Notfall-Handbuch

Ausgabe für die zentrale IT-Administration

Anleitung zum Umgang mit dem Notfallhandbuch

Im Notfall ist es wichtig, sichere Handlungsanweisungen und vorgegebene Maßnahmen zu haben, um den Schaden so gering wie möglich zu halten. Daher wurde dieses Notfallhandbuch erstellt.

Sollten Sie einen Schadensfall (Feuer, Wassereinbruch, Computervirus, Einbruch, etc.) bemerken, gehen Sie folgendermaßen vor:

1. Bewahren Sie Ruhe.
2. Versuchen Sie, den Notfall im Teil A des Notfallhandbuches unter

   Handlungsanweisungen für spezielle Ereignisse **ab Seite 14**

   zu finden. Wenn Sie ihn dort finden, gehen Sie nach dem angegebenen Schema vor.

3. Falls der Notfall nicht aufgelistet ist, stehen Ihnen die Punkte aus Teil B

   Notfall-Zuständige, **ab Seite 25**
   Organisationsrichtlinien, Verhaltensregeln, **ab Seite 26**

   zur Verfügung. Alarmieren Sie in jedem Fall sofort den zuständigen Mitarbeiter.

Grundsätzlich gilt:

- Die im Notfallhandbuch bzw. in Ihrem Auszug abgedruckten Tabellen enthalten Telefonnummern der zuständigen Mitarbeiter und deren Vertreter an den jeweiligen Standorten. Informieren Sie immer direkt Ihre zuständigen Mitarbeiter und warten Sie auf weitere Anweisungen.
- **Nicht jeder Schadensfall ist ein Notfall.** Wenn Sie sich bei einem IT- Problem nicht sicher sind, informieren Sie die IT in Bochum. Die Telefonnummern finden Sie im Teil A des Notfallhandbuches

  In der Notfalldokumentation (Abschnitt D6, Seite 41) ist die Istzeit der Entscheidung zu vermerken.
  Kontaktlisten betroffener Mitarbeiter **ab Seite 12**

  In Bochum wird dann das weitere Vorgehen entschieden.

Die IT- Leitung hofft gemeinsam mit Ihnen, dieses Notfallhandbuch selten bzw. nie benutzen zu müssen. Dafür müssen Sie mitarbeiten und die in der Sicherheitsrichtlinie vorgegebenen Vorschriften beachten.

Inhaltsverzeichnis

Einleitung

1 Was ist ein Notfall?

Der Ausfall eines IT-Systems der Klinikum Muster in Folge eines Sicherheitsvorfalls kann einen großen Schaden nach sich ziehen. So kann der Ausfall eines zentralen IT-Systems zu einem Ausfall des gesamten IT-Betriebs an den Standorten der Klinikum Muster führen. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klimaanlage oder Stromversorgung, kann Störungen des IT-Betriebs nach sich ziehen.
Technisches Versagen muss nicht zwingend die Ursache für den Ausfall von IT-Systemen sein. Ausfälle werden oft durch menschliches Fehlverhalten von Mitarbeitern (z. B. fahrlässige Zerstörung von Gerät oder Daten) oder vorsätzliche Handlungen (z. B. Diebstahl, Sabotage, Viren-Angriff) verursacht. Auch durch höhere Gewalt (wie Feuer, Blitzschlag oder Hochwasser) können hohe Schäden eintreten.
Ein Sicherheitsvorfall stellt für die Klinikum Muster jedoch nicht zwangsläufig einen Notfall dar. Für einen Notfall gilt die folgende Definition:

Ein Notfall tritt ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist und sich daraus ein untragbarer Schaden ergibt.

2 Eskalationsplan für Notfälle

Die Meldung über einen Sicherheitsvorfall oder eine darauf hindeutende Unregelmäßigkeit muss zunächst dahingehend geprüft werden, welches Ausmaß und Bedeutung der Vorfall bzw. die Unregelmäßigkeit hat, um dann entsprechende Maßnahmen zu ergreifen. Innerhalb einer Eskalationsstrategie werden Personen, Zeitpunkte und Medien der Eskalation definiert.

2.1 Eskalationsstufen

Sobald ein Sicherheitsvorfall bekannt wird, ist sofort eine Meldung an die zuständigen Mitarbeiter (ab Seite 7) abzusetzen. Der Meldeempfänger hat die Meldung gemäß den folgenden Stufen zu kategorisieren:

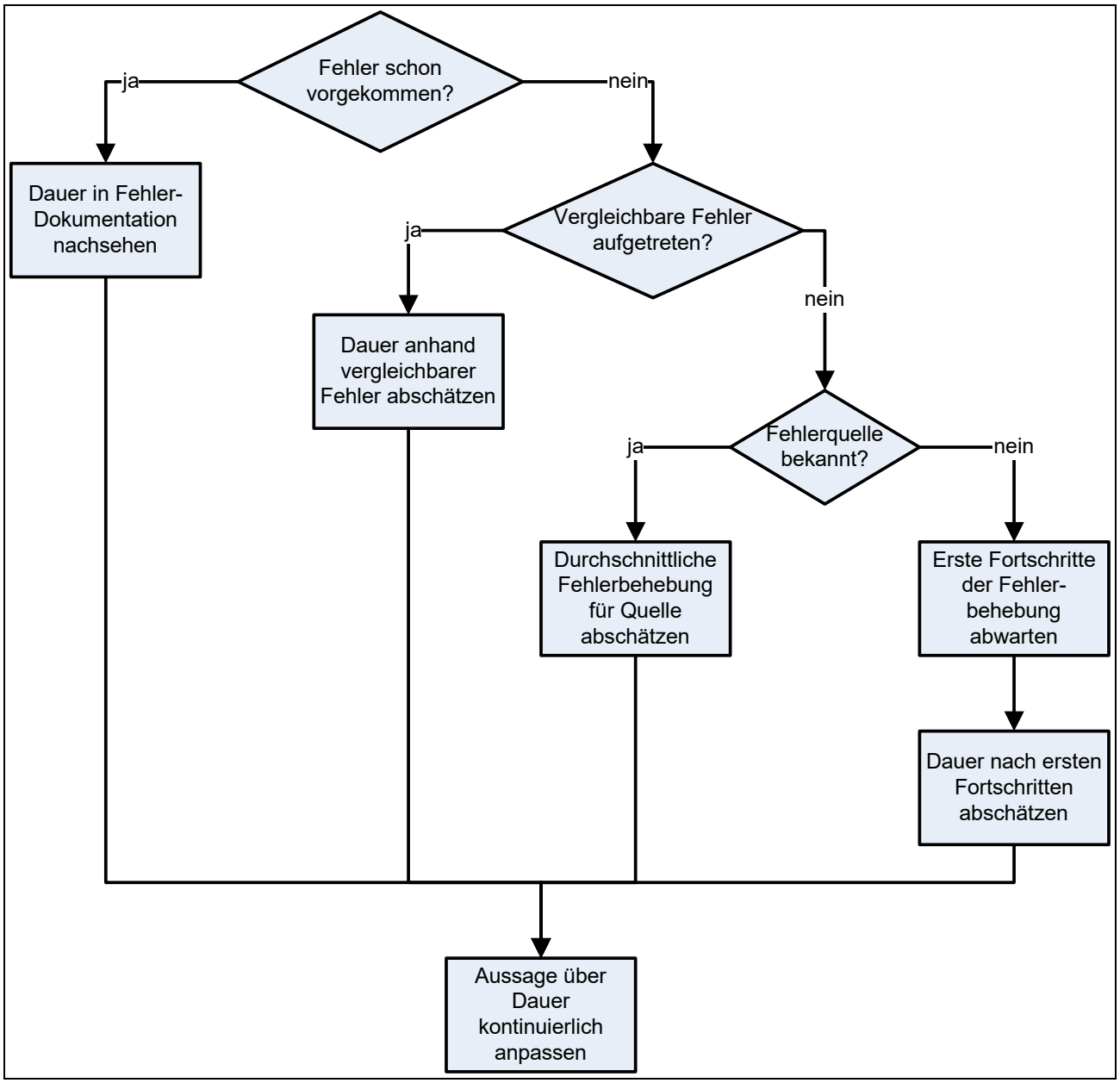
Stufe	Beschreibung	Beispielvorfall	zu informieren (Wie?)	wann?
E1	• Es ist kein existenzieller Schaden zu befürchten. • Der Betriebsfähige Zustand kann innerhalb der tolerierbaren Zeit (ab Seite 27) wieder hergestellt werden.	• Ausfall der DFÜ-Einrichtung • Befall durch unkritische Computerviren	IT-Leiter (schriftlich oder mündlich)	Nach Behebung

Stufe	Beschreibung	Beispielvorfall	zu informieren (Wie?)	wann?
E2	• Es kann ein größerer finanzieller Schaden eintreten. • Die Wahrscheinlichkeit, dass der betriebsfähige Zustand innerhalb der tolerierbaren Zeit (ab Seite 27) wieder hergestellt werden kann ist mittel bis gering.	• Vorsätzliche Zerstörung der Hardware/ Hardwareausfall • Verdacht auf Eindringen ins Netzwerk/ Werksspionage • Ausfall des Navision-Kernsystems	IT-Leiter (mündlich)	Sofort
E3 = Notfallstufe				
E3	• Es kann ein existenzbedrohender wirtschaftlicher Schaden entstehen. • Der betriebsfähige Zustand kann **auf keinen Fall** innerhalb der tolerierbaren Zeit wieder hergestellt werden.	• Brand im Serverraum • Wassereinbruch • Ausfall der Netzteile im Serverschrank • Ausfall des Navision-Kernsystems	IT-Leiter (mündlich) ggf. Feuerwehr/ Polizei (telefonisch)	Sofort

Bei Notfallstufe E3 ist durch den IT-Leiter und ggf. die Geschäftsleitung zu entscheiden, nach welchem der in Abschnitt D5 beschriebenen Notfallszenarien (ab Seite 37) vorzugehen ist. Nach Einrichten des Notbetriebs ist mit der Behebung des Sicherheitsvorfalls fortzufahren.

