scope of these rules includes Messe Frankfurt and its subsidiaries. The Contractor or a supervising contact person of the Contractor on site must ensure compliance with the safety requirements and behaviour.

3. Use of Messe Frankfurt hardware

3.1 The safe handling of stationary workstations and mobile terminals such as notebooks or smartphones at Messe Frankfurt must be ensured at all times. Compliance with the following safety requirements is therefore compulsory.

3.2 Deliberate circumvention or deactivation of existing security measures at Messe Frankfurt is prohibited.

3.3 Damage to equipment, ports or connections, as well as theft and any other events that might affect the security of the IT systems (also known as information security incidents) must be reported to the ServiceDesk-IT of Messe Frankfurt (servicedeskit@messefrankfurt.com; T: +49 (0) 69- 7575 6663) and to the IT security officers (IT-security@messefrankfurt.com)

3.4 When leaving a workstation, the VDU workstation must be locked or the user must log out.

3.5 After use, the VDU workstation must be shut down and confidential documents must be removed from the desk.

4. Use of hardware and software on site

4.1 As a matter of principle, only the hardware and software configurations installed by Messe Frankfurt IT may be used at the VDU workstation/PC/notebook.

4.2 The provided hardware and software may only be used in the context of performing tasks for Messe Frankfurt.

4.3 Any connection and use of private hardware or hardware not provided by Messe Frankfurt is prohibited.

4.4 The software at VDU workstations is installed as part of an automatic software distribution. This means that only authorised software is used that has been installed by IT as part of software distribution. No unauthorised software of any kind may be installed. This applies to both purchased and proprietary software. Compliance with these security requirements ensures that the software used at Messe Frankfurt is handled properly in terms of licensing law.

4.5 Users are prohibited from developing their own programs; this also applies to macro-programming in standard programs (e.g. Excel, Word, Visio, etc.). This is the exclusive responsibility of Messe Frankfurt IT as part of software distribution.

4.6 The downloading of files, information or documents from the Internet that are not required for the performance of tasks is prohibited.

4.7 The personal directory is provided for the storage of information and data not required for third parties. Please bear in mind that no one else is allowed to access it, not even in case of an emergency.

4.8 Music or video files must not be stored on the VDU workstation/PC/notebook, in the personal directories or on the servers of Messe Frankfurt. Storage of music or video files required or used for operational purposes also is only permitted if the copyrights have been acquired or if the copyright holder has issued a corresponding written permission to use or store the files (e.g. in case of radio or TV recordings). Messe Frankfurt has the right to use adequate software to enforce compliance with these rules without prior notice, including deleting music or video files stored without authorisation.

4.9 For security reasons, VDU workstations with unauthorised software/files must be reinstalled by ServiceDesk IT.

4.10 VDU workstations and peripheral equipment (especially printers) must not be modified, exchanged or moved to other rooms without prior authorisation.

4.11 Each user is responsible for carefully handling the equipment provided to them.

5. Handling passwords and access codes

5.1 Passwords and access codes ensure that only authorised users can access the digital content and network of Messe Frankfurt. The assigned user IDs are supplemented by individual passwords. This is intended to prevent unauthorised access to the network of Messe Frankfurt. User ID and password therefore must only be known to the respective user.

5.2 When using hardware and software components for the first time, the initial passwords must be changed in accordance with the system password criteria.

5.3 Once assigned, passwords must not be used for additional services. Messe Frankfurt applies the principle of ‚one service - one password'.

5.4 Passwords must be kept secret, and must not be disclosed to other persons.

5.5 Another person's user ID must not be used for registration; this also applies to substitutions.

5.6 Passwords must not be stored in unencrypted form on either the terminal or file server.

5.7 Authentication features such as eTokens, keys, cards, etc. must be stored carefully, securely, and separate from the terminal. The IT ServiceDesk of Messe Frankfurt must be notified promptly of any loss.

6. Administration

6.1 If external persons and users have access via administrative accounts, such accounts must never be used for activities or operations that do not require elevated privileges.

6.2 Administrative interventions in application operations are only permitted if they have been coordinated with the line manager or system administrator.

6.3 External users with administrative authorisations undertake to obtain on a regular basis information on the state of the art of the applications, IT systems, services and protocols to be managed.

6.4 Any system changes made must be documented in a verifiable manner. Such documentation should at least indicate the type of changes made, as well as when and by whom they were made.

6.5 Administrative activities on particularly security-critical IT systems or in applications require additional security measures to be taken in coordination with the responsible internal teams (dual control principle, detailed logging, change reviews).

7. Remote maintenance

7.1 Access to client systems of Messe Frankfurt via remote access may only be established with the system administrator's explicit agreement.

7.2 As a matter of principle, online services for remote maintenance, e.g. TeamViewer or AnyDesk etc. must not be used. Should it be necessary to use online services, this must be arranged with the IT security officer at Messe Frankfurt.

7.3 In case of remote access via online services, all activities carried out are monitored by external staff of Messe Frankfurt. Access during remote access is restricted to the necessary IT systems and network segments. Access to other devices requires further agreement.

8. Mobile terminals

8.1 To the extent possible, mobile terminals such as notebooks, tablets or smartphones should not be left unattended and/or should be adequately protected against theft. The IT ServiceDesk of Messe Frankfurt must be notified promptly of any loss.

