

IT-Sicherheitshinweise für Einsätze bei der Messe Frankfurt als Auftragnehmer (AN)

1. Allgemeines

Die Informationstechnik (IT) ist für die Messe Frankfurt ein strategischer Unternehmensfaktor. Der reibungslose Betrieb ist, ebenso wie die Absicherung vor unerlaubtem Zugriff Dritter, ein wesentlicher Wettbewerbsfaktor. Ziel dieser Sicherheitsanforderung ist die Sensibilisierung zur Informationssicherheit einerseits und die Gewährleistung eines möglichst störungsarmen Einsatzes des Auftragnehmers andererseits. Sollten Störungen oder atypische Ereignisse bemerkt werden, muss unverzüglich der ServiceDesk IT der Messe Frankfurt informiert werden. Es ist zu berücksichtigen, dass der Ausfall der IT, ein Datenverlust oder der Missbrauch von Daten wettbewerbsrelevante, finanzielle Einbußen für die Messe Frankfurt und ihren Kunden sowie Partner-Unternehmen zur Folge haben kann.

Nachfolgend werden grundsätzliche Anforderungen im Umgang mit ggfs. bereitgestellten IT-Arbeitsmitteln (Hard- und Software und Daten) und in der IT-Infrastruktur der Messe Frankfurt definiert. Gleichzeitig gibt diese Sicherheitsanforderung Empfehlungen und Hinweise zum Umgang und zum Verhalten bei Störungen oder auffälligen Ereignissen. Der Auftragnehmer hat seine Mitarbeiter auf diese IT-Sicherheitshinweise hin zu unterweisen und durch eine aufsichtführende Person oder Ansprechpartner vor Ort zu gewährleisten. Der Schulungsnachweis ist auf Verlangen des Auftraggebers vorzulegen.

2. Anwendungsbereich und Adressat

- 2.1 Für den Einsatz bei der Messe Frankfurt, ob vor Ort oder über die Anbindung von IT-Systemen mit Zugriff auf die Messe Frankfurt IT-Infrastruktur, gelten nachfolgende Verhaltens- und Sicherheitshinweise.
- 2.2 Der Anwendungsbereich dieser Regeln umfasst die Messe Frankfurt und ihre Tochtergesellschaften. Für die Einhaltung der Sicherheitsanforderungen und

-verhaltensweisen hat der AN bzw. ein aufsichtführender Ansprechpartner des AN vor Ort Sorge zu tragen.

3. Nutzung von Hardware der Messe Frankfurt

- 3.1 Der sichere Umgang mit stationären Arbeitsplätzen und mobilen Endgeräten wie Notebooks oder Smartphones bei der Messe Frankfurt muss jederzeit gewährleistet sein. Aus diesem Grund besteht die Verpflichtung zur Einhaltung der nachfolgenden Sicherheitsanforderungen.
- 3.2 Das bewusste Umgehen oder Deaktivieren bestehender Sicherheitsmaßnahmen der Messe Frankfurt ist nicht zulässig.
- 3.3 Beschädigungen an Geräten, Anschlüssen und Verbindungen, als auch Diebstähle und sonstige Ereignisse, die die Sicherheit der IT-Systeme beeinflussen könnten (auch Informationssicherheitsvorfälle genannt) sind an das Messe Frankfurt ServiceDesk-IT (servicedesk@messefrankfurt.com; T: 069- 7575 6663) und die Verantwortlichen für IT-Sicherheit (IT-security@messefrankfurt.com) zu melden.
- 3.4 Wenn der Arbeitsplatz verlassen wird, muss der Bildschirmarbeitsplatz gesperrt oder von diesem abgemeldet werden.
- 3.5 Nach Arbeitsende muss der Bildschirmarbeitsplatz ausgeschaltet werden und vertrauliche Unterlagen vom Schreibtisch entfernt werden.

