
Rapport über die Sicherheitsvorkehrungen in der Informatik

per März 1991

I/S SECURITY: Beschreibung der bestehenden Sicherheitvorkehrungen in den Bereichen:

---

19. März 1991 K.Trachsler
J.Mathys
E.Ingold
E.Horn
P.Roth

Beilagen: Richtlinien betreffend EDV Anmeldung/ Zugriffsberechtigung (87-4487/MJ 30.06.86)

Analyse über das Bundesgesetz über den Schutz von Personendaten (BK0903 90-125592/MJ 16.11.90)

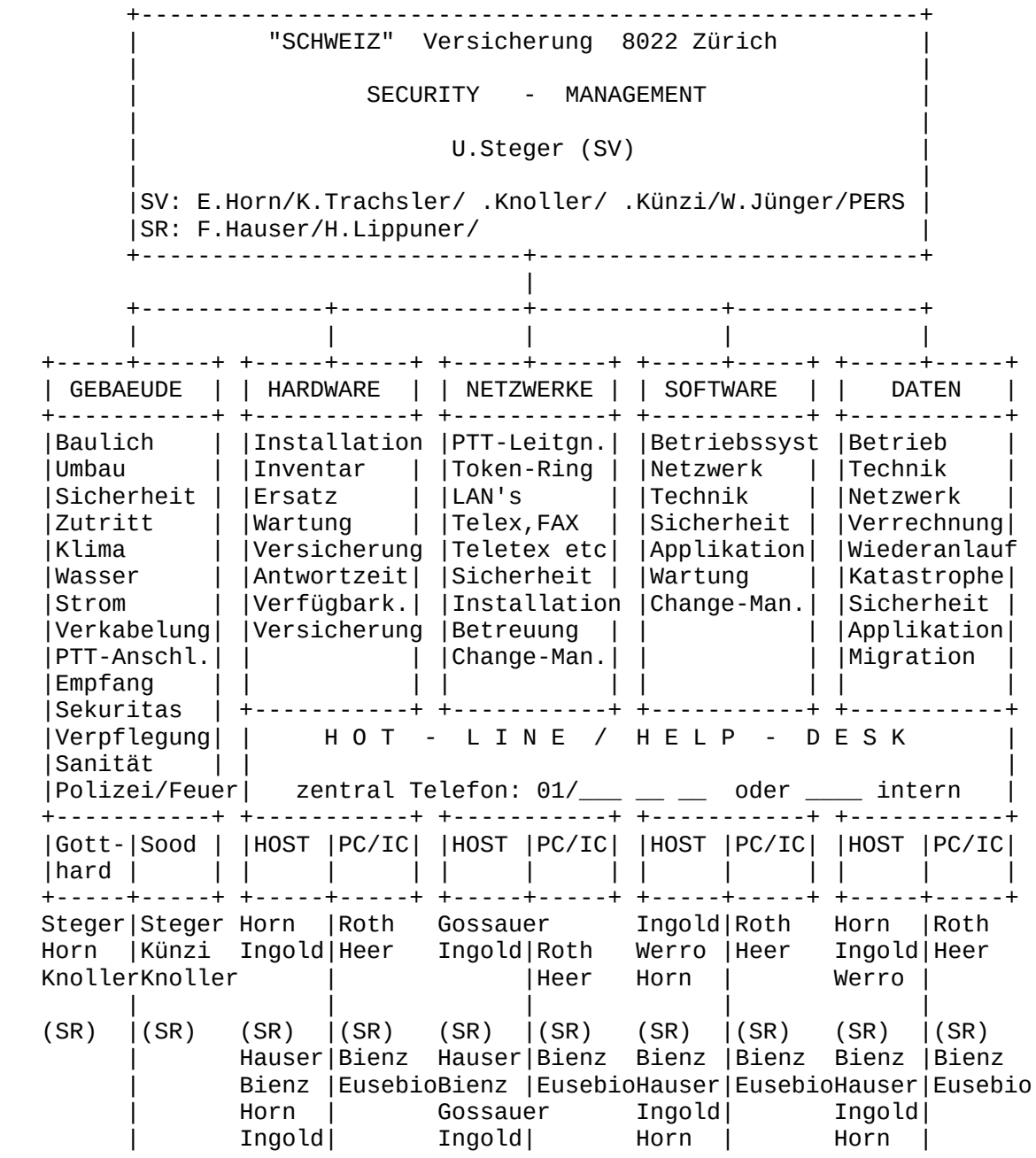
>>

Rapport über die Sicherheitsvorkehrungen in der Informatik

per März 1991

1.1 ORGANISATION UND VERANTWORTLICHKEITEN

1.1.1 ORGANISATION GRAPHISCH



>>

Rapport über die Sicherheitsvorkehrungen in der Informatik

per März 1991

1.1 ORGANISATION UND VERANTWORTLICHKEITEN
(Fortsetzung)

1.1.2 SECURITY MANAGEMENT-STUFEN SOFTWARE UND DATEN

Folgende Security-Management-Stufen sind eingerichtet

a) System-Security-Manager (Technik/Betrieb)

Software: IBM/RACF
User Jes-EXIT
User File-Transfer-EXIT HFTR

Online-Systeme: IBM/TSO ISPF für:
(Eröffnung und Betreuung)
- Anwendungsentwicklung
- Rechenzentrum
- Systemtechnik
- Support und Hot-Line

Terminal-CICS für:
- PC Produktion
- SC Schulung
- TC Test

Applikations-CICS für
- NOVITA .SIGNON (zentral)
.Mailing gesamt
.Telex/FAX/Teletex
.zentr.Textverarbeitung
.Bestandesverwaltungen Direktversicherung
.Prämie, Produktion, Provision, Portefeuille
.Schadenverwaltung
.Adressverwaltung
.Tabellenverwaltung

- SAP .Rechnungswesen für Finanz-, Debitoren- und Kostenverwaltung

- RV .Rückversicherung
SICS für aktive RV (Prod. ISS)
FISP für fak.RV (Prod.Bayer Rück)

>>

