IT-Sicherheitsrichtlinien

Leitfaden zur Nutzung der IT-Infrastruktur und zum sicheren Umgang
mit Daten und Informationen

- Externe Mitarbeiter -

Dresdner Bank

Verteiler:

Geltung	Zielgruppe
bankweit	Externe Mitarbeiter

Angaben zum Dokument:

Name des Dokuments: Leitfaden zur Nutzung der IT-Infrastruktur und zum sicheren Umgang mit Daten und Informationen

Version: 1.0

Stand: 31.01.2001

Autoren: Corporate Center IT, Frankfurt

Management Services

IT-Sicherheit / Datenschutz

Inhaltsverzeichnis

Seite

Einleitung

Als Kreditinstitut muss die Dresdner Bank in besonderem Masse Vorkehrungen zur Sicherstellung der Vertraulichkeit und Sicherheit treffen. Für das Vertragsverhältnis mit externen Dienstleistern gilt deshalb, dass bei der Nutzung der Infrastruktur des Leistungsempfängers die entsprechenden Regelwerke zur Sicherheit zu beachten sind. Die nachfolgenden Hinweise helfen Ihnen, wesentliche Sicherheitsanforderungen in der Praxis zu leben. Informieren Sie sich aber bitte auch über andere Regelwerke zur Informationssicherheit, denn Verstöße können entsprechende rechtliche Konsequenzen nach sich ziehen, die auch die fristlose Beendigung des Vertragsverhältnisses einschließen.

Weitere Informationen können Sie im Intranet (Homepage / Allgemeine Informationen / IT-Sicherheit in der Dresdner Bank Gruppe oder Quick Navigate / IT-Sicherheit) abrufen. Dort finden Sie Ansprechpartner und Adressen, die Ihnen bei Fragen zur Interpretation von Sicherheitsanweisungen weiterhelfen.

Umgang mit geschäftlichen Daten und Informationen

- ☞ Geschäftliche Unterlagen und Informationen, die Sie im Rahmen Ihres Auftrags bearbeiten, sind grundsätzlich vertraulich. Verhalten Sie sich deshalb in der Öffentlichkeit entsprechend zurückhaltend.
- ☞ Geschäftsunterlagen – auch in Form von Abschriften und Fotokopien – dürfen nicht aus den Räumen der Bank mitgenommen werden.
- ☞ Um den Zugriff Unbefugter auf vertrauliche Informationen (in Papierform oder auf Datenträgern) zu verhindern, lassen Sie diese nicht unbeaufsichtigt auf Ihrem Schreibtisch liegen. Bei Dienstschluss nehmen Sie sämtliche Arbeitsunterlagen, insbesondere vertrauliche Informationen, unter Verschluss. Schreibtische und Schränke, in denen dienstliche Unterlagen aufbewahrt werden, müssen abgeschlossen, die Schlüssel sicher verwahrt werden. Nehmen Sie auf keinen Fall geschäftliche Unterlagen unter privaten Verschluss.
- ☞ Lassen Sie keine vertraulichen Informationen in der „grünen Box“ oder Papierkörben liegen. Entsorgen Sie Unterlagen datenschutzgerecht.
- ☞ Speichern Sie keine Daten auf dem lokalen Laufwerk (in der Regel Laufwerk C:\) des überlassenen Computers. Benutzen Sie die zugewiesenen Serverlaufwerke. Damit sind ein entsprechender Zugriffsschutz und vor allem die zentrale Datensicherung für den Fall eines eingetretenen Datenverlustes gewährleistet.
- ☞ Wenn Sie Dateien mit personenbezogenen Daten anlegen, die auf Dauer genutzt werden sollen, beachten Sie bitte die jeweiligen datenschutzrechtlichen Vorschriften. Fragen Sie gegebenenfalls bei Ihrem Datenschutzbeauftragten nach.

