Dokument ID
Titel:
Abteilungskürzel:
Datum:
Version:

Anlage Richtlinie Informationssicherheit für Externe

zu den Einkaufsbedingungen der Volkswagen Financial Services AG für Leistungen auf dem Gebiet der Informationstechnologie (IT) und/oder der elektronischen Information und Kommunikation (TK) („Einkaufsbedingungen“)
Stand: März 2017

Inhaltsverzeichnis

1. Grundlagen Informationssicherheit 3

1.1 Was ist Informationssicherheit? 3

1.2 Welche Informationen müssen geschützt werden? 3

1.3 Verantwortung für Informationssicherheit 3

1.4 Kontakt bei Störungen und Fragen zur Informationssicherheit 4

2. Sicherheitsregelungen für den Arbeitsplatz 4

2.1 Schutz des Arbeitsplatzrechners (PC) 4

2.2 Schutz von Zugangsdaten 5

2.3 Passwort Schutz 5

2.4 Aufbewahrung von Informationen 6

3. Allgemeine Regelungen 6

3.1 Nutzung des Firmennetzwerks 6

3.2 Installation von Software / Hardware auf Unternehmens-PCs 6

3.3 Nutzung des VW FS E-Mail Accounts 6

3.4 Nutzung des Internets 6

3.5 Einsatz von USB Geräten 7

3.6 Einsatz von mobilen Datenträgern 7

3.6.1 Definitionen 7

3.6.2 Datenaustausch mit mobilen Datenträgern 7

3.6.3 Übernahme von Datenträgern 8

3.6.4 Weitergabe von Datenträgern 8

3.6.5 Kennzeichnung 8

3.6.6 Aufbewahrung 8

3.6.7 Versand 9

3.6.8 Entsorgung 9

3.7 Informationsaustausch 9

3.7.1 Weitergabe von Daten und Programmen an Externe 9

3.8 Datenverfügbarkeit 9

3.9 Verschlüsselung 10

3.10 Remotezugriff/Fernzugang 10

3.11 Rückgabe von Firmeneigentum 10

4. Regelungen zum Informationsschutz 11

4.1 Grundsätze zum Umgang mit Informationen 11

4.2 Klassifizierung und Kennzeichnung von Informationen 11
4.3 Verlust 12

1. Grundlagen Informationssicherheit

1.1 Was ist Informationssicherheit?

Informationen sind ein Wirtschaftsgut (Asset) der VW FS AG. Informationen, die das Unternehmen sammelt, verarbeitet, wartet, speichert, versendet und bei Bedarf vernichtet sind wesentlicher Bestandteil der täglichen Arbeit im Unternehmen.

Informationssicherheit beinhaltet den Schutz von Unternehmensinformationen, Software und IT-Infrastruktur vor ungewollter Enthüllung, fehlerhafter Veränderung, Störung oder Vernichtung. Zusätzlich werden Anforderungen bezüglich Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Informationen berücksichtigt.

1.2 Welche Informationen müssen geschützt werden?

Jeder externe Mitarbeiter, der berechtigt mit VW FS AG Systemen arbeitet, hat Zugriff auf Unternehmensinformationen und ist daher ein wichtiger und aktiver Bestandteil der Sicherheitsmaßnahmen. Die VW FS AG definiert drei Arten von Informationen, die geschützt werden müssen:

Geheime Informationen - Geheime Informationen sind Informationen, deren Kenntnis durch Unbefugte das Erreichen von Unternehmenszielen nachhaltig gefährden kann und die daher einem äußerst restriktiven Verteiler sowie strikten Kontrollen unterliegen müssen.

Vertrauliche Informationen - Vertrauliche Informationen sind Informationen, deren Kenntnis durch Unbefugte das Erreichen von Produkt- und Projektzielen gefährden kann und die daher nur einem begrenzten berechtigten Personenkreis zugänglich gemacht werden dürfen. Zu dieser Kategorie gehören auch personenbezogene Informationen, die in ihrem Zusammenhang Aussagen über eine Person erlauben.