4. Der Einsatz von Hard- und Software am Einsatzort

- 4.1 Grundsätzlich gilt, dass am Bildschirmarbeitsplatz/PC/Notebook ausschließlich die von der IT der Messe Frankfurt installierte Hard- und Softwarekonfigurationen zum Einsatz kommen darf.
- 4.2 Die überlassene Hard- und Software darf grundsätzlich nur im Rahmen der Auf-

gabenerfüllung für die Messe Frankfurt genutzt werden.

- 4.3 Der Anschluss und Einsatz privater oder nicht durch die Messe Frankfurt bereitgestellter Hardware ist nicht zulässig.
- 4.4 Die Software am Bildschirmarbeitsplatz wird im Rahmen einer automatischen Softwareverteilung installiert. Das bedeutet, dass ausschließlich autorisierte und von der IT im Rahmen der Softwareverteilung aufgespielte Software zum Einsatz kommt. Die Installation nicht autorisierter Software jedweder Art, ist nicht zulässig. Dies gilt sowohl für gekaufte, wie für eigenentwickelte Software. Die Einhaltung dieser Sicherheitsanforderung gewährleistet in lizenzrechtlicher Hinsicht einen ordnungsgemäßen Umgang mit der bei der Messe Frankfurt eingesetzten Software.
- 4.5 Die Eigenentwicklung von Programmen ist den Anwendenden untersagt, hierzu gehört auch die Makroprogrammierung in Standardprogrammen (z.B. Excel, Word, Visio etc.). Sie unterliegt ausschließlich der IT der Messe Frankfurt und erfolgt im Rahmen der Softwareverteilung.
- 4.6 Das Herunterladen von Dateien, Informationen und Dokumenten aus dem Internet, die für die Aufgabenerfüllung nicht benötigt werden, ist unzulässig.
- 4.7 Das persönliche Verzeichnis wird für die Ablage von Informationen und Daten, die nicht für Dritte benötigt werden, bereitgestellt. Es ist zu berücksichtigen, dass auch im Notfall dort niemand weiteres zugreifen darf.
- 4.8 Die Speicherung von Musik- und Filmdateien auf den Bildschirmarbeitsplatz/PC/Notebook und in den persönlichen Verzeichnissen oder auf den Servern der Messe Frankfurt, ist unzulässig. Auch die Speicherung von betrieblich benötigten bzw. genutzten Musik- und Filmdateien ist nur zulässig, wenn die Urheberrechte erworben wurden oder eine entsprechende schriftliche Genehmigung zur Nutzung bzw. Speicherung der Dateien durch den Urheber (z.B. beim Mitschnitt von

Radio- oder Fernsehsendungen) vorliegt. Die Messe Frankfurt hat das Recht, über entsprechende Software, die Einhaltung dieser Regeln, d. h. auch die Löschung von unberechtigt gespeicherten Musik- und Filmdateien, ohne vorherige Ankündigung durchzusetzen.

- 4.9 Durch nicht berechnete Software/Dateteilen belastete Bildschirmarbeitsplätze müssen aus Sicherheitsgründen vom ServiceDesk IT neu installiert werden.
- 4.10 Bildschirmarbeitsplätze und Peripheriegeräte (insbesondere Drucker) dürfen nicht eigenständig verändert, getauscht oder in andere Räume umgezogen werden.
- 4.11 Jeder Anwendende ist für einen pfleglichen Umgang der ihm überlassenen Geräte verantwortlich.

