Francotyp-Postalia
Francotyp-Postalia

Richtlinie - Informationssicherheit

Verantwortlich: Chief Information Security Officer (CISO)

Diese Richtlinie dient der Sensibilisierung der Mitarbeiter bzgl. des Themas Informationssicherheit.
Verantwortlich für die Umsetzung dieser Richtlinie sind alle Mitarbeiter der FP Gruppe. Vorsätzliche Verstöße können zu arbeitsrechtlichen Konsequenzen führen.

FP Informationssicherheit

Informationssicherheit bedeutet den Schutz von Informationen vor einer Vielzahl von Bedrohungen. Sie trägt wesentlich dazu bei:

- den Geschäftsbetrieb aufrecht zu erhalten,
- gesetzliche Vorschriften einzuhalten,
- das Ansehen des Unternehmens zu schützen,
- personenbezogene Daten zu schützen.

Jedes Auftreten eines Schadprogramms oder ein entsprechender Verdacht einer Phishing E-Mail ist unverzüglich zu melden. Die **nicht vertrauenswürdige E-Mail nicht weiterleiten**, sondern als **Anlage** einer neuen E-Mail an den IT-Service Desk (servicedesk@francotyp.com) senden, so dass eine Analyse möglich ist. Dort wird über das weitere Vorgehen entschieden.
Sie möchten Unregelmäßigkeiten / Probleme melden oder haben Fragen zu Themen der Informationssicherheit bzw. dem Schutz von personenbezogenen Daten? Wenden Sie sich diesbezüglich bitte an iso@francotyp.com**.**

UMGANG MIT DOKUMENTEN UND DATEN

VERTRAULICHKEIT:

Stellen Sie sicher, dass Informationen nur in dafür autorisierte Hände geraten UND nur für den Zweck verwendet werden, für den sie erhoben wurden.

VERFÜGBARKEIT:

Stellen Sie sicher, dass Einrichtungen, Daten sowie Verarbeitungsmethoden (elektronische, händische) funktionssicher und zeitgerecht zur Verfügung stehen.

INTEGRITÄT:

Stellen Sie sicher, dass schützenswerte Daten unversehrt und vollständig bleiben UND bei der Verarbeitung nicht verfälscht werden können.

AUTHENTIZITÄT:

Stellen Sie sicher, dass Urheber (Personen und Technik/Programme) sowie Echtheit von Informationen verlässlich identifiziert und überprüft werden können.
Informationen müssen über ihren gesamten Lebenszyklus hinweg (bis zur sicheren Vernichtung) ihrem Schutzbedarf entsprechend gehandhabt werden. Eine Geheimhaltungspflicht besteht über das Vertragsverhältnis hinaus.

SPEICHERN UND ÜBERTRAGEN VON DATEN

Generell sind alle Unternehmensdaten auf zentral verwalteten und gesicherten Servern zu speichern. Werden zweckgebunden mobile Datenträger genutzt, sind diese zugangsgeschützt aufzubewahren. Eine Übermittlung an Dritte darf nur erfolgen, wenn diese zum Zugriff auf die Daten berechtigt sind. Der Übertragungsweg muss geschützt werden.

KOPIEREN, SCANNEN UND DRUCKEN

Zum Drucker gesandte Drucke müssen unverzüglich abgeholt werden. Nicht abgeholte Dokumente, die keinem Mitarbeiter zuzuordnen sind, sind in den in Kopierräumen aufgestellten abgeschlossenen Papierbehältern oder Aktenvernichtern zu entsorgen.

ZUTRITTSKONTROLLE

Der Zutritt zu allen Räumen ist durch ein Kontrollsystem geregelt. Jeder Mitarbeiter darf nur die Bereiche betreten, für die er eine entsprechende Zutrittsberechtigung hat.
Seien Sie achtsam:
Schließen Sie Türen und sprechen Sie Ihnen unbekannte Personen an. Begleiten Sie Gäste im Haus und melden Sie Auffälligkeiten oder Verstöße unverzüglich!
Verschließen Sie Räume und Fenster und sperren Sie Bildschirme immer, wenn Sie als letzter einen Raum verlassen, sei es auch nur für einen sehr kurzen Zeitraum.