2.2 Entscheidungshilfe für die Eskalation

Der IT-Leiter ist zu informieren, wenn innerhalb von 60 Minuten der Grund eines Navisionausfalls innerhalb der Gruppe nicht gefunden werden kann. Innerhalb dieser 60 Minuten liegt die Fehlerbehebung im Kompetenzbereich der Administratoren.
Für die Entscheidung, welche Eskalationsstufe auszurufen ist, kann bei IT-spezifischen Problemen die nachfolgende Entscheidungshilfe verwendet werden.



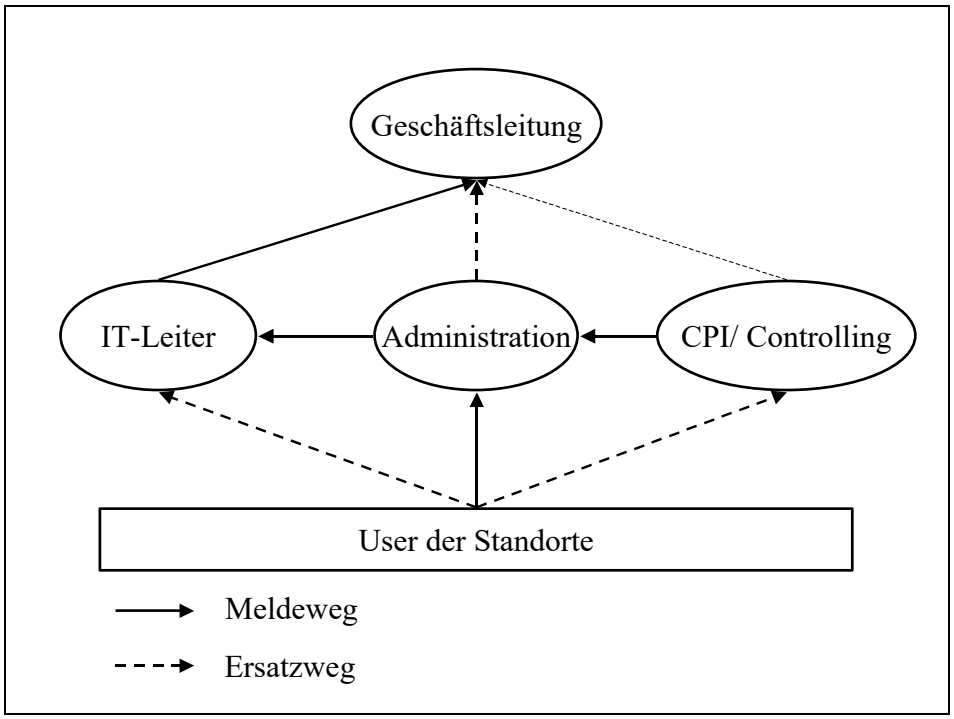
Entscheidungshilfe für die Eskalation

2.3 Eskalationswege

Grundsätzlich geben die Benutzer Sicherheitsvorfälle zunächst an die lokalen Sicherheits- und Notfall-Zuständigen weiter. Die lokalen Sicherheitszuständigen entscheiden sodann ob ein Sicherheitsvorfall vorliegt.
Falls dieser nicht erreichbar ist, wird sofort die IT in Köln benachrichtigt. Eine Liste der Adressen ist in diesem Handbuch enthalten (ab Seite 12).
Falls ein Sicherheitsvorfall vorliegt, melden die lokalen Sicherheitszuständigen diesen an die Administratoren weiter. Diese fragen notwendige Eckdaten des Vorfalls ab und beheben - sofern möglich - das Sicherheitsproblem.

Falls das Sicherheitsproblem nicht in der für das System tolerierbaren Zeit (ab Seite 27) behoben werden kann ist ein Notfall eingetreten. Spätestens in diesem Fall wird der IT- Leiter informiert und

der vorgesehene Notfallplan ausgeführt mit dem Ziel, einen ordnungsgemäßen Geschäftsbetrieb aufrecht zu erhalten.
Die notwendigen Adress- und Telefonlisten sind in den jeweiligen Kapiteln dieses Handbuchs hinterlegt.



Meldewege für Notfälle mit Melde- und Ersatzweg

Grundsätzlich ist vor der Meldung eines Vorfalles durch die Benutzer die am Arbeitsplatz vorliegende Anweisung für die Behebung unkritischer Störungen zu beachten.

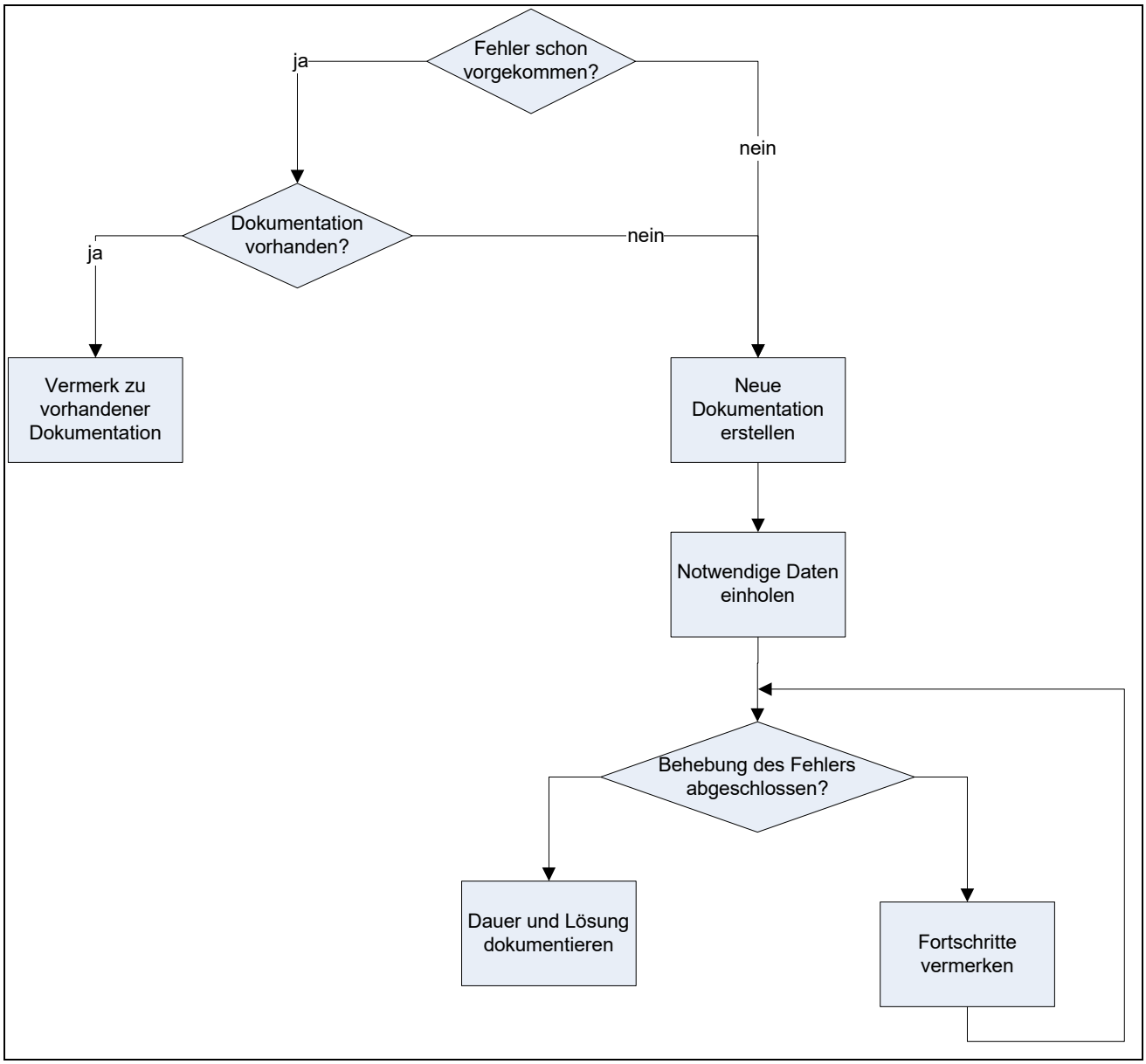
3 Nachbereitung von Notfällen

Nach jedem gemeldeten Notfall ist eine Dokumentation (Abschnitt D6, Seite 41) zu erstellen. Diese enthält folgende Informationen:

- Waren die Angaben des Notfallkonzeptes nachvollziehbar und anwendbar?
- Wie lang waren die Reaktionszeiten?
- Wo besteht Verbesserungspotenzial?
- Wurde die Ursache des Notfalls gefunden und wie sind solche Notfälle zu verhindern?
- Wer hat den Notfall verursacht?
- Welche Kosten hat der Notfall verursacht?