Interne Informationen - Interne Informationen sind Informationen, die nur innerhalb der VW FS Gruppe veröffentlicht werden dürfen und nicht für die allgemeine Öffentlichkeit bestimmt sind. VW FS AG Informationen dürfen an Dritte nicht weitergegeben werden, es sei denn:

- Die Information ist als öffentlich klassifiziert oder
- Der Informationseigentümer hat die Information zur Weitergabe freigegeben oder
- Externe Dritte sind als Dienstleister auf die Information für die Zusammenarbeit angewiesen.

1.3 Verantwortung für Informationssicherheit

Jeder externe Mitarbeiter ist beim Umgang mit Informationen und informationsverarbeitenden Einrichtungen für die Einhaltung von Sicherheitsvorgaben verantwortlich, insbesondere für:

- Das Verhindern von unbefugtem Zugriff
- Das Verhindern von Kompromittierung und Diebstahl von Informationen und informationsverarbeitenden Einrichtungen

- Inhaltliche Richtigkeit der Daten
- Die Einhaltung der gesetzlichen und regulativen Bestimmungen, insbesondere des Bundesdatenschutzgesetzes sowie der Handels- und Steuergesetze und
- Schutz der Rechte und Interessen aller natürlichen und juristischen Personen, die mit der VW FS Gruppe in geschäftlicher Beziehung stehen

1.4 Kontakt bei Störungen und Fragen zur Informationssicherheit

Bei Störungen und Informationssicherheitsvorfällen ist der Enterprise Help Desk (EHD, Tel.: 0531/212-2919) anzurufen.

Nutzen Sie niemals selbst einen Exploit (eine Software, die einen Vorteil aus einem Fehler, einer Störung oder einer Schwachstelle zieht, um ein unbeabsichtigtes Verhalten auf Ihrem Computer zu verursachen), um zu zeigen, dass eine Sicherheitslücke auf Ihrem System (immer noch) vorhanden ist.

2. Sicherheitsregelungen für den Arbeitsplatz

2.1 Schutz des Arbeitsplatzrechners (PC)

Geräte im Einsatz der VW FS AG sind mit aktuellen Schutzprogrammen zum Schutz vor Viren und verschiedensten Formen von Malware ausgerüstet. Die Installation von Schutzprogrammen wird zentral durch die IT vorgenommen. Der Benutzer darf die bei der Installation des PCs eingerichteten Datensicherheitsmaßnahmen nicht deaktivieren.

Da auch neuste Schutzprogramme nicht 100% gegen neue Schadsoftware schützen kann, sind folgende Verhaltensregeln einzuhalten:

- Misstrauen Sie unerwarteten E-Mails und insbesondere ihren Dateianhängen.
- Löschen Sie ungeöffnet zweifelhafte E-Mails die offensichtlich nicht beruflich sind und unaufgefordert eingesendet wurden (z.B.: Werbemails, Scherzmails mit Anhang, etc.) und
- Schließen Sie keine Datenträger mit nicht beruflichem Zusammenhang an die Geräte an

Sperren des PCs:
- Tastaturbefehl **STRG + ALT + ENTF** und Betätigung des Buttons ***Computer sperren***

ODER
- Tastenkombination **WINDOWS + L**

Entsperren des PCs:
- Tastaturbefehl **STRG + ALT + ENTF**

Jeder elektronische Datenträger (Wechselplatte, USB-Stick usw.) der VW FS AG wird vor der Verwendung hinsichtlich schadenstiftender Software (z. B. Computerviren) automatisch untersucht. Auch E-Mail-Anhänge werden beim Empfang automatisch überprüft.

Bei Verlassen des Arbeitsplatzes muss der PC gesperrt werden. Zusätzlich muss die Dunkelschaltung des Bildschirmes so eingerichtet bleiben, dass sie automatisch nach wenigen Minuten Nicht-Benutzung selbsttätig aktiviert wird und nur durch Eingabe des Passwortes wieder aufgehoben werden kann. Damit soll vermieden werden, dass bei unvorhergesehener längerer Abwesenheit Nicht-Berechtigte Zugriff zu Daten und Programmen erhalten.