1.1 ORGANISATION UND VERANTWORTLICHKEITEN
(Fortsetzung)

1.1.2 SECURITY MANAGEMENT-STUFEN SOFTWARE UND DATEN
(Fortsetzung)

b) Personal-Security-Manager (Personal-Administrat.)

- SIGNON (zentral)	. Verwaltung aller Mitarbeiter auf Antrag der Fachverantwortlichen pro Applikationsklasse incl. 4-stufiger Druck-Berechtigung
	. Festlegen Mitarbeiterkurzzeichen
	. Passwort Löschung auf Antrag Fachverantwortlicher
	. Führen Eckdaten für Telefonverzeichnis Online und Batch wie: Name,Vorname, Abteilung, Kostenstelle, zugeteilte Agentur, Sprachcode, Zugriffstyp, Telefonnummer etc. Automatische Terminal-ID.-Speicherung bei Arbeitsplatzbestätigung.
	. Passwort cryptologisiert und nach 3-maliger Falscheingabe sowie nach Austrittsmeldung automatisch gesperrt. Freigabe erfolgt durch Personaladministr.
	. Passwort kann bei jeder Anmeldung geändert werden. Periodisch erfolgt automatisch Aufforderung Passwort zu ändern.
	. Das neue Passwort muss für Wirksamkeit bestätigt werden. Die erstmalige Passworteingabe erfolgt nach seperater Freigabe durch Personaladministration mit dem Benutzerkennzeichen in Grossbuchstaben. Dabei ist eine neues Passwort zwingend. (Systemaufforderung)

>>

1.1 ORGANISATION UND VERANTWORTLICHKEITEN
(Fortsetzung)

1.1.2 SECURITY MANAGEMENT-STUFEN SOFTWARE UND DATEN
(Fortsetzung)

c) Applikations-Security Manager (Fachverantwortung)

- NOVITA (Security: W.Jünger/A.Rohner)

Tabellengesteuert vom Fachverantwortlichen zentral sowie dezentral möglich.

Wichtige Annahmerichtlinien sind fest in Programmen und können nur durch Programmänderung umdefiniert werden.