Verantwortlich für die Nachbereitung ist bei IT-spezifischen Notfällen der jeweilige Systembetreuer. Die Nachbereitung findet im Rahmen eines Audits unter Leitung des IT-Leiters statt. Ein Dokumentationsschema für IT-Notfälle liegt im Abschnitt D dem Notfallhandbuch bei. In der Notfalldokumentation (Abschnitt D6, Seite 41) ist die Istzeit der Entscheidung zu vermerken.

Die Nachbereitung ist nach folgendem Schema vorzunehmen:



4 Revisionen und Test des Notfallkonzeptes

Das Notfallkonzept sollte regelmäßig, mindestens aber einmal im Jahr getestet und durch einen Berater überprüft werden. Sinn ist, das Konzept auf dem Stand der Technik zu erhalten und eine bestmögliche Notfallvorsorge zu gewährleisten.

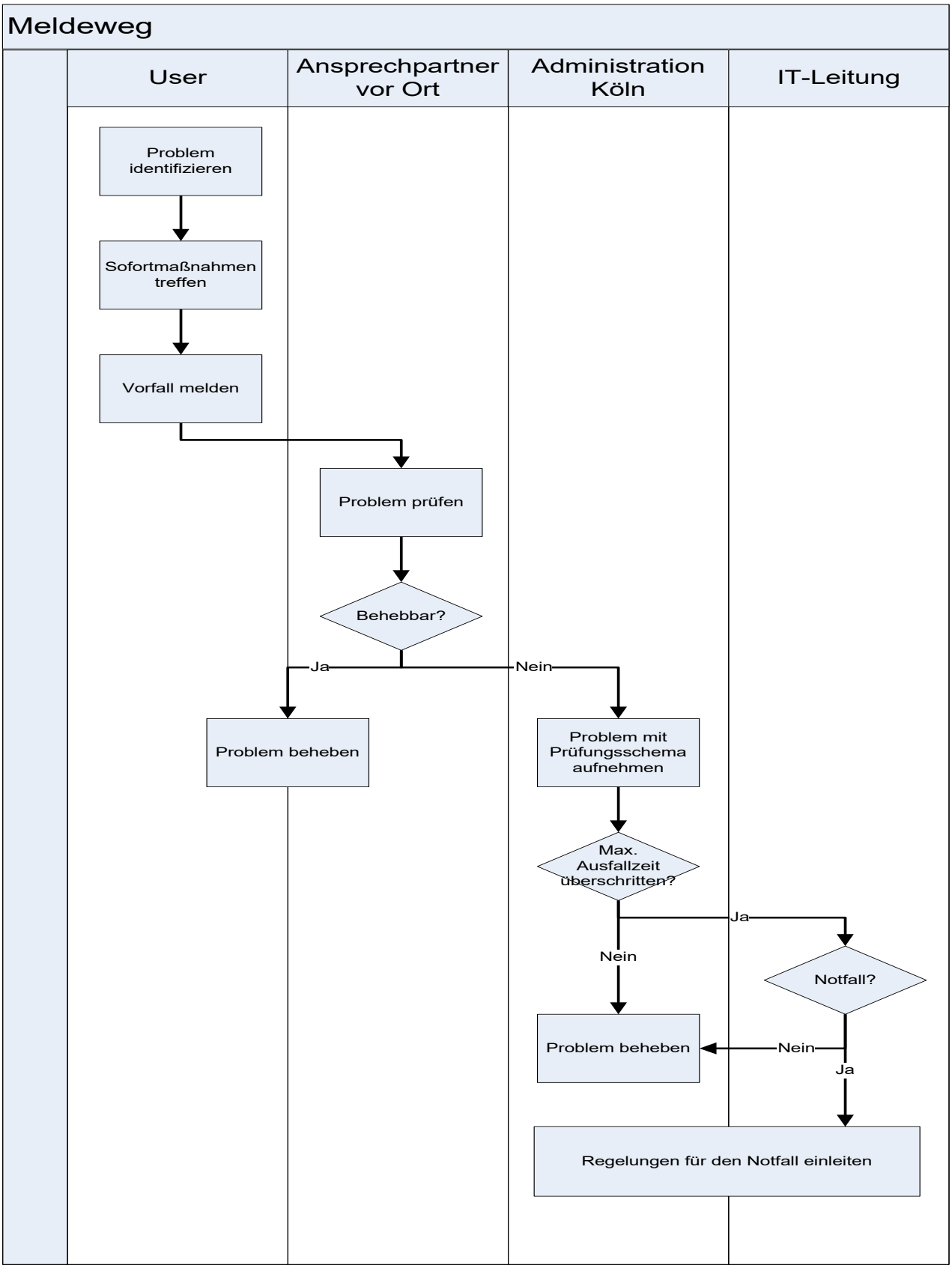
Daher wird nach Abschluss des Notfallhandbuches zur Verbesserung jährlich im Januar ein Audit von einem bis zwei Tagen durchgeführt. Ergebnis dieses Audits ist eine Verbesserung und Aktualisierung dieses Dokumentes.

5 Notfallvorsorge

Zur Vorsorge gegen Notfälle sollten folgende Maßnahmen getroffen werden:

- Vorhalten der Ressourcen zum Wiederherstellen des eingeschränkten IT-Betriebs gemäß Abschnitt D5 (ab Seite 37).
- Erheben aller vorhandenen Sicherheitsmaßnahmen im Rahmen eines standardisierten Basis-Sicherheits-Check um eventuelle Schwachstellen und zugehörige Risiken aufzudecken.
- Anwenden der Bausteine der Schicht 1 „Übergreifende Aspekte“ des IT-Grundschutzhandbuches 2004.
- Überprüfen und ggf. neu Abschließen von Versicherungen gegen Datenausfall, etc.

Teil A Sofortmaßnahmen



A.1 Alarmierung im Notfall

Ein Notfall tritt erst dann ein, wenn eine vorher definierte tolerierbare Ausfallzeit überschritten wurde. Um dieses festzustellen ist die Einhaltung bestimmter Meldewege und Abläufe erforderlich, die den Schaden gering halten.
In diesem Kapitel finden Sie

A.1.1 Alarmierungsplan und Meldewege

Vorgang	Wer?	Sollzeit	Alternative
Notfall-Entscheidung		10 Minuten	

In der Notfalldokumentation (Abschnitt D6, Seite 41) ist die Istzeit der Entscheidung zu vermerken.

A.1.2 Kontaktlisten betroffener Mitarbeiter

Name	Telefon

A.1.3 Zuordnung konkreter Aufgaben für einzelne Personen/Funktionen im Notfall

Notfall	Aufgabe	Verantwortlicher	Vertreter
ORBIS-Ausfall	Bereitstellen des eingeschränkten IT-Betriebs		IT
ORBIS-Ausfall	Wiederherstellen des Ausgangszustands		IT

Notfall	Aufgabe	Verantwortlicher	Vertreter
ORBIS-Ausfall	Information der User		IT
ORBIS-Ausfall	Information der User		IT
ORBIS-Ausfall	Information der User		IT
ORBIS-Ausfall	Information der User		IT
ORBIS-Ausfall	Information der User		IT
ORBIS-Ausfall	Information der User		IT
ORBIS-Ausfall	Information der User		IT

