

Österreichische Post AG
Unternehmenszentrale
Postgasse 8
1010 Wien

Betriebsvereinbarung
zur Nutzung von IT Ressourcen
gem. § 72 PBVG iVm §§ 96, 96 a ArbVG

abgeschlossen zwischen

der Österreichischen Post AG
Postgasse 8
1010 Wien
(hinkünftig Dienstgeber)

und dem

Zentralausschuss der Österreichischen Post AG
Postgasse 8
1010 Wien

20.12.2007
Betriebsvereinbarung


Österreichische Post AG
<http://www.post.at>
Firmensitz: Wien
Firmenbuchnummer: 180219d
Firmenbuchgericht: Handelsgericht Wien
UID: ATU 46674503 DVR: 1008803

20.12.2007

Soweit in dieser Betriebsvereinbarung personenbezogene Bezeichnungen nur in weiblicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung auf bestimmte Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

1) Gegenstand der Betriebsvereinbarung

Gegenstand dieser Betriebsvereinbarung ist die grundsätzliche Regelung betreffend des Zugangs und der Verwendung von IT Ressourcen¹ durch die Mitarbeiterinnen, die Kontrolle der Einhaltung dieser Regelungen, sowie Maßnahmen im Rahmen der Informationssicherheit.

2) Ziele

Ziele dieser Vereinbarung sind:

- Sicherstellung gesetzlicher Vorgaben
- Verhindern von Imageschäden aufgrund von Sicherheitsvorfällen
- Sicherstellung der Kontinuität des Betriebs (Verfügbarkeit, Funktionsfähigkeit und Sicherheit der IT Ressourcen)
- Schadensvermeidung und Schadensbegrenzung
- Gewährleistung eines angemessenen Sicherheitsniveaus des Unternehmens (Sicherstellung der Vertraulichkeit, Verfügbarkeit und Authentizität der gespeicherten und übertragenen Daten)
- Strukturierte Regelung der EDV-Nutzung
- Festlegung der Nutzung von IT Ressourcen für ausschließlich dienstliche Zwecke
- Schutz der personenbezogenen bzw. -bezieharen Daten und des gesprochenen Wortes, somit von Persönlichkeitsrechte, der Mitarbeiterinnen vor unzulässigen Eingriffen, sowie die Vermeidung von Datenmissbrauch.

Dienstgeber und Personalvertretung sind sich darüber einig, dass die im Rahmen dieser Betriebsvereinbarung verwendeten Daten und technischen Systeme nicht für den Zweck einer systematischen, die Menschenwürde verletzenden Kontrolle der Mitarbeiterinnen im Sinne des § 96 Abs. 1 Z. 3 ArbVG eingesetzt und insbesondere die Bestimmungen des § 100 Abs. 3 TKG eingehalten werden.

¹ Begriffsdefinition IT Ressourcen: Darunter werden einerseits IT Komponenten wie Laptop, PC, Server, PDA, Software,... (Komponenten die der elektr. Datenverarbeitung dienen), ebenso wie IT Services (Internet, Intranet, Netzwerke (LAN/WAN), FTP, VPN, etc.. Daten und Zugriffsrechte, verstanden; nicht betroffen sind hiervon Endgeräte die der Sprachtelefonie (Handy und Festnetztelefonie) dienen.

3) Geltungsbereich der Betriebsvereinbarung

1. räumlich: Diese Betriebsvereinbarung gilt für das gesamte Unternehmen.
2. fachlich, persönlich: Die Betriebsvereinbarung findet auf alle Mitarbeiterinnen der Österreichischen Post AG (Beamte, Angestellte und ABGB – Kräfte), welchen IT Ressourcen durch die Österreichische Post AG zur Verfügung gestellt werden, Anwendung.
3. zeitlich: Diese Betriebsvereinbarung tritt mit 1.1.2008 in Kraft und gilt befristet bis 31.12.2008. Sie verlängert sich jeweils automatisch für ein weiteres Jahr, wenn nicht einer der beiden Vertragspartner dem jeweils anderen die Ablehnung der Weiterverlängerung spätestens 6 Monate vor Ablauf der Befristung nachweislich zur Kenntnis bringt.

4) Bedrohungsszenarien

Bedrohungsszenarien können in vielfältiger Form auftreten, sei es durch menschliches Versagen, vorsätzliche Handlung oder organisatorische Mängel.