Ist die Arbeit am PC beendet, sind ein ordnungsgemäßer Systemabschluss durchzuführen und der PC inklusive des Bildschirmes auszuschalten.

2.2 Schutz von Zugangsdaten

Für den Zugang zu den Systemen der VW FS AG sind Zugangsdaten erforderlich. Diese bestehen aus einer Benutzerkennung (DKX- oder DKXS Nummer) und einem Passwort, welches ein sicheres Anmeldeverfahren für alle Systeme darstellt und individuell für Sie erstellt wurde. Für den Fernzugriff ist eine Zwei-Faktor-Autorisierung bestehend aus Passwort und SecureID Token notwendig.

Jeder externe Mitarbeiter ist verantwortlich für alle Handlungen, die mit Hilfe seiner Zugangsdaten verrichtet werden. Der Schutz der Zugangsdaten steht somit in der Verantwortung jedes einzelnen Mitarbeiters.

Erlaubt der externe Mitarbeiter einem zweiten Mitarbeiter an seinem PC zu arbeiten, so muss sich der externe Mitarbeiter vorher aus allen bestehenden Anwendungen (Großrechner, Netzwerk, etc.) und vom System abmelden. Der zweite Mitarbeiter muss sich mit seiner Benutzerkennung und seinem Passwort neu anmelden. Teamarbeit unter Benutzung Ihrer Zugangsdaten ist unter Ihrer direkten Aufsicht erlaubt.

Für Notfälle können spezielle Notfall-User und -Passworte definiert sein. Dies wird im Einzelnen in speziellen Notfall-Verfahren separat geregelt.

2.3 Passwort Schutz

Passwörter dürfen nur dem Benutzer bekannt sein und sollten eine genügend hohe Komplexität aufweisen. Die folgenden Regeln sind zu beachten:

1. Passwörter dürfen Dritten nicht zugänglich gemacht werden (z.B. Mitteilen, offene Notiz, im Klartext speichern, etc.).
2. Das Passwort darf nur dem Benutzer bekannt sein.
3. Initial-Passwörter müssen sofort gewechselt werden.
4. Es sind „starke“ Passwörter zu verwenden. Ein starkes Passwort folgt den Regeln „Length – Strength – Duration“:
    - Length: die Mindestlänge eines Passworts beträgt 10 Zeichen
    - Strength: Kombination aus Buchstaben und 2 Ziffern/bzw. Sonderzeichen, die in keinem Wörterbuch steht mit mindestens 3 der 4 folgenden Kriterien:
        - Großbuchstaben (A-Z)
        - Kleinbuchstaben (a-z)
        - Ziffern (0-9)
        - Sonderzeichen ($, #, *, % …)
    - Duration: Änderung des Passwortes nach einem definierten Zeitraum
5. Passwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sind beispielsweise nicht zur Bildung von Passwörtern geeignet. Es dürfen niemals Trivialpasswörter verwendet werden (z. B.: Passwort, Hund, Auto, 4711; 12345 oder andere nebeneinanderliegende Tasten).
    - Eine einfache Variante zum Erstellen und Merken von starken Passwörtern sind sogenannte Passphrasen: Ein Satz als Passwort wie z.B.: „Ichwar17in1987!“
6. Passwörter sind individuell zu verwenden (keine Mehrfachverwendung).

2.4 Aufbewahrung von Informationen

Vertrauliche und geheime Informationen sind durch angemessene Maßnahmen gegen unberechtigte Einsichtnahme zu schützen:

Vertrauliche Informationen sind in verschlossenen Büromöbeln oder in Räumen, die außerhalb der Arbeitszeit verschlossen und nur von einem berechtigten Personenkreis aufgeschlossen werden können, aufzubewahren.