A.1.4 Notrufnummern

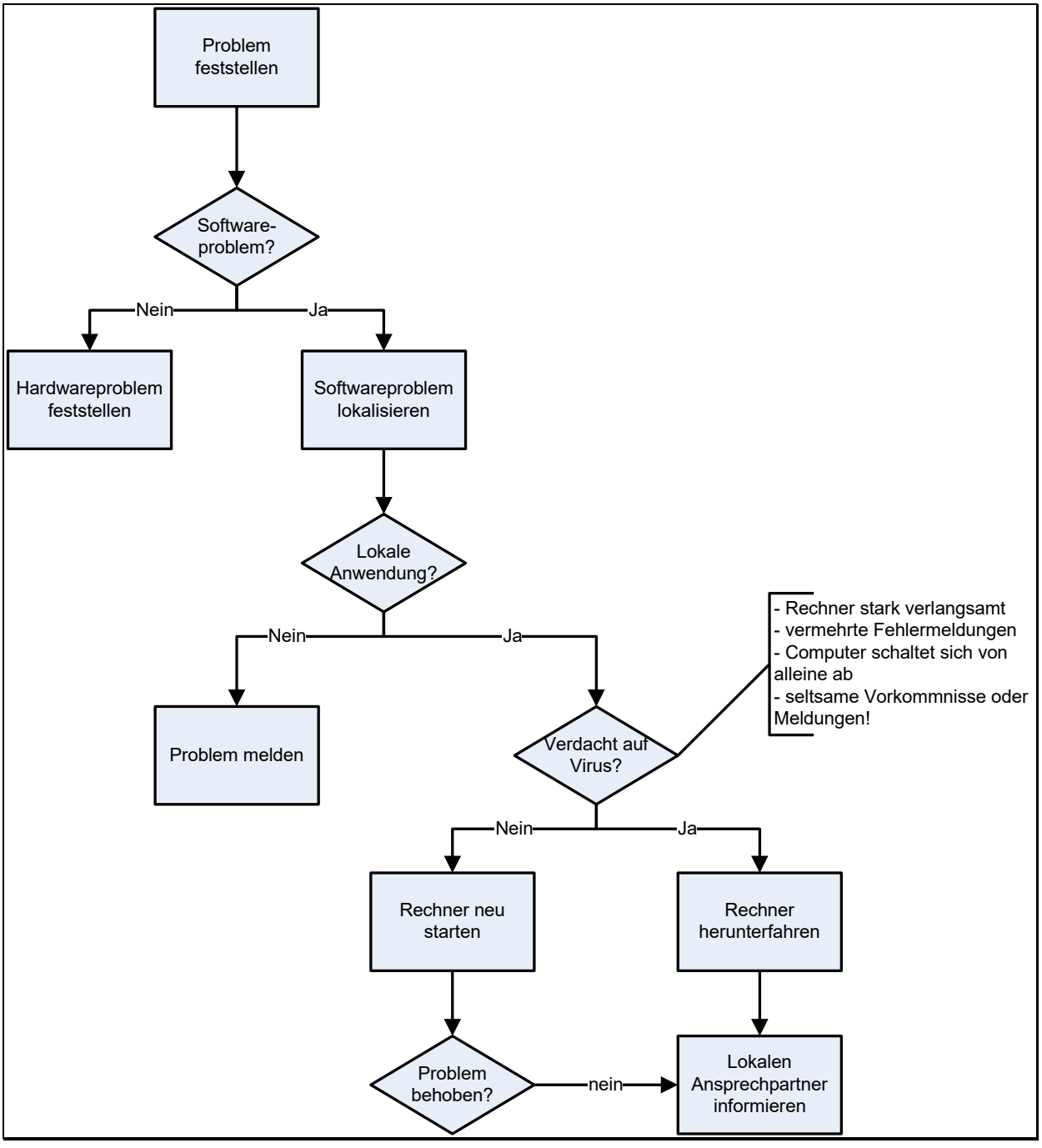
Dienstleister	Ansprechpartner	Telefon
Feuerwehr	Herr Hess	112
Polizei	Jeder	110

A.2 Handlungsanweisungen für spezielle Ereignisse

Sicherheitsvorfälle, die regelmäßig immer wieder vorkommen lassen sich kategorisieren. In diesem Teil finden Sie eine Liste von Sicherheitsvorfällen, die häufig beobachtet wurden und für die Maßnahmen und Handlungsanweisungen festgelegt worden sind. Bitte befolgen Sie diese, sobald Sie einen Sicherheitsvorfall dieser Art beobachten.

A.2.1 Schädigende Software (Viren, Trojaner, o.ä.)

A.2.1.1 Sofortmaßnahmen



A.2.1.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

A.2.1.3 Zu informierende Dienstleister

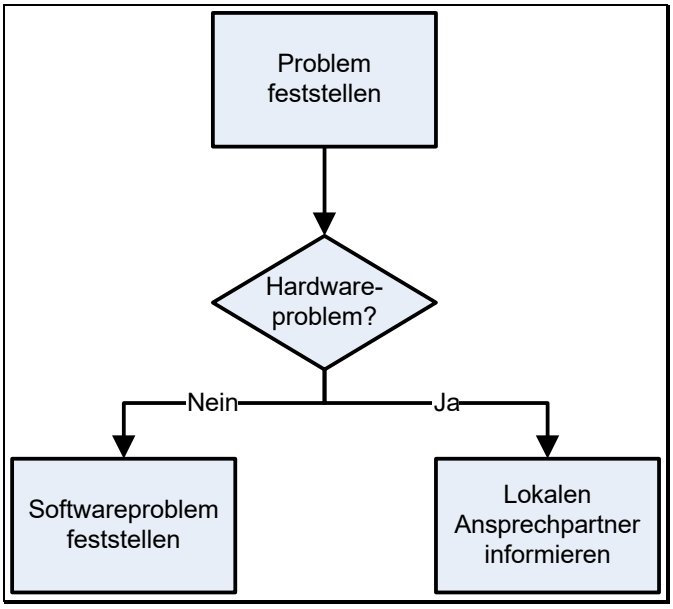
Firma	Ansprechpartner	Telefon

A.2.1.4 Zu informierende Userbetreuer

Name	Firma	Telefon

A.2.2 Hardwareausfall

A.2.2.1 Sofortmaßnahmen



A.2.2.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

A.2.2.3 Zu informierende Dienstleister

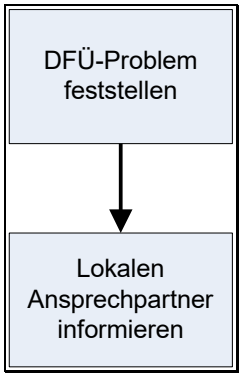
Firma	Ansprechpartner	Telefon

A.2.2.4 Zu informierende Userbetreuer

Name	Firma	Telefon

A.2.3 Ausfall der Datenfernübertragungseinrichtung

A.2.3.1 Sofortmaßnahmen



A.2.3.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

A.2.3.3 Zu informierende Dienstleister

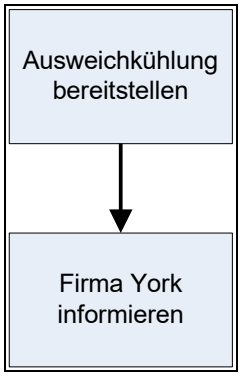
Firma	Ansprechpartner	Telefon

A.2.3.4 Zu informierende Userbetreuer

Name	Firma	Telefon

A.2.4 Ausfall der Klimaanlage

A.2.4.1 Sofortmaßnahmen



A.2.4.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

A.2.4.3 Zu informierende Dienstleister

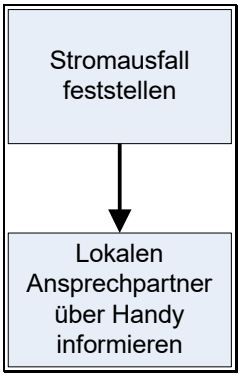
Firma	Ansprechpartner	Telefon

A.2.4.4 Zu informierende Userbetreuer

Name	Firma	Telefon

A.2.5 Stromausfall

A.2.5.1 Sofortmaßnahmen



A.2.5.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

A.2.5.3 Zu informierende Dienstleister

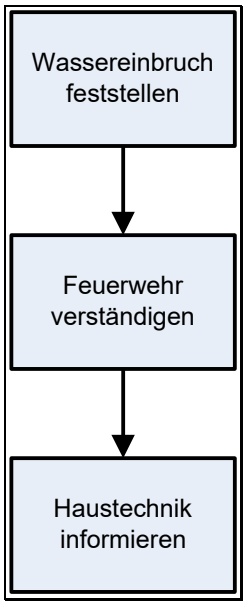
Dienstleister	Ansprechpartner	Telefon

A.2.5.4 Zu informierende Userbetreuer

Name	Firma	Telefon

A.2.6 Wassereinbruch

A.2.6.1 Sofortmaßnahmen



A.2.6.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

A.2.6.3 Zu informierende Dienstleister

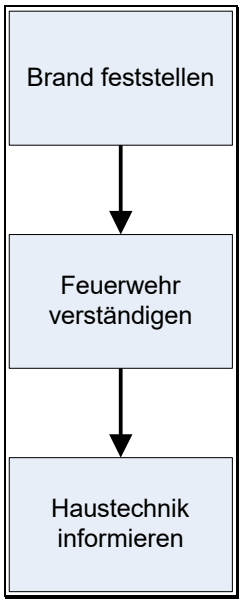
Dienstleister	Ansprechpartner	Telefon

A.2.6.4 Zu informierende Userbetreuer

Name	Firma	Telefon

A.2.7 Brand

A.2.7.1 Sofortmaßnahmen



A.2.7.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

A.2.7.3 Zu informierende Dienstleister

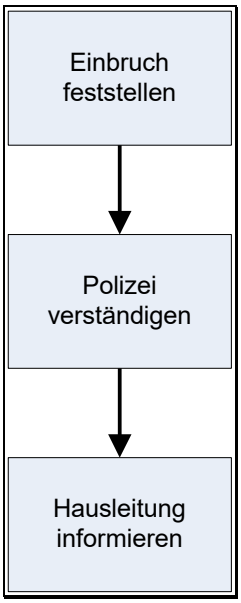
Dienstleister	Ansprechpartner	Telefonnummer