ZUGANGS- UND ZUGRIFFSKONTROLLE

Ob im eigenen Büro oder außerhalb - stellen Sie sicher, dass nur Sie Zugriff auf Ihre Daten, Rechner, IT-Anwendungen sowie Ablageorte und Speichermedien haben. Für die Arbeit mit IT-Ressourcen ist ein

Benutzerkonto erforderlich. Dieses wird auf Antrag des Vorgesetzen durch die IT-Abteilung eingerichtet. Benutzerkonten sind mit einem Passwort geschützt. Passworte sind streng vertraulich, deren Geheimhaltung ist verpflichtend.
Der Anwender trägt die Verantwortung für alle Aktivitäten, die mit seinem Benutzerkonto ausgeführt werden!
Um sicher zu stellen, dass Unbefugte **keinen Zugang zu IT-Anwendungen oder Zugriff auf Daten erhalten, sperren** Sie auch bei kurzen Abwesenheiten den Bildschirm (**Windowstaste + L**). Sorgen Sie für Ihren aufgeräumten Arbeitsplatz und ein aufgeräumtes Umfeld. Halten Sie nur Informationen am Arbeitsplatz verfügbar, die zur Erledigung der jeweiligen Aufgaben benötigt werden. **Nutzen Sie bereitgestellte Ablage- und Verschlusssysteme**, um zu verhindern, dass die Verfügbarkeit, die Vertraulichkeit und die Integrität von Daten negativ beeinflusst werden kann. Bei geplanter Abwesenheit (z.B. längere Besprechungen, Dienstreisen, Urlaub, Fortbildungsveranstaltungen) ist der Arbeitsplatz so zu hinterlassen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Sollten Sie dafür weiteren Stauraum benötigen, wenden Sie sich an Ihren Vorgesetzten. **Jeder Mitarbeiter ist dazu verpflichtet seinen Arbeitslatz aufgeräumt zu hinterlassen.**
Das sichtbare Aufbewahren von Passwörtern (z.B. als Klebezettel am Monitor oder an einem leicht zu erratenden Ort) ist nicht erlaubt. Nutzen Sie zur Aufbewahrung von Passwörtern einen verschlüsselten Passwortsafe.

INTERNETNUTZUNG

Zum Zugriff auf das Internet dürfen ausschließlich die dafür vorgesehenen und mit entsprechenden Schutzeinrichtungen (z. B. Firewall) versehenen Zugangswege genutzt werden.

INFORMATIONEN IN GESPRÄCHEN

Achten Sie darauf, dass sowohl direkte als auch fernmündliche Gespräche mit geschäftlichen Inhalten unter Ausschluss unberechtigter Dritter stattfinden.
Organisatoren einer Besprechung können diese als streng vertraulich einstufen und das Mitführen von Mobiltelefonen und Tablets bzw. aller Geräte, die Gespräche aufzeichnen oder übertragen können, verbieten. Auf dieses Verbot wird in der Termineinladung explizit hingewiesen. Jeder Mitarbeiter muss das Verbot einhalten.

NUTZUNG VON E-MAIL

- die Mailfunktion darf ausschließlich für dienstliche Zwecke genutzt werden.

Francotyp-Postalia
Francotyp-Postalia

- eine Aufforderung zur Weiterleitung von Warnungen oder Aufrufen an Freunde, Bekannte oder Kollegen darf grundsätzlich nicht befolgt werden.
- vor dem Senden von E-Mails müssen immer die E-Mail-Adressen der Empfängerliste überprüft werden, ob tatsächlich die gewünschten Personen die E-Mail erhalten
- nicht mehr benötigte E-Mails sind, soweit keine Aufbewahrungsfristen bestehen, regelmäßig zu löschen.
- bei geplanter längerer Abwesenheit, sind automatisierte E-Mails mit einer Abwesenheitsnotiz zu hinterlegen.
- es dürfen nur Dateianhänge (Attachments) geöffnet werden, die erwartet werden und plausibel sind.
- es dürfen keine FP-Mails auf private oder dritte Mail-Accounts weitergeleitet werden.
- wenn die Möglichkeit besteht, E-Mails verschlüsselt zu senden und zu empfangen, sollte sie genutzt werden.
- bei Versendung sensibler Inhalte (u.a. Klassifikation vertraulich oder streng vertraulich), nach außen muss eine geeignete Verschlüsselung genutzt werden.
- E-Mails, die mit dem Hinweis ACHTUNG: Diese Mail kommt von einem EXTERNEN ABSENDER - bitte VORSICHT beim Öffnen von ANHÄNGEN und im Umgang mit LINKS versehen sind, bitte besonders beachten.

