Luftfrachtnahverkehr
Aircargoexpress
Luftfrachthandling
Zollabfertigung
Luftfrachtlogistik
Luftfrachttrucking
Sendungsverfolgung
tgl. MUC - NUE - FRA

DETZER
AIRCARGO SERVICE GmbH

Urheber/Ersteller:	**Dokumententyp:**	**Datum:**
Prohaska Assistenz	QM-Richtlinie	30.06.2020
Version:	**Anlass:**	**Freigabe:**
Detzer QM 03/ 1.01	IT-Sicherheit	Sven Zelmer Geschäftsführer

IT-Sicherheitsrichtlinie der Detzer Aircargo Service GmbH

Inhaltsverzeichnis:

1. Ziel und Zweck der Richtlinie

Die Richtlinie soll sowohl technisches Know-how schützen, als auch Kunden- und Preisinformationen vor Datenverlust, -missbrauch oder -diebstahl bewahren. Die Daten werden

dementsprechend geschützt, sodass nur autorisierte Nutzer Zugriff haben und weder ein unbefugter noch ein unkontrollierbarer Zugang möglich ist.

2. Geltungsbereich / Verantwortlichkeit

2.1. Die Richtlinie gilt für alle Beschäftigten, die technische Einrichtungen (Scanner) bedienen, dazu zählen Fahrer ebenso wie das Lager- und Büropersonal. Die Richtlinie legt zugleich Mindeststandards für das Home Office oder die Mobilarbeit fest.

2.2. Verantwortlich für Umsetzung und Einhaltung der Richtlinie zeichnet die Geschäftsführung, diese kann Aufgaben an den IT-Verantwortlichen delegieren oder in dieser Eigenschaft als Personalunion agieren.

3. Arbeitsplatz

3.1. Allgemeine Regeln am Arbeitsplatz

Rechner sind bei dauerhaftem Verlassen des Arbeitsplatzes auszuschalten, bzw. der Zugang manuell zu sperren. Dies gilt insbesondere auch für Zeiten geplanter Abwesenheit (z. B. längere Besprechungen, über Nacht/ das Wochenende, Dienstreisen, Urlaub, Fortbildungsveranstaltungen).

3.2. Nutzung der betriebseigenen Hard- und Software

3.2.1. Nutzungsbedingungen, Pflege, Störungsmeldung

Die Verwendung von Instant-Messaging-Programmen ist nicht gestattet, ebenso die Nutzung alternativer E-Mail Clients, die Kommunikation hat hier ausschließlich über Outlook und die vorinstallierten Programme und Anwendungen zu erfolgen. Im Störungsfall oder bei Virenverdacht ist sofort der IT-Dienstleister (aktuell Team ITC Consulting) zu kontaktieren und vor jeglicher weiteren Nutzung der Hard- oder Software deren Handlungsanweisung einzuholen.

3.2.2. Verbote

Betriebsfremde Hardware oder Software ist ohne Zustimmung des IT-Verantwortlichen weder zu installieren, zu speichern oder in irgendeiner Form zu nutzen. Gleiches gilt für Installationen von Programmen ohne Vorhaltung der gültigen Lizenz.

4. Daten

4.1. Speicherung und Datenhaltung

Die Datenspeicherung auf Netzwerklaufwerken oder lokalen Laufwerken erfolgt über den Firmenserver in einem abgeschlossenen, nicht jedermann zugänglichen Serverraum.

4.2. Datensicherheit

Schutz vor unerlaubtem bzw. unbeabsichtigtem Zugriff erfolgt über eine Benutzersteuerung mit verschiedenen Berechtigungsebenen (admins, user, etc…). Wird der Zugriff auf die Daten durch einen Vertreter (zB bei Abwesenheiten, Krankheit etc.) erforderlich, kann dies allein durch einen admin erfolgen.

4.3. Datensicherung

Die Datensicherung erfolgt über ein „raid level 6“ System und entspricht somit dem technischen Standard im Bereich der gewerblichen Infrastruktur.

5. Telefondienste

Umfasst sind Endgeräte (Festnetztelefone, Mobilteile, das Telefaxgerät), die hausinterne Telefonanlage samt Anschlüsse sowie die Mobiltelefone.