Speziell als vertraulich gekennzeichnete Informationen dürfen nicht unbeaufsichtigt liegen gelassen werden.

Geheime Informationen sind durch strikte, umfassende Maßnahmen gegen die unberechtigte Einsichtnahme Dritter zu schützen (z.B. Einschließen in Stahlschrank, elektronischen Zugang mit Zwei-Faktor-Authentisierung sichern).

Nach Ende eines Arbeitstages sind alle vertraulichen und geheimen Informationen verschlossen aufzubewahren („Clean Desk“).

In Dateien vorliegende Informationen, die als „vertraulich“ oder „geheim“ klassifiziert sind, müssen in einer geeigneten Ablagestruktur (z. B. Unterverzeichnisse von Gruppenlaufwerken) gespeichert werden. Die Zugriffe auf diese Ablagestruktur sind restriktiv einzurichten.

3. Allgemeine Regelungen

3.1 Nutzung des Firmennetzwerks

Am Netzwerk der Volkswagen Financial Services Gruppe, abgesehen vom WLAN Gastzugang, dürfen nur PCs betrieben werden, die sich in deren Besitz befinden.

3.2 Installation von Software / Hardware auf Unternehmens-PCs

Entsprechend der Sicherheitsrichtlinie der VW FS AG darf keine nicht lizensierte, nicht freigegebene oder nicht arbeitsbezogene Software auf Unternehmens-PCs installiert werden. Für den Großteil der Anwender bestehen Einschränkungen auf den Unternehmens PCs, die eine Installation von Software verhindern.

Nur autorisiertes Personal aus dem Systembetrieb darf Änderungen an Systemeinstellungen vornehmen, oder Hardware und Software auf Unternehmens PCs installieren.

Hardware darf nur von autorisiertem Personal transportiert werden.

3.3 Nutzung des VW FS E-Mail Accounts

Die Nutzung des VW FS E-Mail Accounts ist zweckgebunden für geschäfltiche Zwecke gestattet. Geschäfliche Informationen dürfen nur an geschäftliche E-Mail Adressen geschickt werden. Das Versenden von geschäftlichen Informationen an private E-Mail Adressen ist ausschließlich dann gestattet, wenn der Kunde / Vertragspartner / Dienstleister von sich aus Informationen per E-Mail anfordert. Hierbei sind E-Mails mit vertraulichen oder geheimen Informationen zu verschlüsseln.

3.4 Nutzung des Internets

Die Nutzung des Internets ist für geschäftliche Belange gestattet.

Die vorstehende Regelung bezieht sich nur auf beantragte und genehmigte Internetzugänge. Ein Rechtsanspruch auf Einrichtung eines Internetzugangs wird hiermit nicht begründet.

Folgende Anforderungen im Hinblick auf Datenschutz und –sicherheit sind zu beachten:

- Über das Internet dürfen keine geheimen oder vertraulichen Informationen (siehe Kapitel 1.2) ohne ausreichende Verschlüsselung übertragen werden. Dies gilt insbesondere für den Datenaustausch mittels elektronischer Post (E-Mail).
- Der Internet-Zugang ist über das User-Management zu beantragen.
- Im Internet verfügbare Dienste (z. B. Mailing-Listen, Microsoft Knowledge Base, etc.) dürfen genutzt werden wenn diese über einen Web-Browser erreichbar sind.
- Aus dem Internet darf keine Software heruntergeladen werden.

3.5 Einsatz von USB Geräten

Die Benutzung privater USB Geräte jeglicher Art ist verboten. Die Benutzung von firmeneigenen USB Geräten kann genehmigt werden.