Die Zugriffsberechtigung lässt sich auf im Versicherungsgeschäft auf Branchenebene definieren und umfasst:

. nur zugeteilte Bestände lesen

. alle Bestände lesen

. Mutieren in 4 Berechtigungsstufen

. Quittierung bei Kompetenzüberschreitung

Der Zugriff für die zentrale Textverarbeitung grenzt sich getrennt für Lesen, Mutieren, Löschen, Kopieren, Einstellen wie folgt ab:

. Koordinator/Benutzer

. Domaine/Sachgebiet

. Dokument/Member

. Zeile und Datenfeld

Ueber die zentrale Textverarbeitung wird auch das Mailing (automatisch aktiviert bei Anmeldung und Aufruf Applikationsbild) der ein-, ausgehende Telexdienst, der ausgehende FAX und div. applikatorische Tabellenverwaltungen maschinell verarbeitet.

>>

1.1 ORGANISATION UND VERANTWORTLICHKEITEN
(Fortsetzung)

1.1.2 SECURITY MANAGEMENT-STUFEN SOFTWARE UND DATEN
(Fortsetzung)

c) Applikations-Security Manager (Fachverantwortung)
(Fortsetzung)

- SAP (Security: S.Weber/D.Koblet)

  Tabellengesteuert vom RW zentral geführt und zugeteilt.

  Der Einstieg zu SAP ist nur möglich, wenn zentrales SIGNON ordentlich erfolgte.

- SICS (Security: P.Kalt)

  Tabellengesteuert vom RV zentral geführt und zugeteilt.

  Der Einstieg zu SICS ist nur möglich, wenn zentrales SIGNON ordentlich erfolgte.

- FISP (Security: J.Kolmorgen/E.Ingold)

  SIGNON über CICS-SNT d.h. die FISP-Benutzer müssen im RACF in USER-Gruppe FISP aufgenommen werden. (Antrag Fachabteilung an Technik)

  Der Einstieg zu FISP ist nur möglich, wenn zentrales SIGNON ordentlich erfolgte.

1.2 MASSNAHMEN FUER DATEN UND DEREN:

1.2.1 IDENTIFIKATIONEN, AUTHORISIERUNG

Die Hauptidentifikation und Authorisierung erfolgt auf Grund der System-Katalog-Trennung unter der Kontrolle von RACF mit folgenden Prefixes:

- System	.	SYSn.	n Nummer für div. Installationen festgelegt durch Installationsvorschriften der IBM etc.
- Produktion	.	TP.	Daten auf Band
		SVP.	Daten auf Disk
	.	SBP.	Bibliotheken für:
		SBPL.	Programme/Sources
		SBN.	
		SBNL.	
		SBPP.	JCL-/ISPF-Prozeduren
- Schulung	.	TS.	Daten auf Band
		SVS.	Daten auf Disk
	.	SBS.	Bibliotheken für:
			Programme/Sources
		SBSP.	JCL-/ISPF-Prozeduren
- Test	.	TT.	Daten auf Band
		SVT.	Daten auf Disk
	.	SBT.	Bibliotheken für:
			Programme/Sources
		SBTP.	JCL-/ISPF-Prozeduren
- TSO-USER	.	SVXuuu.	User-Identifikation
		SVZuuu.	X = Extern
			Z = Intern

TSO-User (im RACF definiert) sind z.Zt. nur Mitarbeiter der Informatik aus:

Systemtechnik
Produktion/Betrieb
Applikations-Entwicklung

>>

1.2 MASSNAHMEN FUER DATEN UND DEREN:
(Fortsetzung)

1.2.2 ZUGRIFFSKONTROLLEN

Die Online Zugriffskontrollen im CICS erfolgen durch das applikatorische SIGNON und für CICS-File-Transfer über den HFTR-Transfer-User-EXIT.

Die Zugriffskontrolle im Batchbetrieb ist mit RACF über den System-Katalog-Prefix in folgende USER-Gruppen mit Accses-Control aufgeteilt:

- Systemtechnik
- Produktion und Schulung
  aufgeteilt in Operation und AVOR
- Test für Applikations-Entwicklung
- TSO-User (nur Informatik Mitarbeiter)

Der TSO-File-Transfer ist für alle USER-Gruppen zu ihren RACF-berechtigten Daten möglich.
(TSO-HFTR-Transer-User-EXIT ist nicht aktiv)

1.2.3 SICHERUNG UND WIEDERHERSTELLUNG

Tägliche Sicherung der IMS-DB's mittels IMAGE-Copy sowie der übrigen produktiven Datenbestände und Bibliotheken mittels entsprechender Software zu fest definierten Zeitpunkten. (+ Wochen- und Jahres-Saves)

Aktives Dynamic-Backouting im CICS für alle VSAM-Dateien und IMS-Datenbanken mit kontrolliertem CICS-Loging und automatischem Emergency-Restart.