5.1. Nutzung

5.1.1. Allgemeines

Die Nutzung sämtlicher Telefondienste ist grundsätzlich nur zu dienstlichen Zwecken gestattet.

5.1.2. Mobiltelefon

Soweit Mitarbeitern ein Mobiltelefon überlassen wird, ist es ausschließlich dienstlichen Zwecken zuzuführen. Überlassene Mobiltelefone sind nicht personengebunden, sondern tätigkeitsbezogen zugeordnet (zB einem Fahrzeug - einer DTS Nummer). Das Mobiltelefon hat daher grundsätzlich am zugeordneten Arbeitsplatz, bzw. im Fahrzeug zu verbleiben.

5.2. Kontrolle

5.2.1. Eine Kontrolle des jeweiligen Anwenderverhaltens kann vereinzelt stattfinden, da die Nutzung allein zu dienstlichen Zwecken erlaubt ist.

5.2.2. Eine Leistungs- und Verhaltenskontrolle insbesondere durch Auswertung von den Nutzern zugeordneten Anwenderprofilen findet dabei nicht statt.

5.2.3. Dienstliche Gespräche sind im Mobilfunknetz auf das nötige Maß zu beschränken. Die Dokumentation über den Einzelgebührennachweis durch den Netzbetreiber wird sich daher vorbehalten.

6. E-Mail und Internet

6.1. Nutzung zu dienstlichen Zwecken

6.1.1. Nutzungsvorgaben zum IT-System „E-Mail“

Das personalisierte Anwenderpostfach ist täglich mehrfach auf Eingänge zu prüfen. Im Fall zu erwartender längerer urlaubs- oder krankheitsbedingter Abwesenheit ist ein Vertreter zu bestimmen, der Einsicht in das Postfach nehmen kann. Ein entsprechender Automatismus hat auch bei unerwarteter Abwesenheit zur erfolgen. Grundsätzlich hat jeder Mitarbeiter in o.g. Fällen eine Abwesenheitsnotiz zu erstellen, in der der jeweilige Vertreter benannt wird. Die Angabe einer standardisierten Signatur am Ende der E-Mail ist verpflichtend.

6.1.2. In der Regel nur dienstlich veranlasste Nutzung von Internet- und E-Mail

Die private Nutzung von Internet und E-Mail Systemen ist untersagt.

6.2. Verhaltensgrundsätze

IT-Systeme „Internet“ und „E-Mail“ dürfen nicht zu Zwecken verwendet werden, die die Interessen, das Ansehen oder die Sicherheit des Unternehmens beeinträchtigen oder die gegen geltende Rechtsvorschriften verstoßen.

6.2.1. Verbote

Der Versand unternehmensrelevanter Daten ohne dienstliche Notwendigkeit an externe E-Mailkonten ist verboten. Ebenso ist das Abrufen, Verbreiten oder Speichern von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen verboten.

6.2.2. Der Download von Software ist nur durch hierzu autorisierte Mitarbeiter und auch nur nach Rücksprache mit dem IT-Verantwortlichen auf Basis Sicherheitsrichtlinie gestattet.

6.2.3. Seiten mit verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Inhalten sind verboten und werden vom Dienstleister blockiert.

6.3. Kontrolle

6.3.1. Erhebung von Protokollen

Es findet eine Auswertung von Log-Dateien zur Zugangsauswertung statt.

6.3.2. Löschung von Protokollen

Die Löschung hierdurch angelegter Protokolle und Anwendungsdaten erfolgt regelmäßig nach gesetzlichen Vorgaben.

6.4. Technische Schutzeinrichtungen der IT-Systeme „E-Mail und Internet“

Das E-Mail-System ist über eine E-Mail-Firewall geschützt und hält auch „Junk-E-Mail“-Ordner für Inhalte fragwürdigen Ursprungs vor. Die IT-Dienstleister sorgen durch ständige Updates für den jeweils aktuellsten Stand der Anti-Virensoftware, es findet keine Übermittlung von eingehenden E-Mails mit Anhängen, deren Umfang mehr als 20 MB

beträgt statt.