Zugang zu IT-Systemen

- ☞ Über den Leistungsempfänger erhalten Sie den für Ihren Auftrag erforderlichen Zugang zu IT-Systemen und Anwendungen der Bank. Dieser erfolgt mit Hilfe einer Benutzerkennung (Betriebsausweis oder User-ID) und eines individuellen Passwortes. Versuchen Sie nie auf Systeme zuzugreifen, für die Sie keine Berechtigungen bekommen haben.
- ☞ Wählen Sie ein Passwort entsprechend den geltenden Passwortregeln.
- ☞ Gehen Sie sorgfältig mit Ihren Identifikations- und Authentisierungsmitteln um. Vermerken Sie Ihr Passwort niemals auf oder unter der Tastatur, am Bildschirm oder als Zettel

auf oder im Schreibtisch. Speichern Sie es nicht klartextlich auf Ihrem PC. Sofern Sie von zu Hause oder von unterwegs Zugang zum Dresdner Bank Netzwerk haben, bewahren Sie die für die Authentisierung benötigte Token Card getrennt von Ihrem Computer auf.

- ☞ Bedenken Sie bitte: Sie sind für alle Ereignisse verantwortlich, die mit Ihrer Benutzerkennung und Ihrem Passwort auf IT-Systemen der Bank ausgeführt werden. Geben Sie deshalb weder Ihren Betriebsausweis noch Ihr Passwort weiter; lassen Sie Ihren Betriebsausweis nicht unbeaufsichtigt liegen.
- ☞ Wenn Sie Ihren Arbeitsplatz verlassen, sperren Sie Ihr Terminal bzw. Ihren PC und entnehmen Sie Ihren Betriebsausweis. Achten Sie darauf, dass bei den Bildschirmschonern der Kennwortschutz aktiviert ist.

Nutzung von IT-Systemen

- ☞ Bedenken Sie, dass Ihnen die Bank Hard- und Software zur Verfügung stellt, um Aufträge schnell und effizient zu erledigen. Unterlassen Sie jeden Missbrauch.
- ☞ Um eine Beeinträchtigung des komplexen IT-Betriebs zu vermeiden, darf private Hard- und Software in der Bank nicht eingesetzt werden. Es ist strikt untersagt, eigene IT-Einrichtungen, zum Beispiel Computer oder Modems, mit IT-Systemen der Bank zu verbinden.
- ☞ Veränderungen an der Hardware dürfen nur durch autorisierte Personen, in der Regel die Administratoren, durchgeführt werden.
- ☞ Software darf nur nach Genehmigung kopiert oder verteilt werden.
- ☞ Zur Vermeidung von Schäden für die IT-Infrastruktur darf auf den Computern nur genehmigte, freigegebene und virenfreie Software installiert werden, die aus vertrauenswürdigen Quellen beschafft wurde. Hierbei müssen lizenzrechtliche Bestimmungen und andere Schutzrechte, auch beim Laden über das Internet, strikt eingehalten werden. Die Installation von Software, auch Share-, Freeware oder Public Domain Software, darf deshalb nur durch autorisierte Administratoren und nach Genehmigung durchgeführt werden.

Nutzung von portablen Computern

- ☞ Sofern es aus betrieblichen Gründen erforderlich ist, Geschäftsdaten auch mobil bearbeiten zu können, wird Ihnen ein portabler Computer zur Verfügung gestellt.
- ☞ Laptops sind bei Dienstschluss einzuschließen. So können Sie Diebstahl und Datenverlusten vorbeugen. Müssen die tragbaren Computer in der Dockingstation verbleiben, sollten Sie den Rechner mit Hilfe eines speziellen Kabels absichern; das Verschließen in der Dockingstation allein ist nicht ausreichend.
- ☞ Auf Laptops und Notebooks dürfen vertrauliche Daten nur dann auf lokalen Laufwerken gespeichert werden, wenn diese mobilen Geräte mit entsprechender Sicherheitssoftware ausgestattet sind, die den Zugriff Unbefugter etwa nach einem Diebstahl des Gerätes verhindert.
- ☞ Als Nutzer eines Laptops oder Notebooks sind Sie dafür verantwortlich, dass nur unbedingt erforderliche Datenbestände lokal gespeichert und diese, sofern erforderlich, regelmäßig auf zentralen Servern gesichert werden.