3.6 Einsatz von mobilen Datenträgern

3.6.1 Definitionen

Als mobile Datenträger werden alle Formen von mobilen, (wieder-) beschreibbaren Medien bezeichnet. Beispiele hierfür sind u. a:

- CD-ROMs, CD-RWs
- DVD-ROMs, DVD-RWs
- USB Laufwerke (z.B. USB-Sticks, USB-Laufwerke…)
- SD/ MMC/ Flash Karten (auch fest eingebaute)
- externe Festplatten
- nichtflüchtiger Speicher (Flashspeicher) in mobilen Endgeräten (z. B. xDAs, Mobiltelefon)

3.6.2 Datenaustausch mit mobilen Datenträgern

Der wichtigste Aspekt im Rahmen des Datenaustausches mittels Datenträgern ist der Schutz vor der Übertragung von Viren in das System. Viren können die erstellten Dokumente bzw. andere auf dem System gespeicherte Daten und Programme verfälschen, zerstören oder löschen. In jedem Fall entsteht für das Unternehmen ein finanzieller Schaden. Zusätzlich besteht die Gefahr, dass Datenträger mit vertraulichen Informationen verloren gehen oder (gewaltsam) entwendet werden.

- Soweit wie möglich, ist auf den Datenträgeraustausch jeglicher Herkunft zu verzichten. Die Möglichkeiten des elektronischen Datenaustausches im Netz sind in jedem Fall zu nutzen!
- Auf VW FS eigenen Rechnern dürfen nur von VW FS ausgegebene Datenträger genutzt werden. Zur Nutzung von nicht-firmeneigenen Datenträgern siehe 3.6.3.
- Die Datenträger dürfen nur für geschäftliche Zwecke genutzt werden.
- Auf eine Speicherung von vertraulichen / geheimen Daten auf transportablen Datenträgern ist, soweit möglich, zu verzichten.
- Alle vertraulichen / geheimen Daten auf nichtflüchtigen Speichermedien sind vor unbefugtem Zugriff zu schützen und mittels Hardware oder Software zu verschlüsseln. Der Schlüssel ist vom Datenträger getrennt zu halten. Diese Regel gilt auch für fest

eingebauten Speicher (Flashspeicher) in Systemen (z. B. xDA). Es gelten die Mindestanforderungen der Passwortfestlegung aus Kapitel 2.3 „Passwort Schutz“. Eine ungeschützte Speicherung von vertraulichen oder geheimen Daten auf transportablen Datenträgern ist nicht erlaubt.

- Unbefugten Personen gegenüber ist der Zugriff auf die Datenträger zu verwehren.
- Der Verlust eines Datenträgers ist umgehend den zuständigen Stellen (interner Fachbreich, bei vertraulichen oder geheimen Informationen Datenschutzbeauftragter und IT Security) anzuzeigen.
- Bei einer Aufbewahrung im Kraftfahrzeug muss der Datenträger so abgelegt werden, dass er von außen nicht sichtbar ist.
- Bei Flug- und Bahnreisen sind Datenträger als Handgepäck zu transportieren. Bei Auslandsreisen müssen die länderspezifischen Regelungen zum Einsatz von Verschlüsselung beachtet werden.

3.6.3 Übernahme von Datenträgern

Das Einspielen von Daten mittels Datenträgern wird in der Regel vom Enterprise Help Desk (EHD) vorgenommen. Diese prüfen den Datenträger auf Viren und kopieren die Daten in das Netzwerk. Die CD-ROM/DVD-ROM-Laufwerke sowie die USB-Ports und Kartenleser sind daher standardmäßig deaktiviert und werden nur in begründeten Ausnahmefällen durch einen formlosen schriftlichen Antrag des Leiters des internen Fachbereichs an Enterprise Help Desk wieder aktiviert. Das Enterprise Help Desk wird dann die Funktionsfähigkeit des Virenprüfprogramms checken. Bei PCs ohne Netzanschluss muss jeder Datenträger vor dem Einspielen auf Viren geprüft werden.

Die Übernahme und das Einspielen von Programmen durch den Benutzer ist nicht gestattet. Programme sind über das Standardverfahren zu beantragen, zu beschaffen und zu installieren.

3.6.4 Weitergabe von Datenträgern

Prinzipiell übernimmt Enterprise Help Desk das Kopieren der Daten auf Datenträgern. Hierdurch wird sichergestellt, dass sich auf den Datenträgern keine anderen Daten mehr befinden.