5. Umgang mit Passwörtern und Zugangscodes

- 5.1 Passwörter und Zugangscodes gewährleisten, dass nur autorisierte Benutzer Zugang zu den digitalen Inhalten und zum Netz der Messe Frankfurt erhalten. Die vergebenen Benutzer-IDs werden durch individuelle Passwörter ergänzt. Ein unbefugter Zugriff auf das Netz der Messe Frankfurt soll dadurch verhindert werden. Das setzt voraus, dass Benutzer-ID und Passwort nur dem jeweiligen Anwendenden bekannt sind.
- 5.2 Initial-Passwörter bei Hard- und Software Komponenten sind bei der ersten Nutzung entsprechend den System-Passwortkriterien zu ändern.
- 5.3 Einmal vergebene Passwörter dürfen nicht für weitere Dienste verwendet werden. Bei der Messe Frankfurt wird das Ein-Dienst-Ein-Passwort Prinzip gelebt.
- 5.4 Passwörter sind geheim zu halten, sie dürfen nicht an andere Personen weitergegeben werden.
- 5.5 Es ist nicht erlaubt, die Benutzerkennung einer anderen Person zur Anmeldung zu nutzen, dies gilt auch bei Stellvertretungen.
- 5.6 Passwörter dürfen nicht in unverschlüsselter Form auf dem Endgerät oder Fileserver gespeichert werden.
- 5.7 Authentisierungsmerkmale wie eToken, Keys, Karten und vergleichbaren Mittel sind sorgfältig, sicher und getrennt vom Endgerät aufzubewahren. Ein Verlust ist umgehend dem ServiceDesk IT der Messe Frankfurt zu melden.

6. Administration

- 6.1 Besitzen externe Personen und Anwendende Zugriffe über administrative Konten, dürfen diese niemals für Aktivitäten oder Tätigkeiten genutzt werden, die keine erhöhten Berechtigungen benötigen.
- 6.2 Administrative Eingriffe in den Anwendungsbetrieb sind nur genehmigt, wenn diese mit dem Fach- oder Systemverantwortlichen abgestimmt sind.
- 6.3 Externe Anwender mit administrativen Berechtigungen verpflichten sich zu regelmäßigen Informationsbeschaffungen zum Stand der Technik der zu verwaltenden Anwendungen, IT-Systemen, Diensten und Protokolle.
- 6.4 Vorgenommene Systemänderungen sind nachvollziehbar zu dokumentieren. Aus der Dokumentation sollte mindestens hervorgehen, welche Änderungen vorgenommen wurden, wann und durch wen diese Änderungen erfolgt sind.
- 6.5 Bei administrativen Tätigkeiten an besonders sicherheitskritischen IT-Systemen oder in Anwendungen sind zusätzliche Sicherheitsmaßnahmen in Absprache mit den zuständigen internen Teams zu treffen (Vier-Augen-Prinzip, ausführliches Logging, Change-Reviews).

7. Fernwartung

- 7.1 Der Zugriff auf Client-Systeme der Messe Frankfurt über einen Fernzugriff darf nur dann aufgebaut werden, wenn der Systemverantwortliche diesem explizit zustimmt.
- 7.2 Der Einsatz von Online-Diensten zur Fernwartung, wie z.B. TeamViewer oder AnyDesk etc. ist grundsätzlich nicht genehmigt. Sollten der Einsatz von Online-Diensten notwendig sein, ist dies mit den Verantwortlichen für IT-Sicherheit der Messe Frankfurt zu regeln.
- 7.3 Bei einem Fernzugriff mittels Online-Diensten werden alle durchgeführten Aktivitäten von externen Mitarbeitenden der Messe Frankfurt überwacht. Während des Fernzugriffs dürfen nur Zugriffe auf die benötigten IT-Systeme und Netzsegmente erfolgen. Ein Zugriff auf andere Geräte ist ohne weitere Absprache nicht genehmigt.