Nachfolgend werden beispielhaft Bedrohungen aufgelistet:

- Einbringung und Verbreitung von Viren, Würmern, Trojanern und anderen Formen von schädlicher Software in die IT Ressourcen
- Angriffe aus jeglichen Netzen (extern, aber auch intern) auf Infrastruktur, Systeme, Sicherheitskomponenten, Anwendungen und Daten
- Manipulation oder Verlust vertraulicher Informationen² und daraus resultierende Gesetzesübertretungen
- Missbrauch der IT Ressourcen für unlautere oder rechtswidrige Zwecke und daraus resultierende Rechtsfolgen und Haftungsansprüche Dritter
- Beeinträchtigung der Verfügbarkeit der IT Ressourcen aufgrund von Sicherheitsverletzungen bzw. von Maßnahmen zu deren Behebung
- Diebstahl, Unterschlagung und Raub von Endgeräten aller Art
- Schädigung des Ansehens des Unternehmens

² Vertrauliche Informationen sind in diesem Zusammenhang auch personenbezogene Daten

5) Grundsätze des Zugangs und der Verwendung von IT Ressourcen

Für den Zugang und die Verwendung der durch das Unternehmen zur Verfügung gestellten IT Ressourcen gelten folgende Grundsätze:

- a. Die Erstentscheidung, welche Mitarbeiterinnen Zugang zu welchen IT Ressourcen erhalten, trifft die zuständige Vorgesetzte/Kostenstellenverantwortliche/Ressourcenverantwortliche. Die IT kann in begründeten Fällen die Entscheidung revidieren³.
- b. IT Anwenderinnen erhalten eine IT Kennung und ein persönliches Passwort, das sie geheim zu halten haben. Es ist ausdrücklich untersagt, das Passwort an andere Personen zu kommunizieren. Das Passwort dient mit der IT Kennung als Nachweis der Identität der IT Anwenderin gegenüber den IT Ressourcen.
- c. Zur Sicherung des optimalen Betriebes der EDV-Systeme und der gespeicherten Daten und vor allem aus Gründen der Lizenz- und Garantiebestimmungen ist die eigenmächtige Installation von Soft- und Hardware nicht gestattet.
- d. Die Verwendung privater IT Ressourcen im Unternehmen ist prinzipiell untersagt, in Ausnahmefällen bedarf es der schriftlichen Zustimmung der Vorgesetzten/Kostenstellenverantwortlichen und der IT Leiterin bzw. deren Stellvertreter oder Bevollmächtigten.
- e. Der Zugang zum Internet hat ausnahmslos über die durch die IT bereitgestellten Netzwerkverbindungen und die entsprechenden Hilfssysteme zu erfolgen. Eine Umgehung der durch die IT konfigurierten Verbindungsmöglichkeiten ist ausdrücklich untersagt. Dieser Grundsatz gilt für sämtliche firmeneigene PCs und Laptops sowie PDA's (Personal Digital Assistants) unabhängig von der Verwendung. Des Weiteren ist eine Anbindung von privaten Komponenten wie z.B.: PC's, PDAs oder Laptops an das Netzwerk nicht gestattet.
- f. Die Verwendung der IT Ressourcen für ungesetzliche Handlungen oder solche Handlungen, die geeignet sind, dem Unternehmen Schaden zuzufügen, ist untersagt. Jeder Mitarbeiterin des Unternehmens ist der Einsatz von nicht legitimer Soft- oder Hardware und sonstiger Mittel, deren Zweck es ist, Informationen auszuspähen, untersagt.
- g. Prinzipiell ist die Verwendung der IT Ressourcen ausschließlich für dienstliche Belange gestattet.
- h. IT Anwenderinnen sind angehalten, die private Nutzung auf ein geringst

³ In jenen Fällen in denen die IT Kriterien für die Berechtigungszuordnung erfüllt werden, jedoch die IT die Berechtigungsvergabe aus anderen Gründen ablehnt, ist die Personalvertretung durch die ablehnende Stelle der IT zu informieren.

mögliches Maß zu begrenzen, wobei hier der Grundsatz gilt, dass jegliche Privatnutzung nur im Falle einer außerordentlichen Situation zulässig ist bzw. wenn diese nicht durch die IT Anwenderin angestrebt wird (z.B. Mailempfang mit privaten Inhalt). Eine allfällige Privatnutzung ist auf das unbedingt zwingende Maß zu beschränken; empfangene Privatmails sind umgehend an eine private Mailadresse weiterzuleiten und zu löschen. Die Mitarbeiterin haftet für die im Rahmen der privaten Nutzung durch sie verschuldete Schäden gemäß Dienstnehmerhaftpflichtgesetz DHG.