6.5. Gefährdung durch Schadprogramme

6.5.1. Präventive Maßnahmen

Präventiv zu Abwehr von Angriffen auf das System ist eine Virenschutz-Software wie auch die lokale Firewall installiert. Der hauseigene Server steht in einem abgeschlossenen und nur einem begrenzten Personenkreis zugänglichen Zentralraum.

6.5.2. Anzeichen von Infektion durch Computer-Schadprogramme oder Maßnahmen bei Verdacht auf Infektion durch Schadprogramme

Bei Zweifeln oder dem Anwender merkwürdig anmutende Vorgänge um Darstellungen, Meldungen oder überlangen Ladezeiten samt Rückmeldungsverlusten hat unverzügliche Meldung an den IT-Verantwortlichen und Dienstleister zu erfolgen. Bei hochgradigen Zweifeln hat hiervon unbenommen sofort eine Unterbrechung des Netzwerkzugang durch ziehen der Anschlusskabel zu erfolgen.

7. Mobile Geräte und externe Datenträger

Zum Bereich mobiler Geräte gehören insbesondere Firmen-Handys, PDAs, Notebooks. Als externe Datenträger werden z.B. CDs, DVDs, USB-Sticks, mobile Festplatten, sonstige Speicher-Chips, Disketten etc. bezeichnet.

7.1. Allgemeine Richtlinien für den Umgang mit mobilen Geräten

PIN bzw. ein Kennwort sind als Minimalschutz für den Start der Geräte vorgesehen, persönlich zugeteilte Firmennotebooks werden komplett verschlüsselt und können sich nur durch einen gesicherten VPN Tunnel auf den Zentralserver aufschalten.

7.2. Herausgabepflicht zum Ende des Arbeitsverhältnisses

Nach Beendigung des Arbeitsverhältnisses sind sämtliche mobilen Geräte und externe Datenträger unverändert zurückzugeben (keine Neuformatierung vor Abgabe).

8. Nutzung von Funknetzen (WLAN/WiFi, Bluetooth etc.)

Die WLAN/WiFi Netze werden für die Scanner Applikationen genutzt. Der Datenbezug ist hierdurch möglichst gering zu halten.

9. Allgemeine IT-Sicherheitsbestimmungen

9.1. Verbote

Die Verwendung von Cracker- oder Hackermethoden ist untersagt, ebenso das Vordringen in Bereiche des Netzwerkes oder einzelner Systeme, die nicht für den Arbeitnehmer selbst

und sein Aufgabengebiet freigegeben oder vorgesehen sind.

9.2. Kennwortgebrauch

9.2.1. Allgemeine Richtlinien für den Umgang mit Kennwörtern

Es sind grundsätzlich nur „komplexe“ Kennwörter zu vergeben. Diese sind vertraulich zu behandeln, eine Änderung aus Sicherheitsgründen nach Ablauf eines bestimmten Zeitraumes (derzeit ca. 3 Monate), ist vom IT-Verantwortlichen zu veranlassen.

9.2.2. Änderung zum Ende des Arbeitsverhältnisses

Kennwörter und Zugangscodes sind spätestens mit Beginn der Freistellungsphase eines Mitarbeiters zum Ende eines Arbeitsverhältnisses zu löschen.

10. Missbrauchskontrolle / Maßnahmen bei Verstößen

Eine gezielte personenbezogene Auswertung kann bei begründetem Verdacht auf missbräuchliche/ unerlaubte Nutzung der IT-Systeme angezeigt sein. Neben arbeitsrechtlichen Sanktionen kann dieses Vorgehen strafrechtliche Konsequenzen mit sich bringen.

11. Ständige Verbesserung der Sicherheitsstandards

Die hier niedergelegten Bestimmungen werden einem jährlichen internen Audit unterworfen und in diesem Rahmen angepasst und aktualisiert.

12. Inkrafttreten

Die IT-Sicherheitsrichtlinie tritt mit sofortiger Wirkung in Kraft.

Flughafen München, 01.07.2020

Kontaktdaten:

IT-Sicherheitsverantwortlicher der Detzer Aircargo Service GmbH:

Sven Zelmer
Detzer Aircargo Service GmbH
Südallee Cargomodul F
85356 München Flughafen

Telefon +49 89 978 8048 923
E Mail sven.zelmer@detzer.com