8. Mobile Endgeräte

- 8.1 Mobile Endgeräte wie Notebooks, Tablets oder Smartphones sollten nach Möglichkeit nicht unbeaufsichtigt sein und/oder vor einem Diebstahl ausreichend geschützt sein. Ein Verlust ist umgehend dem ServiceDesk IT der Messe Frankfurt zu melden.
- 8.2 Wird das mobile Endgerät der Messe Frankfurt in nicht den Messe Frankfurt zugehörigen Büroräumen benutzt, so ist dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen oder das Gerät mitzunehmen. Wird der Raum für längere Zeit verlassen, sollte das mobile Endgerät zusätzlich ausgeschaltet oder ein Zugriffsschutz aktiviert werden, um eine unerlaubte Nutzung zu verhindern.
- 8.3 Bei der Nutzung von mobilen Endgeräten der Messe Frankfurt in öffentlichen Umgebungen (Flughafen, Flugzeug, Bahnhof, Bahn, Restaurant, Café etc.) muss darauf geachtet werden, dass vertrauliche Informationen nicht ausgespäht werden können. Hierzu können ggf. spezielle Folien eingesetzt werden, die ein Einsehen von der Seite verhindern.
- 8.4 Bei der Nutzung privater oder fremder Netzwerke (z. B. privater DSL-Anschluss zu Hause oder WLAN in Flughafen, Hotel, Biergarten etc.) muss der sichere Zugang zum Netz der Messe Frankfurt (VPN) genutzt werden – auch zum Zugang ins Internet. Hierdurch greifen die Sicherheitsmechanismen der Messe Frankfurt und das Endgerät kann nicht durch die fremden Netzwerke beeinträchtigt werden.
- 8.5 Wird ein mobiles Endgerät der Messe Frankfurt verloren, sind die Verantwortlichen der Messe Frankfurt umgehend zu informieren, hier z.B. der ServiceDesk IT und die Verantwortlichen für IT-Sicherheit. Wenn das mobile Endgerät wiedergefunden wird, ist es den Verantwortlichen der Messe Frankfurt zu übergeben, damit es auf mögliche Manipulation geprüft werden kann.
- 8.6 Wenn unberechtigte Änderungen am mobilen Endgerät festgestellt werden, ist dies umgehend den Verantwortlichen der Messe Frankfurt mitzuteilen.
- 8.6 Sollte es möglich sein, einen individuellen Gerätenamen einzustellen, so sind keine Gerätenamen zu wählen, die einen Hinweis auf die Messe Frankfurt oder den Anwendenden enthalten.

9. Mobile Datenträger

Hierzu zählen insbesondere alle CD-/DVD-ROMs, USB-Speicher, mobile Festplatten und z.B. Speicherkarten.

- 9.1 Die Datenträger sollten beschriftet und vor unerwünschtem Zugriff geschützt werden. Vertrauliche Informationen sind zu verschlüsseln. Neben einer Laufwerksverschlüsselung über z.B. Bitlocker oder VeraCrypt, kann hierfür auch eine Datei-Verschlüsselung über verschlüsselte Zip-Container z.B. mittels dem Programm 7-ZIP, eingesetzt werden.
- 9.2 Sollte ein mobiler Datenträger verloren gehen oder ein Verdacht auf eine Manipulation bestehen, sind umgehend die Verantwortlichen der Messe Frankfurt zu kontaktieren. Ebenso ist in diesem Fall anzugeben, welche Informationen auf dem mobilen Datenträger gespeichert sind.
- 9.3 Nicht mehr benötigte Daten sind gemäß dem Stand der Technik zu löschen oder zu vernichten, hierfür können die Verantwortlichen der Messe Frankfurt kontaktiert werden.
- 9.4 Fremde Datenträger (CDs, DVDs, USB-Sticks etc.) müssen vor der Benutzung auf Schadsoftware hin überprüft werden. Hierzu kann das lokale Virenschutzprogramm verwendet werden.

10. Datensicherung der PC-Arbeitsplätze/Notebooks

- 10.1 Arbeitsdaten sind auf dem Netzlaufwerk zu speichern. Nur so kann sichergestellt werden, dass Daten regelmäßig durch die IT der Messe Frankfurt weggesichert werden. Die Festplatte des Arbeitsplatzrechners/Notebooks unterliegt dieser Sicherung nicht. Sollte es erforderlich sein, Daten von einem mobilen Datenträger in das Netzwerk der Messe Frankfurt einzuspielen und ist der entsprechende Anschluss nicht freigegeben, kann das Überspielen der Datenträger über den ServiceDesk IT erfolgen.
- 10.2 Ist es erforderlich, Daten aus dem Netz der Messe Frankfurt auf einen mobilen Datenträger zu kopieren und ist hierfür kein entsprechender Anschluss freigegeben, kann dies auch der ServiceDesk IT veranlassen.