- i. Das Senden von E-Mails und die Nutzung des Intranets/Internets muss unter Rücksicht auf die Systemkapazität und in einem wirtschaftlich vertretbaren Rahmen erfolgen.
Das Versenden von Massenmails (> 100 Adressaten) ist untersagt; Aussendungen der Personalvertretung können in begründeten Fällen⁴ im eigenen Bereich erfolgen, der Regelprozess⁵ wird jedoch für alle nicht zeitkritischen Sendungen eingehalten.
- j. Das Versenden von Mitteilungen über Internet (Mails, Postings auf Webseiten u ä), die gegen die öffentliche Ordnung und Sicherheit oder gegen Rechtsvorschriften verstoßen, andere Benutzerinnen belästigen oder verängstigen oder betrieblichen oder gesetzlichen Geheimhaltungsverpflichtungen widersprechen, ist untersagt
- k. Die Verwendung von IT Ressourcen des Unternehmens für private Erwerbszwecke ist den IT Anwenderinnen ausdrücklich untersagt.
- l. Den Mitgliedern der Personalvertretung ist die Verwendung der IT Ressourcen zur ordnungsgemäßen Erfüllung ihrer Aufgaben (Geschäftsinhalt der Tätigkeit der Personalvertretung) unter Beachtung dieser Betriebsvereinbarung gestattet. Die elektronischen Datenbestände der Personalvertreter sind in einem besonders bezeichneten Ordner⁶ (z.B.: PV Daten) zu speichern.
Auf diesen Ordner (insbesondere auf die darin enthaltenen Fileinhalte) ist, ausgenommen zur Compliance- und Virenschutzprüfung, kein Zugriff Dritter zulässig. Die PV kann, in Abstimmung mit der IT, eine eigenständige⁷ Fileverschlüsselung einrichten, die Systemverträglichkeit muss jedoch sichergestellt werden.
- m. Der unberechtigte Zugriff auf Daten ist verboten.
Ein solcher liegt vor, wenn eine Mitarbeiterin organisatorische/technische Sicherheitsmaßnahmen umgeht, um nicht für sie bestimmte Informationen zu erlangen. Der Zugriff auf nicht gesondert geschützte PublicShares des

⁴ Informationen die im Sinne der Informationsmaßnahmen zeitkritisch zu erfolgen haben (wird von der PV entschieden) sind vom Regelprozess ausgenommen.

⁵ Information geht an das IT AM, diese versendet die Informationen in betriebsschwachen Zeiten unter Berücksichtigung der IT Ressourcen

⁶ Technische Details werden im Rahmen der Implementierung festgelegt.

⁷ Die Verschlüsselung dieses Ordners und deren Handhabung obliegt einzig der Personalvertretung.


20.12.2007

Unternehmens stellt keinen unberechtigten Zugriff dar.

6) Datenaufzeichnungen zum Zweck der Sicherstellung des Betriebs der IT Ressourcen

Soweit im Folgenden nicht abweichend geregelt, werden Datenaufzeichnungen im Rahmen dieser Betriebsvereinbarung ausschließlich von Mitarbeiterinnen der IT und deren Beauftragten vorgenommen bzw. sind nur diesen zugänglich.

Nachfolgende Positionen erörtern die grundlegenden Aufzeichnungen beispielhaft

a. Anomalien

Werden im Rahmen der automatisierten Überwachung⁸ Anomalien im Sinne von signifikanten Abweichungen von der gewöhnlichen Verwendung der IT Ressourcen festgestellt, wird durch die IT die Voranalyse zwecks Abklärung des Vorliegens eines technischen Gebrechens oder technischen Fehlverhaltens (Fehlkonfiguration, Viren, etc.) durchgeführt.

b. Internet:

Es erfolgt eine automatische, zentrale Erfassung von sämtlichen durch IT Anwenderinnen aufgerufenen URLs („Web-Logs“), welche auch die Zuordnung der aufgerufenen Internet-Adressen zu den einzelnen IT Anwenderinnen ermöglicht.