A.2.7.4 Zu informierende Userbetreuer

Name	Firma	Telefon

A.2.8 Einbruch

A.2.8.1 Sofortmaßnahmen



A.2.8.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

A.2.8.3 Zu informierende Dienstleister

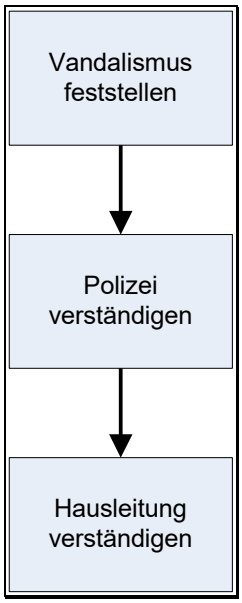
Dienstleister	Ansprechpartner	Telefon

A.2.8.4 Zu informierende Userbetreuer

Name	Firma	Telefon

A.2.9 Vandalismus

A.2.9.1 Sofortmaßnahmen



A.2.9.2 Zu informierende Mitarbeiter

Mitarbeiter	Telefon	Verantwortung

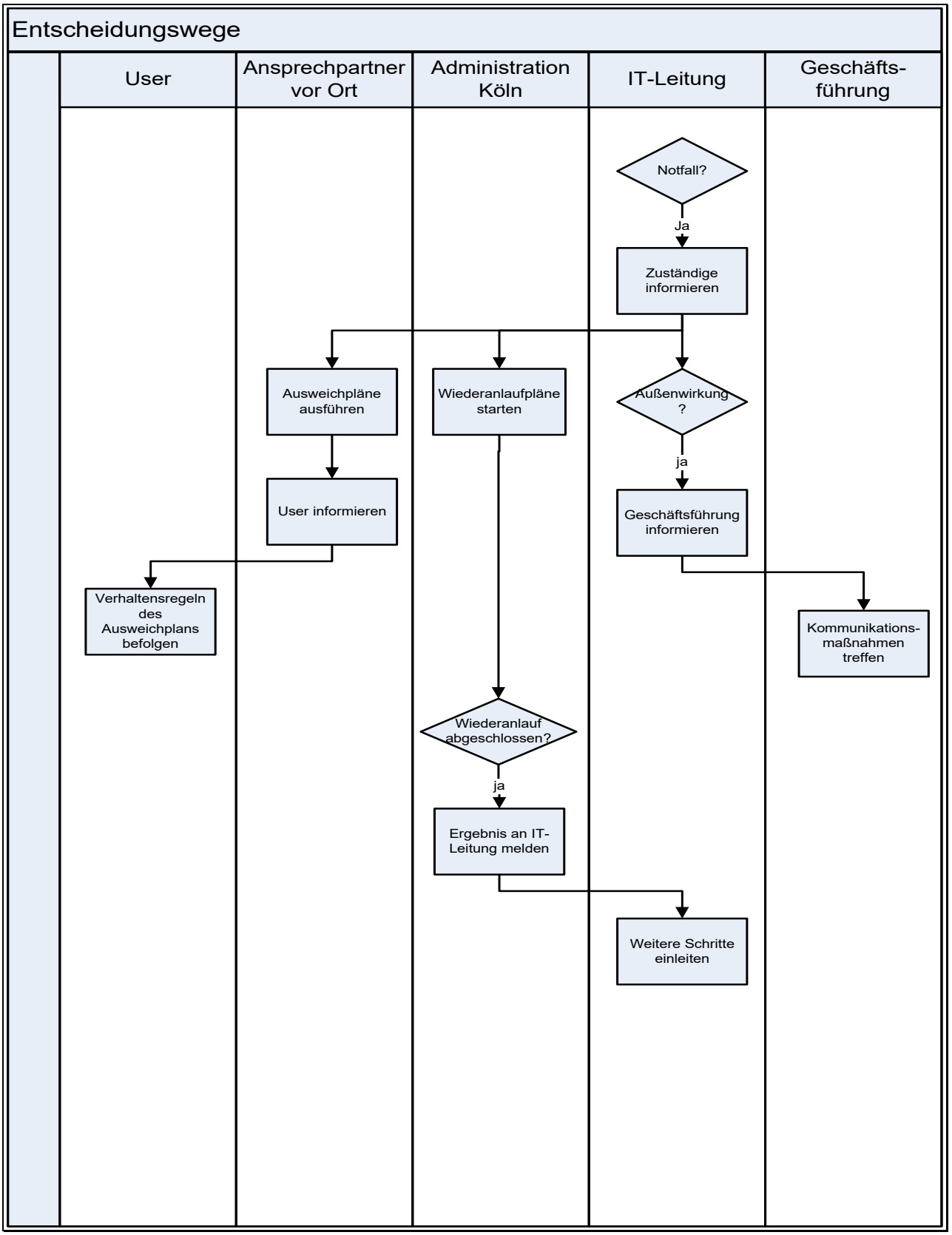
A.2.9.3 Zu informierende Dienstleister

Dienstleister	Ansprechpartner	Telefon

A.2.9.4 Zu informierende Userbetreuer

Name	Firma	Telefon

Teil B Regelungen für den Notfall



B.1 Allgemeine Regelungen

Falls durch die IT-Leitung in Köln entschieden wurde, dass ein Notfall eingetreten ist, gilt es, bestimmte Regelungen zu befolgen. Für den Notfall sind entsprechende Zuständige definiert, die die Entscheidungen treffen. Diese Mitarbeiter sind die Einzigen, die im Rahmen des Notfalls mit Entscheidungen betraut sind. Dieses Kapitel listet auf, welche Regelungen zu beachten sind.

Sie finden in diesem Kapitel:

B.1.1 Notfall-Zuständige

B.1.1.1 Entscheidungsträger im Notfall

Notfall	Entscheidung (Was ist zu tun?)	Wer?	Vertreter?	Sollzeit
Navision Ausfall (Kernsystem)	Nach Schadensanalyse			60 Minuten
Citrix-Ausfall	Nach Schadensanalyse			120 Minuten
Netzausfall LAN	Nach Schadensanalyse			120 Minuten
Netzausfall WAN	Nach Schadensanalyse			120 Minuten
E-Mail Ausfall	Nach Schadensanalyse			120 Minuten
Telefonausfall	Nach Schadensanalyse			60 Minuten

B.1.1.2 Entscheidungshilfe: Wann ist ein Krisen-Fall eingetreten?

Der Krisenfall ist die eskalierte Stufe des Notfalls.
Zu Ermittlung, ob ein Krisenfall eingetreten ist sind folgende Fragen zu beantworten:

- Was ist passiert?
- Welche Anwendungen sind betroffen?
- Wie hoch sind die tolerierbaren Ausfallzeiten (ab Seite 27)?
- Ist die prognostizierte Ausfallzeit über der tolerierbaren Ausfallzeit?
- Kann der eingeschränkte IT-Betrieb einen ordnungsgemäßen Geschäftsablauf unterstützen?

B.1.1.3 Ansprechpartner an den einzelnen Standorten.

Name	Firma	Telefon

B.1.2 Organisationsrichtlinien, Verhaltensregeln

Folgende Verhaltensregeln gelten im Notfall allgemein für alle Mitarbeiter:

- Alle Mitarbeiter haben im Vorfeld die Erstellung des Notfallfallvorsorgekonzeptes (z.B. Erstellung der Dokumentationen) nach Kräften zu unterstützen. Nur durch eine gute Vorbereitung ist es möglich, im Notfall Ruhe zu bewahren und nicht durch unüberlegte Handlungen den Schaden zu vergrößern.
- Unregelmäßigkeiten, die auf einen Sicherheitsvorfall hindeuten, sind gemäß der *Alarmierungspläne* (Teil A, Kapitel 1) unverzüglich zu melden.
- Die *Handlungsanweisungen für ausgewählte Schadensereignisse* (siehe Teil *Handlungsanweisungen für spezielle Ereignisse*) sind einzuhalten.
- Es sind die Anweisungen des Notfall-Verantwortlichen und etwaige spezielle Verhaltensregeln zu beachten.
- Alle Begleitumstände sind ungeschönt, offen und transparent zu erläutern, um damit Schäden zu mindern, schnell Lösungen zu finden und Erkenntnisse zur Verbesserung des IT- Sicherheitskonzeptes zu gewinnen.
- Informationen über den Notfall dürfen nicht an unautorisierte externe Dritte weitergegeben werden.
- Nach einem Notfall ist der sichere Normalzustand wieder herzustellen und an der Aufarbeitung des Notfalls mitzuarbeiten.

B.2 Tabellen der Verfügbarkeitsanforderungen

Um entscheiden zu können, ob ein Notfall eingetreten ist, müssen die Anforderungen an die Verfügbarkeit der einzelnen Systeme aufgelistet werden. Dabei sind die Systeme in drei Stufen der Kritikalität (kritisch, weniger kritisch und nicht kritisch) unterteilt. Die Zeitmessung startet mit dem Zeitpunkt, an dem die IT-Abteilung vom Ausfall Kenntnis erlangt hat.

Ein Notfall tritt erst dann ein, wenn innerhalb der geforderten Zeit eine Wiederherstellung des Vollbetriebes nicht möglich ist (vgl. Notfalldefiniton auf Seite 2).