Aktives IRLM für kontrolliertes Batch-Backouting für alle IMS-Datenbanken mit kontrolliertem IMS-Loging.

Aktives, kontrolliertes Change-Accumalation für IMS-Datenbanken.

Aktives DBRC für gesamte Kontrolle der IMS-Datenbanken auch für das kontrollierte Forward-Recovery.

>>

1.2 MASSNAHMEN FUER DATEN UND DEREN:
(Fortsetzung)

1.2.4 PHYSISCHE SICHERHEIT (DATENTRAEGER)

Die Online-Datenträger sind in einem speziell gesicherten, unterirdischem Raum installiert.

Reserve Drives sind für Aufrechterhaltung des produktiven Betriebes vorhanden. (Zutritt nur für berechtigte Personen mittels Schlüssel)

Die für das Forward-Recovery und für die System- und Applikations-Programme relevanten Bibliotheken täglich erstellten Sicherungen auf Band sowie die für den produktiven Betrieb notwendigen Band-Dateien, werden in einem 3-Stufen Zyklus extern ausgelagert. (Beethovenstrasse Zutritt nur für berechtige Personen).

Die für den laufenden Betrieb notwendigen Band-dateien sind in einem speziellen Raum in Feuer- und Wasser sicheren Tresoren gelagert. (Zutritt nur für berechtigte Personen mittels Badge)

Der Zutritt zu den Bedienungsräumen (Consolen und und Bandstationen) ist nur mittels Badge auf der 3. Stufe möglich.

Stufe 1: RZ-Haupteingang
2. RZ-AVOR-Eingang
3. RZ-Operating-Eingang
4. RZ-Bandtresoren-Eingang

Die erste Stufe ist mit Alarmanlage mit direkter Verbindung zu Sekuritas-Dienst und Polizei gesichert.

Die Räume verfügen über Brandmelder und sind mit Feuerlöscher versehen. Die Fluchtwege sind markiert. Die Brandmeldeanlage steht mit Alarm in direkter Verbindung zur Feuerwehr.

Die Raumtemperatur wird Thermostat gesteuert über-wacht und löst internen Alarm aus. (keine autom. Verbindung zu Externen Stellen)

Ein Wassereinbruch-Alarmsystem existiert nicht.

>>

1.2 MASSNAHMEN FUER DATEN UND DEREN:
(Fortsetzung)

1.2.5 SYSTEM INTEGRITAET

Die System-Integrität wird durch RACF/IRLM/DBRC/ Tages-Saves gem. den in 1. - 1.2.4 dargestellten Punkten und ein maschinell kontrolliertes Change-Management über 4 Stufen für Programme etc. sicher-gestellt.

Stufe 1: Test Betrieb und TSO-User
2. Schulungsbetrieb
3. Produktions-Vorstufe
4. Produktions-Betrieb und Sicherung auf Librarian

Seitens der Fachabteilung und der Revision, werden zudem die relevanten Daten monatlich bei der Folgeprämienavisierung und der Monats-Verarbeitung sowie bei der Jahresend-Verarbeitung auf die fach-liche Richtigkeit geprüft und analysiert.
(Datamanagement W.Jünger Dir.Vers., P.Kalt SICS, J.Kolmorgen FISP, S.Weber RW, M.Bretscher Contr.)

1.2.6 VERSICHERUNGSSCHUTZ

Alle installierte Hard-Ware ist bei der

_____

gegen Feuer, Wasser und
versichert.

????? Gegen Datenverlust besteht keine Versicherung da mittels Sicherungsverfahren ein Verlust sehr unwahrscheinlich ist und eine Versicherung für Datenverlust auf Grund von falsch laufenden eigenen und fremden Programmen nicht üblich ist.