Auf PCs ohne Netzanschluss, mobilen Rechnern oder in genehmigten Ausnahmefällen können die Daten durch den Mitarbeiter auf Datenträgern erstellt werden. Dabei ist sicherzustellen, dass sich auf den Datenträgern nur die weiterzuleitenden Daten befinden. Es ist vom Anwender sicherzustellen, dass diese Datenträger lt. Auskunft der Antivirensoftware virenfrei sind.

Es ist Benutzern nicht erlaubt von mobilen Datenträgern Software auf firmeneigenen Computern zu installieren.

3.6.5 Kennzeichnung

Datenträger sind dem Inhalt entsprechend zu beschriften.

3.6.6 Aufbewahrung

Zur zugriffssicheren Verwahrung von Datenträgern reicht es im Allgemeinen aus, diese in den unternehmensseitig zur Verfügung gestellten Rollcontainern, Schränken etc. zu verschließen. Geheime und vertrauliche Informationen sind generell so aufzubewahren, dass Unbefugte keinen Zugriff haben.

3.6.7 Versand

Bei Versand sind Datenträger gegen mechanische, thermische und magnetische Einflüsse zu schützen. Entsprechende Behältnisse sind über das Bestellsystem zu beschaffen.

3.6.8 Entsorgung

Nicht mehr benötigte Datenträger müssen an die Abteilung „Client Platform & User Management„ zurückgegeben werden, wo sie fachgerecht entsorgt werden.

Die Datenträger sind, insbesondere bei vertraulichen und geheimen Informationen, vom Benutzer vorher zu löschen oder unbrauchbar zu machen.

3.7 Informationsaustausch

Für den sicheren Informationsaustausch sind die Regeln aus Kapitel 4 „Regelungen zum Informationsschutz“ zu beachten.

3.7.1 Weitergabe von Daten und Programmen an Externe

Daten und Programme dürfen an fremde Gesellschaften, Behörden, Institutionen und sonstige Dritte außerhalb der Volkswagen Financial Services Gruppe nur weitergegeben werden, wenn dies gemäß bestehender Regelungen, Anweisungen oder Verfahren erlaubt ist.

3.8 Datenverfügbarkeit

Das Unternehmen ist verantwortlich für die Datenverfügbarkeit im Firmennetzwerk. Alle erstellten Dateien sind im Netzwerk der VW FS AG auf den dafür vorgesehen Netzwerklaufwerken zu speichern. Aufbau und die Struktur abteilungsrelevanter zu sichernden Daten wird innerhalb der Abteilungen bestimmt. Zur Sicherung der Daten sind die vom Usermanagement eingerichteten Netzlaufwerke zu nutzen. Folgender Aufbau der Laufwerke ist zu beachten:

C: lokale Festplatte

G: Abteilungsdaten (Netzlaufwerk)

H: Homeverzeichnis (Netzlaufwerk)

I: Datenaustausch über mehrere Abteilungen

P: Programme vom Server

S: Basisverzeichnis des Datenservers

X: CD-Laufwerk

Jeder Benutzer besitzt das Homeverzeichnis H. Dieses Verzeichnis dient ausschließlich der persönlichen Datensicherung geschäftlicher Belange (z. B. Anwesenheit). Dieses Verzeichnis kann nur der angemeldete Benutzer einsehen, deshalb ist es nicht für den Datenaustausch innerhalb der organisatorischen Einheit geeignet.

Die Daten der lokalen Festplatten (z. B. C:) werden nicht automatisch gesichert und dürfen nicht für die Speicherung von relevanten Dokumenten benutzt werden. Einzige Ausnahme ist das Verzeichnis „Eigene Dokumente“, dessen Inhalt automatisch bei bestehender Verbindung zum Firmennetzwerk auf den Unternehmensservern gesichert wird. Benutzer von Notebooks sind verantwortlich sich so oft wie möglich über VPN oder direkt mit dem Firmennetzwerk zu verbinden, um die Synchronisation der Dokumente im „Eigene Dokumente“ Verzeichnis zu gewährleisten.