Sie finden hier:

B.2.1 Verfügbarkeitsanforderung kritischer Systeme und Anwendungen

Lfd. Nr.	Komponente	Anwendung	An-zahl	Ausfallzeit	Verantwortlich	Vertreter
1	Srv-01-Koeln Srv-02-Koeln Srv-03-Koeln	Domänenmas-ter	3	**Max. 4 Std.**		
2	Csrv01-05-Koeln	Citrix Tserv	5	**Max. 4 Std.**		
3	Navision	Navision Kern	1	**Max. 4 Std.**		
4	Srv02-Koeln	Exchange	1	**Max. 4 Std.**		

B.2.2 Verfügbarkeitsanforderung weniger kritischer Systeme & Anwendungen

Lfd. Nr.	Komponente	Anwendung	Anzahl	Ausfallzeit	Verantwortlich	Vertreter
1	Hu_srv3_cgn	Install-Serv. WINS	1	**Max. 8 Std.**		
2	Ibsrv01-Koeln.Lin.Lo-kal	CRM	1	**Max. 8 Std.**		
3	AAPP01-Koeln AAPP01-Welt	CRM	1	**Max. 8 Std.**		

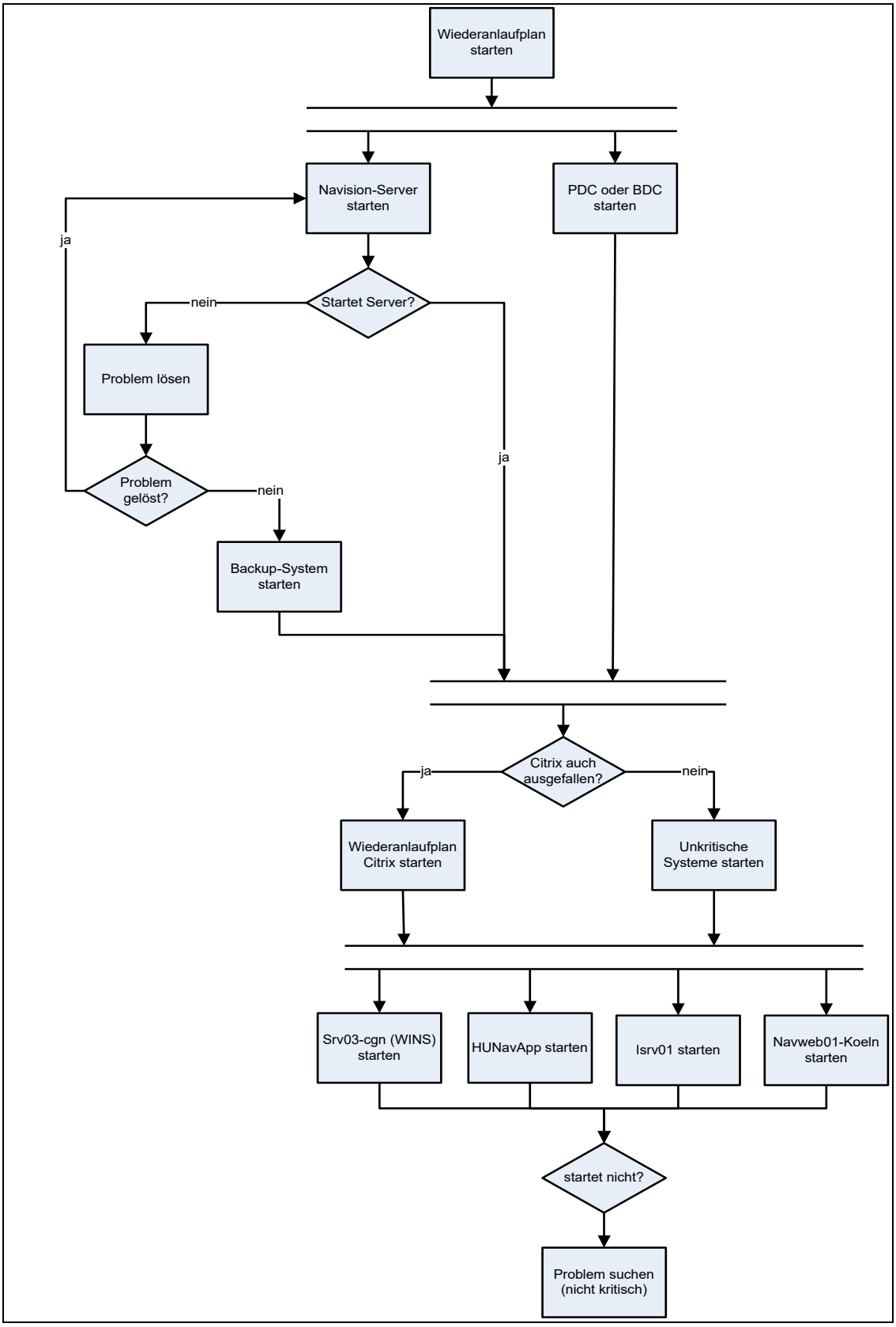
B.2.3 Verfügbarkeitsanforderung nicht kritischer Systeme & Anwendungen

Lfd. Nr.	Komponente	Anzahl	Ausfallzeit	Verantwortlich	Vertreter
1	Hu_Navapp	1	Max. 24 Stunden		
2	Ipevserver	1	Max. 24 Stunden		
3	Prn01-Koeln	1	Max. 24 Stunden		
4	Prn02-Koeln	1	Max. 24 Stunden		
5	Tsrv01-Koeln	1	Max. 24 Stunden		
6	Isrv01-Koeln	1	Max. 24 Stunden		
7	Navweb01-Koeln	1	Max. 24 Stunden		
8	Intranet-srv01	1	Max. 24 Stunden		

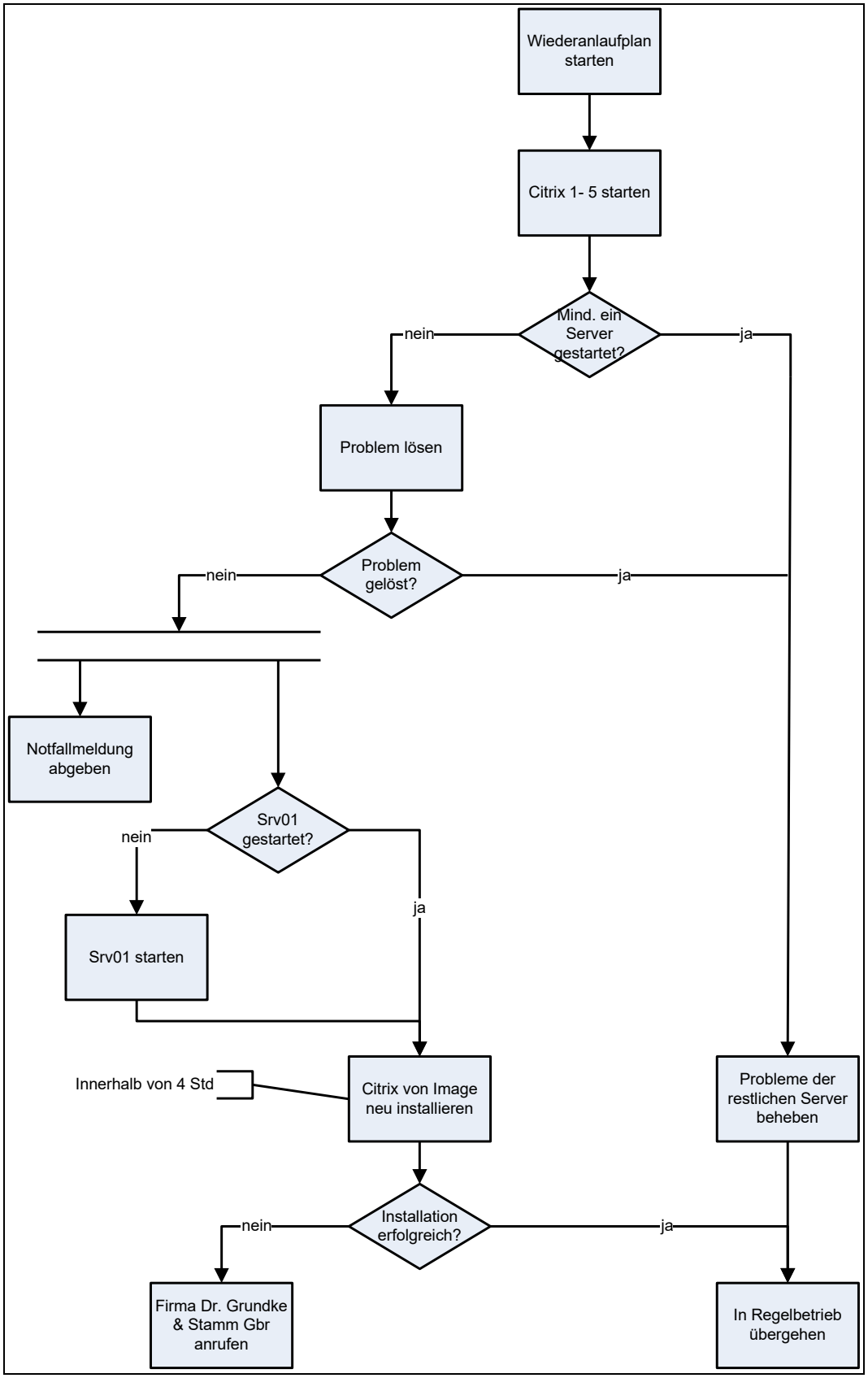
Teil C Wiederanlaufpläne für kritische Komponenten

Dieser Teil ist nur zur Nutzung durch die Administratoren oder externe IT-Dienstleister vorgesehen. Er enthält Ablaufpläne zum Neustart kritischer Komponenten.