>>

1.3 SICHERHEITSVORSCHRIFTEN UND -RICHTLINIEN

Für die nicht systemlich kontrollierten Vorschriften stehen folgende Anweisungen/Richtlinien zur Verfügung:

- Benutzer:
  - Hot Line / Help Desk
  - Bildschirmhandbuch
  - Systembeschreibungen
  - SCHWEIZ Informatik Doku
  - Mailing
  - Help
  - Schulungsangebot
  - Annahmerichtlinien
  - Technische Handbücher
  - Tarife
  - Projektmanagement
  - Betriebskonzept für RZ bei SR
  - Weisungen für Verhalten im Brand- bezw. Katastrophenfall (Gebäude)
  - Weisungen Passworthandhabung und Geräteausschaltung
- Betrieb:
  - Tages-, Wochen-, Monats- und Jahrespläne
  - Recovery-Vorschriften
  - Betriebskonzept MVS
  - Betriebskonzept für RZ bei SR
  - Pikett-Dienst
  - Betriebskonzept für RZ bei SR
  - Systembeschreibungen
  - SCHWEIZ Informatik Doku
  - Zielsetzungen der Informatik
  - Namens-/Identifikations-Richtlinien
  - Projekt-/Change-Management
  - Mailing
  - Help Betrieb
  - Schulungsangebot
  - Weisungen für Verhalten im Brand- bezw. Katastrophenfall (Gebäude)
  - Weisungen Passworthandhabung und Geräteausschaltung

>>

1.3 SICHERHEITSVORSCHRIFTEN UND -RICHTLINIEN
(Fortsetzung)

- System:
  - Betriebskonzept MVS
  - Betriebskonzept für RZ bei SR
  - Installationsvorschriften
  - Installationsvorschriften
  - Systembeschreibungen
  - SCHWEIZ Informatik Doku
  - Zielsetzungen der Informatik
  - Namens-/Identifikations-Richtlinien
  - Projekt-/Change-Management
  - Mailing
  - Help System
  - Schulungsangebot
  - Weisungen für Verhalten im Brand- bezw. Katastrophenfall (Gebäude)
  - Weisungen Passworthandhabung und Geräteausschaltung

- Applikat.:
  - Betriebskonzept MVS
  - Betriebskonzept für RZ bei SR
  - Systembeschreibungen
  - SCHWEIZ Informatik Doku
  - Zielsetzungen der Informatik
  - Analyse-Richtlinien
  - Handbuch Methoden und Verfahren
  - Namens-/Identifikations-Richtlinien
  - Projekt-/Change-Management
  - Mailing
  - Help Applikations-Entwicklung
  - Schulungsangebot
  - Weisungen für Verhalten im Brand- bezw. Katastrophenfall (Gebäude)
  - Weisungen Passworthandhabung und Geräteausschaltung

>>

1.4 DATEN-ZENTRUM / RECHENZENTRUM

Das Data-Zentrum verfügt (siehe auch 1.2.4) über folgende Sicherheitsvorkehrungen:

- Doppelboden für geschlossene Kabelstränge
- Klimaanlage
- Pilleranlage regelt auch kurzfristige Stromschwankungen
- Brandmelder
- Feuerlöscher
- Alarmanlage zu Sekuritas-Dienst, Polizei und Feuerwehr
- Permanente Sekuritas-Ueberwachung ausserhalb Bürozeit (Nachts sowie Samstag/Sonntag)
- Raumtemperaturüberwachung mit internem Alarm
- Schlagfeste, permanent gechlossene Fenster und schwere Anti-Demo-Rolladen.
- Online Daten im Untergeschoss spezielle Räumlichkeiten
- Band-Dateien in Feuer- und Wasser sicheren Tresoren (definierte externe Auslagerung)
- Bedienungsraum (Consolen) und Bandstationen getrennt von Rechner und Online-Daten
- Vorschriften und periodisches Training für Mitarbeiter für Verhalten in Katastrophenfällen
- Fluchtwegsignalisation und Notbeleuchtung
- Spezielle Weisungen/Software (gemäss 1. bis bis 1.2.6) sichern die Qualität, das Recovery sowie die Wiederherstellung der Daten.