8.2 If the mobile terminal of Messe Frankfurt is used in office rooms other than those of Messe Frankfurt, if possible, such room must be locked even if left for a short time, or the device must be removed. If the room is left for a longer period of time, the mobile terminal should also be switched off or access protection should be enabled to prevent unauthorized use.

8.3 When using mobile terminals of Messe Frankfurt in public areas (airport, plane, train station, train, restaurant, coffee shop, etc.), it is important to take care and ensure that confidential information cannot be seen. For example, special films may be used to prevent reading the screen from the side.

8.4 When using private or external networks (e.g. private DSL connection at home or WLAN at airports, in hotels, beer gardens, etc.), secure access to the Messe Frankfurt network (VPN) must be used – including for online access. The security mechanisms of Messe Frankfurt take effect in this, and external networks cannot interfere with the terminal.

8.5 If a mobile terminal of Messe Frankfurt is lost, the responsible persons at Messe Frankfurt must be notified promptly, e.g. the ServiceDesk IT and the IT security officers. If the mobile terminal is located again, it must be handed over to the responsible persons at Messe Frankfurt to be checked for potential tampering.

8.6 The persons responsible at Messe Frankfurt must be notified promptly if unauthorised changes to the mobile terminal are detected.

8.6 Where it is possible to select an individual device name, no device names must be chosen that contain a reference to Messe Frankfurt or to the user.

9. Mobile data carriers

These include in particular all CD/DVD-ROMs, USB memory, mobile hard disks and e.g. memory cards.

9.1 The data carrier should be labelled and protected against unwanted access. Confidential information must be encrypted. In addition to drive encryption, for example via Bitlocker or VeraCrypt, file encryption via encrypted Zip container may also be used, e.g. by using 7-ZIP software.

9.2 If a mobile data carrier is lost or in case of suspected tampering, the persons responsible at Messe Frankfurt must be contacted promptly. The information that is stored on the mobile data carrier must also be specified in this case.

9.3 Any data that is no longer required must be deleted or destroyed in accordance with the state of the art; to that end, the persons responsible at Messe Frankfurt can be contacted.

9.4 External data carriers (CDs, DVDs, USB sticks, etc.) must be checked for malware before use. The local antivirus program can be used for this purpose.

10. Data backup of PC workstations/ notebooks

10.1 Work data must be saved to the network drive. This is the only way to ensure that data is regularly backed up by Messe Frankfurt IT. The workstation's/ notebook's hard disk is not subject to this backup. If data need to be imported from a mobile data carrier into the network of Messe Frankfurt and if the relevant connection has not been approved, the data from the carrier may be transferred via the IT Service Desk.

10.2 If it is necessary to copy data from the network of Messe Frankfurt to a mobile data carrier and if no relevant connection has been approved for this purpose, the ServiceDesk IT can see to this as well.

11. Use of Internet and e-mail mailboxes

11.1 Internet and e-mail mailboxes may not be used for purposes other than the business of Messe Frankfurt.

11.2 Automatic forwarding/redirection to external mailboxes is not permitted.

11.3 When sending business e-mails to external communication partners, confidential information must be encrypted for protection. For example, 7-Zip software with AES encryption may be used for attachments. In addition, it should also be made sure that the e-mail body does not contain any confidential information. In particular, access data such as passwords must not be transmitted by e-mail.

11.4 For protection against malware, any attachments received by e-mail must be scanned for malware before opening them. The IT ServiceDesk or the persons responsible for IT security at Messe Frankfurt must be notified if irregularities are detected in e-mail communication or attachments. Passwords transmitted in e-mails must not be used for decryption or to open attachments.

11.5 When selecting the user ID for online use (outside the business context of Messe Frankfurt), no internal passwords or user names must be used.

12. Messe Frankfurt data

12.1 The data stored on the systems of Messe Frankfurt is the property of Messe Frankfurt.

12.2 Unless required for the performance of the respective task, Messe Frankfurt data must not be disclosed or made accessible to third parties without being related to such task.

13. Disposal of data carriers

13.1 Unusable or obsolete mobile data carriers must be disposed of properly. Appropriate data containers are available for proper disposal.

13.2 Mobile electronic equipment must be returned to the issuing office.

13.3 Data media may under no circumstances be disposed of together with general office waste. The existing data protection containers must be used to dispose of printouts of files with confidential content.

14. Termination of deployment

14.1 Upon termination of the task/work performance by the Contractor's staff (termination of service utilisation), all documents, keys and equipment as well as ID cards and access authorisations received within the context of the activity must be returned to the responsible persons.

14.2 In addition, deletion of the user account must be requested via the ServiceDesk IT.

15. Data protection regulations

15.1 The data protection provisions must be observed when handling personal data. Personal data means individual information on personal circumstances and factual affairs of natural persons. Under applicable data protection laws, processing and use of personal data requires a legal basis.

15.2 Data protection inquiries should be addressed to the company data protection officer.

Contact data:

ServiceDesk IT:
ServiceDeskIT@messefrankfurt.com
+49 (0) 69 75 75 6663

IT Security:
IT-security@messefrankfurt.com

Data Protection:
privacy@messefrankfurt.com