C.1 Wiederanlauf-Plan für Komponente A:Navision Kernsystem



C.2 Wiederanlauf-Plan für Komponente B: Citrix



C.3 Beschreibung des IT-Systems A: KIS Kernsystem

C.3.1 Beschreibung der Hardware-Komponenten

Nr.	Komponente	Hersteller	Lieferant	Beschreibung
K1	Srv01-Koeln	Compaq	CPS	
K2	Srv02-Koeln	Compaq	CPS	
K12	Hu-Navapp	IBM	Cosmo Consult	
K14	Isrv01-Koeln	Dell	Dell	
K15	Navision	IBM	Cosmo Consult	
K18	Hu_srv3_cgn	CPS	Comlink	
K22	Navweb01-Koeln	IBM	Cosmo Consult	

C.3.2 Beschreibung der Software-Komponenten

lfd.-Nr.	Komponente	Hersteller	Lieferant
A1			

C.3.3 Bestandsverzeichnis der Systemsoftware

lfd.-Nr.	Software	Hersteller	Ablageort
Sys1	Windows NT4 Server	Microsoft	Raum 0.10, Schrank 2
Sys2	Windows 2000 Server	Microsoft	Raum 0.10, Schrank 2
Sys3	Microsoft Exchange	Microsoft	Raum 0.10, Schrank 2

C.3.4 Bestandsverzeichnis der Anwendungssoftware

lfd.-Nr.	Software	Hersteller	Ablageort
Asoft1			

C.3.5 Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall

lfd.-Nr.				
Norm1				

C.4 Beschreibung des IT-Systems B: Citrix

C.4.1 Beschreibung der Hardware-Komponenten

Nr.	Komponente	Hersteller	Lieferant
K7	Csrv01-Koeln	Dell	Dell
K8	Csrv02-Koeln	Dell	Dell
K9	Csrv03-Koeln	Dell	Dell
K10	Csrv04-Koeln	IBM	Cosmo Consult
K11	Csrv05-Koeln	IBM	Cosmo Consult

C.4.2 Beschreibung der Software-Komponenten

lfd.-Nr.	Komponente	Hersteller	Lieferant
A3	Citrix	Citrix	Citrix

C.4.3 Bestandsverzeichnis der Systemsoftware

lfd.-Nr.	Software	Hersteller	Ablageort
Sys2	Windows 2000 Server	Microsoft	Raum 0.10, Schrank 2

C.4.4 Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall

lfd.-Nr.	Anwendung	Kapazität CPU	Kapazität RAM	Kapazität HDD
Norm2	Citrix	DCPU 2 x 2 GHz	2 GB RAM	30 GB

C.5 Beschreibung des IT-Systems C: CRM

C.5.1 Beschreibung der Hardware-Komponenten

Nr.	Komponente	Hersteller	Lieferant	Beschreibung
K23	Ibsrv01-Koeln.Lin.Lokal	Dell	Dell	CRM-Sys.-DB
K24	AAPP01-Köln	Dell	Dell	CRM-App.-Server
K21	AAPP01-Welt	Dell	Dell	CRM-App.-Server (in Planung)

C.5.2 Beschreibung der Software-Komponenten

lfd.-Nr.	Komponente	Hersteller	Lieferant
A2	Adito	Adito	Adito

C.5.3 Bestandsverzeichnis der Systemsoftware

lfd.-Nr.	Software	Hersteller	Ablageort
1	Linux Mandrake für AAPP01-Köln/Welt	Mandrake	OpenSource

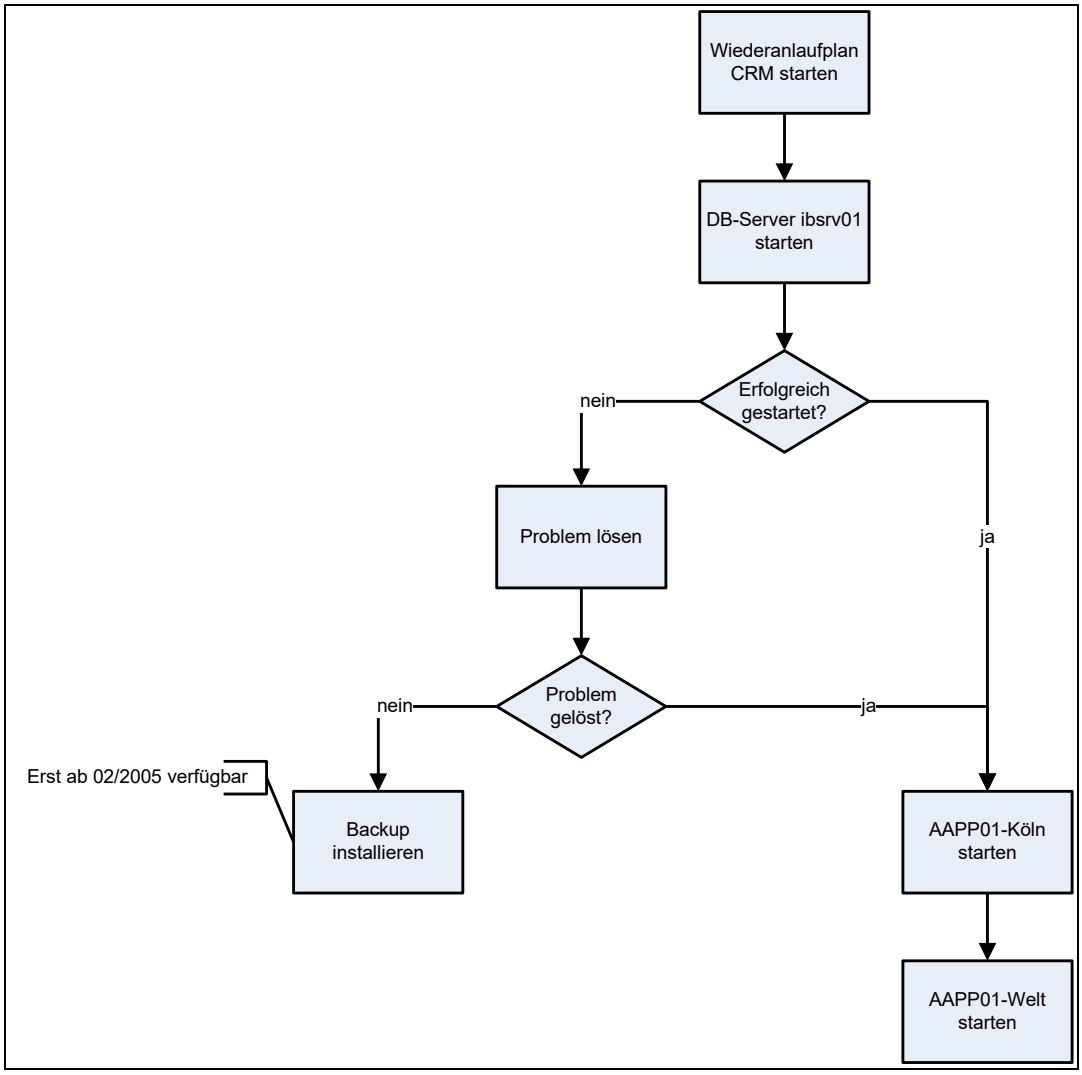
C.5.4 Bestandsverzeichnis der Anwendungssoftware

lfd.-Nr.	Software	Hersteller	Ablageort
Asoft3	Adito	Adito	Raum 0.10, Schrank 2

C.5.5 Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall

lfd.-Nr.	Anwendung	Kapazität CPU	Kapazität RAM	Kapazität HDD
Norm3	CRM	SiCPU 2,4 GHz	2 GB RAM	70 GB Daten, 10 GB System

C.5.6 Wiederanlaufverfahren



C.6 Beschreibung des IT-Systems D : allg. Infrastruktur

C.6.1 Beschreibung der Hardware-Komponenten

Nr.	Komponente	Hersteller	Lieferant	Beschreibung
K3	Srv03-Koeln	HP	Comlink	
K4	Prn01-Koeln	IBM	Cosmo Consult	
K5	Prn02-Koeln	IBM	Cosmo Consult	
K6	Tsrv01-Koeln	IBM	Cosmo Consult	
K13	Ipevserver	HP	CPS	

C.6.2 Beschreibung der Software-Komponenten

lfd.-Nr.	Komponente	Hersteller	Lieferant
A4			

C.6.3 Bestandsverzeichnis der Systemsoftware

lfd.-Nr.	Software	Hersteller	Ablageort
Sys2	Windows 2000 Server	Microsoft	Raum 0.10, Schrank 2