Darüber hinaus werden zentral Filter-Softwareprodukte installiert, welche den Zugriff auf vom Unternehmen als bedenklich oder unerwünscht eingestufte Internet-Seiten verhindern (z.B. wegen rassistischen oder pornographischen Inhalts); die durch diese Filtersoftware geblockten Zugriffsversuche werden zum Zweck der Fehlerauswertung protokolliert.

c. Ein- /Ausgehende E-Mails:

Es ist eine Filter-Software (Virus-Scan) installiert, die automatisch jedes E-Mail und damit verbundene Attachments auf etwaige Viren untersucht. Risikobehaftete E-Mails, bei denen die Gewissheit oder der begründete Verdacht auf Verseuchung mit Viren besteht, werden geblockt bzw. ungesehen gelöscht und der Empfänger/Absender verständigt.

Das Unternehmen kann im Rahmen der Mailarchivierung alle ein- und ausgehenden Mails in entsprechende Archivierungssysteme transferieren;

⁸ Maschinelle Überwachung durch Systeme oder im Rahmen technischer Evaluierungen der IT Mitarbeiterinnen

auf diese ist auch die jeweilige IT Anwenderin zugriffsberechtigt.

- d. Aufzeichnungen über die Nutzung der IT Ressourcen (z.B.: proxy Files) werden innerhalb von sechs Monaten nach der betreffenden Datenerfassung gelöscht, sofern nicht gesetzliche Regelungen oder Erfordernisse der ordnungsgemäßen organisatorischen und technischen IT Betriebsführung eine längere Aufbewahrung verlangen.
- e. Protokollierungen zur Gewährleistung der Datensicherheit gem. § 14 DSGVO 2000 werden – soweit technisch möglich und zweckmäßig – geführt, damit die von den IT Anwenderinnen tatsächlich durchgeführten Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen in Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.

7) Kontrollmaßnahmen, Zugriffe auf und Weitergabe von IT Ressourcen

Soweit im Folgenden nicht abweichend geregelt, werden Kontrollmaßnahmen und Zugriffe im Rahmen dieser Betriebsvereinbarung ausschließlich von Mitarbeiterinnen der IT und deren Beauftragten vorgenommen bzw. sind nur diesen zugänglich. Nachfolgende Positionen erörtern die grundlegenden Kontrollmaßnahmen beispielhaft.

- a. Generell ist der Zugriff auf individuelle Datenbestände der IT Anwenderinnen am Client und auf Servern nur im Anlassfall und zum Zweck der Sicherstellung der Unternehmensinteressen möglich, soweit keine gelinderen Mittel gegeben sind.

Als Anlassfall gelten zum Beispiel:

- Nichterreichbarkeit bei Urlaub/Krankenstand⁹
- Tod
- Ausscheiden einer Mitarbeiterin

Bei Ausscheiden einer Mitarbeiterin werden die dienstlichen Daten – auf Verlangen der Vorgesetzten – diesem oder einer befugten Vertreterin übergeben.

- Private Daten werden - sofern als solche erkennbar - gelöscht.
- Datensicherungsmaßnahmen

⁹ Hierbei ist sofern möglich durch den Linienvorgesetzten das Einverständnis der jeweiligen Mitarbeiterin einzuholen, ist dies nicht möglich so ist der Zugang über die IT unter Angabe der Begründung (Dienstlichen Notwendigkeit, Bestätigung der Nichterreichbarkeit) anzufordern, der Zugriffsantrag wird mit der DSGVO Beauftragten geprüft und ggf. die erforderlichen technischen Maßnahmen veranlasst.