Virengefahr

- ☞ Auf Ihrem Computer ist normalerweise eine Anti-Viren-Software aktiviert. Sie unterstützt dabei, Datenträger (Festplatte, Disketten, CDs) und insbesondere E-Mail-Anhänge automatisch auf Viren zu überprüfen.
- ☞ Wird ein Virus entdeckt oder vermutet, setzen Sie sich bitte unverzüglich mit Ihrem Administrator in Verbindung. Versuchen Sie nicht, ihn selbst zu entfernen.
- ☞ Unterstützen Sie diese Maßnahmen, indem Sie Disketten oder E-Mails zweifelhafter Herkunft nicht nutzen, öffnen, ausführen oder weiterleiten. Im Zweifel löschen Sie E-Mails unverzüglich.

Electronic Mail (E-Mail)

- ☞ E-Mail steht grundsätzlich nur für geschäftliche Zwecke zur Verfügung. Denken Sie daran, dass jedes E-Mail aus der Bank beim Empfänger als Banknachricht erscheint.
- ☞ E-Mails sind mit einer Postkarte zu vergleichen. Sie können grundsätzlich nicht ausschließen, dass Ihre E-Mail von Dritten gelesen werden kann. Es müssen deshalb Sicherheitsmaßnahmen (Verschlüsselung) getroffen werden, wenn besonders vertrauliche Daten über E-Mail, vor allem nach außerhalb, versandt werden sollen. Fragen Sie hierzu Ihren Administrator oder die zuständige Stelle für Informationssicherheit.
- ☞ Für das Verfassen von E-Mails gilt: Fassen Sie sich bitte kurz und verzichten Sie auf eine breite Streuung. Vermeiden Sie das Versenden umfangreicher Dokumente. Nutzen Sie die Möglichkeit, Dateianhänge vor der Versendung zu komprimieren. Achten Sie bei Ihren E-Mails auf einen Inhalt und Stil, wie er bei Geschäftsbriefen üblich ist.
- ☞ Bei der Unterschrift einer E-Mail sorgen Sie bitte dafür, dass neben der Organisationseinheit der Dresdner Bank, für die Sie tätig sind, auch Ihre Ursprungsfirma erkennbar ist.
- ☞ E-Mails, die ausschließlich für einen bestimmten Adressaten bestimmt sind, sollten Sie entsprechend kennzeichnen. Nutzen Sie die verschiedenen Optionen des E-Mail-Systems, mit denen Sie die Weiterleitung steuern oder auch verhindern können.
- ☞ Es versteht sich von selbst, dass beleidigende Äußerungen auch in E-Mails unterbleiben müssen. Der Versand von allem, das andere Personengruppen zum Beispiel in rassistischer, sexistischer, religiöser oder anderer Hinsicht herabsetzen kann, ist ausdrücklich untersagt.
- ☞ Achten Sie auch darauf, dass in einer E-Mail keinerlei Verleumdungen oder sonstige strafrechtlich relevante Äußerungen vorkommen. Informationen oder Äußerungen, die zum Nachteil der Bank ausgelegt werden können, dürfen nicht übermittelt werden.
- ☞ Stellen Sie sicher, dass auch bei Ihrer Abwesenheit E-Mails bearbeitet werden können. Nutzen Sie hierfür die verschiedenen Hilfsmittel Ihres E-Mail-Programms, um E-Mails intern weiterzuleiten.
- ☞ Interne E-Mails dürfen nicht unbesehen oder automatisch an externe Email-Adressen weitergeleitet werden. Dies schließt auch die Weiterleitung an private Email-Adressen ein. E-Mails, die an interne und externe Empfänger gerichtet sind, müssen jeweils separat und mit entsprechenden Hinweisen versandt werden.
- ☞ Ketten-E-Mails oder andere unerwünscht zugesandte Informationen belasten das E-Mail-System und dürfen deshalb nicht weiterverbreitet werden. Löschen Sie eingehende Mails dieser Art umgehend.