>>

1.4 DATEN-ZENTRUM / RECHENZENTRUM

Folgende Sicherheitseinrichtungen fehlen:

- Wassereinbruch Alarm
- altarnativ PTT-Verstärkeramt d.h. Ausweich-Mietleitung vom RZ zu einem NICHT-Zürcher-Verstärkeramt
- sporadische (Stichproben) Kontrollen und Training der Ausfallverarbeitung
- Notstromversorgung (nur wenn notwendig)
- gezielte Abwehrmassnahmen für Terrorismus
- kontrolliertes Sicherheitssystem für die Entwendung von Daten und Software (vor-allem im PC-Bereich)
- Micro-Fichen für RV SICS und FISP
- Sicherheitskonzept für Wahlleitungen z.Zt. nicht installiert
- Sicherheitskonzept für x25 und Endgeräte die als weitere Netzwerk-Rechner einge-setzt werden
- Kryptologisierung der Daten auf dem externen Netz x25/Wahlleitung evtl. auch Mietleitung

>>

1.5 KATASTROPHEN-PLANUNG

Für den Totalausfall des Rechenzentrums sind als Ausfallinformationssystem Microfichen für die Bereiche Direktversicherung und Rechnungswesen vorgesehen.

Eine solche Einrichtung fehlt für die Bereiche RV SICS (P.Kalt) und FISP (J.Kolmorgen)

Die Micro-Fichen werden monatlich erstellt intern u. extern gelagert. (Micro-Fiche-Management: A.Rohner, L.G,rardis für Direkt.Versicherung, S.Weber für RW)

Micro-Fichen-Sicht- und -Kopier-Geräte sind mindestens für alle Geschäftsstellen und für den Hauptsitz vorhanden. (Anzahl: _____ ???)

Für die Zeit von ca. 10 Arbeitstagen könnte die SCHWEIZ Versicherung mit Micro-Fichen leben. Innerhalb dieser Zeit müsste Ersatzsystem eingerichtet sein.

Ein Backup-RZ bezw. eine Option oder ein Vertrag zu einem solchen besteht nicht.

>>

1.6 PERSONAL COMPUTER

Die PC's werden vom IC eingekauft, konfiguriert, installiert und betreut.
Es liegt eine Standard-Konfiguration gem. Empfehlung der SR vor.

Die Schulung erfolgt über ein eigens dafür eingerichtes Schulunscenter mit Ausbildungsangebot zusammen mit der SR.

Für die laufende Sicherstellung der Daten ist in der Standardkonfiguration festgelegte Software mit Sicherstellungs-Empfehlungen installiert.

Die Sicherstellung der USER-Daten ist Sache des des "PC-Eingentümers". Für Recovery stehen im Vorschriften und Hilfen zur Verfügung. Im Bedarfsfalle kann auch der IC-Help-Desk angefordert werden.

Der Zugriffsschutz bei alten Installationen (AT03) erfolgt durch den Benutzer selbst.
Als physische Sicherheit dient ihm dabei der PC-Schlüssel. (2. Schlüssel ist im IC deponiert)

Bei neuen PC's (PS/2) ist der Hard-Ware mässig vorhandene Passwortschutz aktiviert. Der Gehäuseschlüssel ist im IC deponiert er erlaubt das Oeffnen des Gehäuses für Passwort-Killing und Hard-Ware-Erweiterung.

Users von PC's die über IRMA2-Karte an das Remote-3270-Netz angeschlossen sind, haben sich für die Aktivierungs desselben gemäss HOST Vorschrift nochmals anzumelden.

Benutzer der BESY-Software unterliegen einem von der VU festgelegtem zusätzlichen Anmelde- und Change-Management-Verfahren. (E.Hauser/M.Heer)

Stellt das IC bei Releases-Aenderung fest, dass ein PC die Normen nicht mehr erfüllt, kann der PC aus dem Verkehr gezogen und neu konfiguriert werden.
Bei Feststellung solcher Sachverhalte werden die Vorgesetzten sowie die Kontrollstelle informiert.
(einleiten administrative Massnahmen)

>>

Rapport über die Sicherheitsvorkehrungen in der Informatik

per März 1991

BEILAGEN BEILAGEN BEILAGEN
BEILAGEN BEILAGEN BEILAGEN
BEILAGEN BEILAGEN BEILAGEN
BEILAGEN BEILAGEN BEILAGEN
BEILAGEN BEILAGEN BEILAGEN

B1: Richtlinien betreffend EDV Anmeldung/ Zugriffsberechtigung (87-4487/MJ 30.06.86)

B2: Analyse über das Bundesgesetz über den Schutz von Personendaten (BK0903 90-125592/MJ 16.11.90)

>>