3.9 Verschlüsselung

Vertrauliche und geheime Informationen sind verschlüsselt zu übertragen.

Für viele externe Unternehmen ist eine verschlüsselte E-Mail-Verbindung eingerichtet, welche automatisch benutzt wird, wenn das firmeneigene E-Mail-System verwendet wird. Für diese Unternehmen ist keine E-Mail-Verschlüsselung notwendig. Eine Liste dieser Unternehmen findet sich im Intranet unter „TLS (E-Mail Verschlüsselung)“. Dort ist auch erläutert, wie eine neue E-Mail-Verschlüsselung beantragt werden kann.

Für alle anderen Unternehmen kann die Verschlüsselungsfunktion von Kompressionstools wie 7zip genutzt werden, um vertrauliche Informationen zu übermitteln. In diesem Fall ist das benutzte Passwort (siehe dazu auch Kapitel 2.3 „Passwort Schutz“) dem Empfänger über einen anderen Kommunikationsweg zu übermitteln (z.B. Telefon). Die hier benutzten Passwörter dürfen nur einmal benutzt werden.

3.10 Remotezugriff/Fernzugang

Bei Fernzugriffen ist CITRIX[1] zu verwenden. Für firmeneigene Notebooks kann ein Zugriff über VPN auf das Firmennetzwerk gewährt werden.

3.11 Rückgabe von Firmeneigentum

Bei Beendigung der Zusammenarbeit mit der VW FS AG sind alle im Besitz (oder unter der Kontrolle) des externen Mitarbeiters befindlichen Gegenstände, einschließlich (IT-)Geräte, Aufzeichnungen, Unterlagen und Daten an die VW FS AG zurückzugeben.

[1] CITRIX ist eine Software mit der remote innerhalb der VW FS AG gearbeitet werden kann. Der CITRIX Zugang muss beantragt werden.

4. Regelungen zum Informationsschutz

4.1 Grundsätze zum Umgang mit Informationen

Es gilt das „Kenntnis nur, wenn nötig“-Prinzip („need to know“), d.h. Informationen sind nur Personen zur Verfügung zu stellen, die ein berechtigtes betriebliches Interesse daran haben.

Insbesondere *vertrauliche* Informationen dürfen nur den direkt am Prozess Beteiligten zugänglich gemacht werden.

Die Zahl der mit der Bearbeitung *geheimer* Informationen beschäftigten Personen - auch von Besprechungsteilnehmern - ist auf das absolut notwendige Maß zu begrenzen. Mit der Einstufung *geheim* übernehmen Eigentümer und Empfänger die Verantwortung für die Kontrolle über den Verbleib der Unterlagen und/oder Datenträger.

4.2 Klassifizierung und Kennzeichnung von Informationen

Um einen angemessen Informationsschutz zu ermöglichen, müssen alle vorhandenen Informationen klassifiziert werden. Aus dieser Klassifizierung lassen sich notwendige Schutzmaßnahmen und grundsätzliche Vorgaben zum Umgang ableiten. Die folgende Tabelle enthält die Definition der einzelnen Informationsklassen, sowie deren Kennzeichnung, die Einschränkungen zur Weitergabe und das Löschen von Informationen in den einzelnen Klassen:

Vertraulich	
Informationen, deren Kenntnis, Modifizierung, Verlust oder Missbrauch durch Unbefugte das Erreichen von Produkt- und Projektzielen gefährden kann.	
Kennzeichnung:	Auf der ersten Seite des Dokuments, aber nur dann, wenn das Dokument besonderen Schutz gegen fremde Einsichtnahme benötigt
Weitergabe:	Nur an im Prozess beteiligte Personen oder an vertrauenswürdige Dritte, bei Sprachmedien unberechtigtes Zu-/Abhören verhindern.
Löschen und Ensorgung:	Zertifiziertes Löschen (z.B. Datenschutztonne), sichere Löschung von Datenträgern
Beispiel:	Revisionsberichte, Budgetpläne, Kundendaten, Personaldaten