11. Nutzung von Internet und E-Mail-Postfächern

- 11.1 Die Nutzung von Internet und E-Mail-Postfächern ist ausschließlich für dienstliche Zwecke der Messe Frankfurt gestattet.
- 11.2 Eine automatische Weiter-/Umleitung auf externe Postfächer ist nicht gestattet.
- 11.3 Bei Versendung geschäftlicher E-Mails an externe Kommunikationspartner sind vertrauliche Informationen zwingend durch den Einsatz von Verschlüsselung zu schützen. Dazu kann z.B. das Programm 7-Zip mit AES-Verschlüsselung für die Anhänge genutzt werden. Zusätzlich sollte darauf geachtet werden, dass sich keine vertraulichen Informationen im E-Mail-Text befinden. Insb. Zugangsdaten wie Passwörter dürfen nicht per E-Mail übermittelt werden.
- 11.4 Zum Schutz vor Schadprogrammen, müssen empfangene E-Mail Anhänge vor dem Öffnen auf Schadsoftware überprüft werden. Sollten Unregelmäßigkeiten in der E-Mail-Kommunikation oder bei den Anhängen festgestellt werden, muss hierüber der ServiceDesk IT oder die Verantwortlichen für IT-Sicherheit der Messe Frankfurt informiert werden. Passwörter, die in E-Mails übermittelt wurden, dürfen nicht zur Entschlüsselung oder dem Öffnen von Anhängen genutzt werden.
- 11.5 Bei der Auswahl der Benutzererkennung für Anwendung im Internet (außerhalb des Geschäftskontextes der Messe Frankfurt) dürfen interne Passwörter und Benutzernamen nicht verwendet werden.

12. Daten der Messe Frankfurt

- 12.1 Die auf den Systemen der Messe Frankfurt abgelegten Daten sind Eigentum der Messe Frankfurt.
- 12.2 Soweit es die jeweilige Aufgabenerfüllung nicht erforderlich macht, ist es untersagt, ohne Aufgabenbezug Daten der Messe Frankfurt an Dritte weiter zu geben oder Dritten zugänglich zu machen.

13. Entsorgung von Datenträgern

- 13.1 Unbrauchbare oder auszusondernde mobile Datenträger sind ordnungsgemäß zu

entsorgen. Zur sachgemäßen Entsorgung stehen entsprechende Datencontainer zur Verfügung.

- 13.2 Mobile elektronische Geräte sind an die ausgebende Stelle zurückgegeben.
- 13.3 In keinem Fall dürfen Datenträger mit dem üblichen Büromüll entsorgt werden. Ausdrücke von Dateien mit vertraulichem Inhalt müssen über die vorhandenen Datenschutzcontainer entsorgt werden.

14. Beendigung des Einsatzes

- 14.1 Bei Beendigung des Auftrags/ Werkleistung durch Mitarbeiter des AN (Beenden der Inanspruchnahme der Dienstleistung) müssen alle im Rahmen der Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen an den verantwortlichen Stellen wieder zurückzugeben werden.
- 14.2 Zusätzlich muss über den ServiceDesk IT die Löschung des Benutzerkontos beantragt werden.

15. Datenschutzbestimmungen

- 15.1 Beim Umgang mit personenbezogenen Daten müssen die Bestimmungen des Datenschutzes eingehalten werden. Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse natürlicher Personen. Gemäß geltender Datenschutzgesetze ist die Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn es eine Rechtsgrundlage gibt.
- 15.2 Anfragen zum Datenschutz sind an den betrieblichen Datenschutzbeauftragten zu richten.

Kontaktdaten

ServiceDesk IT:
ServiceDeskIT@messefrankfurt.com
069 75 75-66 63

IT-Sicherheit:
IT-security@messefrankfurt.com

Datenschutz:
privacy@messefrankfurt.com