- b. Maßnahmen, die dem Schutz der Unternehmensinformationen dienen, solange sie nicht ausschließlich zielgerichtet auf eine Einzelperson ausgerichtet werden, sind zulässig. (z.B.: Firewall, IDS, Securityscan, Loganalysen, Netzanalyse, Client/Serveranalysen, Complianceprüfungen, etc.)
- c. Die gezielte inhaltliche Einsichtnahme in E-Mails, sofern nicht als privat erkennbar, log-files („Weblogs“) und personenbezogenen Protokolle zum Zweck der Kontrolle darf nur in begründeten Einzelfällen, in denen der begründete Verdacht einer Gefährdung der IT-Ressourcen oder ein schwerwiegender Verstoß gegen die unter Punkt 5 festgelegten Grundsätze zu befürchten ist, erfolgen.
- d. Eine fortlaufend individuelle Detailüberwachung¹⁰ ist nicht zulässig.
- e. Die Weitergabe von Daten an die Vorgesetzte/Kostenstellenverantwortliche/Ressourcenverantwortliche erfolgt jeweils nach dem vier Augenprinzip (IT und Datenschutzbeauftragte) über schriftliche Anforderung des Vorgesetzte/Kostenstellenverantwortlichen/Ressourcenverantwortliche; gleiches gilt im Falle der Datenweitergabe an sonstige Dritte aufgrund gesetzlicher Vorschriften.
Die Weitergabe der Daten, der Zweck der Weitergabe und der Datenempfänger sind zu protokollieren.
- f. Die IT Anwenderin ist im Fall der Weitergabe sie betreffender Daten gem. Punkt 7 e zu verständigen, ausgenommen diese Daten werden zur vollständigen Sachverhaltsermittlung durch das Cert/Cirt Team benötigt. Dem zuständigen Personalvertretungsorgan ist, bei Vorliegen einer entsprechenden Ermächtigung durch die betroffene Mitarbeiterin, auf Verlangen, die betroffene Zugriffsdokumentation vorzulegen.
- g. Das Unternehmen behält sich das Recht vor, in Einzelfällen jederzeit entsprechende technische und organisatorische Maßnahmen zu setzen, um die missbräuchliche und unwirtschaftliche Verwendung der IT-Ressourcen zu verhindern bzw. einzuschränken.
Diese Maßnahmen beziehen sich auf den Einsatz spezieller Soft- und Hardware-Komponenten und die Sperre/Einschränkung der Zugriffsrechte.
- h. Soweit nach Abschluss der Voranalyse gem. Punkt 6a der begründete Verdacht eines Verstoßes gegen die in Punkt 5 festgelegten Grundsätze besteht und keine gelinderen Mittel gegeben sind, ist die IT zur

¹⁰ Gezielte strukturierte und umfassende Kontrolle einer Einzelperson oder eines Clients über einen Zeitrahmen von mehr als vier Wochen

Durchführung einer personalisierten Detailanalyse zur Feststellung des Sachverhaltes berechtigt.

- i. Soweit darüber hinaus der begründete Verdacht auf vertrags- oder strafrechtswidriges Verhalten (bspw. Preisgabe von Geschäfts- oder Betriebsgeheimnissen, sexuelle Belästigung, usw.) vorliegt und eine gesicherte IT Beweisaufnahme erforderlich ist, wird – soweit keine gelinderen Mittel in Frage kommen - das CERT/CIRT Team¹¹ eingebunden und kann auf alle relevanten Daten gem. Punkt 6 zugreifen. Ab diesem Zeitpunkt sind sämtliche Analyse- und Beweissicherungsmaßnahmen und Abläufe entsprechend zu dokumentieren und die Datenschutzbeauftragte zu informieren. Bei Verhärtung der Verdachtsmomente (im Sinne einer signifikanten Abweichung von der gewöhnlichen IT-Nutzung) kann eine personalisierte IT-Detailanalyse¹² durchgeführt werden.

Ab dem Nachweis einer eindeutig bewusst herbeigeführten verbotenen Handlung, ist die Vorgesetzte/Kostenstellenverantwortliche der IT Anwenderin zu informieren; soweit die betroffene IT Anwenderin verständigt wurde kann diese dem Verfahren eine Person ihres Vertrauens¹³ beiziehen.

- j. Verstöße gegen IT-Richtlinien¹⁴ können zu dienst-/arbeitsrechtlichen Konsequenzen führen. Diese reichen von mündlicher Verwarnung, disziplinären Maßnahmen, bis zur Beendigung des Arbeitsverhältnisses. In einzelnen Fällen sind auch zivil- und strafrechtliche Konsequenzen nicht auszuschließen.
- k. IT Informationen, die unter Verletzung dieser Betriebsvereinbarung gewonnen wurden, sind als Beweismittel zur Begründung personeller Maßnahmen unzulässig, eventuell getroffene Maßnahmen sind zurückzunehmen.
- l. IT Administratorinnen und Mitarbeiterinnen mit erweiterten Benutzerrechten (Lokale Administratorin, Client/Serveradministratorinnen)

¹¹ bestehend aus drei Mitarbeiterinnen der IT, einer Mitarbeiterin der Revision und der Datenschutzbeauftragten. Das Cert/Cirt Team setzt sich anlassbezogen zusammen und übt die Tätigkeit in einem 4 Augenprinzip aus, wodurch eine entsprechende Beweissicherung und Sachverhaltsfeststellung erfolgt. Die Befassung des Teams erfolgt im Auftrag der IT bzw. auf Anforderung der Supporteinheiten bei entsprechenden Verdachtsmomenten. Die Zuständigkeit erstreckt sich auf alle IT Ressourcen des Unternehmens.