Geheim	
Informationen, deren Kenntnis, Modifizierung, Verlust oder Missbrauch durch unbefugte Dritte das Erreichen von Unternehmenszielen nachhaltig gefährden kann.	
Kennzeichnung:	„Geheim“- Kennzeichnung oben rechts auf jeder Seite des Dokumentes
Weitergabe:	Nur an bestimmte Personen oder an vertrauenswürdige Dritte, bei Sprachmedien unberechtigtes Zu-/Abhören verhindern. Der Kreis der mit der Bearbeitung beschäftigen Personen wird durch den Informationseigentümer bestimmt und ist auf ein Minimum zu begrenzen.
Löschen und Entsorgung:	Zertifiziertes Löschen (z.B. Datenschutztonne)
Beispiel:	Strategische Planungen, neue Entwicklungen, Gesundheitsdaten

Tipps/Hinweise

- Die Klassifizierung von Informationen erfolgt grundsätzlich bei der Erstellung, spätestens bei der Ablage oder Weitergabe.
- Zugriffe auf Speicherorte für vertrauliche und/oder geheime Dokumente sind restriktiv zu vergeben.
- Im Zweifel sollte die sicherere Einstufung gewählt und/oder der Vorgesetzte hinzugezogen werden.
- Nicht gekennzeichnete Informationen sind als vertraulich zu behandeln, sofern sie nicht eindeutig als „öffentlich“ oder „intern“ eingestuft werden können.
- Die Einstufung „öffentlich“ darf nur durch speziell berechtigte Personen (z.B. Unternehmenskommunikation) vorgenommen werden.
- Personenbezogene Daten gemäß §3 BDSG (z.B. Name mit Adresse) sind als vertraulich zu kennzeichnen. Besondere Arten personenbezogener Daten gemäß §3 Abs. 9 BDSG (z.B. Gesundheitsdaten) sind als geheim zu kennzeichnen.

4.3 Verlust

Über vermisste oder verloren gegangene schutzbedürftige Informationen ist die Sicherheitszentrale unter der Durchwahl **-1717** unverzüglich zu informieren.

Gleiches gilt, wenn Anhaltspunkte für das unbefugte Öffnen verschlossener Aufbewahrungsmöbel vorliegen.

Bei Verlust von schutzbedürftigen Informationen der VW FS AG bei externen Firmen und Partnern ist die Sicherheitszentrale ebenfalls umgehend durch die Firma oder den Partner zu informieren.

Bei Kenntnis oder Verdacht von Datenverlusten aus IT-Systemen (z.B. durch Phishing, Trojaner oder unbefugte Übertragung von Daten außerhalb des Kontrollbereichs der VW FS AG) ist der Enterprise Helpdesk unter der Durchwahl **-2919** bzw. der Chief Information Security Officer (CISO) zu informieren. Diese Ereignisse werden entsprechend den Vorgaben zur Behandlung von IT-Sicherheitsvorfällen (IT Security Incident Management) behandelt.

Werden besonders sensible personenbezogene Daten durch die VW FS AG, einer ihrer Mitarbeiter oder durch einen weisungsgebundenen Dienstleister („Auftragsweise Verarbeitung von personenbezogenen Daten“) unrechtmäßig übermittelt oder gelangen sie Dritten auf sonstige Weise unrechtmäßig zur Kenntnis, ist der Datenschutzbeauftragte unverzüglich zu unterrichten. Zu den sensiblen personenbezogenen Daten zählen z.B.:

- Daten zu Bank- und Kreditkartenkonten,
- besondere Arten personenbezogener Daten (z. B. Gesundheitsdaten)
- Daten über strafbare Handlungen oder Ordnungswidrigkeiten (z. B. Geldwäsche, Betrug, Insolvenzstraftaten) bzw. den Verdacht darauf