- ☞ Über Internet-Mail erhaltene Informationen sollten Sie überprüfen, bevor Sie sie geschäftlich nutzen. Behandeln Sie Nachrichten aus dem Internet als potentiell nicht vertrauenswürdig.
- ☞ Da durch den Zugang zu privaten oder über das World Wide Web erreichbaren, freien Mail-Services von Banksystemen aus Sicherheitssysteme der Bank unwirksam werden können, ist deren Nutzung nicht gestattet.

Internet-Dienste

- ☞ Der Zugang zum Internet steht grundsätzlich nur für geschäftliche Zwecke zur Verfügung. Verbindungen zum Internet über dezentrale Modems oder ISDN-Karten sind aus Sicherheitsgründen strikt untersagt. Der Zugang erfolgt ausschließlich über zentrale Internet-Übergänge.
- ☞ Der Zugriff auf Seiten mit pornografischen, rassistischen, diskriminierenden oder sonstigen radikalen Inhalten sowie das Abspeichern und Verbreiten entsprechender Informationen und Bilder ist untersagt. Der Zugriffsversuch auf diese Seiten wird automatisiert abgewiesen.
- ☞ Für die Teilnahme an Chat-Diensten, die Subskription von Newsgruppen oder die Anmeldung/Registrierung bei Online-Services ist die schriftliche Zustimmung des Leistungsempfängers erforderlich. Sofern Sie von solchen Services Gebrauch machen, denken Sie daran: auch hier gilt das Gebot der Vertraulichkeit. Bankinterne Angelegenheiten dürfen über diesen Weg nicht an die Öffentlichkeit gelangen. Bedenken Sie, dass Ihre Äußerungen auf die Bank zurückgeführt werden können. Über diese Services publizierte Informationen dürfen nicht als offizielle Stellungnahme der Bank ausgelegt werden können.
- ☞ Beleidigende oder verleumderische Äußerungen, die Diskriminierung von Minderheiten, der Aufruf zu Straftaten oder andere Informationen, die zum Nachteil der Bank ausgelegt werden können, dürfen in keinem Fall verbreitet werden.
- ☞ Informationen, die aus dem Internet abgerufen werden, müssen als potentiell unzuverlässig angesehen werden, es sei denn sie stammen aus einer nachweislich zuverlässigen Quelle.

Telefax und Telefon

- ☞ Telefax und Telefon gehören zu den alltäglichen Arbeitsmitteln. Allerdings sind mit diesen Services auch Risiken verbunden. Helfen Sie mit, dass auf diesem Weg nicht durch sorgloses Verhalten vertrauliche Informationen offengelegt werden.
- ☞ Verständigen Sie vor dem Absenden eines Faxes mit besonders sensiblen Daten den Adressaten über den konkreten Zeitpunkt der Übermittlung. Vergewissern Sie sich, dass der Adressat unter der Ihnen bekannten Fax-Anschlussnummer erreichbar ist. Lassen Sie sich den Erhalt gegebenenfalls bestätigen.
- ☞ Versehen Sie jede Telefax-Sendung mit Datum, Absender, Adressat, Telefonnummer, Faxnummer und Seitenzahl. Sofern landesüblich oder geschäftlich angewiesen, fügen Sie auch eine Haftungsausschlussformel (sogenannter Disclaimer) hinzu.
- ☞ Die unbefugte Nutzung des Telefons verursacht Kosten. Sperren Sie deshalb, soweit technisch möglich, bei Dienstschluss Ihr Telefon ab, um Missbrauch vorzubeugen.

Information bei besonderen Vorkommnissen

☞ Bei besonderen Vorkommnissen, zum Beispiel Diebstahl oder Virenbefall, informieren Sie bitte unverzüglich Ihren direkten Ansprechpartner beim Leistungsempfänger sowie die zuständigen Administratoren.