LENKUNG VON INFORMATIONEN

Der Ersteller einer Information ist dafür verantwortlich, dass diese nur den für den Zweck der Information relevanten Personen zur Kenntnis gelangt.
Er ist für die Klassifizierung seiner Informationen verantwortlich und muss festlegen, ob und wie diese gekennzeichnet und entsprechend behandelt werden muss.
Attribute zur Klassifizierung: öffentlich, intern, vertraulich, streng vertraulich.
Fehlt eine Klassifizierung, gilt automatisch die Einstufung „intern“ - d.h. intern unbegrenzt verfügbar und darf nicht öffentlich verbreitet werden.

UNTERWEGS

Als häufigste Gefahr gilt immer noch der Datenverlust durch Handys, Smartphones, USB-Sticks und Notebooks.
Achten Sie stets auf die Ihnen anvertrauten Geräte und Unterlagen und lassen Sie sie nicht unbeaufsichtigt (auch nicht bei Zollkontrollen). Verwenden Sie ein Blickschutzfolie (Notebook) bei Arbeiten außerhalb der Geschäftsräume.

Mobile Daten sind möglichst verschlüsselt zu speichern. **Außerhalb des FP-Netzwerkes ist stets eine sichere VPN-Verbindung zu nutzen.**
Bei Diebstahl und Verdacht auf fremden Zugriff (auch des VPN-Token) ist unverzüglich der FP IT Service-Desk zu informieren.

DIENSTLICHE NUTZUNG

Vom Arbeitgeber zur Verfügung gestellte IT-Systeme (PC, Notebook, Smartphone etc.) sind nur im Rahmen der mit der Ausrüstung übergebenen Nutzungsbedingungen zu verwenden.

SCHUTZ PERSONENBEZOGENER DATEN

Sie müssen:

- auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (**Rechtmäßigkeit, Treu und Glauben, Transparenz**);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (**Zweckbindung**);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**);
- sachlich richtig und auf dem neuesten Stand sein (**Richtigkeit**);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (**Speicherbegrenzung**);
- in einer Weise verarbeitet werden, die eine angemessene **Sicherheit der Daten** gewährleistet.

SCHUTZ VOR SCHADPROGRAMMEN

- die auf jedem IT-System installierten Schutzmaßnahmen (z. B. Virenschutz) dürfen vom Anwender weder in der Konfiguration verändert noch deaktiviert werden
- öffnen Sie keine E-Mail-Anhänge,
    - die Ihnen merkwürdig erscheinen
    - wenn in den Nachrichten nicht explizit auf die Anhänge verwiesen wird
    - klicken Sie keine dubiosen Links an
    - mit den Endungen *.exe, *.msi, sowie *.zip- und *.rar-Archive, wenn Sie nicht aus einer vertrauenswürdigen Quelle kommen

- seien Sie skeptisch bei unerwarteten Rechnungen, Bewerbungen, Schreiben von Anwälten, etc.
- fragen Sie im Zweifelsfall bei dem Absender nach
- falls Sie feststellen, dass mit Ihrem PC etwas nicht stimmt oder Sie merken, dass Sie sich tatsächlich einen Verschlüsselungstrojaner eingefangen haben:
    - ziehen Sie im Zweifelsfall den Stecker
    - fahren Sie den PC schnellstmöglich herunter
    - Informieren Sie den Service-Desk

E-Mail: servicedesk@francotyp.com

HARDWARE, SOFTWARE & VERNETZUNG

IT-Systeme und sonstige technische Arbeitsmittel dürfen nur genutzt werden, wenn Sie von der IT-Abteilung zur Verwendung freigegeben wurden.
Eine Vernetzung nicht freigegebener oder privater Geräte mit der Infrastruktur des Unternehmens darf nicht erfolgen. Geräte dürfen nicht an andere Personen weitergegeben werden.
Das Installieren von Software auf Arbeitsplatzsystemen oder anderen dienstlich bereitgestellten IT-Systemen, sofern diese nicht explizit dafür bereitgestellt wurden, ist grundsätzlich untersagt.