¹² z.B.: Die Detailanalyse erfolgt nach Sicherstellung der IT Ressourcen und der Feststellung, dass kein technisches Gebrechen oder technisches Fehlverhalten (Fehlkonfiguration, Viren,..etc.) der Auslöser einer Anomalie ist.

¹³ Betriebsrat, Personalvertretung, Mitarbeiter,...

¹⁴ IT Richtlinien werden anlassbezogen im Intranet publiziert und den Mitarbeiterinnen nachweislich zur Kenntnis gebracht

werden durch die IT einer gesonderten Kontrolle¹⁵ unterworfen. (verstärkte Log-Aufzeichnung der IT Systeme, etc.). In jenen Fällen, in denen ein Verdacht¹⁶ auf nicht legitimierte Aktivitäten¹⁷ vorliegt, ist gem. Pos. 6e vorzugehen.

8) Qualifizierung der Benutzerinnen

- a Die Mitarbeiterinnen sind für den sicheren und wirtschaftlichen Umgang mit den IT Ressourcen zu sensibilisieren.
Nutzungsvorgaben und IT Richtlinien sind den Mitarbeiterinnen mindestens einmal jährlich zur Kenntnis zu bringen.
- b Mitwirkungsrechte der Personalvertretung
Der Zentralkommission hat das Recht, gemäß § 89 Z 2 ArbVG jederzeit die Einhaltung der Betriebsvereinbarung zu überprüfen. Die Ergebnisse personifizierter Detailanalysen (siehe Pos. 7 e.) werden dem zuständigen Organ der Personalvertretung, nach entsprechender schriftlicher Ermächtigung durch die Mitarbeiterin, zur Verfügung gestellt.
- c Wenn bestimmte Tatsachen darauf hindeuten, dass die Verfügbarkeit, Funktionsfähigkeit und Sicherheit der der jeweils betroffenen Mitarbeiterin überlassenen IT-Ressourcen oder die Vertraulichkeit, Verfügbarkeit und Authentizität der darin gespeicherten bzw. übertragenen Daten nicht mehr gewährleistet ist, hat die betroffene Mitarbeiterin die Pflicht, unverzüglich die IT-Abteilung zu informieren.

9) Paritätische Kommission

- a Allfällige Abstimmungsmaßnahmen und Sachverhaltsklärungen werden durch eine paritätisch besetzte Kommission behandelt.
Diese setzt sich aus folgenden Personen/Funktionen zusammen:
 - i. IT Sicherheitsmanagerin (1)
 - ii. Datenschutzbeauftragte (1)
 - iii. Vertreterin Personalmanagement (1)
 - iv. Vertreterin des Zentralkommissiones (3)

¹⁵ z.B.: fortlaufende Aufzeichnung der Zugriffsmaßnahmen, Detaillierte Erfassung von Systemeingriffen zum Zweck der Nachvollziehbarkeit der IT Leistung/Services

¹⁶ Begründeter Verdacht auf ein vertrags-/rechtswidriges Verhalten vorliegt

¹⁷ z.B.: nicht für das Aufgabengebiet typische Aktivitäten/Maßnahmen d.h. bei Erkennen von Anomalien in der Systemlandschaft

| Wien, am 20.12.2007



Für die Österreichische Post AG
GD Dr. Anton Wais


20/12/2007

Für den Zentralausschuss
Gerhard Fritz (Vors.)



Für die Österreichische Post AG
Dr. Rudolf Jettmar

Anhang 1: Cert/Cirt Mitarbeiter

Anhang 1:**Nominierte Mitglieder der Arbeitsgruppe Cert/Cirt****Bereich:**

SE Informationstechnologie
SE Informationstechnologie
SE Informationstechnologie
Konzernrevision

Name:

Jürgen Mang, MAS, Msc, Msc
Andreas Reiter, Ing.
Christoph Niederhametner
Toth Peter

Ansprechperson Cert/Cirt:

Jürgen MANG MAS, MSc, MSc
Österreichische Post AG
Informationstechnologie
IT Sicherheitsmanager
Postgasse 8
1010 Wien
Tel.: +43 (0) 57767 22725
Mobil: +43 (0) 664 624 6110
E-Mail: juergen.mang@post.at