

Informationssysteme betreiben

INHALTSVERZEICHNIS

Informationssysteme betreiben.....	2
Wiederanlaufsicherstellung	2
Maßnahmen zur Sicherstellung des Wiederanlaufs	2
Systemberechtigungen	2
Berechtigungskonzept Darstellung	2
Datenschutz und Datensicherheit.....	3
Datenschutz "technische Möglichkeiten"	3
Kreditkartenstruktur "Recordbeschreibung"	3
Accounting	3
Messgrößen für die Verrechnung	3
Systemhandhabung	4
Überprüfungspunkte	4

Informationssysteme betreiben

Informationssysteme betreiben

Wiederanlaufsicherstellung

Maßnahmen zur Sicherstellung des Wiederanlaufs

Massnahme	Begründung
<ul style="list-style-type: none">• Wiederanlaufplan erstellen	<ul style="list-style-type: none">• Notwendig, um in einem Katastrophenfall schnell und sicher die nötigen Entscheidungen zu fällen
<ul style="list-style-type: none">• Wiederanlaufplan testen	<ul style="list-style-type: none">• Nötig damit das ganze Prozedere eibgeübt werden kann und Schwachstellen laufend verbessert werden können
<ul style="list-style-type: none">• Wiederanlaufplan unterhalten	<ul style="list-style-type: none">• Wichtig damit Änderungen wie:<ul style="list-style-type: none">• Unternehmensstrategie• Organisation• IT-Umfeld (HW- SW)• Umfeld (politisch, Wirtschaftlich..)• Personelle in den verschiedene Teams usw.• Laufend angepasste werden können
<ul style="list-style-type: none">• Krisenstab etablieren	<ul style="list-style-type: none">• Nötig, damit alle Wiedererstellungs Massnahmen koordiniert werden

Systemberechtigungen

Berechtigungskonzept Darstellung

Darstellungsform	Inhalt
CRUD Diagramm	<ul style="list-style-type: none">• Entitätstypen zu Funktionen• Daten zu Abteilungen• Personen zu Daten
3-Matrizen-Diagramm	<ol style="list-style-type: none">1. Daten zu Funktionen2. Organisation zu Funktionen3. Daten zu Organisation

Informationssysteme betreiben

Datenschutz und Datensicherheit

Datenschutz "technische Möglichkeiten"

•	Datenzugriff nur mittels Berechtigungsprofil und Passwort (Call-Back) "Autorisierung – Identifizierung"
•	sensible Daten chiffrieren
•	Trennung von den persönlichen Daten und den Geschäftsdaten. Nur einzelne geschützte Funktionen/Transaktionen können die kompletten Daten sehen
•	Ein Zugriffslogfile führen und allen Benutzern mitteilen, dass jeder Zugriff, speziell auf die sensiblen Daten, aufgezeichnet wird "Zugriffsüberwachung/Protokollierung"
•	Nur an bestimmten und geschützten Arbeitsplätzen sind Laufwerke für Disketten verfügbar

Kreditkartenstruktur "Recordbeschreibung"

•	Karten-ID
•	Kunden-ID
•	Gültigkeit (von und bis Datum)
•	PIN-Code
•	Anzahl Fehlversuche
•	Betrags-Limite
•	Bezug
•	Ausstellungsdatum
•	Ausstellungs-ID (Angaben wer und wo die letzte Kartenmutation durchgeführt hat, chiffrierte Daten)
•	Benutzungsort (welches Hotel der Kunde zur Zeit Gast ist)
•	Benutzungsprofile (Chiffrierte Berechtigungen)
•	Zimmercode
•	Berechtigungen extern
•	Reserve

Accounting

Messgrößen für die Verrechnung

•	Diskplatzbedarf pro Benutzer
•	Anzahl Transaktionen pro Benutzer
•	Anzahl Tape-Handling
•	Traffic auf Netzwerk
•	CPU-sekunden pro Applikation
•	Benutze Services (Office, Mail, SAP, usw) Grundbetrag pro Applikation
•	Grundbetrag pro HW-Device (Terminal, Drucker, PC, Scanner usw)

Informationssysteme betreiben

Systemhandhabung

Überprüfungspunkte

•	Dokumentation up to Date
•	Wissenstand des Benutzers
•	Funktionalität des Systems können die benötigten Funktionen benutzt werden
•	Plausibilisierung der Eingaben
•	Umständlichkeit der einzelnen Maskenabfolge
•	Zuviele Menulevels (rauf und runtersteigen)
•	Fehlende Möglichkeiten von Massenverarbeitungen (Fakturierung ev. Jede einzeln)
•	Fehlende Möglichkeit mehrere Fenster gleichzeitig geöffnet zu haben