C.6.4 Bestandsverzeichnis der Anwendungssoftware

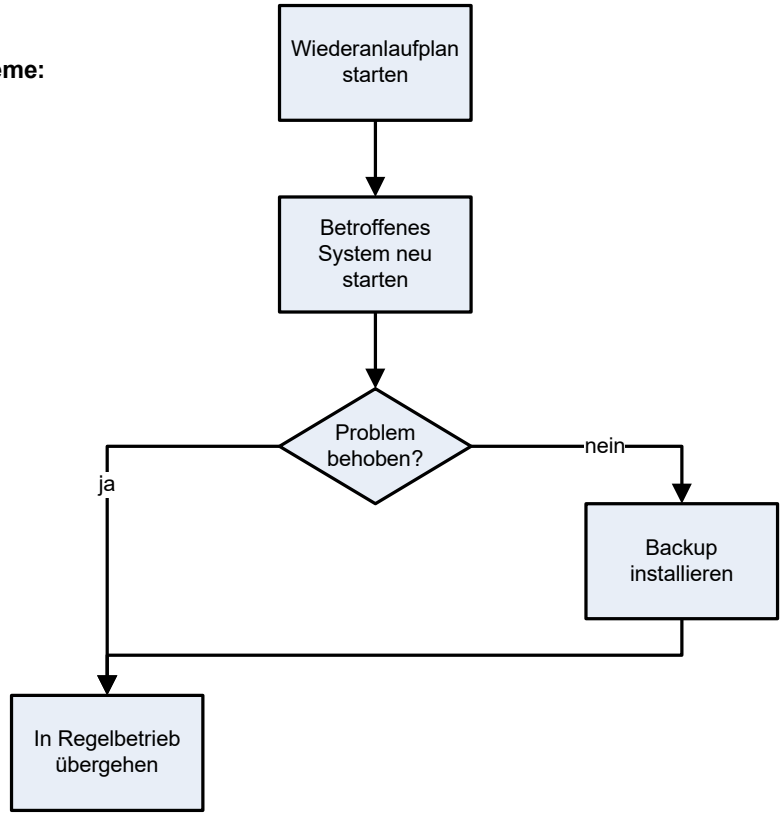
lfd.-Nr.	Software	Hersteller	Ablageort
-	-	-	-

C.6.5 Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall

lfd.-Nr.	Anwendung	Kapazität CPU	Kapazität RAM	Kapazität HDD
Norm4	Print/ Ipev	PIII 800 GHz	512 MB RAM	20 GB Platten

C.6.6 Wiederanlaufverfahren

Betroffene Systeme:
Srv03-Koeln
Prn01-Koeln
Prn02-Koeln
Tsrv01-Koeln
Ipevserver



C.7 Lagerorte der Datensicherung

Die Klinikum Muster verfügt über ein Datensicherungskonzept nach dem Großvater-Vater-Sohn Prinzip. Die Datensicherungsbänder werden in unterschiedlichen Intervallen an baulich getrennten Orten gelagert. Die folgenden Abschnitte beschreiben die Lagerung, die Art der gesicherten Daten und das Sicherungsintervall unterteilt nach den jeweiligen Lagerorten.
Für die Regelungen zur Datensicherung, der Datensicherungssoftware und der allgemeinen Datensicherungspolitik der Klinikum Muster gilt das Datensicherungskonzept, das in der zentralen Administration vorliegt.

C.7.1 Lagerort 1: Vorzimmer der Administration

Lagerart: Möbeltresor (feuerfest)
Schlüsselverwalter (Raum): IT-Administration, Herr Hess (Generalschlüssel)
Schlüsselverwalter (Safe): Schlüsselkasten IT
Sicherungsart: Bandsicherung

gesicherte Daten:

System	Intervall	Sicherungsart

C.7.2 Lagerort 2: Schmitz-Halle

Lagerart: feuer- und einbruchssicherer Safe
Schlüsselverwalter (Halle): (Generalschlüssel)
Schlüsselverwalter (Safe): Schlüsselkasten IT
Sicherungsart: Bandsicherung

gesicherte Daten:

System	Intervall	Sicherungsart

Am Ende eines Kalendermonats verbleibt die letzte Vollsicherung des Monats am Lagerort 2 und wird dort für 12 Monate aufbewahrt. Die übrigen Sicherungen des Monats werden wieder an Lagerort 1 vorgehalten.

C.8 Szenarien eingeschränkter IT-Betrieb

C.8.1 Notfallszenario 1

C.8.1.1 Beschreibung

Nach einem Totalausfall der IT und ggf. weiterer Infrastruktur z.B. bei Brand ist folgende Betriebsfähigkeit wieder herzustellen:

Zur Kontaktaufnahme mit Versicherungen etc. sind die Daten aus dem Kernsystem einem User zur Bearbeitung zugänglich zu machen, damit Werte aus der Buchhaltung etc. zur Schadensregulierung zur Verfügung stehen.

C.8.1.2 Anforderungen an den IT-Betrieb

Folgende IT-Ausrüstung ist zur Herstellung des unter Punkt 5.1.1 genannten Betriebszustandes bereitzustellen:

- 1 Client PC mit Monitor/Maus/Tastatur oder 1 Notebook
  - CPU: 800 MH
  - RAM: 256 MB
  - HDD: 60 GB
  - ggf. DLT/LTO Laufwerk und SCSI-Anschluss
  - Betriebssystem: Windows 2000 Server

C.8.2 Notfallszenario 2

C.8.2.1 Beschreibung

Nach einem Totalausfall der IT ist folgende Betriebsfähigkeit wieder herzustellen:

Der Standort wird in einen Notfallbetrieb mit mindestens 15 Benutzern versetzt. Die Datensicherung muss für die Dauer dieses Zustandes von Hand vorgenommen werden. Die Außenstandorte werden nicht mit angeschlossen.

C.8.2.2 Anforderungen an den IT-Betrieb

Folgende IT-Ausrüstung ist zur Herstellung des unter Punkt 5.1.1 genannten Betriebszustandes bereitzustellen:

  - 1 Servercomputer CPU: Pentium IV – Doppel-CPU 3 GHz
  - RAM: 4 GB
  - HDD: 2x 60 GB, 1x 12 GB
  - DLT/LTO Laufwerk bzw. SCSI-Anschluss
  - Betriebssystem: Windows 2000 Server

- 15 PCs mit Monitor/Tastatur/Maus oder 15 Notebook-PCs
  - CPU: Pentium III 400 MHz
  - RAM: 128 MB

    - HDD: 20 GB
    - Betriebssystem: Windows ab WIN98
- 1 Switch/ 1 Hub 100 mBit
- Netzwerkkabel

C.8.3 Notfallszenario 3

C.8.3.1 Beschreibung

Nach einem Totalausfall der IT ist folgende Betriebsfähigkeit wieder herzustellen:

> Der Standort und die Außenstandorte sind mit mindestens 3 Usern pro Standort in Betriebsfähigkeit zu versetzen.

C.8.3.2 Anforderungen an den IT-Betrieb

Folgende IT-Ausrüstung ist zur Herstellung des unter Punkt 5.1.1 genannten Betriebszustandes bereitzustellen:

- 1 Servercomputer
    - CPU: Pentium IV – Doppel-CPU 3 GHz
    - RAM: 4 GB
    - HDD: 2x 60 GB, 1x 12 GB
    - DLT/LTO Laufwerk bzw. SCSI-Anschluss
    - Betriebssystem: Windows 2000 Server
- 1 Servercomputer Citrix
    - CPU: Pentium IV – Doppel-CPU 2 GHz
    - RAM: 2 GB
    - HDD: 60 GB
    - Betriebssystem: Windows 2000 Server
- 15 PCs mit Monitor/Tastatur/Maus oder 15 Notebook-PCs
    - CPU: Pentium III 400 MHz
    - RAM: 128 MB
    - HDD: 20 GB
    - Betriebssystem: Windows ab WIN98
- 1 Switch/ 1 Hub 100 mBit
- Netzwerkkabel

C.9 Wichtige Informationen

C.9.1 Hersteller- und Lieferantenverzeichnis

Komponente	Firma	Kontakdaten	Telefonnummer	Vertragsref./ Kd.-Nr.
Serverkomponen-ten				
Netzwerk/ Kommunikation				
Telefonanlage				
Citrix				
Klimaanlage				

C.9.2 Dokumentationsschema Notfallnachbereitung

Störungslogbuch Nummer: _____ **Eintrager:** _____

Datum: _____

Betroffenes IT-System: **sonstiger IT-Notfall:** ☐

System A ☐ **System B** ☐ **System C** ☐ **System D** ☐

Waren die Angaben des Notfallkonzeptes nachvollziehbar und anwendbar?
Ja ☐ **Nein** ☐

Wenn nein, was kann verbessert werden: _____

_____

_____

Wie lang waren die Reaktionszeiten? (in Minuten)

Vorgang	**Reaktionszeit**

Ursache des Notfalls? _____

_____

Verursacher? _____ **Kosten:** _____

Wie können solche Notfälle in Zukunft verhindert werden?

_____

_____

_____

protokolliert am: _____ Maßnahmen umgesetzt am: _____

Handzeichen IT-Leiter: _____ Handzeichen IT-Leiter: _____